ETSI TS 119 475 V1.1.1 (2025-10)

TECHNICAL SPECIFICATION

Electronic Signatures and Trust Infrastructures (ESI); Relying party attributes supporting EUDI Wallet user's authorization decisions

Reference
DTS/ESI-0019475

Keywords
digital certificate, digital 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 Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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] establishes the legal framework for electronic identification and trust services within the internal market, including the provision and use of the European Digital Identity Wallet (EUDIW). In this context, entities acting as wallet-relying parties are required to be registered by a Member State and to interact with the EUDIW using verifiable credentials. Commission Implementing Regulation (CIR) (EU) 2025/848 [i.2] further specifies the technical and procedural requirements for such interactions, including the use of wallet-relying party access certificates and, where applicable, registration certificates.

Wallet-relying party access certificates, issued by authorized certificate providers under Member State supervision, enable authentication of relying parties by the wallet, ensuring that only registered entities may interact with the EUDIW. Policy requirements for providers of wallet-relying party access certificates are outside of the scope of the present document. Where implemented, registration certificates provide structured, machine-readable information about the relying party's declared purposes, applicable entitlements, and authorized data requests. Requirements of registration certificates are specified in the present document. Together, these certificates support user transparency, attribute minimization, and secure data handling by allowing the EUDIW to evaluate whether requests are consistent with the relying party's authorized scope and role. The present document specifies the technical profiles, encoding rules, and policy requirements for the issuance and use of such certificates in compliance with the applicable regulatory framework.

Commission Implementing Regulation (EU) 2024/2979 [i.5] specifies requirements for an "embedded disclosure policy' which is a set of rules, embedded in an electronic attestation of attributes by its provider, that indicates the conditions that a wallet-relying party has to meet to access the electronic attestation of attributes. The attributes included in a wallet-relying party access certificate or wallet-relying registration certificate, including identity and roles, may be used as input to control disclosure of wallet held information to relying parties. Further requirements on embedded disclosure policies are outside of the scope of the present document.

1 Scope

The present document specifies requirements for the use of certificate-based attestations that support the identification and authorization of wallet-relying parties when interacting with the European Digital Identity Wallet (EUDIW), in accordance with eIDAS Regulation (EU) No 910/2014 [i.1], and Commission Implementing Regulation (EU) 2025/848 [i.2].

Specifically, the present document defines:

1) policy and profile requirements for **wallet-relying party registration certificates** used to convey the authorizations, 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 mapping of wallet-relying party information, such as entitlements, identifiers in both certificates;

3) recommendations for coordination between providers of WRPRC and WRPAC.

The specification builds upon existing ETSI standards including ETSI EN 319 411-1 [4], ETSI EN 319 412-1 [1], ETSI EN 319 412-2 [2], ETSI EN 319 412-3 [3], and complements the legal framework established under eIDAS for trust service provision, digital identity, and wallet interoperability.

The present document does not define requirements for the design, implementation, or internal operation of the European Digital Identity Wallet itself, in particular it is assumed that attributes in registration certificates are confirmed by the register.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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 are necessary for the application of the present document.

[1] ETSI EN 319 412-1: "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

[2] ETSI EN 319 412-2: "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".

[3] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".

[4] 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".

[5] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[6] IETF RFC 7519: "JSON Web Token (JWT)".

[7] IETF RFC 8392: "CBOR Web Token (CWT)".

[8] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions; Part 1: Country codes".

[9] IETF RFC 5646: "Tags for Identifying Languages".

[10] Recommendation ITU-T X.520: "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

[11] IETF RFC 5322: "Internet Message Format".

[12] IETF RFC 5341:"The Internet Assigned Number Authority (IANA) tel Uniform Resource Identifier (URI) Parameter Registry".

[13] IETF RFC 8820: "URI Design and Ownership".

[14] IETF RFC 8089: "The "file" URI Scheme".

[15] ISO 639:2023: "Code for individual languages and language groups".

[16] ISO 8601-1:2019: "Date and time — Representations for information interchange — Part 1: Basic rules".

[17] 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".

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

[19] IETF RFC 9052: "CBOR Object Signing and Encryption (COSE)", August 2022.

[20] IETF RFC 9360: "CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates", February 2023.

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.

NOTE: The eIDAS regulation as amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[i.2] Commission Implementing Regulation (EU) 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.3] Commission Implementing Regulation (EU) No 1352/2013 of 4 December 2013 establishing the forms provided for in Regulation (EU) No 608/2013 of the European Parliament and of the Council concerning customs enforcement of intellectual property rights.

[i.4] Commission Implementing Regulation (EU) 2022/1860 of 10 June 2022 laying down implementing technical standards for the application of Regulation (EU) No 648/2012 of the European Parliament and of the Council with regard to the standards, formats, frequency and methods and arrangements for reporting.

[i.5] 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.6] OpenID for Verifiable Presentations 1.0.

[i.7] Architecture and Reference Framework 2.4.0.

[i.8] EUDI Wallet TS02: "Specification of systems enabling the notification and subsequent publication of Provider information".

[i.9] EUDI Wallet TS05: " Specification of common formats and API for Relying Party Registration information".

[i.10] EUDI Wallet TS07: "Specification of Common Interface for Data Deletion Requests to Relying Parties".

[i.11] 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.12] ETSI TS 119 495: "Electronic Signatures and Trust Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking".

[i.13] ISO 17442-1:2020: "Financial services — Legal entity identifier (LEI) Part 1: Assignment".

[i.14] Commission Implementing Regulation (Eu) No 1352/2013 of 4 December 2013 establishing the forms provided for in Regulation (EU) No 608/2013 of the European Parliament and of the Council concerning customs enforcement of intellectual property rights.

[i.15] Commission Implementing Regulation (EU) 2020/2244 of 17 December 2020 laying down rules for the application of Directive (EU) 2017/1132 of the European Parliament and of the Council as regards technical specifications and procedures for the system of interconnection of registers and repealing Commission Implementing Regulation (EU) 2015/884.

[i.16] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax.

[i.17] Council Regulation (EU) No 389/2012 of 2 May 2012 on administrative cooperation in the field of excise duties and repealing Regulation (EC) No 2073/2004.

[i.18] Commission Implementing Regulation (EU) 2021/1042 of 18 June 2021 laying down rules for the application of Directive (EU) 2017/1132 of the European Parliament and of the Council as regards technical specifications and procedures for the system of interconnection of registers and repealing Commission Implementing Regulation (EU) 2020/2244.

[i.19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.20] ETSI TS 119 152-1: "Electronic Signatures and Trust Infrastructures (ESI); CB AdES (CBOR-AdES) digital signatures Part 1: Building blocks and CB-AdES baseline signatures".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in eIDAS Regulation [i.1], ETSI EN 319 411-1 [4], and the following apply:

European digital identity wallet: As defined in eIDAS Regulation [i.1].

national register of wallet-relying parties: national electronic register used by a Member State to make information on wallet-relying parties registered in that Member State

NOTE: As defined in CIR (EU) 2025/848 [i.2].

provider of wallet-relying party access certificates: natural or legal person mandated by a Member State to issue wallet-relying party access certificates to wallet-relying parties registered in that Member State

NOTE 1: As defined in CIR (EU) 2025/848 [i.2].

NOTE 2: In context of the present document, a provider of wallet-relying party access certificates is a trust service provider.

provider of wallet-relying party registration certificates: natural or legal person mandated by a Member State to issue wallet-relying party registration certificates to wallet-relying parties registered in that Member State

NOTE 1: As defined in CIR (EU) 2025/848 [i.2].

NOTE 2: In context of the present document, a provider of wallet-relying party registration certificates is a trust service provider.

registrar of wallet-relying parties: body responsible for establishing and maintaining the list of registered wallet-relying parties established in their territory and who has been designated by a Member State

NOTE: As defined in CIR (EU) 2025/848 [i.2].

wallet-relying party: relying party that intends to rely upon wallet units for the provision of public or private services by means of digital interaction

NOTE: As defined in CIR (EU) 2025/848 [i.2].

wallet-relying party access certificate: certificate for electronic seals or signatures authenticating and validating the wallet-relying party issued by a provider of wallet-relying party access certificates

NOTE: As defined in CIR (EU) 2025/848 [i.2].

wallet-relying party registration certificate: data object that describes the intended use of the relying party and indicates the attributes the relying party has registered to intend to request from users

NOTE 1: As defined in CIR (EU) 2025/848 [i.2].

NOTE 2: The registration certificate may serve multiple purposes. One is to indicate the intended use and requested attributes declared by the relying party. Another is to include additional entitlements or metadata relevant only for the wallet ecosystem and not used in access control decisions. The certificate can be seen as a structured export of registration data maintained by the registrar, tailored for a specific use case within the wallet framework.

WRP certificate: wallet-relying party access certificate or/and wallet-relying party registration certificate

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CIR Commission Implementing Regulation
CRL Certificate Revocation List
CWT CBOR Web Token

NOTE: As defined in IETF RFC 8392 [7].

DCQL Digital Credentials Query Language

NOTE: As defined in [i.6].

EAA Electronic Attestation of Attributes
EORI Economic Operators Registration and Identification number

NOTE: As defined in CIR (EU) No 1352/2013 [i.14].

EUDIW European Digital Identity Wallet
JWT JSON Web Token

NOTE: As defined in IETF RFC 7519 [6].

LEI Legal Entity Identifier

NOTE: As defined in CIR (EU) 2022/1860 [i.4].

OCSP Online Certificate Status Protocol
QTSP Qualified TSP
TSP Trust Service Provider
VAT Value-Added Tax registration number
WRP Wallet-Relying Party
WRPAC Wallet-Relying Party Access Certificate
WRPRC Wallet-Relying Party Registration Certificate

3.4 Notations

Each requirement is identified as follows:

<3 letters service component> - < the clause number> - <2 digit number - incremental>.

Where the service components are:

- OVR: General requirement (requirement applicable to more than 1 component)
- GEN: Certificate Generation Services
- REG: Registration Services
- REV: Revocation Services
- DIS: Dissemination Services

4 General concepts

4.1 Wallet-Relying Parties Certificates

The following types of certificates are defined in CIR (EU) 2025/848 [i.2]:

- Wallet-Relying Party Access Certificates (WRPACs):
  these certificates are issued by authorized certificate providers exclusively to WRPs registered in a national register, in compliance with Article 7 and Annex IV of CIR (EU) 2025/848 [i.2]. They are used for authenticating the WRP when interacting with the EUDIW and support electronic signature or electronic seal. WRPACs allow the EUDIW to verify the identity of the WRP, or an intermediary acting on behalf it, and ensure the authenticity and integrity of the request from the WRP, or intermediary, to the wallet.

NOTE 1: In line with Annex IV of CIR (EU) 2025/848 [i.2], access certificates include specific identification and contact information of the WRP and be subject to continuous monitoring, validation, and revocation procedures.

NOTE 2: Policy requirements for providers of WRPACs are defined in the ETSI TS 119 411-8 [17].

- Wallet-Relying Party Registration Certificates (WRPRCs):
  where implemented by a Member State under Article 8 of CIR (EU) 2025/848 [i.2], these certificates provide information from national register of wallet-relying parties including the intended use of the WRP and indication the attributes that the WRP intends to request from a wallet. They are designed to support transparency, attribute minimization, and user awareness. A WRPRC complies with syntactic and semantic harmonisation requirements defined in Annex V of CIR (EU) 2025/848 [i.2] and are based on published certificate policies and practice statements.

NOTE 3: Use of WRPRC together with WRPAC secures privacy and supports user awareness.

Additionally, the following supporting instruments may be used to supplement WRP identification and secure communication:

- Electronic Attestations of Attributes (EAAs):
  EAAs may be used to express additional attribute information about the WRP. Their use is aligned by national registration policies and attribute schemas but they do not replace mandatory access certificates where required by regulation.

NOTE 4: Future developments of wallet-related standards may lead to the WRPRC being issued in the form of an EAA.

All certificates described in the present document are issued by providers and issuers authorized under applicable Union and national law, and listed on national trusted lists in accordance with Article 22 of eIDAS [i.1].

NOTE 5: An issuer of electronic seal or electronic signature certificates is recognized as a Trust Service Provider.

4.2 Wallet-Relying party roles

The classification of WRPs into distinct roles is essential to ensure the secure and transparent functioning of the EUDIW. These roles support authorization to specific functions and may enable the EUDIW to inform users about the regulatory status and entitlements of WRPs during interactions.

Roles represent formal entitlements assigned to WRPs and serve as a basis for authorizing their access to personal data and attributes from the wallet. These entitlements are expressed in WRPRCs in accordance with Article 8 and Annex V of CIR (EU) 2025/848 [i.2], and are also registered in the national registers under Annex I, point 12 of CIR (EU) 2025/848 [i.2].

Each role is uniquely identified by a suitable identifier in form of an OID or URI. Identifiers for the roles defined in CIR (EU) 2025/848 [i.2], Annex I Nr. 12 are defined in Annex A. According to CIR (EU) 2025/848 [i.2], Annex I Nr. 13 the EU Member States may provide additional sub-entitlements for the case of a Non_Q_EAA by including information about provided attributes. The entitlements may be expressed as OIDs or structured URIs in certificate profiles and registration data formats.

The following entitlements are defined at European Union level and are used consistently in all registrars and WRPRCs:

- Service_Provider - General service provider
- QEAA_Provider - Qualified trust service provider issuing qualified electronic attestations of attributes
- Non_Q_EAA_Provider - Trust service provider issuing non-qualified electronic attestations of attributes
- PUB_EAA_Provider - Public sector body or its agent issuing electronic attestations of attributes from authentic sources
- PID_Provider - Provider of person identification data
- QCert_for_ESeal_Provider - QTSP issuing qualified certificates for electronic seals
- QCert_for_ESig_Provider - QTSP issuing qualified certificates for electronic signatures
- rQSealCDs_Provider - QTSP managing remote qualified electronic seal creation devices
- rQSigCDs_Provider - QTSP managing remote qualified electronic signature creation devices
- ESig_ESeal_Creation_Provider - Non-qualified provider for remote signature/seal creation

NOTE: Annex A provides OID numbers and URI for presented entitlements.

These entitlements can be used in interactions between EUDIW and relying party to control the information disclosed to the relying party, for example when the relying party is a TSP or other service provider to allow the disclosure of information as required for issuance of certificate, attestation or signing. The role may be used to control disclosure of information based on an embedded disclosure policy as specified in Article 10 of CIR (EU) 2024/2979 [i.5].

Additional value for attribute for sub-entitlements may be present in the WRPRC. Clause A.3 provides identifiers for sub-entitlements defined in ETSI TS 119 495 [i.12].

4.3 Wallet-Relying Party Access Certificates (WRPACs)

WRPACs are digital certificates used by registered WRP, or an intermediary acting on its behalf WRP, to authenticate themselves to the EUDIW. Their primary function is to ensure that any request for data or attributes sent to the EUDIW originates from a legitimate, authorized party listed in a national register of WRPs.

WRPACs are issued by entities designated as **providers of wallet-relying party access certificates** under the authorization of a Member State. These providers are trust service providers issuing electronic seal or electronic signature certificates that operate in accordance with applicable legal and technical frameworks.

The present document does not define the policy and security requirements resulting from paragraph 3 of Annex IV of CIR (EU) 2025/848 [i.2]; those requirements are specified in a ETSI TS 119 411-8 [17]. Clause 5.1 of the present document specifies mapping serving to both providers of WRPAC and WRPRC for coordination.

WRPACs are certificates associated with a private key under the control of the WRP, or an intermediary acting on its behalf WRP. A single WRP or intermediary may possess multiple WRPACs - especially when operating through several independent or distributed instances. In such cases, each WRPAC identifies the same WRP entity, but allows differentiation between specific instances to which it is assigned. The data necessary to distinguish among these instances, however, remains out of scope of the present standard.

4.4 Wallet-Relying Party Registration Certificates (WRPRCs)

WRPRCs are structured data objects that describe the intended use and attribute access scope of a WRP registered in a national register. They serve as a transparency mechanism, enabling wallet users to understand what information a WRP is allowed to request and under which legal or functional entitlement. These certificates support data minimization, informed user consent, and enforcement of attribute access policies within the EUDIW ecosystem.

In accordance with Article 8 of the CIR (EU) 2025/848 [i.2], Member States may mandate or allow the issuance of WRPRC by authorized providers of wallet-relying party registration certificates. These certificates are only issued to WRPs with a valid entry in a national register and reflect the relying party's declared use cases, entitlements, and data request policies. In cases where a WRPRC is not issued, the EUDIW retrieves the relevant information from the national register using the data structures specified in the present document.

NOTE 1: This dual approach ensures that EUDIW can consistently access the intended use and attribute access policies of a WRP, either from a WRPRC or directly from the national register. It preserves interoperability across different Member State implementations while maintaining transparency and user control.

NOTE 2: The present document does not specify API for EUDIW communication with national registers.

A WRPRC is formatted as signed JSON Web Tokens (JWT) [6] or CBOR Web Tokens (CWT) [7] and complies with the syntactic and semantic requirements specified in Annex V of CIR (EU) 2025/848 [i.2]. Both tokens have to be signed with an Advanced Electronic Signature (ADES) with the B-B profile.

WRPRCs are issued by providers of wallet-relying party registration certificates that are recognized as trust service providers.

While no separated policy specification currently governs the issuance of WRPRCs, the present document specifies in clause 6.3 the requirements applicable to issuers of such certificates. These include provisions related to syntactic and semantic compliance with Annex V of CIR (EU) 2025/848 [i.2], signing formats, certificate lifecycle management, and the alignment of issued content with national registration and authorization processes. Issuers comply with the relevant general requirements defined in ETSI EN 319 411-1 [4], including those related to identity verification, certificate management, and trust service provider obligations.

NOTE 3: To support recognition and transparency, providers of Wallet-Relying Party Registration Certificates (WRPRCs) may be presented on the EU Trusted List, either as qualified or non-qualified trust service providers, depending on the applicable national supervision and conformity assessment framework.

4.5 Registration and access certificate relation

WRPRC and WRPAC serve distinct but complementary purposes within the EUDIW ecosystem. While the WRPAC ensures WRP authentication, the WRPRC conveys the WRP's declared use cases and data access policies to both the EUDIW and the end user. Together, they form a dual-layer trust framework, where the WRPAC guarantees the WRP's identity and authentication, and the WRPRC ensures entitlements, transparency and data minimization.

WRPACs and WRPRCs are technically and logically linked through the identity of the WRP. The key data enabling this link is the WRP identifier, which serves as the primary element for associating both certificates. To ensure coherence and data consistency, good practice recommends that WRPRC issuance be based on the information already included in the previously issued WRPAC. This guarantees alignment in the identification of the WRP across both types of certificates.

The basis for data included in both certificates stems from the national register of WRPs, as specified in Annex B of the present document. In order to maintain data consistency between WRPAC and WRPRC, clause 5.1 provides a detailed mapping between the data fields defined in Annex B and the respective profiles used for WRPAC and WRPRC.

It should be noted that any instance-specific information included in WRPAC, such as indicators used to differentiate between instances of the same WRP, may not be registered in the national register of WRPs, but this does not affect the link between WRPAC and WRPRC. Only WRP identification data, as defined in Annex B, are used to establish and validate this relationship

WRP when acting through an intermediary, the intermediary presents its own WRPAC to authenticate the connection with the wallet. Additionally, WRP presents a WRPRC on behalf of the final relying party, indicating the identity, purpose, and authorized data access for the transaction. In accordance with point 14 of Annex I to CIR (EU) 2025/848 [i.2], the intermediary indication field are included in the WRPRC when a WRP acts through an intermediary. This means that a separate WRPRC is issued for each intermediary used, clearly identifying both the final WRP and the intermediary presenting the request to the wallet. This ensures traceability and policy enforcement throughout the data access chain.

4.6 Certificate issuance

4.6.1 General provisions

Each Member State establishes and maintains at least one **national register of wallet-relying parties**. This register contains information on entities established within the Member State that are authorized to interact with EUDIWs. To support transparency, accessibility, and interoperability, the register is available without prior authentication via both a human-readable website and a machine-readable API interface as stated in Annex II to CIR (EU) 2025/848 [i.2].

Each Member State designates at least one **registrar of wallet-relying parties** responsible for managing the **national register of wallet-relying parties**. The **registrar of wallet-relying parties** oversees the processing of registration applications, verification of the relying party's identity and legal status, and the maintenance and timely updating of registry records in accordance with applicable national and EU requirements.

Each Member State authorizes at least one **provider of Wallet-Relying Party Access Certificates** (Certificate Authority) to issue and manage WRPAC.

Member States may also authorize one or more **provider of Wallet-Relying Party Registration Certificates** to issue and manage WRPRC.

Figure 1 illustrates the organizational and technical components required at the Member State level to support the registration and certification of WRPs in accordance with the regulatory framework for the EUDIW.

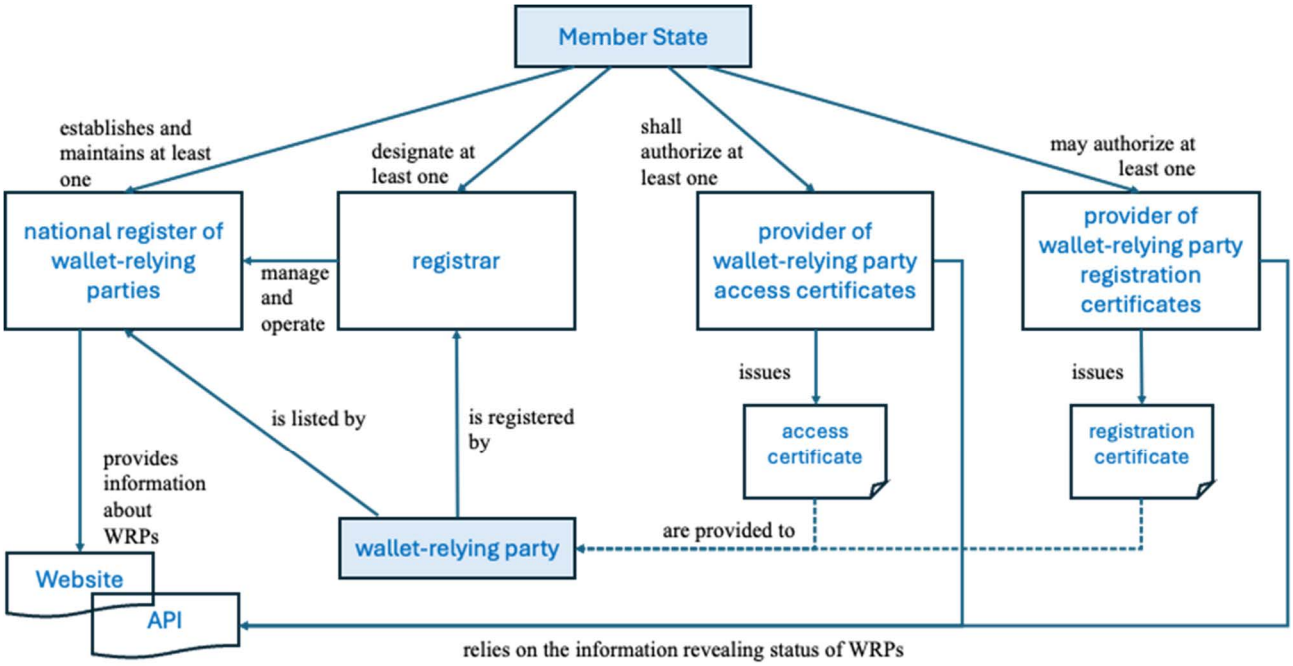

Figure 1: Institutional architecture for registration of wallet-relying parties

4.6.2 WRPAC and WRPRC policies

The following provisions apply to all entities authorized to provide WRP certificates.

The provider is authorized or designated by the Member State in which it operates to issue WRP certificates.

The designation complies with the applicable national policy as specified in Article 4(1) of CIR (EU) 2025/848 [i.2].

Policy requirements for providers of wallet-relying party access certificates are defined in ETSI TS 119 411-8 [17].

Policy requirements for providers of wallet-relying party registration certificates are defined in clause 6.

Providers of WRPRC conforming to the present document's normative requirements may use OIDs defined in the present document in its documentation and in the WRPRC it issues.

4.6.3 Identity proofing of WRPs

Before a WRP is registered in the national register of WRPs, the registrar carries out identity proofing in accordance with Article 6 of CIR (EU) 2025/848 [i.2]. This may be performed either directly by the registrar or by authorized entities acting on its behalf, and follows the requirements set out in ETSI TS 119 461 [i.11], which provides the normative foundation for identity proofing processes.

The registrar may delegate identity proofing tasks to authorized third parties in particular, to providers of WRP certificates - who may verify the identity of the WRP and its legal representatives. Such delegation complies with the applicable national registration policy, which specifies authorization procedures and requirements for identification and authentication in accordance with CIR (EU) 2025/848 [i.2], Article 4(3)(a).

The registrar may also authorize the provider of WRP certificates to collect registration forms and supporting documentation on its behalf. This delegation is explicitly defined and governed by the national registration policy.

According to ETSI TS 119 411-8 [17], the issuance of WRPAC requires that the identity of the WRP is verified and that the attributes included in the certificate map to verified identity attributes, as further specified in clause 5.1 of the present document.

Where the national registration policy requires WRP certificates to be issued solely on the basis of a direct request from the registrar, the provider of the certificate does not perform separate identity proofing and relies entirely on the identity proofing carried out by the registrar.

NOTE: Annex D provides use cases description where WRP certificate providers interact with registrar.

The national registration policy, in accordance with Article 4 of CIR (EU) 2025/848 [i.2] specifies all roles, responsibilities, and procedural requirements applicable to providers of WRP certificates in relation to identity proofing.

However, WRPRC is not linked to signing or sealing keys and therefore does not require full identity proofing for every issuance. Instead, the issuance of a WRPRC may reflect updates to the WRP registration data and does not necessarily trigger a new identity verification. It is assumed that identity proofing has already been performed during either the WRP registration or the issuance of the corresponding WRPAC.

To ensure privacy and data protection, WRPRCs are only issued to the party they pertain to, so that the use of the certificate remains under the control of the designated WRP.

For both WRPAC and WRPRC providers, the national register of WRPs - as specified in Annex B - serves as an authoritative source of identity attributes. The data it contains can be relied upon in identity verification procedures. Where a WRPAC or WRPRC provider performs the initial identity proofing, this may also serve as a trusted basis for the registration of the WRP in the national register, without requiring redundant identity verification steps.

5 Certificate profile requirements

5.1 WRP Identification attributes matching

5.1.1 WRP Identification attributes

GEN-5.1.1-01: The WRPRC certificate shall include identification attributes of WRP registered in the national WRP register matching WRPAC certificate.

GEN-5.1.1-02: Before issuing a WRPRC, the certificate provider shall verify that the identifier included in the WRPAC of the WRP matches an identifier included in the WRPRC, in order to ensure coherence and linkability between both certificates.

GEN-5.1.1-03: If other identification attributes (e.g. names, organizational units) differ between the WRPRC and the WRPAC, the linkage between the certificates shall rely solely on the matching identifier.

GEN-5.1.1-04: If the WRPRC includes multiple identifiers, at least one shall correspond to an identifier present in the WRPAC.

5.1.2 WRP Legal person identification attributes mapping

GEN-5.1.2-01: If the WRP certificate is issued to the legal person WRP the mapping in Table 1 applies.

Table 1: Mapping of legal person identification attributes

Attribute in register	Class as specified in Annex B	Attribute in WRPAC	Attribute in WRPRC
tradeName	B.2.1 WalletRelyingParty	`commonName` following ETSI EN 319 412-3 [3], clause 4.2.1	`name` as defined in clause 5.2
supportURI	B.2.1 WalletRelyingParty	Subject Alternative Name URI as specified in IETF RFC 5280 [5], clause 4.2.1.6 encoded as `uniformResourceIdentifier`	`support_uri` as defined in clause 5.2
legalName	B.2.3 LegalPerson	organizationName as defined in ETSI EN 319 412-3 [3], clause 4.2.1	`sub.legal_name` as defined in clause 5.2
establishedBylaw	B.2.3 LegalPerson	- not present	- not present
type	B.2.5 Class Identifier	`organizationIdentifier` as defined in clause 5.1.3 of the present document	`sub.id` as defined in clause 5.1.3 and in clause 5.2
identifier	B.2.5 Class Identifier		
postalAddress	B.2.2 LegalEntity	- not present	- not present
country	B.2.2 LegalEntity	`countryName` as defined in ETSI EN 319 412-3 [3], clause 4.2.1	`country` as defined in clause 5.2
email	B.2.2 LegalEntity	Subject Alternative Name email as specified in IETF RFC 5280 [5], clause 4.2.1.6 encoded as `rfc822Name`	- not present
phone	B.2.2 LegalEntity	Subject Alternative Name `otherName` as specified in IETF RFC 5280 [5], clause 4.2.1.6 encoded as telephoneNumber following X.520 [10], clause 6.7.1 `id-at-telephoneNumber`	- not present
infoURI	B.2.2 LegalEntity	- not present	`info_uri` as defined in clause 5.2
NOTE 1: `id-at-telephoneNumber` attribute is registered under OID: 2.5.4.20. NOTE 2: The table provides the mapping of WRPAC attributes as defined in ETSI TS 119 411-8 [17].			

GEN-5.1.2-02: If the tradeName attrribute is not present in the register, the `commonName` shall follow the requirements defined in ETSI EN 319 412-3 [3], LEG-4.2.1-8.

5.1.3 WRP Legal person semantic identifier mapping

GEN-5.1.3-01: The organizationIdentifier shall follow the semantics defined in ETSI EN 319 412-1 [1], clause 5.1.4.

GEN-5.1.3-02: The three initial characters as defined in ETSI EN 319 412-1 [1] LEG-5.1.4.03 shall follow the mapping in Table 2.

GEN-5.1.3-03: The identifier included in the `sub.identifier` attribute of WRPRC shall follow the semantics defined in GEN-5.1.3-01.

Table 2: Mapping of legal person semantic identifier

Type value defined in clause B.2.5 Class Identifier	Description	Semantic identifier initial characters as defined in ETSI EN 319 412-1 [1], clause 5.1.4
http://data.europa.eu/eudi/id/EORI-No	Economic Operator Registration and Identification Number (EORI-No) according to (EU) No 1352/2013 [i.14]	EOR (see note)
http://data.europa.eu/eudi/id/LEI	Legal Entity Identifier (LEI) according to (EU) No 2022/1860 [i.4] and ISO 17442-1 [i.13]	LEI
http://data.europa.eu/eudi/id/EUID	European Unique Identifier (EUID) according to (EU) 2020/2244 [i.15] and (EU) 2021/1042 [i.18]	NTR (as defined in ETSI EN 319 412-1 [1] LEG-5.1.4-07)
http://data.europa.eu/eudi/id/VATIN	Value Added Tax Identification Number (VATIN) according to the Council Directive 2006/112/EC [i.16]	VAT
http://data.europa.eu/eudi/id/TIN	Taxpayer Identification Number (TIN)	VAT
http://data.europa.eu/eudi/id/Excise	Excise Number according to Article 2 (12) of the Council Regulation (EC) No. 389/2012 [i.17]	EXC (see note)
NOTE: A future version of ETSI EN 319 412-1 [1] is planned which takes into account the EOR and EXC semantic identifiers.		

5.1.4 WRP Natural person identification attributes mapping

GEN-5.1.4-01: If the WRP certificate is issued to the natural person WRP the mapping in Table 3 applies.

Table 3: Mapping of natural person identification attributes

Attribute in register	Class as specified in Annex B	Attribute in WRPAC	Attribute in WRPRC
tradeName	B.2.1 WalletRelyingParty	commonName as defined in ETSI EN 319 412-2 [2], clause 4.2.4	name as defined in clause 5.2
supportURI	B.2.1 WalletRelyingParty	Subject Alternative Name URI as specified in IETF RFC 5280 [5], clause 4.2.1.6 encoded as uniformResourceIdentifier	support_uri as defined in clause 5.2
givenName	B.2.4 NaturalPerson	givenName as defined in ETSI EN 319 412-2 [2], clause 4.2.4	sub.given_name as defined in clause 5.2
familyName	B.2.4 NaturalPerson	surname as defined in ETSI EN 319 412-2 [2], clause 4.2.4	sub.family_name as defined in clause 5.2
dateOfBirth	B.2.4 NaturalPerson	- not present	- not present
placeOfBirth	B.2.4 NaturalPerson	- not present	- not present
type	B.2.5 Class Identifier	serialNumber	sub.id
identifier	B.2.5 Class Identifier	as defined in clause 5.1.5 of the present document	as defined in clause 5.1.5 and in clause 5.2
postalAddress	B.2.2 LegalEntity	- not present	- not present
country	B.2.2 LegalEntity	countryName as defined in ETSI EN 319 412-2 [2], clause 4.2.4	country as defined in clause 5.2
email	B.2.2 LegalEntity	Subject Alternative Name email as specified in IETF RFC 5280 [5], clause 4.2.1.6 encoded as `rfc822Name`	- not present
phone	B.2.2 LegalEntity	Subject Alternative Name otherName as specified in IETF RFC 5280 [5], clause 4.2.1.6 encoded as telephoneNumber following Rec. ITU-T X.520 [10], clause 6.7.1 id-at-telephoneNumber	- not present
infoURI	B.2.2 LegalEntity	- not present	info_uri

NOTE 1: The table provides the mapping of WRPAC attributes as defined in ETSI TS 119 411-8 [17].
NOTE 2: Attribute `tradeName` included in WRPAC and WRPRC is in format suitable for presentation to EUDIW user.
NOTE 3: `id-at-telephoneNumber` attribute is registered under OID: 2.5.4.20.

GEN-5.1.4-02: If the `tradeName` attrribute is not present in the register, the `commonName` shall follow the requirements defined in ETSI EN 319 412-2 [2] NAT-4.2.4-15.

5.1.5 WRP Natural person semantic identifier mapping

GEN-5.1.5-01: The `serialNumber` with shall follow the semantics defined in ETSI EN 319 412-1 [1], clause 5.1.3.

GEN-5.1.5-02: The three initial characters as defined in ETSI EN 319 412-1 [1], NAT-5.1.3-03 shall follow the mapping in Table 4.

GEN-5.1.5-03: The identifier included in the `sub.identifier` attribute of WRPRC shall follow the semantics defined in GEN-5.1.3-01.

Table 4: Mapping of natural person semantic identifier

Type value defined in clause B.2.5	Description	Semantic identifier initial characters as defined in ETSI EN 319 412-1 [1], clause 5.1.3
http://data.europa.eu/eudi/id/VATIN	Value Added Tax Identification Number (VATIN) according to the Council Directive 2006/112/EC [i.16]	TIN
http://data.europa.eu/eudi/id/TIN	Taxpayer Identification Number (TIN)	TIN

NOTE: For natural person identification national schemes may be used following ETSI EN 319 412-1 [1], NAT-5.1.3-03 point (7).

5.2 WRPRC profile requirements

5.2.1 Format

GEN-5.2.1-01: The WRPRC shall be formatted as signed JSON Web Token (JWT) [6] or CBOR Web Token (CWT) [7].

GEN-5.2.1-02: The WRPRC shall comply with the syntactic and semantic requirements specified in Annex V paragraph 3 of CIR (EU) 2025/848 [i.2].

GEN-5.2.1-03: The WRPRC shall be signed with the digital signature of provider of the wallet-relying party registration certificates.

NOTE: Electronic seal certificate or electronic signature certificate of the provider of the wallet-relying party registration certificates is published on the relevant trusted list.

GEN-5.2.1-04: The JWT shall be signed with a JSON Advanced Electronic Signature with the B-B profile as defined in ETSI TS 119 182-1 [18].

GEN-5.2.1-05: The CWT shall be signed with an Advanced Electronic Signature following structure as defined in IETF RFC 9052 [19] and IETF RFC 9360 [20].

NOTE: New standard ETSI TS 119 152-1 [i.20] will provide guidance for CBOR AdES signatures.

5.2.2 JWT Header Attributes

GEN-5.2.2-01: The JWT formatted header of the WRPRC shall include the fields defined in Table 5.

Table 5: Mapping of WRPRC header attributes

Attribute in register	Class defined in Annex B	Field in WRPRC	Sub field	Description
- (technical) -	-	typ	-	Specifies the type of the Web Token. The value is set to rc-wrp+jwt for JWT.
- (technical) -	-	alg	-	Indicates the algorithm used to sign the JWT as defined in clause 5.1.2 of ETSI TS 119 182-1 [18].
- (technical) -	-	x5c	-	Contains the whole certificate chain to verify the JWT or CWT as defined in clause 5.1.8 of ETSI TS 119 182-1 [18].
- (technical) -	-	b64	-	The header as defined in clause 5.1.2 of ETSI TS 119 182-1 [18] with value set "true" (the WRPRC is serialized in the compact form).
- (technical) -	-	cty	-	Content type as defined in clause 5.1.3 of ETSI TS 119 182-1 [18] list with the value "b64".
NOTE: Columns 1 and 2 are not referenced to the Annex B.				

5.2.3 CWT Header Attributes

GEN-5.2.3-01: The CWT formatted technical attributes of the WRPRC shall include the fields defined in Table 6.

Table 6: Mapping of WRPRC header attributes

Attribute in register	Class defined in Annex B	Field in WRPRC	Sub field	Description
- (technical) -	-	`typ`	-	Specifies the type of the Web Token. The value is set to rc-wrp+cwt for CWT.
- (technical) -	-	`alg`	-	Indicates the algorithm used to sign the CWT as specified in IETF RFC 9052 [19], clause 3.1.
- (technical) -	-	`x5chain`	-	Contains the whole certificate chain to verify the CWT as specified in IETF RFC 9360 [20], clause 2.
- (technical) -	-	`content type`	-	Content type as specified in IETF RFC 9052 [19], clause 3.1.
NOTE: New standard ETSI TS 119 152-1 [i.20] will provide guidance for CBOR AdES signatures.				

5.2.4 Payload Attributes

GEN-5.2.4-01: The payload of the WRPRC shall include all fields provided by registry specified in Table 7.

Table 7: Mapping of WRPRC payload attributes

Attribute in register	Class defined in Annex B	Field in WRPRC	Sub field	Description
tradeName	B.2.1 WalletRelyingParty	`name`	-	The subject of the WRPRC trade name.
legalName	B.2.2 LegalEntity	`sub`	`legal_name`	(Only for legal person).
givenName	B.2.4 NaturalPerson	`sub`	`given_name`	(Only for natural person).
familyName	B.2.4 NaturalPerson	`sub`	`family_name`	(Only for natural person).
identifier	B.2.2 LegalEntity	`sub`	`id`	-
country	B.2.2 LegalEntity	`country`	-	-
registryURI	B.2.1 WalletRelyingParty	`registry_uri`	-	URL pointing to the national registry API endpoint of the registered WRP.
srvDescription	B.2.1 WalletRelyingParty	`service`	-	Descriptions of the services provided by the WRP.
lang	B.2.6 MultiLangString	`service`	`lang`	Language identifier, referring the BCP47 language tag format defined in RFC 5646 [9].
content	B.2.6 MultiLangString	`service`	`value`	Service description in specified language.
entitlement	B.2.1 WalletRelyingParty	`entitlements`	-	A list of entitlements assigned to the WRP as specified in Annex A.
privacyPolicy	B.2.7 IntendedUse	`privacy_policy`	-	URL to the WRP's privacy policy explaining data processing and storage practices.
infoURI	B.2.2 LegalEntity	`info_uri`	-	URL general-purpose web address.
supervisoryAuthority	B.2.1 Class WalletRelyingParty	`dpa`	-	Data Protection Authority.

Attribute in register	Class defined in Annex B	Field in WRPRC	Sub field	Description
email	B.2.2 LegalEntity	`dpa`	`email`	The URL of web form provided by the Data Protection Authority supervising the Relying Party, which Users can use to report suspicious attribute presentation requests.
phone	B.2.2 LegalEntity	`dpa`	`phone`	An e-mail address of that DPA, on which the DPA is prepared to receive reports about suspicious attribute presentation requests from Users.
infoURI	B.2.2 LegalEntity	`dpa`	`uri`	A telephone number of that DPA, on which the DPA is prepared to receive reports about suspicious attribute presentation requests from Users.
- (technical) -	-	`policy_id`	-	List of policy identifiers as defined in clause 6.1.3.
- (technical) -	-	`certificate_policy`	-	URL to the certificate policy and certificate practice statement.
- (technical) -	-	`iat`	-	Unix timestamp indicating when the WRP was issued.
- (technical) -	-	`status`	-	A URI to a status list presenting information about validity of the WRPRC.
NOTE 1: Columns 1 and 2 provide mapping to the Annex B. NOTE 2: The sub field always identifies the relying party or the final relying party in case of intermediated transactions. It does not refer to the intermediary itself, even when the intermediary presents the WRPRC. This ensures that the subject consistently reflects the entity on whose behalf the data access is performed. NOTE 3: IETF RFC 5646 [9] provides coding for requirements of ISO 639 [15]. NOTE 4: WRPRCs are not issued for WRPs registered solely for the purpose of acting as an intermediary.				

GEN-5.2.4-02: The `sub.id` field specified in GEN-5.2.4-01 shall include the Identifier as specified in clause 5.1.2 for legal person or clause 5.1.4 for natural person; and match with the registered identifier of the WRP according to national registration policy.

GEN-5.2.4-03: The `entitlements` field specified in GEN-5.2.4-01 shall include at least one entitlement specified in clause A.2.

GEN-5.2.4-04: If the `entitlements` field specified in GEN-5.2.4-01 include at least one identifier specified in Annex A clause A.3, it shall also include an identifier specified in clause A.3.1.

GEN-5.2.4-05: If the WRPRC is issued to QEAA_Provider, Non_Q_EAA_Provider or PUB_EAA_Provider for the purpose of attestation provision as specified in clause 4.2 the payload of the WRPRC should include fields provided by the registry specified in Table 8.

Table 8: Mapping of attestation provider attributes

Attribute in register	Class defined in Annex B	Field in WRPRC	Sub field	Description
providesAttestations	B.2.1 WalletRelyingParty	`provided_attestations`	-	A set of credentials issued by the WRP with EAA entitlements.
format	B.2.9 Credential	`provided_attestations`	`format`	Format of the credential.
meta	B.2.9 Credential	`provided_attestations`	`meta`	Metadata to identify the credential type.
claim (present only if provided by the registry)	B.2.9 Credential	`provided_attestations`	`claim`	Objects that specifies attributes in the requested attestation.
NOTE 1: Columns 1 and 2 provide mapping to the Annex B. NOTE 2: Use of Credential sub-fields in the `provided_attestations` is used for both self-declared attestations and ones that are referenceable in an attestation catalogue. If once the attestation provider has their provided credential/s listed on the Catalogue of Attestations of the EU the `meta` subfield points to URL of the credential's machine-readable scheme in the catalogue.				

GEN-5.2.4-06: If the WRPRC is issued to the service provider as specified in clause 4.2 the payload of the WRPRC shall include all the fields provided by the registry specified in Table 9.

Table 9: Mapping of service provider attributes

Attribute	Class	Field	Sub field	Description
credential	B.2.7 Class IntendedUse	`credentials`	-	A set of credential queries, used to request credentials from the Wallet. The EUDIW will use this information to perform an over-asking validation.
format	B.2.9 Credential	`credentials`	`format`	Format of the attestation
meta	B.2.9 Credential	`credentials`	`meta`	Object defining additional properties.
claim	B.2.9 Credential	`credentials`	`claim`	Array of objects that specifies attributes in the requested attestation. If not available, all attributes are requested.
purpose	B.2.7 Class IntendedUse	`purpose`		A list describing the purpose of the WRPRC.
lang	B.2.6 MultiLangString	`purpose`	`lang`	Language identifier, referring the BCP 47 language tag format defined in IETF RFC 5646 [9].
content	B.2.6 MultiLangString	`purpose`	`value`	Purpose description provided in the language specified above.
intendedUseIdentifier (present only if provided by the registry)	B.2.7 Class IntendedUse	`intended_use_id`		Unique identifier of the intended use if provided by the registry.
NOTE 1: Columns 1 and 2 provide mapping to the Annex B. NOTE 2: IETF RFC 5646 [9] provides coding for requirements of ISO639 [15].				

GEN-5.2.4-07: The payload of the WRPRC may include fields specified in Table 10.

Table 10: Mapping of WRP optional attributes

Attribute	Class	Field	Sub field	Description
isPSB	B.2.1 WalletRelyingParty	public_body	-	Boolean indicating whether the WRP is a public sector body
- (technical) -	-	`exp`	-	Expiration time of the JWT/CWT as a Unix timestamp
supportURI	B.2.1 WalletRelyingParty	`support_uri`	-	URL or email address to use in data deletion or portability requests related to the WRP
usesIntermediary	B.2.1 WalletRelyingParty	`act`	-	Used when the WRP operates via an intermediary
usesIntermediary	B.2.1 WalletRelyingParty	`act`	`sub.id`	Identifier of the intermediary as specified by the intermediary WRPAC
usesIntermediary	B.2.1 WalletRelyingParty	`act`	`sub.name`	`commonName` of the intermediary as specified by the intermediary WRPAC
NOTE 1: Columns 1 and 2 provide mapping to the Annex B. NOTE 2: When the act field is present, the nested sub parameter identifies the intermediary acting on behalf of the relying party. This field is only used in cases involving intermediated interactions and is omitted when the relying party communicates directly with the wallet.				

GEN-5.2.4-08: The `exp` field in the WRPRC payload shall indicate a time not later than 12 months after the issuance time specified in the `iat` field specified in GEN-5.2.4-01.

GEN-5.2.4-09: If the WRPRC is issued to a WRP acting through intermediary, the WRPRC shall include the second field **sub** that matches the semantic identifier of the intermediary as specified in clause 5.1.

NOTE 1: This structure supports granular, auditable, and privacy-preserving handling of credentials and intended use, aligned with DCQL [i.6] standards and practical requirements for transparency and governance.

NOTE 2: See Annex C for a decoded example of the WRPRC.

6 Policy requirements for WRPRC

6.1 General provisions for certificate providers

6.1.1 General requirements

OVR-6.1.1-01: The general requirements specified in ETSI EN 319 411-1 [4], clause 5.1 shall apply.

6.1.2 Certification Practice Statement requirements

OVR-6.1.2-01: The general requirements specified in ETSI EN 319 411-1 [4], clause 5.2 shall apply.

OVR-6.1.2-02: If the provider of WRPRC is also issuing WRPAC, then the provider shall follow the requirements defined in ETSI TS 119 411-8 [17].

6.1.3 Certificate Policy name and identification

OVR-6.1.3-01: WRPRC shall include a certificate policy identifier which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application.

The policy identifier for the ETSI certificate policy described in the present document is:

```
-- WRPRC: certificate policy for wallet-relying party registration certificates
issued to EUDIW wallet-relying parties in accordance with the revised eIDAS Regulation;
wrprc OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) eudiwrpa(19475) policy-identifiers(3) wrprc (1)}
```

OVR-6.1.3-02: The policy shall be referenced in each WRPRC in a machine-processable and human-readable format.

6.1.4 Participants

OVR-6.1.4-01: The requirements identified in ETSI EN 319 411-1 [4], clause 5.4 shall apply.

OVR-6.1.4-02: The WRPRC provider shall include a clear description of the public key infrastructure hierarchy and certification paths from the end-entity wallet-relying party registration certificates up to the top of the hierarchy used for issuing them, while indicating the expected trust anchor(s) in such hierarchy and paths.

6.1.5 Certificate Usage

Wallet-relying party registration certificates issued under the policy identifier defined in clause 6.1.3 are aimed to support the provision of attributes of WRPs as defined in CIR (EU) 2025/848 [i.2].

6.2 Trust Service Providers practice

6.2.1 Publication and Repository Responsibilities

OVR-6.2.1-01: The requirements specified in ETSI EN 319 411-1 [4], clause 6.1 shall apply.

6.2.2 Identification and Authentication

6.2.2.1 Naming

REG-6.2.2.1-01: The requirements identified in clause 5 shall apply.

6.2.2.2 Initial identity validation

REG-6.2.2.2-01: The WRPRC provider shall verify that the WRP is listed in the national register of wallet-relying parties at the time of issuance.

REG-6.2.2.2-02: The WRPRC provider shall ensure that at the time of issuance the information requested to be included in the certificate matches the information available in the national register of wallet-relying parties.

REG-6.2.2.2-03: The WRPRC provider shall ensure that at the time of issuance WRP holds at least one WRPAC and the WRPAC certificate is valid.

REG-6.2.2.2-04: If the registrar of wallet-relying parties provides rules or policy for validation of these attributes, the WRPRC provider shall comply with the given rules.

NOTE: Providers of WRPRCs are dependent on what is provided by the WRP national register.

REG-6.2.2.2-05: If the request for certificate is provided directly by the wallet-relying registrar the WRPRC provider may rely on the identity proofing of wallet-relying party provided by the wallet-relying registrar.

REG-6.2.2.2-06: The WRPRC provider may provide identity proofing and identity proofs for the wallet-relying party registrar for the purpose of registration.

NOTE 1: WRPRC issuance may not require separate identity proofing of the WRP if its issuance follows entries in the WRP register.

NOTE 2: Requirements for identity proofing are defined in ETSI TS 119 461 [i.11].

NOTE 3: Annex D provides use case description where WRP certificate provider acts as proxy for registrar.

6.2.2.3 Identification and authentication for revocation requests

REV-6.2.2.3-01: The requirements identified in ETSI EN 319 411-1 [4], clause 6.2.4 shall apply.

In addition, the following shall apply:

REV-6.2.2.3-02: The provider of wallet-relying party access certificates shall update, if needed, the procedure for submission of WRPRC revocation requests by WRP registrar or data protection authorities in its certificate policy or practice statement.

REV-6.2.2.3-03: In addition, the provider of WRPRC shall update, if needed, a communication method, for notifications from the competent supervisory bodies about changes of relevant regulatory information of the WRP which can affect the validity of the WRPRC.

REV-6.2.2.3-04: The WRPRC provider issuing WRPRCs shall establish and apply secure procedures for the identification and authentication of entities requesting the revocation of a certificate.

REG-6.2.2.3-05: Revocation requests shall only be accepted from:

- the registrar of wallet-relying parties responsible for the relying party's registration;
- the relying party itself or its authorized representative, where permitted under national registration policy; and
- a competent authority designated by the Member State.

NOTE: National registration policy requirements are defined in Article 4 of CIR (EU) 2025/848 [i.2].

REG-6.2.2.3-06: The WRPRC provider shall authenticate the requester using means appropriate to the sensitivity of the certificate and the context of the request. This may include:

- verification against registration data from the national register;
- use of qualified electronic signatures or seals;
- pre-established secure communication channels; and
- additional validation steps defined in the WRPRC provider's certificate policy or in the national registration policy.

REG-6.2.2.3-07: The WRPRC provider shall record the identity of the revocation requester and maintain audit logs of the revocation transaction in accordance with its applicable retention and audit requirements.

REG-6.2.2.3-08: The WRPRC provider shall process validated revocation requests without undue delay and update the certificate status accordingly in the revocation repository.

6.2.3 Certificate Life-Cycle Operational Requirements

6.2.3.1 Certificate Application

REG-6.2.3.1-01: The requirements identified in ETSI EN 319 411-1 [4], clause 6.3.1 shall apply.

6.2.3.2 Certificate application processing

REG-6.2.3.2-01: The requirements identified in ETSI EN 319 411-1 [4], clause 6.3.2 shall apply.

6.2.3.3 Certificate issuance

GEN-6.2.3.3-01: The following requirements GEN-6.3.3-01, GEN-6.3.3-02, GEN-6.3.3-05 identified in ETSI EN 319 411-1 [4], clause 6.3.3 shall apply.

6.2.3.4 Certificate acceptance

OVR-6.2.3.4-01: The requirements identified in ETSI EN 319 411-1 [4], clause 6.3.4 shall apply.

6.2.3.5 Key Pair and Certificate Usage

No policy requirement.

NOTE : For WRPRC key pair is not generated.

6.2.3.6 Certificate Renewal

REG-6.2.3.6-01: Before WRPRC renewal the provider shall repeat the verification of the WRP attributes to be included in the WRP register.

6.2.3.7 Certificate Re-key

No policy requirement.

NOTE: For WRPRC key pair is not generated.

6.2.3.8 Certificate Modification

No policy requirement.

NOTE: Certificate modification refers to the issuance of a new certificate.

6.2.3.9 Certificate Revocation and Suspension

REV-6.2.3.9-01: The requirements specified in ETSI EN 319 411-1 [4], clause 6.3.9 shall apply.

In addition, the following shall apply:

REV-6.2.3.9-02: The provider of WRPRC shall implement measures and processes to continuously monitor any changes in the WRP national register in which WRP to whom they have issued WRPRCs are registered.

REV-6.2.3.9-03: The provider of WRPRC shall enable receiving information's from the registrar when the registration of WRP is suspended or cancelled.

REV-6.2.3.9-04: The provider of WRPRC shall revoke any WRPRC when the registration of the WRP is suspended or cancelled.

REV-6.2.3.9-05: The WRPRC provider shall provide to the WRP registrar an interface to request certificate revocation following the procedure defined in the certificate policy or national registration policy.

REV-6.2.3.9-06: The revocation procedure shall allow the WRP registrar to specify a reason, which can be descriptive rather than in a standard form, for the revocation.

NOTE: Where the WRP intends to revoke a certificate, the revocation request may be submitted to the registrar of wallet-relying parties. The registrar then forwards the validated request to the WRPRC provider in accordance with national policy. This ensures consistent oversight and traceability in the certificate lifecycle.

REV-6.2.3.9-07: The WRPRC provider shall revoke the WRPRC without undue delay when changes in the national register require it, in particular when:

- the content of the WRPRC is no longer accurate or consistent with the registered information; or
- the registration of the wallet-relying party is modified, suspended, or cancelled.

6.2.3.10 Certificate Status Services

CSS-6.2.3.10-01: The requirements specified in ETSI EN 319 411-1 [4], clause 6.3.10 shall apply.

NOTE : WRPRC providers do not provide OCSP service.

CSS-6.2.3.10-02: The WRPRC provider shall make the status list publicly available for validation.

CSS-6.2.3.10-03: The status list shall be accessible over a stable and high-availability endpoint to ensure continuity of WRPRC validation.

CSS-6.2.3.10-04: The WRPRC provider shall update the status list without undue delay upon a change in the status of a WRPRC.

CSS-6.2.3.10-05: If a compressed encoding is used for the status list payload, the issuer shall ensure that standard compression mechanisms are used to maximize compatibility with EUDIWs.

CSS-6.2.3.10-06: The WRPRC provider shall implement automated mechanisms to continuously monitor any changes in the national register of wallet-relying parties for those to whom WRPRCs have been issued.

6.2.3.11 End of Subscription

No policy requirement.

6.2.3.12 Key Escrow and Recovery

No policy requirement.

NOTE : For WRPRC key pair is not generated.

6.2.4 Facility, Management and Operational Controls

OVR-6.2.4-01: The requirements identified in ETSI EN 319 411-1 [4], clause 6.4 shall apply.

6.2.5 Technical Security Controls

OVR-6.2.5-01: The requirements identified in ETSI EN 319 411-1 [4], clause 6.5 shall apply.

6.2.6 Certificate, Status List Profiles

6.2.6.1 Certificate Profile

GEN-6.2.6.1-01: The WRPRC shall be issued according to the relevant certificate profile defined in clause 5.2.

GEN-6.2.6.1-02: The WRPRC shall include the policy identifier defined in clause 6.1.3.

GEN-6.2.6.1-03: The WRPRC shall include a unique identifier (id) for the WRPRC in a machine-readable format, suitable for use as a reference in a Status List.

GEN-6.2.6.1-04: The status field shall include:

- `idx`: A numeric string indicating the position in the bitstring; and
- `uri`: A URI identifying the full status list credential.

GEN-6.2.6.1-05: The value of `idx` shall be unique for each WRPRC issued by the same issuer and correspond to a valid index within the bitstring of the referenced status list credential.

GEN-6.2.6.1-06: The WRPRC provider shall ensure that the status list credential referenced in status is published in a verifiable format.

6.2.6.2 Status List Profile

REV-6.2.6.2-01: The WRPRC provider shall publish a status list structure that enables offline or near-real-time verification of the validity of issued WRPRC, including revocation and suspension status.

REV-6.2.6.2-02: The status list shall consist of a compact array of status bits, where each group of bits corresponds to the status of an individual WRPRC issued by the provider.

REV-6.2.6.2-03: The WRPRC shall ensure that each WRPRC includes a reference to:

- the status list's unique identifier (e.g. URI); and
- the position index assigned to that WRPRC within the status list.

REV-6.2.6.2-04: The status list shall support at least one of the following status semantics:

- valid: the WRPRC is currently trusted and has not been revoked;
- revoked: the WRPRC is no longer valid;
- suspended: the WRPRC is temporarily disabled.

REV-6.2.6.2-05: The status list shall be protected using a digital signature compliant with the JOSE, such as JWS, over the entire JSON structure or its cryptographic digest.

6.2.7 Compliance Audit and Other Assessment

NOTE: See ETSI EN 319 411-1 [4], clause 6.7.

6.2.8 Other Business and Legal Matters

OVR-6.2.8-01: The requirements identified in ETSI EN 319 411-1 [4], clause 6.8 shall apply.

6.2.9 Other Provisions

OVR-6.2.9-01: The requirements identified in ETSI EN 319 411-1 [4], clause 6.9 shall apply.

Annex A (normative): WRP identifiers

A.1 OID identifiers

The entitlement identifier for the WRPRC described in the present document is:

```
id-etsi-wrpa-entitlement OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) eudiwrpa(19475) entitlement(1)}
```

A.2 WRP entitlement identifiers

A.2.1 Service_Provider

Entitlement	Service_Provider
Description	General service provider
OID	id-etsi-wrpa-entitlement 1
URI	https://uri.etsi.org/19475/Entitlement/Service_Provider

A.2.2 QEAA_Provider

Entitlement	QEAA_Provider
Description	Qualified trust service provider issuing qualified electronic attestations of attributes
OID	id-etsi-wrpa-entitlement 2
URI	https://uri.etsi.org/19475/Entitlement/QEAA_Provider

A.2.3 Non_Q_EAA_Provider

Entitlement	Non_Q_EAA_Provider
Description	Trust service provider issuing non-qualified electronic attestations of attributes
OID	id-etsi-wrpa-entitlement 3
URI	https://uri.etsi.org/19475/Entitlement/Non_Q_EAA_Provider

A.2.4 PUB_EAA_Provider

Entitlement	PUB_EAA_Provider
Description	Public sector body or its agent issuing electronic attestations of attributes from authentic sources
OID	id-etsi-wrpa-entitlement 4
URI	https://uri.etsi.org/19475/Entitlement/PUB_EAA_Provider

A.2.5 PID_Provider

Entitlement	PID_Provider
Description	Provider of person identification data
OID	id-etsi-wrpa-entitlement 5
URI	https://uri.etsi.org/19475/Entitlement/PID_Provider

A.2.6 QCert_for_ESeal_Provider

Entitlement	QCert_for_ESeal_Provider
Description	QTSP issuing qualified certificates for electronic seals
OID	id-etsi-wrpa-entitlement 6
URI	https://uri.etsi.org/19475/Entitlement/QCert_for_ESeal_Provider

A.2.7 QCert_for_ESig_Provider

Entitlement	QCert_for_ESig_Provider
Description	QTSP issuing qualified certificates for electronic signatures
OID	id-etsi-wrpa-entitlement 7
URI	https://uri.etsi.org/19475/Entitlement/QCert_for_ESig_Provider

A.2.8 rQSealCDs_Provider

Entitlement	rQSealCDs_Provider
Description	QTSP managing remote qualified electronic seal creation devices
OID	id-etsi-wrpa-entitlement 8
URI	https://uri.etsi.org/19475/Entitlement/rQSealCDs_Provider

A.2.9 rQSigCDs_Provider

Entitlement	rQSigCDs_Provider
Description	QTSP managing remote qualified electronic signature creation devices
OID	id-etsi-wrpa-entitlement 9
URI	https://uri.etsi.org/19475/Entitlement/rQSigCDs_Provider

A.2.10 ESig_ESeal_Creation_Provider

Entitlement	ESig_ESeal_Creation_Provider
Description	Non-qualified provider for remote signature/seal creation
OID	id-etsi-wrpa-entitlement 10
URI	https://uri.etsi.org/19475/Entitlement/ESig_ESeal_Creation_Provider

A.3 Service provider sub-entitlements identifiers

A.3.1 Payment Service Provider Identifiers

Account Servicing Payment Service Provider	https://uri.etsi.org/19475/SubEntitlement/psp/psp-as
Payment Initiation Service Provider	https://uri.etsi.org/19475/SubEntitlement/psp/psp-pi
Account Information Service Provider	https://uri.etsi.org/19475/SubEntitlement/psp/psp-ai
Payment Service Provider issuing card-based payment instruments	https://uri.etsi.org/19475/SubEntitlement/psp/psp-ic
UnspecifiedPayment Service Provider	https://uri.etsi.org/19475/SubEntitlement/psp/unspecified
NOTE 1: Payment service providers roles and entitlements are as defined in ETSI TS 119 495 [i.12], clause 4.2. NOTE 2: Future editions of the present document may include other sub-entitlements defined at national or EU level.	

Annex B (normative): Wallet-Relying Party Attributes

B.1 Introduction

The present Annex defines a common data model for representing WRP attributes as part of the issuance and validation of WRPAC and WRPRC. The attribute classes and structures described herein are intended to support consistent interpretation of registration data by wallets and relying parties. While the data model reflects the current practices described in the EUDI Architecture Reference Framework (ARF) [i.7] and EU Technical Specifications TS2 [i.8] and TS5 [i.9].

The present annex purpose is to establish a clear and interoperable encoding format for certificate generation and processing.

The attributes defined in the present Annex are limited to those relevant for WRPs and are aligned with the requirements set out in Commission Implementing Regulation (EU) 2025/848 [i.2], Annex I. The specification does not impose any obligation on Member States to restructure their registers. The present Annex serves as a normative basis for encoding and interpreting registration certificate content in a harmonised and machine-readable way.

The data model makes use of standard data types such as String, Integer, Boolean, and structured classes (e.g. MultiLangString, Identifier, Credential). These are defined for clarity and are not intended to prescribe implementation details in national systems. The described format enables reliable interpretation of WRPRC payloads by digital wallets, including attribute filtering, language localization, and entitlement verification.

B.2 Wallet-Relying Party Attributes Classes

B.2.1 Class WalletRelyingParty

Attribute	Multiplicity	Type	Description	Link to CIR (EU) 2025/848 [i.2]
tradeName	[0..1]	string	The trade name (common name, service name) of the WRP	Annex I.2
supportURI	[1..*]	string	The support URI for the service provided by the WRP	Annex I.7(a)
serviceDescription	[1..*]	Array of MultiLangString objects	Array of arrays with localized descriptions of the services provided by the WRP	Annex I.8
intendedUse	[0..*]	IntendedUse	The intended use to request specific electronic attestations of attributes from a wallet.	Annex I.9 Annex I.10
isPSB	[1..1]	boolean	The WRP is a public sector body	Annex I.11
entitlement	[1..*]	string	Set of entitlements of the WRP as specified in Annex A	Annex I.12
providesAttestations	[0..*]	Credential	Set of sub-entitlements of the WRP, present only if any entitlement of the WRP is of type QEAA_Provider, Non_Q_EAA_Provider, PUB_EAA_Provider or PID_Provider	Annex I.13
supervisoryAuthority	[1..1]	LegalEntity	The competent data protection supervisory authority	Annex IV.3(g) Annex V.3(f)
registryURI	[1..1]	string	The URL for the national registry API of the registered WRP	Article 3(5)
usesIntermediary	[0..*]	WalletRelyingParty	Indicates whether the WRP depends on use of at least one intermediary	Annex I.14

NOTE: The supportURI provides the contact point where users or other parties can reach the WRP for support purposes, including at least one channel for submitting data deletion requests, as required by the TS7 [i.10] and CIR (EU) 2025/848 [i.2], Annex I point 7(a).

B.2.2 Class LegalEntity

Attribute	Multiplicity	Type	Description	Link to CIR (EU) 2025/848 [i.2]
legalPerson	[0..1]	LegalPerson	Specific attributes of a legal person Only one legalPerson or naturalPerson atrribute may be present.	Annex I.1
naturalPerson	[0..1]	NaturalPerson	Specific attributes of a natural person Only one legalPerson or naturalPerson atrribute may be present.	Annex I.1
identifier	[0..*]	Identifier	Identifiers of the legal entity, as stated in an official record.	Annex I.3
postalAddress	[1..1]	string	The postal address of the legal entity.	Annex I.4
country	[1..1]	string	Specifies the alpha-2 country code according to ISO 3166-1 [8] of the country in which the legal entity is established, or the string "EU" for providers operating on a European level.	Annex I.6
email	[0..*]	string	Specify one or more email addresses according to IETF RFC 5322 [11] of the legal entity.	Annex I.7(c)
phone	[0..*]	string	Specify one or more phone numbers of the legal entity starting with the '+' symbol as the international code prefix and the country code, followed by numbers only as specified in IETF RFC 5341 [12].	Annex I.7(b)
infoURI	[0..*]	string	Specify one or more Unique Resource Identifiers (URIs) according to IETF RFC 8820 [13] with webpages for information about the legal entity.	Annex I.5

NOTE: The infoURI provides a general-purpose web address where users and other parties can access public information about the WRP, such as its services, legal notices, terms of use, and privacy policies. It is intended for informational and transparency purposes and complements, but does not replace, the dedicated support contact points provided via supportURI.

B.2.3 Class LegalPerson

Attribute	Multiplicity	Type	Description	Link to CIR (EU) 2025/848 [i.2]
legalName	[1..*]	string	Legal name of the legal person, as specified in an official record.	Annex I.1
establishedBylaw	[0..*]	Law	Legal basis on which the legal person is established.	-

B.2.4 Class NaturalPerson

Attribute	Multiplicity	Type	Description	Link to CIR (EU) 2025/848 [i.2]
givenName	[1..1]	string	First name(s) of the natural person including middle name(s) where applicable, as specified in official records.	Annex I.1
familyName	[1..1]	string	Last name(s) or surnames of the natural person, as specified in official records.	Annex I.1
dateOfBirth	[0..1]	string	Data of birth of the natural person, as specified in official records.	Annex I.1
placeOfBirth	[0..1]	string	Place of birth of the natural person, as specified in official records.	Annex I.1

B.2.5 Class Identifier

Attribute	Multiplicity	Type	Description	Link to CIR (EU) 2025/848 [i.2]
type	[1..1]	string	Is the type of the identifier specified by a URI according to IETF RFC 8820 [13], whereas the following URIs are defined in the present document: • http://data.europa.eu/eudi/id/EORI-No - Economic Operator Registration and Identification Number (EORI-No) according to (EU) No 1352/2013 [i.14] • http://data.europa.eu/eudi/id/LEI - Legal Entity Identifier (LEI) according to (EU) No 2022/1860 [i.4] and ISO 17442-1 [i.13] • http://data.europa.eu/eudi/id/EUID - European Unique Identifier (EUID) according to (EU) 2020/2244 [i.15] and (EU) 2021/1042 [i.18] • http://data.europa.eu/eudi/id/VATIN - Value Added Tax Identification Number (VATIN) according to the Council Directive 2006/112/EC [i.16] • http://data.europa.eu/eudi/id/TIN - Taxpayer Identification Number (TIN) • http://data.europa.eu/eudi/id/Excise - Excise Number according to Article 2 (12) of the Council Regulation (EC) No. 389/2012 [i.17]	Annex I.3
identifier	[1..1]	string	The identifier, which identifies the LegalEntity.	Annex I.3

NOTE: Additional type identifiers may be defined at national or EU level.

B.2.6 Class MultiLangString

Attribute	Multiplicity	Type	Description	Link to CIR (EU) 2025/848 [i.2]
lang	[1..1]	string	Specifies the country code of the localized text. A two-letter Alpha-2 language code according to ISO 639 [15] (Set 1).	-
content	[1..1]	string	The localized text as a string.	-

NOTE: This class supports the representation of multilingual content and is used to structure the serviceDescription attribute as defined in clause B.2.1 or IntendedUse as defined in clause B.2.7.

B.2.7 Class IntendedUse

Attribute	Multiplicity	Type	Description	Link to CIR (EU) 2025/848 [i.2]
purpose	[1..*]	MultiLangString	One or more purposes of the intended data processing according to Article 5 1. (b) of Regulation (EU) 2016/679 [i.19].	Article 8.2(b)
privacyPolicy	[1..*]	Policy	Specifies the privacy policy of the intended use.	Article 8.2(g)
createdAt	[1..1]	string	Validity start date for the intended use in ISO 8601-1 [16] YYYY-MM-DD format.	-
revokedAt	[0..1]	string	End date for the validity of the intended use in ISO 8601-1 [16] YYYY-MM-DD format.	-
credential	[1..*]	Credential	Set of potentially requestable attestations which may be requested by the WRP within the scope of the present intended use of data.	Annex I.9
intendedUseIdentifier	[1..1]	string	Registrar-provided unique identifier of the registered intended use.	-

NOTE: The intendedUseIdentifier is optional and reserved for future implementations.

B.2.8 Class Policy

Attribute	Multiplicity	Type	Description	Link to CIR (EU) 2025/848 [i.2]
type	[1..1]	string	The type of the policy in form of a URI according to IETF RFC 8820 [13], whereas the following URIs are defined in the present document: http://data.europa.eu/eudi/policy/privacy-policy - is a Privacy Policy.	Article 8.2(g)
policyURI	[1..1]	string	The policy URI in form of a URL according to IETF RFC 8089 [14] where the policy is published.	Article 8.2(g)

NOTE: In Context of WRP attributes only Privacy policy is present.

B.2.9 Class Credential

Attribute	Multiplicity	Type	Description	Link to CIR (EU) 2025/848 [i.2]
format	[1..1]	string	Format of the attestation.	Annex I.9 Annex I.13
meta	[1..1]	string	Object defining additional properties.	Annex I.9 Annex I.13
claim	[0..*]	Claim	Array of objects that specifies attributes in the requested attestation. If not available, all attributes are requested.	Annex I.9 Annex I.13

NOTE: For guidance see OpenID4VP [i.6].

B.2.10 Class Claim

Attribute	Multiplicity	Type	Description	Link to CIR (EU) 2025/848 [i.2]
path	[1..1]	string	A path pointer that specifies the path to a claim within the Credential.	-
values	[0..1]	string	Array of strings, integers or boolean values that specifies the expected values of the claim.	-

NOTE: For guidance see OpenID4VP [i.6].

B.2.11 Class Law

Attribute	Multiplicity	Type	Description	Link to CIR (EU) 2025/848 [i.2]
lang	[1..1]	string	Two-letter Alpha-2 language code according to ISO 639 [15] (Set 1).	-
legalBasis	[1..1]	string	Legal basis according to which a LegalPerson is established as such or the access to a specific Claim is required or recommended.	-

NOTE: Only used in context of LegalPerson.

Annex C (informative): Registration Certificate example

Following code presents an example of the Registration Certificate:

```
{
  "typ": "rc-wrp+jwt",
  "alg": "ES256",
  "b64": "true",
  "cty": ["b64"],
  "x5c": [],}
.
{
  "name": "Example GmbH",
  "purpose": [
    {
      "lang": "en-US",
      "value": "Required for checking the minimum age"
    },
    {
      "lang": "de-DE",
      "value": "Benötigt für die Überprüfung des Mindestalters"
    }
  ],
  "info_uri": "https://example.com",
  "country": "DE",
  "sub": {
    "leagal_name": ""Example GmbH,
    "id": "LEIXG-529900T8BM49AURSDO55"
  },
  "privacy_policy": "https://example-company.com/en/privacy-policy",
  "policy_id": [
      "0.4.0.19475.3.1"
   ],
  "certificate_policy": "https://registrat.example.com/certificate-policy",
  "iat": 1683000000,
  "credentials": [
    {
      "format": "dc+sd-jwt",
      "meta": {
        "vct_values": [
          "https://credentials.example.com/identity_credential"
        ]
      },
      "claims": [
        { "path": ["given_name"] },
        { "path": ["family_name"] },
        { "path": ["address", "street_address"] }
      ]
    },
    {
      "format": "dc+sd-jwt",
      "meta": {
        "vct_values": [
          "https://othercredentials.example/mdl""
        ]
      },
      "claims": [
        { "path": ["given_name"] },
        { "path": ["family_name"] },
        { "path": ["address", "street_address"] }
      ]
    }
  ],
  "entitlements": [
    "https://uri.etsi.org/19475/Entitlement/Non_Q_EAA_Provider"
  ],
  "provided_attestations": [
    {
      "format": "dc+sd-jwt",
      "meta": {
        "vct_values": [
          """
        ]
      }
```

```
    }
  ],
  "public_body": false,
  "service": [[
    {
      "lang": "en-US",
      "value": "Bundesagentur für Sprunginnovationen"
    },
    {
      "lang": "de-DE",
      "value": "Federal Agency for Breakthrough Innovations"
    }
  ]],
  "status": {
    "status_list": {
      "idx": 0,
      "uri": "https://example.com/statuslists/1"
    }
  },
  "act": {
    "sub": "DE:EX-987654381"
  }
}
```

Annex D (informative): WRP registration use cases

D.1 Use case 1: Integrated model

In this model, the registrar and certificate provider are the same entity. The registration and issuance processes are tightly coupled and managed under a single authority. This ensures streamlined control, traceability, and alignment between registration records and issued certificates. It may simplify governance and reduce latency but requires the registrar to maintain full certificate lifecycle capabilities.

D.2 Use case 2: Registrar-initiated issuance

In this model, the registrar completes the registration and then initiates the certificate issuance by instructing a designated certificate provider. The WRP does not need to interact directly with the provider. This model ensures strong linkage between registration and WRP certificate issuance, with the registrar controlling when and how certificates are generated. It is suitable when Member States centralize the registration workflow while outsourcing issuance.

NOTE 1: WRPAC and WRPRC may be separate entities.

NOTE 2: Model allows the authorization of one or more WRPAC and/or WRPRC providers.

D.3 Use case 3: RP-initiated issuance post-registration

In this model, the registrar performs the registration, and later the relying party contacts a certificate provider to request issuance. The provider is responsible for verifying that the relying party is listed in the national register and that the data matches. This model enables decentralised certificate management and can accommodate market-based competition among WRPAC and WRPRC providers, while still relying on authoritative registration data.

D.4 Use case 4: Provider-assisted registration

In this model, the WRPAC or WRPRC provider acts as a proxy to the registrar, handling both the submission of registration data and the issuance of the certificate once the registration is confirmed. This enables one-stop-shop onboarding for relying parties and reduces complexity on the registrar's side. It is particularly useful when service providers assist relying parties in navigating national registration procedures.

NOTE 1: WRPAC and WRPRC may be separate entities.

NOTE 2: Model allows the authorization of one or more WRPAC and/or WRPRC providers.

Annex E (informative): Regulatory requirements for WRP certificate providers

E.1 Wallet-Relying Party Access Certificates (WRPAC)

In accordance with Article 7 and Annex IV of the CIR (EU) 2025/848 [i.2], WRPACs are issued exclusively to entities whose registration as WRP has been validated and is active.

Each WRPAC is associated with a unique cryptographic key pair, where the private key is securely managed and controlled by the WRP, and used to generate electronic signatures or electronic seals of the request sent to EUDIW.

WRPAC include the following WRP attributes as specified in Annex I of the CIR (EU) 2025/848 [i.2], Annex I:

1) The name of the wallet-relying party, as stated in an official record together with identification data of that official record (CIR Annex I point 1).

2) A user-friendly name of the wallet-relying party (CIR Annex I point 2).

3) One or more identifiers of the wallet-relying party (such as EORI, LEI, or VAT numbers) (CIR Annex I point 3).

4) Uniform Resource Locator (URL) belonging to the wallet-relying party (CIR Annex I point 5).

5) Indicator of the Member State where the wallet-relying party is established (CIR Annex I point 6).

6) Contact information of the wallet-relying party (CIR Annex I point 7).

7) Machine processable reference to the applicable certificate policy (CIR Annex IV point 3(k)).

E.2 Wallet-Relying Party Registration Certificates (WRPRC)

In accordance with Article 8 of the CIR (EU) 2025/848 [i.2], Member States may mandate or allow the issuance of WRPRC by authorized providers of wallet-relying party registration certificates. These certificates are only issued to WRPs with a valid entry in a national register and reflect the relying party's declared use cases, entitlements, and data request policies.

WRPRC include the following WRP attributes as specified in Annex I of the CIR (EU) 2025/848 [i.2] Annex I:

1) The name of the wallet-relying party, as stated in an official record together with identification data of that official record (CIR Annex I point 1).

2) A user-friendly name of the wallet-relying party (CIR Annex I point 2).

3) One or more identifiers of the wallet-relying party (such as EORI, LEI, or VAT numbers) (CIR Annex I point 3).

4) Uniform Resource Locator (URL) belonging to the wallet-relying party (CIR Annex I point 5).

5) Indicator of the Member State where the wallet-relying party is established (CIR Annex I point 6).

6) Additional attributes specifying entitlements and intended use (CIR Annex I points 8-15):

   - The list of data or attributes the relying party declared to request for each intended use.
   - A user-friendly description and technical name for each intended use.
   - An indication of whether the relying party is a public sector body.
   - One or more formal entitlements (roles), (CIR Annex I point 12).

- A URL to the privacy policy explaining the processing of EUDIW data.
- A general access policy used by the EUDIW to detect and signal out-of-scope data requests.
- A machine-readable reference to the applicable certificate policy and practice statement (CIR Annex V).

NOTE 1: URL in point 4 may be optional for WRPRC but is required for WRPAC.

WRPRC is formatted as signed JSON Web Tokens (JWT) [6] or CBOR Web Tokens (CWT) [7] and comply with the syntactic and semantic requirements specified in Annex V of CIR (EU) 2025/848 [i.2]. Both tokens have to be signed with an Advanced Electronic Signature (ADES) with the B-B profile.

WRPRCs are issued by providers of wallet-relying party registration certificates that may be recognized as trust service providers.

While no separated policy specification currently governs the issuance of WRPRCs, the present document specifies in clause 6.3 the requirements applicable to issuers of such certificates. These include provisions related to syntactic and semantic compliance with Annex V of CIR (EU) 2025/848 [i.2], signing formats, certificate lifecycle management, and the alignment of issued content with national registration and authorization processes. Issuers also comply with the relevant general requirements defined in ETSI EN 319 411-1 [4], including those related to identity verification, certificate management, and trust service provider obligations.

NOTE 2: To support recognition and transparency, providers of Wallet-Relying Party Registration Certificates (WRPRCs) may be presented on the EU Trusted List, either as qualified or non-qualified trust service providers, depending on the applicable national supervision and conformity assessment framework.

E.3 Registration and access certificate relation

WRPRC and WRPAC serve distinct but complementary purposes within the EUDIW ecosystem. While the WRPAC ensures WRP authentication, the WRPRC conveys the WRP's declared use cases and data access policies to both the EUDIW and the end user. Together, they form a dual-layer trust framework, where the WRPAC guarantees the WRP's identity and authentication, and the WRPRC ensures entitlements, transparency and data minimization.

Table E.1 outlines the key differences and relationships between these two types of certificates, CIR (EU) 2025/848 [i.2].

Table E.1: WRPAC and WRPRC comparison

Aspect	WRPAC	WRPRC
Purpose	Authenticates WRP in interactions with the wallet	Provides intended use and attributes requested by the WRP or information about service provided to the wallet
Regulation Basis	Article 7, Annex IV	Article 8, Annex V
Issued To	Registered WRP	Registered WRP
Includes Entitlements	No	Yes
Includes Intended Use	No	Yes
Used For	WRP authentication	Transparency and user awareness
Contains Contact Info	Yes (Annex I, 1-3, 5-7)	Yes (Annex I, 1-3, 5-7)
Cryptographic Binding	X.509 certificate with private key	No, claim bound to the Access Certificate by identifier

Table E.2 lists the attributes identifying a WRP, as defined in Annex I of CIR (EU) 2025/848 [i.2] present in both WRPAC and WRPRC.

NOTE: While the CIR (EU) 2025/848 [i.2] applies, each certificate conveys distinct information. A WRPRC is always presented together with a WRPAC. To avoid duplication, information included in the WRPAC it is not recommended be repeated in the WRPRC. This separation facilitates attribute discovery by the EUDI Wallet, as each attribute can be clearly located in one certificate or the other.

Table E.2: WRP identification attributes

WRP attribute	WRP Information element (Annex I)	Included in WRPAC (Annex IV)	Included in WRPRC (Annex V)	Notes
Subject	CIR (EU) 2025/848 [i.2], Annex I point 1 Name & ID data from official record	Mandatory where applicable	Mandatory where applicable	-
Friendly name	CIR (EU) 2025/848 [i.2], Annex I point 2 User-friendly name	Optional Mandatory if subject is not applicable	Optional Mandatory if subject is not applicable	-
Identifier(s)	CIR (EU) 2025/848 [i.2], Annex I point 3 Identifiers (EORI, VAT, etc.)	Mandatory at least one	Mandatory at least one	CIR (EU) 2025/848 [i.2] states possibility use of many identifiers, for interoperability reasons at least one of identifiers is the same in both certificates
URL	CIR (EU) 2025/848 [i.2], Annex I point 5 WRP Uniform Resource Locator URL	Mandatory	Optional	-
Country code	CIR (EU) 2025/848 [i.2], Annex I point 6 Country code for certain identifiers	Mandatory	Mandatory	-
Intermediary	CIR (EU) 2025/848 [i.2], Annex I point 15 Association to the intermediary that the WRP is relying upon	No	Optional	It includes identifier of the intermediary present in its WRPAC

When a WRP acts through an intermediary, the intermediary presents its own WRPAC to authenticate the connection with the EUDIW. In parallel, the WRP provide a WRPRC that identifies the final relying party, states the intended purpose, and defines the authorized data access for the transaction. In accordance with point 14 of Annex I to CIR (EU) 2025/848 [i.2], the WRPRC also indicates the intermediary involved. A separate WRPRC is therefore required for each intermediary, explicitly binding the intermediary and the final WRP. This arrangement provides the EUDIW with transparent information about the actual relying party behind the request and ensures traceability, accountability, and enforcement of attribute access policies across the data access chain.

If no WRPRC is available, the EUDIW retrieves the relevant registration data directly from the national register, using the data structures defined in the present document. In such cases, the register acts as the authoritative source of the relying party's identity, purpose, and entitlements, ensuring that the wallet can still enforce attribute access policies and provide informed user consent even without a WRPRC.

Annex F (informative): Change history

Date	Version	Information about changes
September 2025	V1.1.1	First publication

History

Version	Date	Status
V1.1.1	October 2025	Publication