ETSI TR 119 462 V1.1.1 (2026-03)

TECHNICAL REPORT

Electronic Signatures and Trust Infrastructures (ESI);
Wallet interfaces for trust services and signing

Reference
DTR/ESI-0019462

Keywords
electronic signature, identity, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The eIDAS Regulation (EU) No 910/2014 [i.1], as amended by Regulation (EU) 2024/1183 [i.2] and Directive (EU) 2022/2555 [i.3], establishes the legal framework for electronic identification and trust services within the internal market, including provisions for the European Digital Identity Wallet (EUDIW). The EUDIW enables individuals and legal entities to identify and authenticate across borders and sectors, and to access both public and private services in a secure and user-controlled manner.

A key component of this ecosystem is the integration of trust services that issue electronic attestations of attributes and support qualified electronic signature and seal creation. These services enable the secure exchange of verifiable data and the execution of legally valid transactions, in line with the high level of assurance required by the Regulation.

As outlined in the Architecture Reference Framework 2.6.0 (ARF) [i.4], the EU Digital Identity Wallet (EUDIW) interacts with multiple actors, including trust service providers and relying parties, in a secure, standardized, and interoperable way. This necessitates a clear and comprehensive specification of all interfaces' requirements to ensure consistency, transparency, and legal compliance across implementations.

The present document identifies and consolidates interface requirements that are already defined across various existing specifications, aligning them with the legal and architectural context of the European Digital Identity framework. At the same time, it highlights critical gaps and points to areas where further standardization is needed to ensure coherent, secure, and interoperable interactions between EUDIWs, trust service providers, and relying parties. The present document aims to support future standardization efforts by clarifying expectations, reducing fragmentation, and enabling consistent implementation across the EU.

1 Scope

The present document provides an overview and analysis of the interfaces enabling interactions between the European Digital Identity Wallet (EUDIW) and trust service providers, including those related to electronic signing.

In particular, the present document:

- Describes the functional models and potential interface patterns between EUDIWs and trust service providers, covering scenarios where trust service providers issue certificates or attestations of attributes, as well as scenarios where they act as relying parties.
- Outlines architectural considerations and interface components relevant to the creation of electronic signatures, especially where the trust service provider manages or operates the signature creation device.
- Presents representative use cases demonstrating how the EUDIWs may be applied in trust service contexts such as electronic signatures, electronic seals, certificate issuance, and issuance of electronic attestation of attributes.
- Identifies areas where existing interface specifications may support EUDIW-trust service integration, and highlights aspects that require harmonised specifications to ensure secure and interoperable implementations.

The present document aims to inform ongoing and future standardization by providing a structured foundation for interface design between EUDIWs and trust services, supporting a consistent and trustworthy ecosystem.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[i.3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance).

[i.4] Architecture and Reference Framework (ARF) EU Digital Identity Network 2.6.0.

[i.5] Commission Implementing Regulation 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets.

[i.6] Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets.

[i.7] Commission Implementing Regulation 2024/2980 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards notifications to the Commission concerning the European Digital Identity Wallet ecosystem.

[i.8] Commission Implementing Regulation 2024/2982 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards protocols and interfaces to be supported by the European Digital Identity Framework.

[i.9] Commission Implementing Regulation 2025/848 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties.

[i.10] ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.11] ETSI EN 319 411-1: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.12] ETSI TS 119 431-1: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD/SCDev".

[i.13] ETSI TS 119 431-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".

[i.14] ETSI TS 119 471: "Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services".

[i.15] ETSI TS 119 432: "Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation".

[i.16] ETSI EN 319 102-1: "Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.17] ETSI EN 319 411-2: Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

[i.18] EN 419 241-1: "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements", (produced by CEN).

[i.19] ISO/IEC 18013-5: Personal identification --- ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application.

[i.20] ETSI TS 119 412-6: "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers".

[i.21] ISO/IEC 23220-3: "Cards and security devices for personal identification — Building blocks for identity management via mobile devices".

[i.22] SD-JWT-based Verifiable Credentials (SD-JWT VC).

[i.23] CTAP: "Client to Authenticator Protocol (CTAP) Proposed Standard", July 14, 2025.

NOTE: Also available at https://github.com/eu-digital-identity-wallet/eudi-doc-standards-and-technical-specifications/issues/365.

[i.24] HAIP - OpenID4VC High Assurance Interoperability Profile, OpenID Foundation.

[i.25] OpenID4VCI - OpenID for Verifiable Credential Issuance, OpenID Foundation.

[i.26] OpenID4VP - OpenID for Verifiable Presentations, OpenID Foundation.

[i.27] ETSI EN 319 132-1: "Electronic Signatures and Trust Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.28] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.29] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.30] ETSI TS 119 182-1: "Electronic Signatures and Trust Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures".

[i.31] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers".

[i.32] CSC API V2.2: "Cloud Signature Consortium Architectures and protocols for remote signature applications.".

[i.33] OASIS: "PKCS #11 Cryptographic Token Interface Base Specification Version 3.1".

[i.34] ETSI TS 119 475: "Electronic Signatures and Trust Infrastructures (ESI); Relying party attributes supporting EUDI Wallet user's authorization decisions".

[i.35] ETSI TS 119 411-8: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 8: Access Certificate Policy for EUDI Wallet Relying Parties".

[i.36] W3C®: "Digital Credential", Working Draft 13 January 2026.

[i.37] W3C®: "Verifiable Credential Data Model v2.0".

[i.38] ETSI EN 319 162-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers".

[i.39] ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".

[i.40] ETSI TS 119 461: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects".

[i.41] ETSI TS 119 472-1: "Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 1: General requirements".

[i.42] ETSI TS 119 472-2: "Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 2: Profiles for EAA/PID Presentations to Relying Party".

[i.43] ETSI TS 119 472-3: "Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 3: Profiles for issuance of EAA or PID".

[i.44] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[i.45] ETSI TS 119 479-3: "Electronic Signatures and Trust Infrastructures (ESI); Technological Solutions for the EU Digital Identity Framework; Part 3: Support for EAA within AdES signatures".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 119 401 [i.10], ETSI TS 119 431-1 [i.12], ETSI TS 119 431-2 [i.13], ETSI TS 119 471 [i.14] and the following apply:

Certification Authority (CA): authority trusted by one or more users to create and assign certificates

NOTE: See ETSI TS 319 411-1 [i.11].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 119 401 [i.10], ETSI TS 119 431-1 [i.12], ETSI TS 119 432-2 [i.13], ETSI TS 119 471 [i.14] apply.

4 General concepts

4.1 Digital Identity Wallet

4.1.1 European Digital Identity Wallet

The European Digital Identity Wallet (EUDIW) is an electronic identification means issued under an EU-recognized scheme that enables a natural or legal person to securely manage their identity data and interact with trust service ecosystems in both online and offline environments.

Under Article 5a(4)(a) of the eIDAS Regulation [i.1], the EUDIW empowers the user to:

- securely request, obtain, select, combine, store, delete, share and present, under their sole control, Person Identification Data (PID) and Electronic Attestations Of Attributes (EAA);
- authenticate to relying parties, including for access to public and private sector services, with support for selective disclosure of personal data;
- and to sign using Qualified Electronic Signatures (QES) or seal using qualified electronic seals (QSealS).

The EUDIW operates in interaction with Trust Service Providers (TSPs) for:

- Identity proofing;
- Electronic attribute issuance;
- Remote signature/seal creation.

a) Interaction with TSPs for Identity Proofing

The EUDIW enables users to initiate secure sessions with TSPs that verify the user's identity in accordance with eIDAS Regulation [i.1], Article 24 and identity proofing standards [i.40]. After verification, the identity data is securely bound to the EUDIW and can be reused as a trusted basis for further trust services, including electronic attestations, signatures, and delivery.

b) Interaction with TSPs for Issuance of Electronic Attestations of Attributes

The EUDIW provides a secure and authenticated interface for obtaining Electronic Attestations of Attributes (EAA) from TSPs, including Qualified Trust Service Providers (QTSPs), non-qualified Electronic Attestation of Attribute Service Providers (EAASPs) and Public Sector Electronic Attestations of Attributes (PUB-EAAs).

c) Interaction with Signature Creation Service Providers (SCSPs) for QES/QSealS

To support qualified electronic signatures or seals, the EUDIW integrates with Signature Creation Service Providers (SCSPs), which may be QTSPs operating remote Qualified Signature Creation Devices (QSCDs).

4.1.2 Digital Identity Wallet basic architectural components

The architecture of the EUDIW is based on the layered and modular structure described in the ARF [i.4]. This framework defines the main functional and technical components required to ensure interoperability, user control, trust, and privacy in the cross-border use of the EUDIW.

The ARF [i.4] distinguishes between EUDIW ecosystem actors, EUDIW core components, and supporting services.

The main architectural components of the EUDIW are:

- Wallet Unit (WU): the software and secure hardware components (e.g. WSCD) installed on the user's device, responsible for storing, managing, and presenting PID and EAAs.
- Wallet Secure Cryptographic Device (WSCD): a certified secure component that performs sensitive cryptographic operations and protects signature and seal keys.
- Wallet Secure Cryptographic Application (WSCA): application logic managing access to the WSCD and enabling signing/sealing operations.
- PID Provider: the entity responsible for verifying the identity of the user and issuing the PID in accordance with the eIDAS framework.
- EAA Providers: electronic attestation of attributes trust services as defined in ETSI TS 119 471 [i.14].
- Signature Creation Service Provider (SCSP): signature creation service as defined in ETSI TS 119 431-2 [i.13].
- Presentation and Access Interfaces: APIs and user interfaces allowing the user to present PID and EAAs to relying parties in both online and offline contexts, supporting selective disclosure and consent-based sharing.

4.2 Wallet interfaces

4.2.1 Interfaces defined in eIDAS Regulation

The present clause describes interfaces between the EUDIW and external actors, as directly established in the eIDAS Regulation [i.1]. The listed interfaces have been derived from a structured review of the legal requirements set out in Article 5a(4) and 5a(5), which define the core functionalities of the EUDIW, including interactions with trust service providers and relying parties.

The purpose of this analysis is to identify the interfaces that are directly relevant to TSPs, including providers of identity, electronic attestation of attributes, and qualified electronic signatures and seals. The ARF [i.4] is referenced to map each legal provision to its corresponding technical and architectural realization.

Table 1: Interfaces and their descriptions defined in eIDAS

Description of the Interface	Requirement from the Regulation	Reference to the Regulation Article [i.1]	Reference to the ARF [i.4]
EUDIW ← TSP (PID/EAA Issuance)	EUDIW supports issuance interface for PID, (Q)EAAs or qualified and non-qualified certificates.	Art 5a(5)(a)(i)	4.6.5, 6.6.2, Annex A.2.3 Topic 10
EUDIW ← RP (Request/Validation)	RP requests/validates PID and EAA.	Art 5a(5)(a)(ii)	6.6.3.6
EUDIW → RP (Presentation/Sharing)	EUDIW supports presentation of PID/EAA/selectively disclosure data.	Art 5a(5)(a)(iii)	6.6.3, Annex A.2.3.1 (OIA_01, OIA_05-06)
EUDIW → UI (Trust Mark and Consent)	EUDIW displays EU Trust Mark and allow consent for data sharing.	Art 5a(5)(a)(iv)	6.5.3.6, Annex A.2.3 Topic 19 (DASH_09(b))
EUDIW ← Onboarding Source	EUDIW supports secure onboarding with high assurance eID.	Art 5a(5)(a)(v)	6.6.2.6, Annex A.2.3 Topic 10 (ISSU_05)
EUDIW → EUDIW (P2P Exchange)	EUDIW allows secure P2P data sharing.	Art 5a(5)(a)(vi)	6.6.4, Annex A.2.3 Topic 30
EUDIW → RP (RP Authentication)	EUDIW authenticates and validates RP before data sharing.	Art 5a(5)(a)(vii-viii)	6.6.3.2
EUDIW → RP/Authorities (Erasure Requests)	EUDIW allows users to submit erasure requests and reports to authorities.	Art 5a(5)(a)(ix-x)	6.6.3.13, Annex A.2.3 Topic 48
EUDIW → Signature/Seal Provider	EUDIW supports creation of QES/QSeal.	Art 5a(a)(xi)	2.4, 3.9, Annex A.2.3 Topic 16
EUDIW ← User	Verifies the authenticity and validity of EUDIW and RP	Art 5a(8)(a)	6.5.2.2
NOTE: The direction of the arrow in the table above indicates the party initiating communication.			

4.2.2 Interfaces defined in Commission Implementing Regulations (CIRs)

The present clause describes interfaces between the EUDIW and external systems or actors as established in secondary legislation - specifically, the Commission Implementing Regulations (CIRs) [i.5], [i.6], [i.7], [i.8], [i.9], issued under the revised eIDAS Regulation [i.1]. These CIRs define mandatory technical and procedural specifications for EUDIW operations, including credential issuance, cryptographic binding, trust mark handling, transaction logging, and revocation notifications.

The included interfaces have been selected based on their importance to trust service providers, including Qualified Trust Service Providers (QTSPs), Signature Creation Service Providers (SCSPs), and Electronic Attestation of Attribute Service Providers (EAASPs). Where applicable, each interface is referenced to both its legal basis and its corresponding technical definition in the ARF [i.4].

Table 2: Interfaces and their descriptions defined in CIRs

Description of the Interface	Requirement from the Regulation	Reference to the CIR Article	Reference to the ARF [i.4]
EUDIW ← PID/EAA Provider	Issue PID/EAA securely to EUDIW with revocation support.	CIR 2024/2977 [i.5] Art 3-5 [i.7]	6.6.2, 6.6.5.4, Annex 2 Topics 7, 10
EUDIW → PID/EAA Provider	Provide EUDIW Unit Attestation to issuer before credential issuance.	CIR 2024/2977 [i.5] Art 3	6.6.2.3.1, Topic 9, 10 (ISSU_30)
EUDIW ↔ WSCD	Use secure cryptographic hardware for key protection and signing.	CIR 2024/2979 [i.6] Art 4-6	4.3.2, 4.5
EUDIW ↔ RP	Authenticate RP, support selective disclosure, consent, offline sharing.	CIR 2024/2982 [i.8] Art 5, CIR 2024/2979 [i.6] Art 8-10	4.2.4, 6.6.3.2, 6.6.4, Topic 1 (OIA_07), 6, 9 (WUA_17)
EUDIW Logging	Log all user transactions with RP/TSP and allow export.	CIR 2024/2979 [i.6] Art 9	Annex 2 Topic 19
EUDIW Disclosure Control	Enforce embedded disclosure policies and user control.	CIR 2024/2979 [i.6] Art 10	6.6.2.7, Annex 2 Topic 43
EUDIW ↔ QES/QSeal Engines	Enable user to generate qualified signatures and seals.	CIR 2024/2979 [i.6] Art 11-12	2.4, 4.3.3, Topic 16
EUDIW ← RP	Verify RP registration and attribute request match.	CIR 2025/848 [i.9], CIR 2024/2982 [i.8] Art 3	6.4.2, 6.4.3, Annex 2 Topic 6, 44
EUDIW ← Intermediaries	Display intermediary and RP, enforce transparency.	CIR 2025/848 [i.9], CIR 2024/2982 [i.8] Art 3	3.11, 6.6.3.4, 6.6.3.5, Annex 2 Topic 6, 52
NOTE: The direction of the arrow in the table above indicates who is the actor initiating communication.			

4.2.3 Interfaces defined in ARF

The present clause consolidates interface definitions between the EUDIW and the actors as described in the ARF [i.4]. These interfaces may not be fully reflected in the eIDAS Regulation [i.1] or its implementing acts, but they form an essential part of the operational architecture of the EUDIW.

The interfaces listed here result from a targeted analysis of the ARF [i.4], specifically those that are critical for trust service providers-including identity proofing, attribute issuance, qualified signature creation, relying party authentication, and revocation checking. Each interface entry includes a reference to the corresponding section or requirement set within the ARF and applicable supporting standards (e.g. ETSI TS 119 431-1 [i.12], ISO 18013-5 [i.19]).

Table 3: Interfaces and their descriptions defined in ARF

Interface Name	Description	External Actor	Standards/References
Request & Receive PID	Interface for identity proofing: EUDIW requests Person Identification Data from the PID Provider	PID Provider	• ARF (3.4, Annex 2 Topic 10 (B), Annex 3.1) [i.4]; • CIR 2024/2977 [i.5]; • CIR 2024/2982 [i.8]; • ISO 18013-5 [i.19]; • SD-JWT VC [i.22]; • W3C Digital Credentials API [i.36]; • OpenID4VCI [i.25].
Request & Receive EAA/QEAA	Interface for attestation attributes: EUDIW requests EAAs from EAASP (qualified/non-qualified)	(Q)EAA Provider	• ARF (3.6, 3.8, Annex 2 Topic 10 (C), Topic 12) [i.4]; • CIR 2024/2977 [i.5]; • ISO 18013-5 [i.19]; • SD-JWT VC [i.22]; • W3C VCDM (for EAA) [i.37]; • W3C Digital Credentials API [i.36]; • OpenID4VCI [i.25].
Request & Receive PuB-EAA	Similar to above, but for public-sector-issued EAAs from authentic sources (PUB-EAA Providers)	Public-body EAASP	• ARF (3.7, 3.10, Annex 2 Topic 10, Topic 12) [i.4]; • CIR 2024/2977 [i.5]; • CIR 2024/2982 [i.8]; • ISO 18013-5 [i.19]; • SD-JWT VC [i.22]; • W3C VCDM (for EAA) [i.37]; • W3C Digital Credentials API [i.36]; • OpenID4VCI [i.25].
Signature/Seal Creation Request	Interface for invoking Qualified Signature Creation via WSCD or remote QSCD operated by a SCSP	Qualified SCSP/QTSP	• ARF (3.9, Annex 2 Topic 16) [i.4]; • CSC API [i.32]; • ETSI EN 319 142-1 (PAdES) [i.29]; • ETSI EN 319 132-1 (XAdES) [i.27]; • ETSI TS 119 182-1 (JAdES) [i.30]; • ETSI EN 319 122-1 (CAdES) [i.28]; • ETSI EN 319 162-1/-2 (ASiC) [i.31] [i.38]; • ETSI TS 119 101 [i.39]; • EN 419 241-1 [i.18]; • ETSI TS 119 431-1 [i.12]; • ETSI TS 119 431-2 [i.13].
Relying Party Authentication & Consent	EUDIW authenticates relying party, displays request, collects user consent	Relying Party (Service Provider)	• ARF (6.6.3.2, 6.6.3.3, 6.6.3.5, Annex 2 Topic 6) [i.4]; • ISO 18013-5 [i.19]; • OpenID4VP [i.26].
Revocation and Validity Checking	Check and update status of issued PIDs or EAAs via revocation or validation services	Revocation/Validation Services	• ARF (6.6.3.7, Annex 2 Topic 7) [i.4]; • ETSI EN 319 411-1 [i.11]; • ETSI EN 319 411-2 [i.17].

The ARF [i.4] also defines the following interfaces: Wallet Provider Interface, User Interface, Secure Cryptographic Interface, and the WSCA-to-WSCD interface. The present document does not provide specifications for those interfaces.

4.3 Wallet interfaces for trust services

TSPs operating under the eIDAS Regulation [i.1] and its implementing acts are key actors in the European Digital Identity Framework. Their interactions with the EUDIW meet a set of functional, legal, and technical requirements that ensure security, user control, privacy, and cross-border interoperability.

These apply to:

- Electronic Attestation of Attribute Providers (EAASPs), including Qualified EAASPs and Public Sector EAA issuers (PUB-EAAs),
- Certificate Issuers, including Qualified Trust Service Providers (QTSPs) issuing qualified certificates for electronic signatures or seals,
- Remote Signature Creation Service Providers (SCSPs),
- Registered Electronic Delivery Service Providers (REDS),
- and other TSPs interfacing with EUDIW.

Table 4: EUDIW TSP interface identified requirements

Requirement	Description	Source or requirement in ARF [i.4]
User Identification	TSPs reliably identify the EUDIW holder using PID and/or EAA-based identity attributes.	6.6.2 PID or attestation issuance, 6.6.3 PID or attestation presentation to Relying Party,
User Consent	All issuance, signing, or delivery actions are based on explicit user consent, which is collected and presented through the EUDIW interface.	5.6.2 (transactional data), 6.6.3.5 (Wallet Unit obtains User approval for presenting selected attributes), Annex 2 Topic 6 (B).
Interoperable and Secure Interfaces	TSPs support standardized interaction protocols (listed in the present document) to enable secure and privacy-respecting exchanges with the EUDIW. Interface endpoints are required to support mutual authentication, selective disclosure, and device binding mechanisms.	4.4.3.4 (profiling OpenID4VP [i.26] in remote flows), 5.6.1 (attestation presentation: ISO/IEC 18013-5 [i.19] & OpenID4VP [i.26]), 5.6.2 (transactional data), 5.3.2-5.3.4 (attestation formats & proofs), Annex 2 Topic 1.
Validation of EUDIW and Device	Before issuing credentials or initiating services, TSPs verify the integrity and authenticity of the EUDIW through mechanisms such as Wallet Unit Attestation (WUA). Where applicable, attestations and certificates are bound to a Wallet Secure Cryptographic Device (WSCD).	6.6.2.3 (PID Provider or Attestation Provider validates the Wallet Unit), 6.6.2.4 (PID Provider or Attestation Provider verifies that WUA is not revoked), Annex 2 Topic 9, Annex 2 Topic 10 (ISSU_30).
EAA Delivery and Cryptographic Binding	EAAs and certificates are delivered securely to the EUDIW, ensuring binding to the user and/or device using cryptographic references. Transactional services ensure that delivery metadata, timestamps, and integrity proofs are traceable and bound to verified identities.	6.6.2.3.3 Verifies that PID key or device-bound attestation key is protected by the WSCD, 5.6.2 (transactional data), 6.6.2.6 (User activates the PID).
Revocation and Status Management	TSPs provide real-time or asynchronous mechanisms for revocation, suspension, or status verification of issued EAAs and certificates. EUDIW queries these services securely and reliably.	6.6.5.4 PID or Attestation Revocation, Annex 2 Topic 7 - Attestation revocation and revocation checking.

Requirement	Description	Source or requirement in ARF [i.4]
Audit, Logging, and Notifications	Interactions with the EUDIW are logged and made auditable. Where applicable, TSPs report events (e.g. issuance, revocation, breaches) to authorities or registries in accordance with CIR 2024/2980 and 2025/848.	6.6.3.13 (Wallet Unit enables the User to report suspicious requests by a Relying Party and to request a Relying Party to erase personal data); Annex 2 Topic 19, CIR 2024/2979 [i.6] Art. 9 (transaction logs by wallet instances); Notifications framework in CIR 2024/2980 (ecosystem notifications) [i.7].
Trust Framework Participation	TSPs are listed in national or European-level trust lists.	3.5 (Trusted List Provider), 6.3.2.2-6.3.2.4 (access & registration certificates; trusted lists); 6.4.2-6.4.3 (RP registration/suspension); Annex 2 Topic 31.

Table 5 provides an overview of the primary interfaces defined for interaction between the EUDIW and different types of TSPs. These include providers of EAAs, certificates, remote signature creation, and other services supporting qualified trust operations under the eIDAS [i.1] framework.

The listed interfaces were identified through analysis of the EUDIW interface model described in the ARF [i.4], the eIDAS [i.1] Regulation and its Implementing Acts, and relevant ETSI standards. Each interface reflects a functional connection point necessary for compliant service delivery, secure user interaction, and support for digital transactions involving identity or signature services.

Table 5. Interfaces for interaction between the EUDIW and TSPs

Identifier	Name	Description	References in the present document	Reference to standards supporting interface
IN_RP_1	Online authentication interface	Interface for TSP acting as RP to request and receive Personal Identification Data (PID) and EAA in the process of identity validation or request for specific attributes.	Clause 5.2	ETSI TS 119 461 [i.40], ETSI TS 119 472-1 [i.41], ETSI TS 119 472-2 [i.42].
IN_RP_2	Interface for request for signature	Interface for RP to initialize the signing process. Primarily allows RP to receive information about online SCA and authentication information.	Clause 5.3	ETSI TS 119 472-1 [i.41], ETSI TS 119 472-2 [i.42], ETSI TS 119 432 [i.15], ETSI EN 319 102-1 [i.16] Including Transaction Data Authorization
IN_TSP_1	New attributes EAA handover interface	Interface for TSP issuing EAA in the process of EAA handover.	Clause 6.4	ETSI TS 119 472-3 [i.43].
IN_TSP_2	Interface for remote signature creation	Interface enabling the creation of the electronic signature with the EUDIW when signature is created by a remote signature service.	Clause 7.4	ETSI EN 319 102-1 [i.16], ETSI TS 119 431-2 [i.13], ETSI TS 119 432 [i.15].

Identifier	Name	Description	References in the present document	Reference to standards supporting interface
IN_TSP_3	Interface for new certificate handover	Interface for handover of the signature certificate. Registration and identity proofing of the certificate subject may use the IN_RP_1 interface.	Clause 7.5	ETSI TS 119 432 [i.15].
IN_QSCD_LOCAL	Interface for local signature creation	Interface enabling the creation of the electronic signature with the EUDIW when keys are stored on the local QSCD.	Clause 7.4	OUT OF SCOPE
IN_SCA	Interface for handling signature creation process	Interface enabling functionality of providing signing attributes and a certificate to the Signature Creation Application.	Clause 7.3	ETSI EN 319 102-1 [i.16].

4.4 Wallet interfaces for signature creation

The present clause describes the use of the EUDIW to support the creation of Qualified Electronic Signatures (QES) and Qualified Electronic Seals (QSeals). Signature creation can be performed using either:

- a local Qualified Signature Creation Device (QSCD) integrated into the EUDIW environment; or
- a remote QSCD operated by a Qualified Trust Service Provider (QTSP).

The EUDIW interface enables users to securely initiate and authorize the creation of digital signatures, in compliance with eIDAS and ETSI standards. It provides consistent interaction mechanisms with the Signature Creation Application (SCA), whether it is embedded in the EUDIW or hosted externally.

EUDIW providers are expected to:

- support secure and privacy-preserving user authentication to signature services.;
- ensure that a qualified certificate bound to a QSCD is obtained and linked to the user;
- enable SCA to sign any data provided by the user;
- support signature format PAdES [i.29];
- optional support signature formats XadES [i.27], CAdES [i.28], JAdES [i.30], and ASiC [i.31].

Signature initiation involves user awareness and consent. The EUDIW allows users to preview signing context (e.g. document hash, transaction metadata), approve the action, and receive confirmation of signature creation. It is also required to support signature history tracking and transparency features to enable users' control.

Multiple models of signature integration are supported:

- full integration of SCA within the EUDIW;
- redirection to an external remote SCA operated by a QTSP;
- use of the EUDIW as SIC in the process of SAD generation following SCAL2 requirements from EN 419 241 [i.18], clause 5.10;
- use of the EUDIW as an authentication component following SCAL2 requirements from EN 419 241 [i.18], clause 5.10.

The present document takes into account the following standards specifying Signature Creation interface requirements: ETSI TS 119 431-1 [i.12], ETSI TS 119 431-2 [i.13], ETSI TS 119 432 [i.15], ETSI EN 319 102-1 [i.16], ETSI EN 319 411-1 [i.11], ETSI EN 319 411-2 [i.17], CSC API V2.2 [i.32].

5 Interface for authentication and identification

5.1 Identity proofing

When issuing a Qualified Certificate or a Qualified Electronic Attestation of Attributes for a trust service, a Qualified Trust Service Provider verifies the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate or the qualified electronic attestation of the attribute is issued.

Supporting standards:

Standard	Description
ETSI TS 119 461 [i.40].	Requirements for TSPs for the identity proofing process
ETSI TS 119 472-1 [i.41].	EAA Profile

5.2 Interface for online identification and authentication

The interface for online identification and authentication enables requests and receives Personal Identification Data (PID) and Electronic Attestation of Attributes (EAA) during the identity validation process or when requesting specific attributes.

The interface enables a Relying Party (RP) - which may also be a Trust Service Provider (TSP) - to request and receive PID, and/or EAAs from the EUDIW, for identity validation, attribute-based access control, or service provisioning.

This interface supports online interactions, where the RP actively engages the EUDIW user in a data presentation session and receives a structured response.

According to the ARF [i.4], this interface is governed by the Presentation Phase, especially in: Section 6.6.3: PID or attestation presentation to Relying Party, Annex 2 - Topic 1: Accessing Online Services with a Wallet Unit (OIA_04-OIA_07), Annex 2 - Topic 6: High-Level Requirements for Relying Party Authentication and Attribute Requests (Req. RPA_01-RPA_07, RPA_09-RPA_11): defining how the request is structured, secured, and consented.

The core pattern includes:

- Request: The RP sends an authenticated presentation request to the EUDIW.
- Authentication: The EUDIW authenticates the RP Instance, ensuring the User is correctly informed about the Relying Party's identity.
- Consent: The EUDIW displays the request to the user, including the purpose, legal basis, data categories, and RP identity.
- Presentation: Upon user approval, the EUDIW prepares and returns the requested PID or attributes, respecting selective disclosure rules.

ARF [i.4] specifies OpenID4VP [i.26] as the preferred protocol for implementing this interface:

- Based on OAuth 2.0 Authorization Framework RFC 6749 [i.44]
- Adapted to support Verifiable Credentials (SD-JWT VC [i.22], ISO mDL [i.19])
- Enabling secure binding between the RP, the data request, and the resulting presentation.

Key Components:

- Presentation Request: Structured JSON object signed by the RP or transmitted via URI.
- Verifiable Presentation: JWT or SD-JWT VC response containing selectively disclosed claims.
- Response Binding: The EUDIW signs the response or uses cryptographic proof to ensure authenticity and user control.

Reference:

[i.4] ARF - Annex 2, Topic 1 Accessing Online Services with a Wallet Unit: OIA_03a - OIA_04 specifying the protocols for the presentation interface.

Security and Privacy Measures

- Mutual Authentication: WRP authenticates itself using a WRP certificate: access and registration (cf. CIR 2025/848 [i.9]).
- User Consent: EUDIW is required to always obtain explicit user consent before presenting any data.
- Selective Disclosure: The EUDIW supports attribute-level granularity using SD-JWT or mDL containers.
- Audit and Logging: All presentations will be logged within the EUDIW for user traceability (CIR 2024/2979 [i.6]).

Supporting standards:

Standard	Description
ETSI TS 119 472-1 [i.41]	EAA Profile
ETSI TS 119 472-2 [i.42]	EAA/PID Presentation to relying party
OpenID4VP [i.26]	EAA/PID Presentation to relying party
ETSI TS 119 411-8 [i.35]	Relying Party Access Certificates
ETSI TS 119 475 [i.34]	Relying Party Registration Certificates

5.3 Interface for request for signature

The interface allows a Relying Party (RP)-typically a service provider requiring a legally binding transaction-to initiate a digital signature request by the user via the EUDIW.

This interface is used to transfer the signature request parameters, authenticate the user, and facilitate a secure process redirect to the Signature Creation Application (SCA).

This interface does not perform the signature itself but initiates the signature workflow.

The interface is functionally dependent on the mechanisms described in clause 5.2:

- reuses the OpenID4VP [i.26] based request structure to deliver the transaction context (e.g. document hash, signing intent);
- follows the same authentication and consent process, ensuring that the RP is properly identified and authorized;
- builds on the secure presentation layer used for PID/EAA.

In effect, the interface extends the interface specified in clause 5.2 by adding signature-specific elements, such as:

- Signature metadata (e.g. hash to be signed, document ID)
- Signature policy references (e.g. AdES type, legal value)
- Optional request for qualified signature creation via remote or local QSCD

Depending on the deployment model, this interface may also pass the signed metadata to an external SCA (e.g. operated by QTSP), or activate EUDIW's internal SCA module with appropriate binding to the WSCD or remote QSCD.

Supporting standards:

Standard	Description
ETSI TS 119 472-2 [i.42]	EAA/PID Presentation to relying party (including transaction data)
OpenID4VP [i.26]	EAA/PID Presentation to relying party (including transaction data)
ETSI TS 119 432 [i.15]	Protocols for remote digital signature creation, including delegation to Signature Creation Application (SCA)
ETSI EN 319 102-1 [i.16]	General requirements for AdES and QES creation, including user intent and consent.
CSC API [i.32]	Remote signature creation API

6 Interface for EAA issuance

6.1 Interface description

The interface between European Digital Identity Wallets (EUDIW) and Trust Service Providers (TSPs) issuing Electronic Attestations of Attributes (EAAs) relies on the OpenID for Verifiable Credential Issuance (OpenID4VCI) [i.25] protocol profiled for high assurance. In particular, the issuance profile builds on OpenID4VC-HAIP [i.24] and extends it to meet EUDIW ecosystem requirements, including the use of Wallet Unit Attestation (WUA), metadata carried by the Issuer, and binding of issued EAAs to wallet-controlled keys.

The interface requires signed Issuer Metadata and supports discovery of credential formats, embedded disclosure policy pointers, reuse policies, and the inclusion of access and registration certificates for the PID/EAA Provider. These elements enable the EUDIW to authenticate the issuer, obtain policy signals, and conduct the issuance flow using either the Authorization Code Flow or the Pre-Authorized Code Flow defined by OpenID4VCI [i.25].

The profile and interface for EAA issuance are specified in the ETSI TS 119 472-3 [i.43].

The formats for EAAs are specified in ETSI TS 119 472-1 [i.41].

Normative building blocks include:

- Issuer Metadata (signed JWS) with credential configuration, access certificate chain, and optional registration certificate.
- EAA issuance flows and request/response requirements (Credential Offer, Pushed Authorization Request, Token Request, Credential Request/Response, Notification).
- Support for EAA formats, including profiles not natively covered by OpenID4VCI [i.25] (e.g. X.509 Attribute Certificate-based EAA).

Related trust service and credential requirements are provided in ETSI TS 119 471 (EAASP policy/security) [i.14], ETSI EN 319 411-1 [i.11] and ETSI EN 319 411-2 [i.17] (certification policies), ETSI TS 119 411-8 (Access Certificates) [i.35], ETSI TS 119 475 (Registration Certificates/RP attributes) [i.34], and ISO/IEC 23220-3 (EUDIW issuance phase) [i.21].

6.2 Wallet user identification

User identification and any prerequisite enrolment or attribute validation are performed in accordance with clause 5 of the present document. The TSP may leverage attributes previously issued to the user and, where necessary, obtain additional attributes from authoritative sources. If needed for identification or authorization of the holder, the TSP may use presentations via clauses 5.1 and 5.2 of the interface before proceeding with issuance.

Supporting standards:

Clauses 5.1 and 5.2 provide information about supporting standards.

6.3 Issuer discovery

Discovery of issuer capabilities and prerequisites is performed via Issuer Metadata retrieved and validated by the wallet. The metadata is a JWS whose protected header carries the issuer's access certificate chain (x5c), and whose body enumerates supported credential configurations, formats, and optional registration certificate information (issuer_info). This enables the wallet to authenticate the issuer and prepare the correct authorization and credential requests.

Supporting standards:

Standard	Description
OpenID4VCI [i.25]	Verifiable Credential Issuance interface defining the ./well-known for the Issuer Metadata.
HAIP [i.24]	OpenID4VC High Assurance Interoperability Profile defines the x5c in the Issuer Metadata.
ETSI TS 119 472-3 [i.43]	Profiles for issuance of EAA or PID defining requirements for the Issuer Metadata.

6.4 Electronic Attestation of Attribute issuance

Issuance follows the OpenID4VCI [i.25] profile and supports Authorization Code and Pre-Authorized Code flows. In the case of the Issuer-started process, the Credential Offer is sent to the EUDIW which then proceeds through the Pushed Authorization Request (PAR) and Authorization Request as well, Token Request, and is completed with a Credential Request that proves possession or presents attestations for the keys to which EAAs will be bound.

Supporting standards:

Standard	Description
ETSI TS 119 471 [i.14]	EAA Service provider policy requirements.
ETSI TS 119 472-1 [i.41]	EAA Profile.
ETSI TS 119 472-3 [i.43]	Profiles for issuance of EAA or PID.
OpenID4VCI [i.25]	Verifiable Credential Issuance interface.
ETSI TS 119 475 [i.34]	Relying Party Registration Certificates (EAA issuer registration certificate).
HAIP [i.24]	OpenID4VC High Assurance Interoperability Profile requirements for the OpenID4VCI [i.25].

6.5 Electronic Attestation of Attribute lifecycle management

Lifecycle management covers status changes and re-issuance mechanics signalled through the issuance profile and related policies:

- Revocation and status: Issuers can later signal status via mechanisms associated with the EAA format and ecosystem policies; wallets are expected to process status and embedded disclosure policies when presenting EAAs. (See EDP and reuse-policy signalling in Issuer Metadata.)
- Renewal and refresh: Where supported, refresh tokens may be used to obtain new credentials subject to issuer risk assessment and wallet storage considerations; issuers are expected to perform an evaluation of attribute sensitivity before enabling refresh.

Supporting standards:

Standard	Description
ETSI TS 119 471 [i.14]	EAA Service provider policy requirements.
ETSI TS 119 472-3 [i.43]	Profiles for issuance of EAA or PID.
OpenID4VCI [i.25]	Verifiable Credential Issuance interface (batch issuance).
HAIP [i.24]	OpenID4VC High Assurance Interoperability Profile RECOMMENDS the usage of Refresh token.

7 Interfaces for the creation of an electronic signature

7.1 Interface components

7.1.1 Functional model

The present document uses the functional model of a Signature Creation Environment (SCE) specified in clause 4.1 of ETSI EN 319 102-1 [i.16], consisting of:

- a signer who wants to create a signature;
- a Driving Application (DA) which represents the environment (e.g. a business application) that the signer uses to access signing functionality; and
- a Signature Creation System (SCS) which implements the signing functionality using:
  - a Signature Creation Application (SCA); and
  - a Signature Creation Device (SCDev).

Figure 1 illustrates the data flow between the EUDIW and SCE during signature creation interaction processes. The SCE components use EUDIW as a data source and for secure interaction with Signer.

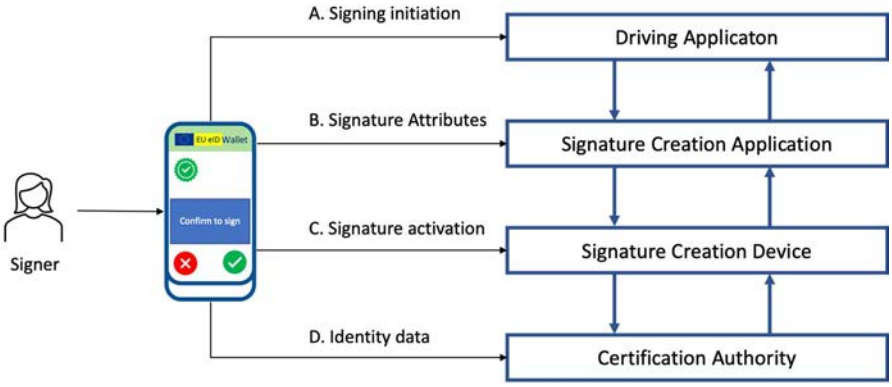

Figure 1: Signature creation with the EUDIW data flow

All the components specified in the figure interact with the EUDIW or are part of the wallet implementation. If components are external services, they act as relying parties and utilize the data provided by the EUDIW to facilitate the signing process. It defines the recipient of the data transmitted by the EUDIW, while the direct or indirect method of data transmission by various components may depend on the implementation. It is permissible for different functions to be aggregated and realized through a single interaction with the EUDIW or through multiple interactions with the EUDIW.

The present document specifies the use of the EUDIW in the signing process in four basic functions, which can be implemented through various interfaces, either through multiple interactions with the EUDIW or in a single interaction. These functions represent the logical execution of actions in interaction with the component but can be implemented using EUDIW's standard mechanism, which is the EAA Presentation.

Those includes following interfaces:

- Signing initiation (A)
- Signature attributes (B)
- Signature activation (C)
- Identity data (D)

An analysis of possible extensions for signature creation interfaces is provided in Annex B.

7.2 Signing initiation interface

The signer, using the EUDIW, provides the DA with instructions for selecting the signing method, indicating the choice of SCA. The relying party prepares the document through the DA, and the DA initiates the signing flow with the SCA. The DA may be part of the relying party, a standalone signing portal, possibly merged with SCA, or a local wallet/device component.

If a SCA is preselected by agreement, initiation can be implicit.

Supporting standards:

Standard	Description
OpenID4VP [i.26]	OpenID for Verifiable Presentations; Transaction data in request/presentation
ETSI TS 119 432 [i.15]	Protocols for remote digital signature creation; DA invokes the SCA and provides SD(R).

7.3 Signature attributes interface

The signer, using the EUDIW, provides Signature attributes to the SCA, which collects and assembles them with the SD(R) and the certificate identifier into the DTBS.

ETSI TS 119 479-3 [i.45] regarding support for EAA within AdES signatures is under development.

Supporting standards:

Standard	Description
OpenID4VP [i.26]	OpenID for Verifiable Presentation; Transaction data in request/presentation.
ETSI TS 119 472-1 [i.41]	EAA Profile.
ETSI TS 119 472-2 [i.42]	Profiles for EAA/PID Presentations to Relying Party.
ETSI TS 119 412-6 [i.20]	Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers.

7.4 Signature activation interface

The signer authenticates to the SCA using the EUDIW; the SCA then initiates Signature Activation with the SSA controlling the SCDev. The EUDIW acts as the SIC and runs SAP with the SAM to generate SAD, which the SAM verifies to enable SCDev to create the signature value.

Supporting standards:

Standard	Description
OpenID4VP [i.26]	OpenID for Verifiable Presentation; Transaction data in request/presentation
ETSI TS 119 432 [i.15]	Protocols for remote digital signature creation; Signature activation
ETSI TS 119 431-1 [i.12]	TSP services operating a remote QSCD/SCDev
ETSI TS 119 431-2 [i.13]	TSP service components supporting AdES digital signature creation
CSC API [i.32]	Architectures and protocols for remote signature applications

7.5 Identity data interface

The EUDIW provides the signer's identity data for just-in-time certificate issuance (e.g. one-time signing key), which is then returned and bound to the active signing session.

Interfaces for online identification and authentication, and for a signature request are described in clauses 5.2 and 5.3 of the present document.

Supporting standards:

Standard	Description
ETSI TS 119 431-1 [i.12]	TSP services operating a remote QSCD/SCDev
ETSI TS 119 431-2 [i.13]	TSP service components supporting AdES digital signature creation
ETSI TS 119 461 [i.40]	Policy and security requirements for trust service components providing identity proofing of trust service subjects

8 Wallet interface for other trust services

8.1 General provisions

Trust services use the EUDIW for user identification and authentication. The identification process may utilize the PID functionality or specific attributes provided by the EUDIW. Depending on the type of service and the legal and regulatory requirements, the services may use identification with varying Levels of Assurance. Trust services may also use other EAA defined at the level of standards, EU, or local law for the authentication of previously registered users. Trust services may particularly define and issue EAA and attributes needed to authenticate their own users independently. Annex A to the present document provides an open list of use cases for the EUDIW by trust service providers.

Annex A (informative): List of use cases for the interaction of the EUDIW with trust services

A.1 Attributes enabling interaction with trust services

The Electronic Attestation of Attributes stored in the EUDIW and presented in interaction with trust service enables authentication and authorization to specific trust services.

EXAMPLE 1: Attribute enabling time stamping service.

EXAMPLE 2: Attribute confirms payment for certificate issuance.

A.2 Initiation of RDS - The EUDIW holder is a receiver

The Electronic Attestation of Attributes stored in the EUDIW and presented in interaction with the Driving Application initializes the process of registered delivery to the EUDIW holder. The EUDIW holder in this process is receiving party.

A.3 Initiation of RDS - The EUDIW holder is a sender

The Electronic Attestation of Attributes stored in the EUDIW and presented in interaction with the Driving Application initializes the process of registered delivery to the other party. The EUDIW holder in this process is sending party.

Annex B:
Analysis of optional extensions supporting digital signature creation with EUDIW

B.1 Interface components

B.1.1 Functional model

The functional model is specified in clause 7.1.1 of the present document.

Interface components specified in the present clause are for analysis of optional extensions for future updates of the present document.

B.1.2 Signature creation wallet interactions

B.1.2.1 Signing initiation (A)

Purpose: The signer, with the use of the EUDIW, provides the Driving Application (DA) with instructions for the selection of the signing method, indicating the choice of the Signature Creation Application (SCA).

Example: The EUDIW provides a token that enables redirecting the signer to the SCA and securely transferring the document information to be signed from the DA to SCA.

Description: During initiation, the Relying Party (RP) interacts with the DA to make the document to be signed known, and the signer interacts with the DA to start the signing flow.

- The DA could be part of the RP services (e.g. a web-bank or car rental portal), in which case the document preparation is fully handled by the RP.
- The DA could be a remote service (e.g. a signing portal). In this scenario, the DA and SCA are merged.
- The DA could be part of the wallet or another app on the signer's device.

Additional notes: The choice of SCA can be made by the DA or the RP in this case, signing initiation does not occur.

B.1.2.2 Signature Attributes (B)

Purpose: Signer with the use of the EUDIW provides Signature Attributes to be collected by the Signature Creation Application (SCA) and included in the DTBS.

Example: A power of attorney held by the EUDIW as an Electronic Attestation of Attributes can be shared with the SCA and included as evidence in a signed document.

Description: EUDIW enables the signer to select and provide signature attributes that will be embedded in the DTBS or bound to the signature as signed properties.

Additional notes: The RP can also provide some of the signed attributes - in particular, commitment type indication.

B.1.2.3 Signature Activation (C)

Purpose: Signer with the use of the EUDIW authenticates to the Signature Creation Device (SCDev) to enable creation of the signature value.

Example: SCDev is implemented by Server Signing Application (SSA) for remote signature, Signature Activation creates a Signature Activation Data (SAD) as implementation of the Signature Activation Protocol (SAP) according to the architecture for server signing of ETSI TS 119 432 [i.15], clauses 5.2-5.4.

Description: The signer authenticates with EUDIW to the SCA or the SSA controlling SCDev, depends on which component TSP hosts. If the TSP is hosting only the SSA then the SCA can be provided i.e. directly in the signer environment or by a different TSP. TSP managing SCA and/or SSA can delegate the authentication and authorization processes to an external party (e.g. to an identity and/or an authentication provider).

Additional notes: When the SAD validation succeeds, the corresponding signing key may be used by SCDev for signature operations on behalf of the signer.

B.1.2.4 Identity Data (D)

Purpose: The EUDIW provides the signer's identity data for certificate issuance.

Example: The EUDIW provides the signer's personal identity data for the signer's initial identity validation and to issue a short-term certificate for one-time signing key use in signature creation.

Description: When the transaction requires the issuance of a certificate (e.g. one-time signing key), the EUDIW supplies the signer's identity data and, where applicable, supporting EAAs to the TSP via the SCA for identity proofing in accordance with ETSI TS 119 461 [i.40].

B.1.3 Signature creation scenarios

Figure B.1 documents generic scenarios for signature creation. Scenarios are based on components specified above. The list of scenarios is not exhaustive and may be expanded based on available use cases. This list enables the identification of scenarios that are supported by the present document.

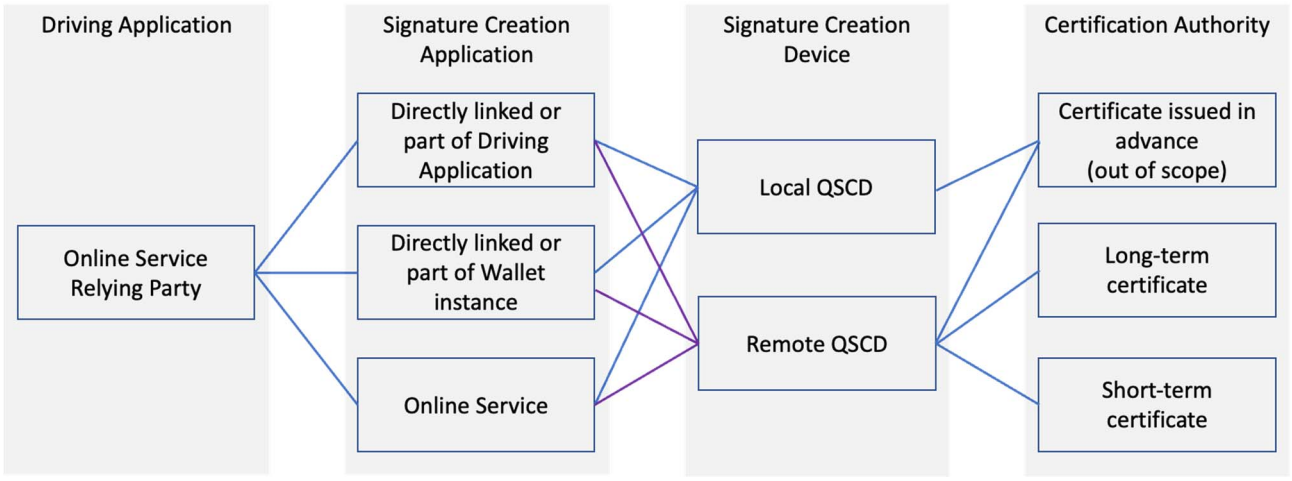

Figure B.1: Signature creation scenarios

Below are the options associated with each scenario.

- **Driving Application (DA)**
  - An online service or application provided by the Relying Party.
  - Part of the Wallet Solution (Out of scope of the present document).
  - Desktop application (Out of scope of the present document).
  - Another solution directly linked to the Signature Creation Application (Out of scope of the present document).
- **Signature Creation Application (SCA)**
  - An online service or application provided by the same entity as Driving Application or directly associated with Driving Application.
  - An application directly associated, internally connected with, or part of the EUDIW.

- A separate online service provided by a third party (including TSP).

- **Signature Creation Device (SCDev)**
  - Local device integrated with or connected to the EUDIW.
  - Remote-based on external Server Signing Application.

- **Certificate Authority (CA)**
  - Long-term certificate issued in advance (Out of scope of the present document).
  - Long-term certificate and authentication with the use of the EUDIW to activate the key.
  - Based on PID data and the issuance of a short-term certificate for one-time signing key signature creation.

The present clause aims to provide an understanding of the various possibilities and models for using the individual components related to signing. The scenarios presented are informational and do not constitute an exhaustive list. Based on the interface elements specified in the present document, other scenarios for executing the signing process can be developed.

B.1.4 Remote signature creation models

The present clause defines the components necessary for executing the remote signing process based on a digital identity EUDIW. The elements described below do not constitute an exhaustive list and may be supplemented with other solutions that support the signing process. The components specified in the present clause are entirely based on the requirements of the following standards required for remote signature creation: ETSI TS 119 431-1 [i.12], ETSI TS 119 431-2 [i.13], ETSI TS 119 432 [i.15], CSC API V2.2 [i.32], EN 419 241-1 [i.18].

As specified in clause B.1.3, the Signature Creation Application can be a remote solution implemented via an online application or a solution installed in the EUDIW environment (part of the EUDIW application or the environment in which it is installed).

Interaction with the Remote Signature Creation Device requires the generation of Signature Activation Data (SAD) compliant with the ETSI TS 119 431-1 [i.12]. EUDIW acts as a Signature Interaction Component (SIC) following Transaction data for authorization as specified in ETSI TS 119 472-2 [i.42], Annex A and OpenID4VP [i.26], clause 8.4.

EN 419 241-1 [i.18] defines SCAL2 requirements for Signature Activation Protocol (SAP) for the generation of Signature Activation Data (SAD). The SAD is set, computed by SIC, or is the result of a secured interaction between the Signature Activation Module (SAM) and the SIC through the Server Signing Application (SSA), to authorize the signing operation within the Signature Creation Device (SCDev), and the SAD is transmitted to the SAM through the SSA to authorize the signing operation within the SCDev for a dedicated DTBS/R. According to EN 419 241-1 [i.18], the SIC is a piece of software and/or hardware operated in the signer's environment under its sole control.

If the EUDIW is used for remote signature activation, the following two options are recognized:

- SAD is directly generated by the EUDIW, which acts as a SIC;
- SAD is generated outside of the EUDIW; EUDIW is used for signer authentication to the authorization server.

If SAD is directly generated by the EUDIW, the model may be one of the following:

SAD generation options	Models in the present document
1 The direct function of the EUDIW	Outside of the scope of the present document
2 Identification data presentation by the EUDIW on the request of SSA acting as RP	• `WalletApp_Auth` • `RemoteApp_Auth`
3 Specific EAA (SIC_EAA) presentation by the EUDIW on the request of SSA acting as RP	• `Wallet App_SADGen` • `RemoteApp_SADGen`

Regardless of the above, interaction may involve providing identifying data used for certificate issuance or authentication based on attributes contained in the EUDIW to use a long-term certificate.

The following presents the division of the different models for remote electronic signature creation.

	SCA is directly linked to the EUDIW	SCA is remote application
EUDIW, as a SIC, directly generates SAD	`WalletApp_SADGen`	`RemoteApp_SADGen`
EUDIW is used to authenticate, and SAD is generated outside of the EUDIW	`WalletApp_Auth`	`RemoteApp_Auth`

B.1.5 Models description

B.1.5.1 WalletApp_SADGen model

The `WalletApp_SADGen` model comprises the following provisions:

- Signature Creation Application (SCA) is part of or directly linked to the digital identity EUDIW, executed within the same device or internally connected to it.
- The EUDIW provides Signature Initiation Component (SIC) with the capability to generate Signature Activation Data (SAD) in accordance with the requirements of the ETSI TS 119 432 [i.15] protocol.

NOTE: Multiple deployment variants may be possible: the EUDIW and the SCA component may run entirely on one device, or may be distributed across two or more mutually trusted and interconnected devices.

The following figure presents the main components of the `WalletApp_SADGen` model

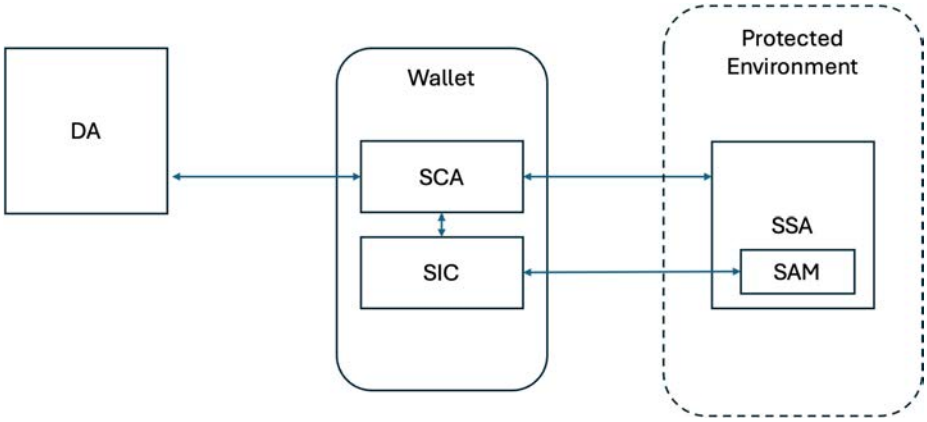

Figure B.2: WalletApp_SADGen model

Supporting standards:

Standard	Components	Description
ETSI TS 119 432 [i.15]	Wallet to SSA	Interaction between wallet and SSA
ETSI EN 319 102-1 [i.16]	SCA	Requirements for SCA
CSC API [i.32]	SCA to SSA	Requesting signature creation protocol
(no standard)	DA to wallet	Requirements for the DA requestion signature from the wallet
(no standard)	SCA to SIC (in the same device)	

B.1.5.2 RemoteApp_SADGen model

The `RemoteApp_SADGen` model comprises the following provisions:

- Signature Creation Application (SCA) is an online application or a solution accessible to the EUDIW via the Internet.

- The EUDIW provides Signature Initiation Component (SIC) with the capability to generate Signature Activation Data (SAD) in accordance with the requirements of the ETSI TS 119 432 [i.15] protocol and policy requirements of ETSI 119 431-1 [i.12] and ETSI 119 431-2 [i.13].
- The SCA handles the information exchange with the Server Signing Application (SSA) through a direct secure channel.

NOTE 1: An example implementation is a SCA running on a desktop computer, where the wallet user interacts with the SCA via a web interface that establishes a session with the EUDIW.

NOTE 2: The secure and trusted channel between the SCA and the SSA may be realized using different technical approaches, provided that the selected approach achieves the required security properties.

Figure B.3 presents the main components of the `RemoteApp_SADGen` model:

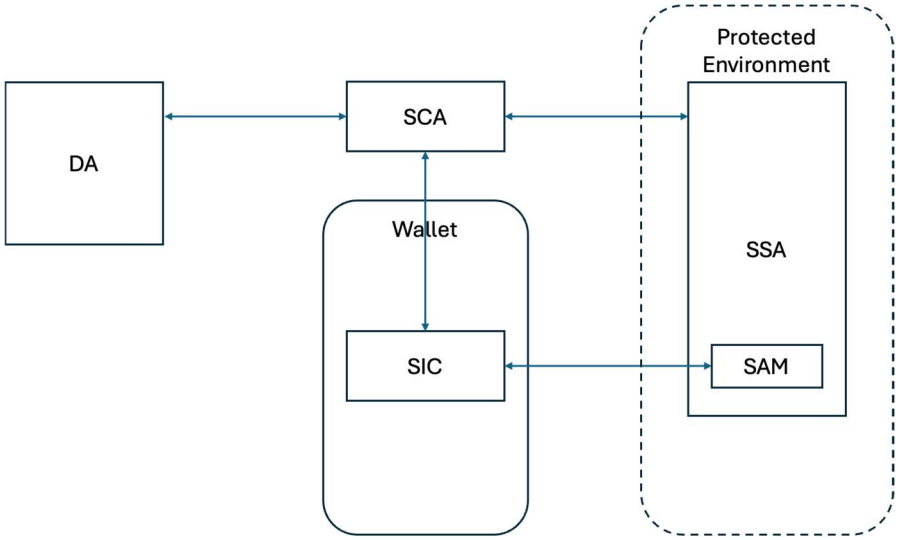

Figure B.3: RemoteApp_SADGen model

Supporting standards:

Standard	Components	Description
ETSI TS 119 432 [i.15]	Wallet to SSA	Interaction between wallet and SSA
ETSI EN 319 102-1 [i.16]	SCA	Requirements for SCA
(no standard)	SCA to SIC	SAD is created by SIC with use of (transaction data generated by wallet)
CSC API [i.32]	SCA to SSA	signDoc endpoint
(no standard)	DA to SCA	Interaction between the DA and SCA

B.1.5.3 `WalletApp_Auth` model

The `WalletApp_Auth` model comprises the following provisions:

- Signature Creation Application (SCA) is a part of or directly linked to the digital identity EUDIW, executed within the same device or internally connected to it.
- The EUDIW does not directly interact with the Signature Activation Module (SAM).
- The EUDIW's Signature Interaction Component (SIC) only facilitates authentication to the Authentication Server (Auth Srv). As a result of this interaction, the Signature Activation Data (SAD) is created.
- The SCA handles the information exchange with the Server Signing Application (SSA) through a direct secure channel.

NOTE: Auth Srv can support the OAuth 2.0 [i.44] protocol.

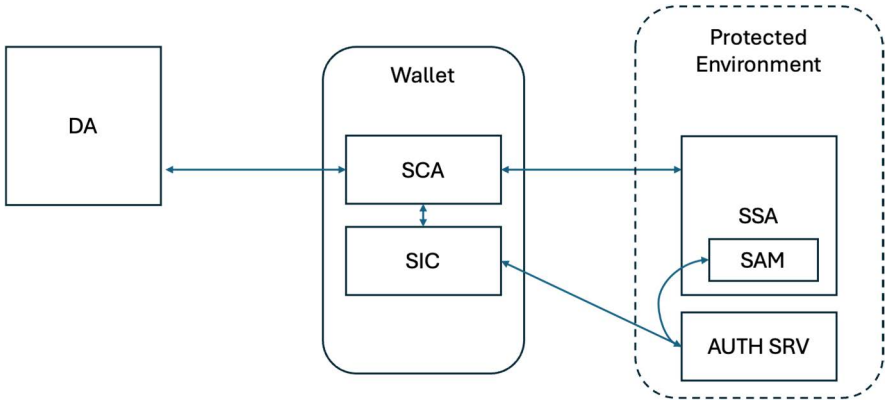

Figure B.4: WalletApp_Auth model

Supporting standards:

Standard	Components	Description
ETSI TS 119 432 [i.15]	Wallet to SSA	Interaction between wallet and SSA.
CSC API [i.32]	SCA to SSA	signDoc endpoint.
ETSI EN 319 102-1 [i.16]	SCA	Requirements for SCA.
OpenID4VP [i.26]	SIC to AUTH SRV	Interaction between SIC and AUTH SRV to generate SAD.
(no standard)	DA to wallet (SCA	Initiates signature creation in the wallet by DA.
(no standard)	SCA to SIC (in the same device)	
OAuth 2.0 [i.44]	SAD	OAuth 2.0 access token with rich authorization details that contains the DTBS/R and link to authentication.

B.1.5.4 `RemoteApp_Auth` model

The `RemoteApp_Auth` model comprises the following provisions:

- Signature Creation Application (SCA) is an online application or a solution accessible to the EUDIW via the Internet.
- The EUDIW does not directly interact with the Signature Activation Module (SAM).
- The EUDIW's Signature Initiation Component (SIC) only facilitates authentication to the Authentication Server (Auth Srv). As a result of this interaction, the Signature Activation Protocol (SAP) is constructed, and the Signature Activation Data (SAD) is created.
- The SCA handles the information exchange with the Server Signing Application (SSA) through direct secure channel.

NOTE 1: It is possible to implement the SCA on a desktop computer connecting to the EUDIW through a web interface.

NOTE 2: A secure and trusted communication channel between the SCA and the SSA can be implemented using various techniques.

NOTE 3: Auth Srv may provide the OAuth 2.0 protocol [i.44].

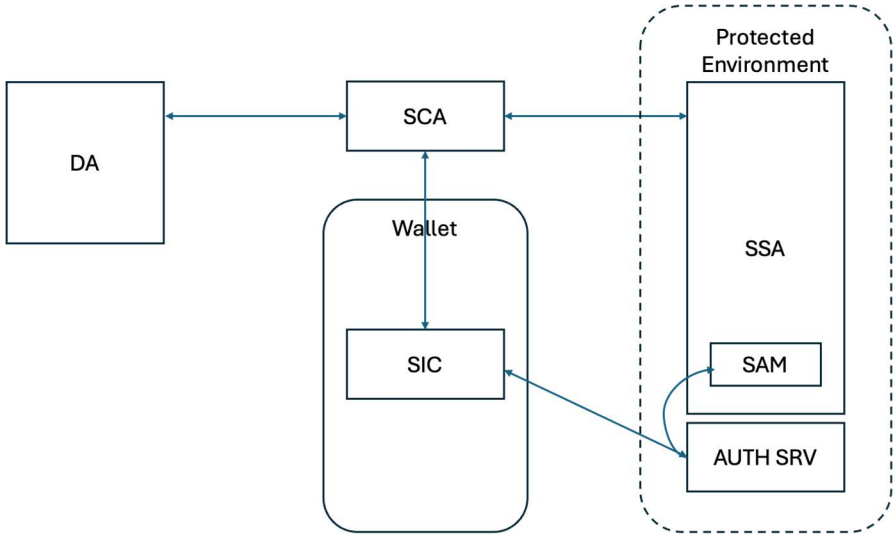

Figure B.5: RemoteApp_Auth model

Supporting standards:

Standard	Components	Description
CSC API [i.32]	DA to SCA	CSC signDoc
OAuth 2.0 [i.44]	SIC to AUTH SRV	OAuth 2.0 as explained in CSC version 2
CSC API [i.32]	SCA to SSA	CSC sighHash
OAuth2.0 [i.44]	SAD	OAuth 2.0 access token with rich authorization details that contains the DTBS/R and link to authentication.
(no standard)	SCA to SIC	Interaction between SCA and SIC

B.2 Digital Signature Certificates Issuance

B.2.1 Signature keys local in the EUDIW

The private key is protected by a local device (e.g. a cryptographic card, SIM card, or a secure component of the mobile device on which the EUDIW is installed). The present document recognizes this possibility but does not define detailed requirements for the interface between the EUDIW and the Signature Creation Device (SCDev).

Supporting standards:

Standard	Description
PKCS#11 [i.33]	For local devices

B.2.2 Certificates supporting remote signature

B.2.2.1 Remote signature based on long-term certificate

The signer holds a long-term certificate for signature creation, and the EUDIW is used to authenticate the signer for using the key located in the Remote SCDev. Issuing a certificate for signature creation with the use of the EUDIW may require additional information maintained in the digital identity EUDIW, which will enable subsequent authentication and key activation.

Supporting standards:

Standard	Description
ETSI TS 119 431-1 [i.12]	Management of signing keys
ETSI EN 319 411-1 [i.11]	Requirements for certificate issuance

B.2.2.2 Remote one-time signing key signature based on short-term certificate

The signer does not possess a certificate, and the EUDIW provides the identity of the signer to the Trust Service Provider for short-term certificate issuance. Keys for creating the electronic signature are generated remotely as and used for a one-time or one-session electronic signature.

Supporting standards:

Standard	Description
ETSI TS 119 431-1 [i.12]	Management of signing keys
ETSI TS 119 431-2 [i.13]	Signature creation
ETSI EN 319 411-1 [i.11]	Requirements for certificate issuance

B.2.3 Certificate issuance and assignment

For a certificate for signature creation to be recognized by the EUDIW, the following requirements need to be completed:

- private keys associated with the certificate generated and stored in SCDev;
- digital signature certificate related to private keys issued by Certification Authority;
- authentication means to activate private keys. Private keys use handover to the signer.

All those provisions are defined by ETSI EN 319 411-1 [i.11] and ETSI EN 319 411-2 [i.17].

Enabling EUDIW signing requires:

a) Certificate issuance and key generation (Issuance).

b) Certificate and SCDev linking to the EUDIW (Linking).

c) Authentication means the provision to Signer (Means provision).

The present document recognizes the following interfaces for new certificate issuance:

1) If the EUDIW is linked or connected to local SCDev directly (not defined in the present document):

   a) Issuance: Certificate issuance, key generation and SCDev provision.

   b) Linking: EUDIW enables a direct link to the SCDev and provides this information to SCA.

   c) Means provision: provision of PIN or other authentication factors required to activate the private key. A call-for-sign mechanism may be provided via PKCS#11 [i.33].

2) If the EUDIW uses Remote SCDev to support long-term certificates:

   a) Issuance: Presentation of attributes to prove identity or outside of the EUDIW.

   b) Linking: CA provides to the EUDIW certificate information (e.g. EAA with certificate information).

   c) Means provision: the SIC data required to activate the private key are provided to the EUDIW (e.g. SIC_EAA).

3) If the EUDIW uses Remote SCDev to support one-time signing key use in signature creation:

   a) Issuance: Presentation of attributes to prove identity.

   b) Linking: Session-based - not needed for single use.

   c) Means provision: session-based activation. No persistent means are required for single-use certificates.

4) The EUDIW is QSCD (optional - not specified here).

Supporting standards:

Standard	Description
ETSI EN 319 411-1 [i.11]	Requirements for issuing certificates
ETSI EN 319 411-2 [i.17]	Requirements for qualified certificates
ETSI TS 119 431-1 [i.12]	Management of signing keys
ETSI TS 119 431-2 [i.13]	Signature creation

B.2.4 Certificate information in EAA

Signature creation with the EUDIW may require information about the certificate accessible from the EUDIW. The present document defines EAA with a signing certificate as the Signature Certificate Electronic Attestation of Attributes (SC_EAA).

Supporting standards:

Standard	Description
(no standard)	No standard for inclusion of electronic signature certificate in the EAA
ETSI TS 119 472-1 [i.41]	EAA profile

B.2.5 EAA as authenticator

Using the EUDIW for authentication purposes to activate a Qualified Electronic Signature may require the creation of an attribute, the presentation of which will allow the signer to authenticate for certificate creation. This authentication can be implemented in all four models described in clause B.1.4.

Using an attribute for authentication allows for managing access to authentication externally by managing the lifecycle of a specific attribute. When using attribute presentation for authentication, its validity needs to be verified.

The use of the attribute can also be combined with transaction data specified in ETSI TS 119 472-2 [i.42], Annex A and OpenID4VP [i.26], clause 8.4, which allows linking DTBSR to a specific signing process.

Supporting standards:

Standard	Description
ETSI TS 119 472-2 [i.42].	Profiles for EAA/PID Presentation to relying party (transaction data)
OpenID4VP [i.26]	EAA/PID Presentation to relying party (transaction data)

B.2.6 Including EAA as a signing attribute

Some signatures will require the inclusion of Electronic Attribute Attestations (EAA) in the structure of the signed document. Considering that EAAs can exist independently or be associated with the EUDIW, both independent EAAs and those presented by the EUDIW should be taken into account. Two scenarios should be considered: the EAA is directly included in the document structure as issued by the EAA issuer, or the signature includes an EAA presentation made by the EUDIW.

ETSI 319 102-1 [i.16] defines that the Signature Creation Application (SCA) is responsible for collecting all attributes needed in the signing process. In a situation where the SCA is an external Remote Application, it is possible for the SCA to act as a Relying Party (RP), which requests presentation of attributes to be included in the signed document.

NOTE: One can also consider a model where the SCA, directly implemented by the EUDIW, acts as a RP for its own presentations. In this case, including the EAA involves the EUDIW making a presentation for its own needs and then including this presentation in the structure of the signed document.

Supporting standards:

Standard	Description
ETSI TS 119 472-2 [i.42]	Profiles for EAA/PID Presentation to relying party (transaction data)
OpenID4VP [i.26]	EAA/PID Presentation to relying party (transaction data)
ETSI EN 319 102-1 [i.16]	General requirements for AdES and QES creation, including user intent and consent

History

Version	Date	Status
V1.1.1	March 2026	Publication