



Brussels, **XXX**
[...](2026) **XXX** draft

ANNEXES 1 to 5

ANNEXES
to the
COMMISSION IMPLEMENTING REGULATION
amending Implementing Regulation (EU) 2025/848 as regards applicable standards and
specifications

ANNEX I

In Annex I, the following point 16 is added:

‘16. Where applicable, an association to the wallet-relying party that is relying upon the intermediary to whom the wallet-relying party access certificate has been issued and that is acting on behalf of the relying party who intends to rely upon the wallet.’.

ANNEX II

'ANNEX II

1. REQUIREMENTS FOR ELECTRONIC SIGNATURES OR SEALS APPLIED TO THE INFORMATION MADE AVAILABLE ON REGISTERED WALLET-RELYING PARTIES

- JavaScript Object Notation ('JSON');
- IETF 7515 for JSON Web Signatures.

2. REQUIREMENTS ON THE SINGLE COMMON API

(1) The single common API shall:

- (a) be a REST API, supporting JSON as a format and signed in accordance with the relevant requirements specified in Section 1 to this Annex;
- (b) enable any requestor, without prior authentication, to search and request information about registered wallet-relying parties;
- (c) enable the searches and requests referred to in point (b) to provide the requestor with complete lists from the register, allowing for partial matches based on the parameters defined in Annex VI;
- (d) ensure that replies to requests referred to in point (b) that match at least one wallet-relying party include one or more statements on information about registered wallet-relying parties and information according to Annex VI, current and historic wallet-relying party access certificates and wallet-relying party registration certificates;
- (e) be published as an OpenAPI version 3, together with the appropriate documentation and technical specifications ensuring interoperability across the Union;
- (f) provide security functions, including security by default and by design, to ensure the availability and integrity of the API and the availability of information through it.

- (2) The statements referred to in paragraph 1, point (d) and in paragraph 4 to this section 2 shall be provided in the form of electronically signed or sealed JSON files and comply with the format and structure for electronic signatures or seals set out in Section 1.
- (3) The read and write methods supported by the open API endpoint of a national register shall comply with the specifications set out in Annex VI, in paragraphs 1 to 10.
- (4) The statements on information provided by the open API of a national register shall comply with the specific data schema set out in Annex VI, tables 1 to 11.'.

ANNEX III

Annex IV is amended as follows:

- (1) point (3), first paragraph is amended as follows:
- (2) The text “shall, as applicable, comply with at least the normalised certificate policy (‘NCP’) requirements as specified in standard ETSI EN 319 411-1 version 1.4.1 (2023-10)” is replaced by the text “shall comply with standard ETSI TS 119 411-8 V1.1.1 (2025-10)”.
- (3) point 3(k) is amended as follows:
 - (a) the third indent is replaced by the following:

‘- the information referred to in Annex I, points 1, 2, 3, 5, 6, 7, (a), (b) and (c) and 16;’;
 - (b) the following fourth indent is added:

‘- a reference to the national register in which the relying party is registered.’.

ANNEX IV

In Annex V, the following point 7 is added:

‘7. The wallet-relying party registration certificate profile, certificate policy and certificate practice statement that apply to the provisioning of wallet-relying party registration certificates shall comply with the requirements laid down in ETSI TS 119 475 V1.1.1. (2025-10) Electronic Signatures and Trust Infrastructures (ESI); Relying party attributes supporting EUDI Wallet user's authorisation decisions.’.

ANNEX V

‘ANNEX VI

Technical specifications for the common API

1. The read methods of the common API for national registers of wallet-relying parties shall be open for public access.
2. The common API shall provide one of the following parameters for searching and querying complete data sets of registered wallet-relying parties matching with provided query parameters:
 - (a) official or business registration number, returning the complete data set of each of the registered wallet-relying parties matching the value provided for this parameter; of the list of matching wallet-relying parties; of the list of matching wallet-relying parties;
 - (b) official company name or trade name, returning the complete data set of each of the registered wallet-relying parties matching the value provided for this parameter;
 - (c) URL of the wallet-relying party's privacy policy, returning the complete data set of each of the registered wallet-relying parties matching the value provided for this parameter;
 - (d) type of entitlement, returning the complete data set of each of the registered wallet-relying parties matching the value provided for this parameter;
 - (e) type of attestations provided, returning the complete data set of each of the registered wallet-relying parties matching the value provided for this parameter;
 - (f) type of attestation requested, returning the complete data set of each of the registered wallet-relying parties matching the value provided for this parameter within their registered intended use;
 - (g) Registrar-provided unique identifier of registered intended use, returning the complete data set of the registered wallet-relying party matching the value provided for this parameter in their WalletRelyingParty.IntendedUse.intendedUseIdentifier information;
 - (h) reliance upon an intermediary, returning the complete data set of each of the registered wallet-relying parties that have the attribute WalletRelyingParty.usesIntermediary present;
 - (i) official company name or trade name of an intermediary, returning the complete data set of each of the registered wallet-relying parties that have the value provided for that parameter in their WalletRelyingParty.usesIntermediary information.
3. Where query results match at least one wallet-relying party, the response shall provide:
 - (a) a set of information registered to the corresponding wallet-relying party consisting of the full contents of WalletRelyingParty class for given instance without the WalletRelyingParty.physicalAddress attribute;
 - (b) Where relevant, the complete wallet-relying party access certificate histories consisting of the certificate transparency log information in accordance with

RFC 9162, made available by the relevant providers of wallet-relying party access certificates, if the registrar of wallet-relying parties is not acting as the relevant provider of wallet-relying party access certificates.

4. The public access endpoint shall provide a GET /wrp endpoint for making parameterised queries.
 - (a) The supported query parameters shall be at least the following:
 - each filterable field (identifier, legalname, tradename, policy, entitlement, providesattestation, usesintermediary, isintermediary, intendedUseIdentifier, intendedUseClaimPath, intendedUseCredentialMeta, intendedUseCredentialFormat) is defined as a query parameter;
 - in: query: Specifies that the parameter is a query parameter;
 - name: The name of the query parameter;
 - schema: Defines the data type of the query parameter (mostly string, with boolean for isintermediary);
 - description: Provides a brief explanation of what the query parameter filters by.
 - (b) Where no query parameters are included, the method shall return the full list of registered wallet-relying parties in the Registry;
 - (c) The endpoint shall also support cursor-based pagination, and methods to query the Registry based on Intended Use components - the four intendedUse filters;
 - (d) The endpoint shall support the combination of multiple filters in one query.
5. A successful GET (response code 200) shall be JWS-signed response body for a successful GET (200) shall be an array of matching WalletRelyingParty objects.

The public access API endpoint shall also support a /wrp/check-intended-use (GET): A dedicated check endpoint for querying 'Intended use' including the four mandatory and one optional parameter shall be supported. This endpoint shall provide a JWS-signed boolean TRUE or FALSE response, determined by the queried parameter in the Registrar's Intended use information for the specific Wallet-Relying Party.
6. Registrars shall take into consideration the vulnerabilities that an open, comprehensive query interface enables for both malicious or non-malicious users of the interface.
7. The write methods for each national register of wallet-relying parties shall only be accessible for API clients that the Member State has authorised.
8. The applicable authorisation mechanism shall be documented by the Member State, with the addition of a securitySchemes section in components and of a security section at the root level or at the path/operation level in the individual instance in accordance with the OpenAPI specification v3.2.0 (19 September 2025).
9. The common Registry API write methods are defined below:
 - (a) The API path shall be path: /wrp;
 - (b) The following methods shall be supported:

- POST is for creating a new WalletRelyingParty. The method shall support a request body with the WalletRelyingParty schema compliant with the data schema specified in table 1 of the present Annex, and shall return a ‘201’ on success;
 - PUT is for updating an existing WalletRelyingParty. The method shall support a request body with the WalletRelyingParty schema compliant with the data schema specified in table 1 of the present Annex, and shall return 200 on success or 404 if not found;
 - DELETE is for the deletion of an existing WalletRelyingParty. The method shall support a request body with the WalletRelyingParty identifier compliant with the data schema specified in table 1 of the present Annex, and shall return a 204 on success.
10. The data format for the information available through the open API provided by the national wallet-relying party register shall comply with the data schemas described in Tables 1 through 11, where:
- 10.1 In Table 1, the attribute “isPSB” shall be provided and be set to false where the registered entity is not a public sector body;
 - 10.2 In Table 1, the attribute “providesAttestations” shall be present if any entitlement of the wallet-relying party is expressed as ‘QEAA_Provider’, as ‘Non_Q_EAA_Provider’, as ‘PUB_EAA_Provider’ or as ‘PID_Provider’, for the purpose of listing the attestation type(s) (credential) the wallet-relying party intends to issue to wallet units.

The referenced attestation types that may be listed in this attribute “providesAttestations” shall, where applicable, be included in the catalogues of schemes for the attestation of attributes referred to in Article 7 of Implementing Regulation (EU) No 2025/1569;
 - 10.3 In Table 8, the attribute “establishedBylaw” shall be present in case of a public sector body that is responsible for an authentic source and shall be present in case of any other public sector body, where applicable.

Table 1

Data schema for each wallet-relying party registered in the national register of wallet-relying parties

Attribute	Multi plicity	Type	Description
legalPerson	[0..1]	LegalPerson (table 8)	specifies the specific attributes of a legal person.
naturalPerson	[0..1]	NaturalPerson (table 9)	specifies the specific attributes of a natural person.

Identifier	[1..*]	Identifier (table 10)	shall be present to specify one or more identifiers of the natural or legal person, as stated in an official record together with the identification data of that official record, where applicable.
postalAddress	[0..*]	string	may be present to specify the postal address of the legal entity in accordance with clause 6.6.1 of recommendation ITU-T X.520.
Country	[1..1]	string	specifies the alpha-2 country code in accordance with ISO 3166-1 of the country in which the legal entity is established, or the string "EU" for providers operating in the Union.
email	[0..*]	string	may be present to specify one or more email addresses in accordance with RFC5322 of the legal entity.
phone	[0..*]	string	may be present to 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 as specified in RFC2806.
infoURI	[0..*]	string	may be present to specify one or more Unique Resource Identifiers (URIs) according to RFC3986 with web pages for information about the legal entity.
providerType	[1..1]	string	specifies the type of the provider according to its sub-class: <ul style="list-style-type: none"> • WRPRRegistrar • WalletProvider • PIDProvider • PubEEAPProvider • WRPAccCertProvider • WalletRelyingParty
policy	[1..*]	Policy (table 7)	specifies the type and URL of a webpage where the relevant service policy or privacy policy or terms and

			conditions statement of the provider are located, where applicable.
x5c	[0..*]	string	specifies a sequence of X.509 certificate chains according to RFC 7515, where each certificate chain is compliant to RFC 3647 and RFC 5280, if used by the provider for all its services. Specifying more than one certificate chain here allows to support key rollover procedures. In case of a Trust Service Provider, this element is not present, as the relevant certificate chains are assigned to the individual Trust Service.
tradeName	[0..1]	string	may be present to specify the trade name or service name of the wallet-relying party which can be familiar to the User, where applicable.
supportURI	[1..*]	Array of strings	specifies the support URI for the service provided by the wallet-relying party.
srvDescription	[1..*]	Array of MultiLangString objects (table 4)	contains an array of arrays with localised descriptions of the services provided by the wallet-relying party.
intendedUse	[0..*]	Array of IntendedUse objects (table 2)	array of IntendedUse objects -in order to specify intended use cases in which the wallet-relying party intends to rely on attestations of attributes of a wallet user presented by a wallet unit. IntendedUse is not required from wallet-relying parties that register only to act as a designated intermediary.
isPSB	[1..1]	boolean	indicates whether the wallet-relying party is a public sector body or not.
entitlement	[1..*]	Array of strings	specifies the set of entitlements of the wallet-relying party in form of a URI in accordance with RFC3986. A provider of electronic attestations of attributes that requires the presentation of another attestation during issuance of their own attestation shall register both as a

			<p>Service_Provider and with their attestation provider entitlement in a single registration. The following URIs are specified for the types of entitlement or entitlements of the wallet-relying parties as set out in Annex I, point 12:</p> <ul style="list-style-type: none"> • https://uri.etsi.org/19475/Entitlement/Service_Provider • https://uri.etsi.org/19475/Entitlement/QEAA_Provider • https://uri.etsi.org/19475/Entitlement/Non_Q_EAA_Provider • https://uri.etsi.org/19475/Entitlement/PUB_EAA_Provider • https://uri.etsi.org/19475/Entitlement/PID_Provider • https://uri.etsi.org/19475/Entitlement/QCert_for_ESeal_Provider • https://uri.etsi.org/19475/Entitlement/QCert_for_ESig_Provider • https://uri.etsi.org/19475/Entitlement/rQSealCDs_Provider • https://uri.etsi.org/19475/Entitlement/rQSigCDs_Provider • https://uri.etsi.org/19475/Entitlement/ESig_ESeal_Creation_Provider
providesAttestations	[0..*]	Array of Credential objects (table 5)	<p>a list of self-declared or referenced attestation types the wallet-relying party intends to issue to wallet units.</p> <p>The attribute to be referenced for a catalogued attestation type is its catalogue-assigned attestation schema URI (SchemaMeta.Schema.uri)</p>
supervisoryAuthority	[1..1]	LegalEntity (table 6)	<p>specifies the competent-supervisory authority-according to Article 46a of Regulation (EU) No 910/2014 in charge of supervising the wallet-relying party, and provides the necessary contact information towards that supervisory authority, at least in one of the following forms email, phone or infoURI attributes.</p>
registryURI	[1..1]	string	URI for the API of the national register of

			wallet-relying parties.
usesIntermediary	[0..*]	Array of WalletRelyingParty objects (table 1)	where present, indicates whether the wallet-relying party depends on at least one designated intermediary and lists the needed information (WalletRelyingParty.identifier, WalletRelyingParty.tradeName and WalletRelyingParty.registryURI) of the designated intermediaries the registered wallet-relying party depends on.
isIntermediary	[1..1]	boolean	indicates whether the wallet-relying party is registered as a designated intermediary or not. This attribute is set to false if usesIntermediary attribute is present.

Table 2
Mandatory data schema for listing intended use

Attribute	Multiplicity	Type	Description
purpose	[1..*]	Array of <i>MultiLangString</i> objects (table 4)	specifies one or more purposes of the intended data processing according to Article 5b(2), point (c) of Regulation (EU) No 910/2014, and, where applicable, Article 5(1), point (b) of Regulation (EU) No 2016/679. The purpose shall be capable of localisation to the user's language (lang) in accordance with Annex E of ETSI TS119612 V2.3.1.

privacyPolicy	[1..*]	Array of <i>Policy</i> objects (table 7)	specifies the privacy policy of the intended use. Policy.type shall be of type privacy statement. The privacy policy shall be capable of localisation to the user's language (lang) in accordance with Annex E of ETSI TS119612 V2.3.1.
intendedUseIdentifier	[1..1]	<i>string</i>	unique identifier of the registered intended use.
createdAt	[1..1]	<i>string</i>	validity start date of the intended use in accordance with [ISO86011] YYYY-MM-DD format.
revokedAt	[0..1]	<i>string</i>	end date for the validity of the intended use in accordance with [ISO86011] YYYY-MM-DD format. The intended use may be marked to expire at given date, or may be revoked by the wallet-relying party as necessary.
credential	[1..*]	Array of <i>Credential</i> objects (table 5)	specifies the set of electronic attestations of attributes which

			may be requested by the wallet-relying party.
--	--	--	---

Table 3
Mandatory data schema for listing attributes within a requested electronic attestations of attributes

Attribute	Multiplicity	Type	Description
path	[1..1]	non-empty array of strings, nulls and non-negative integers	a path pointer that specifies the path to a claim within the Credential in accordance with OpenID Connect for Verifiable Presentations 1.0, OpenID Foundation, 9 July 2025 [OpenID4VP] sections 6.3. and 7. Section 7.1 specifies use of path for Credentials in sd-jwt-vc format, and Section 7.2 for Credentials in mso_mdoc format.
values	[0..1]	an array of strings, integers or boolean values	optional array of strings, integers or boolean values that specifies the expected values of the claim (used to indicate that the Wallet should return the claim only if the type and value of the claim both match exactly for at least one of the elements in the array). See OpenID Connect for Verifiable Presentations 1.0, OpenID Foundation, 9 July 2025 [OpenID4VP] Sections 6.3. and 6.4.1.

Table 4
Mandatory data schema for listing localised descriptions of the services provided by the wallet-relying party

Attribute	Multiplicity	Type	Description
lang	[1..1]	string	specifies the country code of the localised text.
content	[1..1]	string	the localised text as a string.

Table 5

Mandatory data schema for listing self-declared or referenced attestation types the wallet-relying party intends to issue to wallet units

Attribute	Multiplicity	Type	Description
format	[1..1]	string	specifies the format of the attestation. For valid values, see enumerations listed in OpenID Connect for Verifiable Presentations 1.0, OpenID Foundation, 9 July 2025 [OpenID4VP] Appendix B.
meta	[1..1]	string	an object defining additional properties requested by the Verifier (including the credential type) that apply to the metadata and validity data of the Credential. The properties of this object are defined per Credential Format - see OpenID Connect for Verifiable Presentations 1.0, OpenID Foundation, 9 July 2025 [OpenID4VP] Section 6.1 and annex B.3.5 for SD-JWT VC format, and annex B2.3 for the mdoc format defined in ISO/IEC 18013-5:2021.
claim	[0..*]	Claim (table 3)	a non-empty array of objects that specifies attributes in the requested attestation. See OpenID Connect for Verifiable Presentations 1.0, OpenID Foundation, 9 July 2025 [OpenID4VP] Section 6.3.

Table 6

Mandatory data schema for listing competent supervisory authority

Attribute	Multiplicity	Type	Description
legalPerson	[0..1]	LegalPerson (table 8)	specifies the specific attributes of a legal person. This attribute is present, where the legal entity is a private or public legal person.

naturalPerson	[0..1]	NaturalPerson (table 9)	specifies the specific attributes of a natural person. This attribute is present, where the legal entity is a natural person.
identifier	[0..*]	Identifier (table 10)	may be present in order to specify one or more identifiers of the legal entity, as stated in an official record together with the identification data of that official record, if applicable.
postalAddress	[0..*]	string	may be present in order to specify the postal address of the legal entity in line with clause 6.6.1 of recommendation ITU-T X.520.
country	[1..1]	string	specifies the alpha-2 country code according to ISO 3166-1 of the country in which the legal entity is established, or the string "EU" for providers operating in the Union.
email	[0..*]	string	may be present in order to specify one or more email addresses according to RFC5322 of the legal entity.
phone	[0..*]	string	may be present in order to 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 RFC2806.
infoURI	[0..*]	string	may be present in order to specify one or more Unique Resource Identifiers (URIs) according to RFC3986 with web pages for information about the legal entity.

Table 7

Mandatory data schema for listing the privacy policy

Attribute	Multiplicity	Type	Description
type	[1..1]	string	<p>specifies the type of the policy in the form of a URI according to RFC3986. The following URIs are to be understood in the manner indicated:</p> <ul style="list-style-type: none"> • http://data.europa.eu/eudi/policy/trust-service-practice-statement- is a Trust Service Practice statement according to clause 6.1 of ETSI EN 319 401. • http://data.europa.eu/eudi/policy/terms-and-conditions- is a Terms and Conditions statement according to clause 6.2 of ETSI EN 319 401. • http://data.europa.eu/eudi/policy/privacy-statement- is a Privacy Statement to fulfil the information requirements of Article 12 et seq. of Regulation (EU) No 2016/679. • http://data.europa.eu/eudi/policy/privacy-policy- is a Privacy Policy according to the clauses 3.14 and 5.6 of ISO/IEC 29100. • http://data.europa.eu/eudi/policy/registration-policy- is a Registration Policy according to Article 4 of Draft of the CIR for RP-Registration.
policyURI	[1..1]	string	specifies the policy URI in form of a URL according to RFC1738 where the policy is published.

Table 8

Mandatory data schema for listing legal person

Attribute	Multiplicity	Type	Description
legalName	[1..*]	string	specifies the legal name of the legal person, as specified in an official record.

establishedBylaw	[0..*]	Law (table 11)	specifies the legal basis on which the legal person is established.
------------------	--------	----------------------	---

Table 9
Mandatory data schema for listing natural person

Attribute	Multiplicity	Type	Description
givenName	[1..1]	string	specifies the current first name(s) of the natural person including middle name(s) where applicable, as specified in official records and the set of person identification data as set out in the Annex to Implementing Regulation (EU) No 2024/2977.
familyName	[1..1]	string	specifies the current last name(s) or surnames of the natural person, as specified in official records and the set of person identification data as set out in the Annex to Implementing Regulation (EU) No 2024/2977.
dateOfBirth	[0..1]	string	specifies the data of birth of the natural person, as specified in official records and the set of person identification data as set out in the Annex to Implementing Regulation (EU) No 2024/2977, where present.
placeOfBirth	[0..1]	string	specifies the place of birth of the natural person, as specified in official records and the set of person identification data as set out in the Annex to Implementing Regulation (EU) No 2024/2977, where present.

Table 10
Mandatory data schema for listing identifiers of the legal entity

Attribute	Multiplicity	Type	Description
type	[1..1]	string	<p>is the type of the identifier specified by a URI according to RFC3986, whereas the following URIs are defined in the present document:</p> <ul style="list-style-type: none"> • http://data.europa.eu/eudi/id/EORI-No - Economic Operator Registration and Identification Number (EORI-No) according to (EU) No 1352/2013 • http://data.europa.eu/eudi/id/LEI - Legal Entity Identifier (LEI) according to (EU) No 2022/1860 and ISO 17442 • http://data.europa.eu/eudi/id/EUID - European Unique Identifier (EUID) according to (EU) 2020/2244 and (EU) 2021/1042 • http://data.europa.eu/eudi/id/VATIN - Value Added Tax Identification Number (VATIN) according to the Council Directive 2006/112/EC • http://data.europa.eu/eudi/id/TIN - Taxpayer Identification Number (TIN) • http://data.europa.eu/eudi/id/Excise - Excise Number according to Art. 2 (12) of the Council Regulation (EC) No 389/2012.
identifier	[1..1]	string	is the identifier, which identifies the LegalEntity under consideration.

Table 11

Mandatory data schema for listing the legal basis on which the legal person is established

Attribute	Multiplicity	Type	Description
lang	[1..1]	string	is the two-letter Alpha-2 language code according to ISO 639 (Set 1).
legalBasis	[1..1]	string	specifies the legal basis according to which a LegalPerson is established as such or the access to a specific Claim is required or

			recommended.
--	--	--	--------------