EUROPEAN
COMMISSION

Brussels, XXX
[…](2026) XXX draft

ANNEXES 1 to 14

ANNEXES

to the

COMMISSION IMPLEMENTING REGULATION

amending Implementing Regulation (EU) 2024/2977, (EU) 2024/2979, (EU) 2024/2980 and (EU) 2024/2982 as regards applicable standards and specifications and correcting Implementing Regulation (EU) 2024/2980

ANNEX I

'*ANNEX*

Technical specifications for person identification data referred to in Article 3(3)

(1) Set of natural person identification data

Table 1: Mandatory person identification data for the natural person

Data identifier	Definition
family_name	Current last name(s) or surname(s) of the user to whom the person identification data relates.
given_name	Current first name(s), including middle name(s) where applicable, of the user to whom the person identification data relates.
birth_date	Day, month, and year on which the user to whom the person identification data relates was born.
birth_place	The country as an Alpha-2 country code as specified in ISO 3166-1, or the state, province, district, or local area or the municipality, city, town, or village where the user to whom the person identification data relates was born.
nationality	One or more Alpha-2 country codes as specified in ISO 3166-1, representing the nationality of the user to whom the person identification data relates.
portrait	Facial image of the wallet user compliant with the quality requirements for a full frontal image type as set out in ISO/IEC 19794-5, clauses 8.2, 8.3, and 8.4, and without the headers or blocks as specified in clause 5 of ISO/IEC 19794-5 except for the image data itself (a JPEG).

– Where an attribute value is not known for the person or cannot otherwise be issued as part of the person identification dataset, Member States shall use an attribute value appropriate to the situation instead.

Table 2: Optional person identification data for the natural person

Data identifier	Definition
resident_address	The full address of the place where the user to whom the person identification data relates currently resides or can be contacted (street name, house number, city etc.).
resident_country	The country where the user to whom the person identification data relates currently resides, as an Alpha-2 country code as specified in ISO 3166-1.
resident_state	The state, province, district, or local area where the user to whom the person identification data relates currently resides.

resident_city	The municipality, city, town, or village where the user to whom the person identification data relates currently resides.
resident_postal_code	The postal code of the place where the user to whom the person identification data relates currently resides.
resident_street	The name of the street where the user to whom the person identification data relates currently resides.
resident_house_number	The house number where the user to whom the person identification data relates currently resides, including any affix or suffix.
personal_administrative_number	A value assigned to the natural person that is unique among all personal administrative numbers issued by the provider of person identification data. Where Member States opt to include this attribute, they shall describe in their electronic identification schemes under which the person identification data is issued, the policy that they apply to the values of this attribute, including, where applicable, specific conditions for the processing of this value.
family_name_birth	Last name(s) or surname(s) of the person identification data user at the time of birth.
given_name_birth	First name(s), including middle name(s), of the person identification data user at the time of birth.
sex	Values shall be one of the following: 0 = not known; 1 = male; 2= female; 3= other; 4 = inter; 5 = diverse; 6 = open; 9 = not applicable; For values 0, 1, 2 and 9, ISO/IEC 5218 applies.
email_address	Electronic mail address of the user to whom the person identification data relates [in conformance with RFC 5322].
mobile_phone_number	Mobile telephone number of the user to whom the person identification data relates, starting with the '+' symbol as the international code prefix and the country code, followed by numbers only.

(2) Set of legal person identification data

Table 3: Mandatory person identification data for the legal person

Data element
current legal name
a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time

– Where a data element is not known for the person or cannot otherwise be issued as part of the person identification dataset, Member States shall instead use an attribute value appropriate to the situation.

Table 4: Optional person identification data for the legal person

Data element
current address
VAT registration number
tax reference number
European unique identifier referred to in Directive (EU) 2017/1132
Legal Entity Identifier (LEI) referred to in Commission Implementing Regulation (EU) 2022/1860
Economic Operator Registration and Identification (EORI) referred to in Commission Implementing Regulation (EU) No 1352/2013
excise number provided in Article 2(12) of Council Regulation (EC) No 389/2012

(3) Set of metadata about person identification data

Table 5: Metadata about the person identification data

Data identifier	**Definition**	**Presence**
expiry_date	Date (and if possible time) when the person identification data will expire.	mandatory
issuing_authority	Name of the administrative authority that issued the person identification data, or the ISO 3166 Alpha-2 country code of the respective Member State if there is no separate authority entitled to issue person identification data.	mandatory
issuing_country	Alpha-2 country code, as specified in ISO	mandatory

	3166-1, of the country or territory of the provider of the person identification data.	
trust_anchor	The URL location at which a machine-readable version of the trust anchor for verifying the person identification data is available free of charge.	mandatory
document_number	A number for the person identification data, assigned by the provider of person identification data.	optional
issuing_jurisdiction	Country subdivision code of the jurisdiction that issued the person identification data, as specified in ISO 3166-2:2020, Clause 8. The first part of the code shall be the same as the value for the issuing country.	optional
location_status	The location of validity status information on the person identification data where the providers of person identification data revoke person identification data.	optional
issuance_date	Date, and if possible time, when the person identification data was issued and/or the administrative validity period of the person identification data began.	optional

(4) Encoding of natural person identification data attributes

– Person identification data of natural persons shall be issued in ISO/IEC-mdoc and SD-JWT VC formats as specified in the standard set out in Annex II to Implementing Regulation (EU) 2024/2979.

– The encoding of person identification data of natural persons shall comply with the technical specifications in sections 4.1 and 4.2 to this Annex.

4.1 Encoding of person identification data in ISO/IEC-mdoc format

– The attestation type for person identification data in ISO/IEC mdoc format shall be "eu.europa.ec.eudi.pid.1". The identifier of the namespace for the person identification data attributes specified in this Annex shall be "eu.europa.ec.eudi.pid.1". Where the person identification data includes attributes that are not defined in this Annex, these attributes shall be defined within a domestic person identification data namespace that uses the general format eu.europa.ec.eudi.pid. [ISO 3166-1 alpha-2 country code or the ISO 3166-2 region code] followed by an optional dot and version number. Where, the domestic namespace is used, it shall be published, including all attribute identifiers, their definition, presence and encoding format, in a scheme that complies with Article 8 of Implementing Regulation (EU) 2025/1569.

– The person identification data attributes and metadata of natural persons as set out in sections 1 and 3 of this Annex shall be included in person identification data as data elements.

– The requirements of encoding person identification data in ISO/IEC-mdoc format are set out in Table 6:

Table 6: Requirements of encoding person identification data in ISO/IEC-mdoc format

Data Identifier	Attribute identifier	Encoding format
family_name	family_name	Tstr
given_name	given_name	Tstr
birth_date	birth_date	full-date
birth_place	place_of_birth	place_of_birth
Nationality	Nationality	nationalities
resident_address	resident_address	Tstr
resident_country	resident_country	Tstr
resident_state	resident_state	Tstr
resident_city	resident_city	Tstr
resident_postal_code	resident_postal_code	Tstr
resident_street	resident_street	Tstr
resident_house_number	resident_house_number	Tstr
personal_administrative_number	personal_administrative_number	Tstr
Portrait	Portrait	Bstr
family_name_birth	family_name_birth	Tstr
given_name_birth	given_name_birth	Tstr
Sex	Sex	Uint
email_address	email_address	Tstr
mobile_phone_number	mobile_phone_number	Tstr
expiry_date	expiry_date	tdate or full-date
issuing_authority	issuing_authority	Tstr
issuing_country	issuing_country	Tstr

document_number	document_number	Tstr
issuing_jurisdiction	issuing_jurisdiction	Tstr
location_status	-	-
issuance_date	issuance_date	tdate or full-date
trust_anchor	trust_anchor	Tstr

– The notation of the encoding format of the attributes specified in Table 6 shall use representation types as specified in RFC 8610 - Concise Data Definition Language (CDDL - June 2019), with the following additional requirements:

(a) a tstr shall be encoded in UTF-8;

(b) a tstr shall support the full unicode range;

(c) a tstr shall have a maximum length of 150 characters;

(d) a date shall be encoded as specified in RFC 8943 (November 2020);

(e) a full-date shall be interpreted as #6.1004(tstr), where tag 1004 is as specified in RFC 8943;

(f) a tdate attribute shall contain a date-time string as specified in RFC 3339 - Date and Time on the Internet: Timestamps, (July 2002), in accordance with RFC 8949 - Concise Binary Object Representation (CBOR) (December 2020), section 3.4.1;

(g) a full-date attribute shall contain a full-date string as specified in RFC 3339, in accordance with RFC 8943;

(h) a representation of a date in attributes shall, unless otherwise indicated:

– not use fractions of seconds;

– not use a local offset from UTC; the time-offset defined in RFC 3339 shall be to "Z".

(i) an integer (major types 0 and 1) shall be as small as possible, in accordance with RFC 8949, section 4.2;

(j) a place_of_birth shall contain at least one of the following key-value pairs: "country", "region", or "locality";

(k) the expression of the length in a bstr, tstr, array or map shall be as short as possible, in accordance with RFC 8949, section 4.2;

an indefinite-length items shall be made into a definite-length item, in accordance with RFC 8949, section 4.2;

(l) the attribute nationality shall be encoded as an array of Alpha-2 country codes as specified in ISO 3166-1. Where CDDL notation as specified in RFC 8610 is used, the encoding of this attribute shall be:

– nationalities = [+ CountryCode]

– CountryCode = tstr; Alpha-2 country code specified in ISO 3166-1

– where the wallet user to whom the person identification data relates has multiple nationalities and the provider of person identification data attests to these multiple nationalities, the provider of person identification data may include all the nationalities in the person identification data.

– the attribute place_of_birth shall be encoded as a type place_of_birth. Where CDDL notation as specified in RFC 8610 is used, the encoding of this attribute shall be:

```
place_of_birth                                                    =
{
 ? "country": tstr  ; a single alpha-2 country code as specified in ISO 3166-1
 ? "region": tstr    ; the name of a state, province, district, or local area
 ? "locality": tstr  ; the name of a municipality, city, town, or village
}
```

4.2 Requirements of encoding person identification data in SD-JWT VC format

– The person identification data attributes and metadata specified in this section shall be included in a person identification data as claims.

– All claims in the issued person identification data, referenced in the previous indent, shall be selectively disclosable individually, except those claims defined as non-selectively disclosable in SD-JWT VC.

– Table 7 specifies the encoding of claim names that are public names.

– Table 8 specifies the encoding of claim names that are specific to the person identification data.

– A JSON string used in person identification data encoded in SD-JWT VC shall be encoded in UTF-8 and shall support the full unicode range, unless explicitly specified otherwise in the Table 8 below or the references therein.

– The standard JWT claims nbf and exp shall be used to express the technical validity period of person identification data compliant with SD-JWT VC.

Table 7: Requirements for encoding person identification data in SD-JWT VC format using public names

Data Identifier	Attribute identifier	Encoding format
family_name	family_name	String
given_name	given_name	String
birth_date	Birthdate	string, ISO 8601-1, YYYY-MM-DD format
birth_place	place_of_birth	JSON structure
Nationality	Nationalities	array of strings
resident_address	address.formatted	String
resident_country	address.country	String

resident_state	address.region	String
resident_city	address.locality	String
resident_postal_code	address.postal_code	String
resident_street	address.street_address	String
resident_house_number	address.house_number	String
family_name_birth	birth_family_name	String
given_name_birth	birth_given_name	String
email_address	Email	String
mobile_phone_number	phone_number	String
Portrait	Picture	string; data URL containing a base64-encoded portrait in JPEG format

Table 8: Requirements for encoding person identification data in SD-JWT VC format using private names

Data Identifier	Attribute identifier	Encoding format
expiry_date	date_of_expiry	String
issuance_date	date_of_issuance	String
personal_administrative_number	personal_administrative_number	String
Sex	Sex	Number
issuing_authority	issuing_authority	String
issuing_country	issuing_country	String
document_number	document_number	String
issuing_jurisdiction	issuing_jurisdiction	String
location_status	-	-
trust_anchor	trust_anchor	String

– The base type of person identification data shall be "urn:eudi:pid:1", included in the vct claim. All person identification data shall use types in the namespace "urn:eudi:pid:".

– Where person identification data include attributes that are not specified in this Annex, these attributes shall be defined within a domestic type.

– Where the domestic type is used, it shall be published, including all claim identifiers, their definition, presence and encoding format, in a scheme in compliance with Article 8 of Implementing Regulation (EU) 2025/1569.

(5) Trust infrastructure details

The list of providers of person identification data made available by the Commission in accordance with Implementing Regulation (EU) 2024/2980 shall enable authentication of person identification data.’

ANNEX II

'ANNEX Ia

Cryptographic mechanisms referred to in Article 5a

European Cybersecurity Certification Group, Sub-group on Cryptography: 'Agreed Cryptographic Mechanisms' published by the European Union Agency for Cybersecurity ('ENISA')[1].'

[1] https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en

ANNEX III

'ANNEX Ib

Technical specifications for wallet instance attestations and wallet unit attestations referred to in Article 6(2a)

(1) Wallet instance attestation and wallet unit attestation

(a) Format requirements

– FR-WIA-1: A wallet instance attestation shall be a JSON Web Token (JWT) as specified in RFC7519, signed or sealed by the wallet provider by means of a compact JAdES baseline B signature.

– FR-WUA-1: A wallet unit attestation shall be a JWT as specified in RFC7519, signed or sealed by the wallet provider by means of a compact JAdES baseline B signature.

(b) Transport requirements

– TR-WIA-1: The wallet instance attestation format shall be as specified in Appendix E of OpenID for Verifiable Credential Issuance v1.0[2] ('OID4VCI'), and sent to the authorisation server in the pushed authorisation request and the token request.

– NOTE: OID4VCI shall use credential issuer metadata and authorisation server metadata to specify the need for the wallet instance attestation and wallet unit attestation.

– TR-WIA-2: The wallet instance attestation shall be signed or sealed by the wallet provider.

– TR-WIA-3: The wallet instance attestation shall be sent along with a Proof-of-Possession ('PoP') as specified in Appendix E of OID4VCI.

– TR-WIA-3.1: Where a wallet instance attestation is sent to the wallet instance, it shall have a time-to-live of less than 24 hours. The difference between the time indicated in the 'exp' header parameter and the time of issuance shall be less than 24 hours.

– TR-WUA-1: The wallet unit attestation shall be a key_attestation element sent within the OID4VCI Credential Request, either as `attestation` proof type or in the header of a `jwt` proof type.

  – TR-WUA-1.1: The key_attestation element shall be extended to include a eudi_wallet_info element as specified in C-claim-2, containing specific information related to wallet units.

– TR-WUA-2: During issuance, wallet units shall include in the proofs field the wallet unit attestation in a 'jwt' proof type or a wallet unit attestation with their Credential Request to the credential issuer.

  – NOTE: The 'jwt' acts as a PoP of the keys.

(c) Content

[2] OpenID for Verifiable Credential Issuance v1.0, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

- C-WIA-1: The content of the wallet instance attestation shall be as specified in Appendix E of OID4VC.
  - C-WIA-1.1: The wallet instance attestation shall include the required attributes from the specification and the eudi_wallet_info claim as specified in C-claim-2 and shall contain general_info as specified in C-claim-3.
- C-WUA-1: The content of the wallet unit attestation shall be as specified in the key_attestation as specified in Appendix D of OID4VCI.
  - C-WUA-1.1: The key_storage attribute of the key_attestation shall be used to indicate the attack potential resistance of the wallet secure cryptographic device ('WSCD') or keystore where the attested keys are stored.
  - C-WUA-1.2: The wallet unit attestation shall include the required attributes and the eudi_wallet_info claim as specified in C-claim-2 and shall contain both general_info as specified in C-claim-3, and wscd_info as specified in C-claim-4.
  - C-WUA-1.3: The wallet unit attestation shall include the status object as specified in Appendix D.1 of OID4VCI.
  - C-WUA-1.4: Where a wallet unit attestation is sent as an attestation proof type, it shall also include a `c_nonce` as specified in Appendix F.3 of OpenID4VCI.
- C-claim-1: Specific attributes for the wallet ecosystem shall be placed in a eudi_wallet_info object claim in the wallet instance attestation and wallet unit attestation.
- C-claim-2: The eudi_wallet_info object claim shall include the following information:

Attribute	Multiplicity	Type	Description
general_info	required in both WIA and WUA	general_info	Specifies general information on the wallet unit.
key_storage_info	required in a WUA about a WSCD. optional for a WUA about a keystore.	key_storage_info	Specifies information on the key storage containing the attested keys.

- C-claim-3: The general_info object shall include the following information:

Attribute	Multiplicity	Type	Description
wallet_provider_name	required	String	Name of wallet provider, as listed on

			the list of wallet providers specified in CIR 2024/2980
wallet_solution_id	required	String	Identifier of the wallet solution, as listed on the list of wallet providers specified in CIR 2024/2980
wallet_solution_version	required	String	Version of the wallet solution
wallet_solution_certification_information	required	JSON/string	Object containing information on the conformity assessment body that certified the wallet solution, the certification number, etc.

– C-claim-4: The key_storage_info object shall include the following information:

Attribute	Multiplicity	Type	Description
storage_type	recommended	String	One of the following values of technical implementation of the WSCD or keystore: "remote", "local_external", "local_internal", "local_native" or "hybrid".
storage_certification_information	required	JSON / string	Information about the certification achieved by the WSCD or keystore, including the scheme under which certification was achieved (for example, Common Criteria, GlobalPlatform), the requirements that were evaluated (for example, the Protection Profile used), the evaluation level, and, where relevant, any other relevant information. It shall be possible to determine if the key storage is a WSCD on the basis of the information in this

			field.

(d) Life cycle

– LC-WIA-1: The wallet instance attestation shall be short-lived and be consumed upon usage.

– LC-WUA-1: During re-issuance of person identification data or electronic attestation of attributes, the wallet unit shall send a new wallet unit attestation in the credential request to the providers of person identification data and providers of electronic attestation of attributes.

(2) Operational requirements

(a) Transport Requirements

– TR-WP-WIA-1: The wallet provider shall verify the integrity of the wallet instance before signing a wallet instance attestation.

– TR-WP-WIA-2: The wallet provider shall ensure that the wallet unit it provides has wallet instance attestations needed for the issuance of person identification data, qualified electronic attestations of attributes and electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source.

– TR-WP-WIA-3: The wallet provider shall ensure that the wallet unit it provides uses a wallet instance attestation only once.

– TR-WP-WUA-1: The wallet provider shall generate and sign the wallet unit attestation.

– TR-WP-WUA-2: The wallet provider shall verify that the keys attested to in the wallet unit attestation are stored in secure hardware as specified in the key_attestation.

– TR-WP-WUA-3: The attested_keys element of a key_attestation shall contain at least one key to support the batch issuance of person identification data, qualified electronic attestations of attributes, and electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source.

  – TR-WP-WUA-3.1: Where a wallet unit includes their wallet unit attestation in a `jwt` element, the wallet unit attestation shall be signed or sealed by the wallet unit with the key at index 0 of the `attested_keys` array within the `key_attestation` element.

– TR-WP-WUA-4: The wallet provider shall ensure that the wallet unit it provides uses a wallet unit attestation only once and each public key corresponding to a private key stored in the wallet secure cryptographic device or keystore shall only be included in one wallet unit attestation.

– TR-WP-WUA-5: The wallet provider shall provide a wallet unit with different wallet unit attestations for the wallet secure cryptographic device and for each of its keystores.

(b) Life cycle

– LC-WP-WUA-1: The wallet provider shall choose the technical validity period of the wallet unit attestation as specified in LC-WP-WUA-2 and LC-WP-WUA-5 and shall maintain the revocation mechanism as specified in R-WP-WUA-1 until this period has passed.

  – LC-WP-WUA-1.1: The key_attestation JWT shall contain a field exp denoting the technical expiration period of the key_attestation.

– LC-WP-WUA-2: The wallet provider may choose to issue wallet unit attestations with different validity periods.

  – LC-WP-WUA-2.1: When choosing the validity period of wallet unit attestations, the wallet provider shall at least consider security, user privacy and interoperability, and the needs of the provider of person identification data.

– LC-WP-WUA-3: The wallet provider shall ensure that a wallet unit may always present a wallet unit attestation for their wallet secure cryptographic device with a remaining validity period of at least 31 days.

– LC-WP-WUA-4: The wallet provider shall ensure that the wallet unit collects the Credential Issuer Metadata as specified in section 12.2.2 of OpenID4VCI during issuance of person identification data.

  – LC-WP-WUA-4.1: Where a `preferred_ttl` attribute as specified in C-PAP-WUA-2 is included in the "Credential Issuer Metadata", the wallet unit shall send the wallet unit attestation available to them with (`exp` - (current time + `preferred_ttl`)) as short as possible and positive. Where such wallet unit attestations are not available to the wallet unit it shall send a key attestation with (current time + `preferred_ttl`) - `exp`) as short as possible.

– LC-WP-WUA-5: A wallet unit shall send a wallet unit attestation with a validity of at least one month to providers of person identification data during issuance of person identification data.

– LC-WP-WUA-6: The wallet provider shall keep a record of the wallet unit attestations that are associated with which wallet units.

  – LC-WP-WUA-65.1: Where a wallet unit is to be revoked, a wallet provider shall revoke all wallet unit attestations associated with this wallet unit.

(c) Revocation

– R-WP-WUA-1: Where a wallet unit attestation has a validity period longer than 24 hours, the status lists, as defined in the IETF token status list[3], shall be used as a revocation mechanism as specified in Appendix D of OpenID4VCI specification for wallet unit attestations. The status element of key_attestation shall be used.

  – R-WP-WUA-1.1: For privacy reasons, a status list shall, where appropriate, relate to at least 10000 attestations.

[3] Token status list (TSL), draft-ietf-oauth-status-list-17, published 30 January 2026, https://www.ietf.org/archive/id/draft-ietf-oauth-status-list-17.txt

– R-WP-WUA-1.2: Multiple status lists may be active for a single wallet provider.

– R-WP-WUA-1.3: The status list shall be compressed to reduce its size.

(3) Requirements for providers of person identification data and providers of electronic attestation of attributes

(a) Transport requirements

– TR-PAP-WIA-1: Where the provider of person identification data or the provider of electronic attestation of attributes receives a wallet instance attestation, it shall check that the signature of the JWT verifies under the public key of the wallet provider as indicated in the trusted list of wallet providers set out in Implementing Regulation (EU) 2024/2980.

– TR-PAP-WIA-2: Where the provider of person identification data or the provider of electronic attestation of attributes receives a wallet instance attestation, it shall check that the wallet instance attestation has not expired.

– TR-PAP-WIA-4: Where the provider of person identification data or a provider of electronic attestation of attributes receives a wallet instance attestation, it shall check that the signature of the PoP verifies under the public key that is present in the cnf.

– TR-PAP-WUA-1: The provider of person identification data and the provider of electronic attestation of attributes shall verify that the signature of the wallet unit attestation verifies under the public key of the wallet provider public key as indicated in the trusted list of wallet providers set out in Implementing Regulation (EU) 2024/2980.

– TR-PAP-WUA-2: The provider of person identification data and the provider of electronic attestation of attributes shall verify that the signature of the ‘jwt’ element matches the key at index 0 of the attested_keys array within the key_attestation element included in the jwt.

– TR-PAP-WUA-3: Where the provider of person identification data or the provider of electronic attestations of attributes receives a wallet unit attestation in a `jwt` proof type, it shall verify that the `jwt` element includes a valid `c_nonce` from their `nonce_endpoint` in the `nonce` field of the `jwt`.

(b) Life cycle

– LC-PAP-WUA-1: The technical validity period of person identification data or of an electronic attestation of attributes shall end before the technical validity period of the wallet unit attestation shown to the provider of person identification data in the process of issuance of person identification data.

– LC-PAP-WUA-2: The provider of electronic attestation of attributes that issues electronic attestation of attributes by or on behalf of a public sector body responsible for an authentic source, may choose a technical validity period of the electronic attestations of attributes independently of the technical validity for the wallet unit attestation used during issuance.

– LC-PAP-WUA-3: Where the provider of person identification data issues person identification data with a validity period equal to or less than 24 hours, they shall only verify the validity period of the wallet unit attestation at the time of issuance of the person identification data.

– LC-PAP-WUA-4: Where the provider of person identification data issues person identification data with a validity period of more than 24 hours, they shall check the revocation status of the wallet unit attestation received in relation to issuance at least once every 24 hours for the validity period of the person identification data.

  – LC-PAP-WUA-4.1: Where the wallet unit attestation is revoked, the provider of person identification data shall revoke the person identification data.

– LC-PAP-WUA-5: As the revocation status list is publicly available, the provider of electronic attestations of attributes may check the revocation status of the wallet unit attestation and revoke its attestation where the wallet unit attestation is revoked.

(c) Content

– C-PAP-WUA-1: The provider of person identification data shall ensure that the person identification data it issues is bound to a key originating from a wallet unit attestation the key storage of which is a wallet secure cryptographic device.

– C-PAP-WUA-2: Where the provider of person identification data or the provider of electronic attestation of attributes communicates their preferences regarding the expiration period of a wallet unit attestation as specified in LC-WP-WUA-4.1, they shall use the following `preferred_ttl` attribute in the "Credential Issuer Metadata endpoint" as specified in section 12.2.2 of OpenID4VCI, within the `key_attestations_required` object claim. The `preferred_ttl` attribute shall include the following information:

Attribute	Multiplicity	Type	Description
preferred_ttl	optional	Integer	An integer specifying the preference of the provider of person identification data or electronic attestation of attributes for the validity in number of seconds of a WUA used during the issuance protocol.

ANNEX IV

‘ANNEX Ic

List of standards referred to in Article 6(3)

The standard Annex C clause C.3 to ETSI TS 119 461 V2.1.1 (2025-02) applies with the following adaptations:

(1) 2.1 Normative references

[1] ETSI EN 319 401 V3.1.1 (2024-06): ‘Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers’.

[8] ‘Methodology for sectoral cybersecurity assessments’, ENISA, September 13, 2021

(2) C.3 Use cases for issuance of qualified certificate or qualified electronic attestations of attributes in accordance with Article 24(1), (1a) and (1b) of Regulation (EU) No 910/2014

[CONDITIONAL] QTS-C3-01: Where identity verification for qualified certificate or a qualified electronic attestation is done in conjunction with identity verification to issue authoritative evidence, that identity verification process shall:

– have been, in accordance with Regulation (EU) No 910/2014, peer reviewed or certified by an accredited conformity assessment body to comply with assurance level high, or

– comply with the requirements set out in clauses C3.1 to C3.6.

(3) C.3.4 Use case for identity proofing by other identification means

QTS-C.3.4-06A: The independent conformity assessment body referred to in [CONDITIONAL] QTS-C.3.4-06, point c) shall be accredited as per Article 3 (18) of Regulation (EU) No 910/2014, and, if all applicable requirements are fulfilled, the assessment should result in a certificate of compliance based on a certification audit. This formal certification process shall be based on a security evaluation process that refers to the levels of assurance defined for notified electronic identification means or certified European Digital Identity Wallets under Regulation (EU) No 910/2014 and shall include rigorous testing to evaluate resistance against potential security threats. These evaluations shall employ pertinent technical standards to demonstrate robustness against such attacks.

(4) 9.2.3.4 Use case for automated operation

USE-9.2.3.4-04: The IPSP shall establish target values for the FAR and FRR, based on a risk analysis and its threats intelligence procedure, by following the methodology established in the ENISA report ‘Methodology for sectoral cybersecurity assessments’ [8] or an equivalent methodology, in fully automated identity proofing processes. These target values shall be equal to or lower than those set for hybrid use cases, when they exist. The IPSP shall maintain these target values for FAR and FRR consistently, supported by a risk analysis and its threats intelligence procedure.

(5) 8.3.3 Validation of physical identity document

VAL-8.3.3-21: The effectiveness of the measures for complying with the requirements VAL-8.3.3-05X, VAL-8.3.3-05A, VAL-8.3.3-05B, VAL-8.3.3-05C, VAL-8.3.3-07A and VAL-8.3.3-07X, shall be tested by an accredited laboratory or a

national competent authority, whenever they are designated, at the latest by 19 August 2027 and be repeated every second year.

(6) 7.12. Termination and termination plans

OVR-7.12-02: The termination plan shall comply with the requirements set out in the implementing acts adopted pursuant to Article 24(5) of Regulation (EU) No 910/2014 [i.1].'

ANNEX V

‘ANNEX II

List of standards referred to in Article 8

The technical specifications set out in clauses 4, 5, 6 and 7 of ETSI TS 119 472-1 V1.1.1 (2025-12) apply. They shall be read with the following adaptations to ETSI TS 119 472-1 V1.1.1 (2025-12):

(1) 2.1. Normative references

[3] IETF SD-JWT VC: "SD-JWT-based Verifiable Credentials (SD-JWT VC) draft-ietf-oauth-sd-jwt-vc-13", November 2025;

[16] ETSI EN 319 412-1 V1.4.4 (2021-05): "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

[17] ETSI TS 119 412-6 V1.1.1 (2025-09): "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers".

[25] IETF Token Status List (TSL), draft-ietf-oath-status-list-17: "Token Status List", 30 January 2026.

(2) 5.2.1.1 Introduction

Clause 6 of IETF SD-JWT VC [3] defines the SD-JWT VC Type Metadata, that can be associated with a type of an SD-JWT VC, as well as a method for retrieving the Type Metadata and processing rules of a SD-JWT VC EAA .

(3) 5.2.1.4 EAA schema

The Type Metadata may contain at the property `schema_uri`, whose value shall be a URL pointing to a JSON Schema document describing the structure of the SD-JWT VC EAA.

(4) 5.2.10.1 General requirements

– EAA-5.2.10.1-05: The status JSON object’s type member shall be a JSON string.

The following string value is defined for the type member of status:

– "TokenStatusList": for token status list as specified in IETF draft-ietf-oauth-status-list-17 [25].

(5) 5.2.10.2 Requirements for EU Qualified EAA (QEAA)

– QEAA-5.2.10.2-01: If a SD-JWT VC QEAA does not contain the `shortLived` claim, it shall include the EAA `status` claim.

(6) 5.2.10.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (PuB-EAA)

– PuB-EAA-5.2.10.3-01: If a SD-JWT VC PuB-EAA does not contain the `shortLived` claim, it shall include the EAA `status` claim

(7) 6.2.10.1 General requirements

– EAA-6.2.10.1-01: When an electronic attestation of attributes compliant with ISO/IEC mdoc uses the attestation status list mechanism as set out in EAA-

6.2.10.1-02.2 or the attestation revocation list mechanism as set out in EAA-6.2.10.1-02.3, its MobileSecurityObject (MSO) shall contain the status structure, as specified in EAA-6.2.10.1-17, which contains MSO revocation information.

– EAA-6.2.10.1-01.1: When implementing the identifier list mechanism, the status element shall contain the identifier_list element as set out in EAA-6.2.10.1-11.

– EAA-6.2.10.1-01.2: When implementing the status list mechanism, the status element shall contain the status_list element as set out in EAA-6.2.10.1-13.

– NOTE:

  – The status structure contains a reference to an MSO revocation list.

  – The MSO revocation list is a COSE_Sign1 structure that indicates whether a particular MSO is revoked or not.

  – The status structure contains all the information necessary for the wallet-relying party to determine whether the MSO revocation list is authentic.

– EAA-6.2.10.1-02: The provider of person identification data, the provider of qualified electronic attestations of attributes or the provider of electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source shall use one of the following methods for revocation of person identification data, qualified electronic attestations of attributes or electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source:

  – EAA-6.2.10.1-02.1: Where they only issue short-lived electronic attestations of attributes having a validity period of equal to or less than 24 hours, then revocation shall never be necessary.

  – EAA-6.2.10.1-02.2: Use an attestation status list mechanism to encode the revocation information as a status list.

  – EAA-6.2.10.1-02.2.1: The status list mechanism revokes an MSO based on whether the bit of the issuer-defined bit position in the MSO is set to true in the status list.

  – EAA-6.2.10.1-02.2.2: The status list mechanism shall be as specified in the token status list (draft-ietf-oauth-status-list-17) specification.

  – EAA-6.2.10.1-02.3: Use an attestation revocation list mechanism to encode the revocation information as an identifier list.

  – EAA-6.2.10.1-02.3.1: The identifier list mechanism revokes an MSO based on whether the issuer-defined identifier in the MSO is present on the identifier list.

  – EAA-6.2.10.1-02.3.2: EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 and EAA-6.2.10.1-11 specify the identifier list mechanism, based on the requirements from the token status list specification including the commonality between the status list and identifier list mechanism.

– EAA-6.2.10.1-03: When status element is used for person identification data, qualified electronic attestations of attributes or electronic attestations of

attributes provided by or on behalf of a public sector body responsible for an authentic source, the status 'revoked' shall be exclusively used.

– EAA-6.2.10.1-03.1: For a status list this implies that only values "valid" and "invalid" as specified in the token status list specification shall be used.

– EAA-6.2.10.1-03.2: For the identifier list, only revoked MSOs, as opposed to temporarily suspended MSOs, are put in the identifier list.

– EAA-6.2.10.1-04: Where an MSO is revoked, the MSO shall be permanently revoked.

– EAA-6.2.10.1-05: Verification of the MSO revocation list is optional for the wallet-relying party and, where applicable, verification shall follow the verification requirements specified in the token status list specification and the requirements status set out in in EAA-6.2.10.1-01.

– EAA-6.2.10.1-05.1: Where a wallet-relying party needs to be able to verify the revocation status of person identification data or electronic attestations of attributes, it shall support both the attestation status list mechanism and the attestation revocation list mechanism as set out in EAA-6.2.10.1-02.

– EAA-6.2.10.1-06: The identifier_list and status_list in the MSO may contain the certificate element.

– EAA-6.2.10.1-06.1: Where the certificate element is present, it shall contain a certificate containing the public key that signed or sealed the top-level certificate in the x5chain element in the MSO revocation list structure.

– EAA-6.2.10.1-06.1.1: The wallet-relying party instance shall use that certificate as a trust anchor for the verification of the x5chain element in the MSO revocation list structure.

– EAA-6.2.10.1-06.2: Where the certificate element is not present, the top-level certificate in the x5chain element in the MSO revocation list structure shall be signed or sealed by the certificate used to sign the top-level certificate in the x5chain element of the MSO.

– EAA-6.2.10.1-06.2.1: The wallet-relying party instance shall use that certificate as a trust anchor for the verification of the x5chain element in the MSO revocation list structure.

– EAA-6.2.10.1-07: An MSO revocation list shall be implemented in accordance with the token status list specification as a status list token in CWT format.

– EAA-6.2.10.1-08: For the MSO revocation list for the identifier list and status list mechanism, the following requirements apply:

  – the exp claim shall be present;

  – the ttl claim may be present;

  – the aggregation_uri claim in the IdentifierList or StatusList claim may be present and the provider of person identification data, the provider of qualified electronic attestations of attributes, or the provider of electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source may use the aggregation_uri claim to indicate support for the aggregation mechanism as specified in the token status list specification;

- the CWT shall be a COSE_Sign1 object using one of the following signature algorithms for calculating the signature:
  (a) “ES256” (ECDSA with SHA-256)
  (b) “ES384” (ECDSA with SHA-384)
  (c) “ES512” (ECDSA with SHA-512)
  (d) ”ES256” shall be used with curves P-256 and brainpoolP256r1;
  (e) “ES384” shall be used with curves P-384, brainpoolP320r1 and brainpoolP384r1;
  (f) “ES512” shall be used with curves P-521 and brainpoolP512r1;
- the CWT shall contain the x5chain in the protected header that contains the certificate or chain of certificates to verify the signature of the MSO revocation list.
- the extended key usage of the object identifier specified in the token status list specification may be used for the status list and the identifier list signing certificate and the wallet-relying party instances may support the extended key usage of object identifiers specified in the token status list specification and for the object identifier, the provider of qualified electronic attestations of attributes, or the provider of electronic attestations of attributes provided by or on behalf of a public sector body are not to make the extended key usage field critical when using the extended key usage OID specified in the token status list specification.

– EAA-6.2.10.1-09: In deviation to the requirements of the token status list specification, for the identifier list mechanism the following requirements apply:
  - the value of the type claim shall be “application/identifierlist+cwt”;
  - the StatusList claim shall not be present in the CWT claims set;
  - the IdentifierList structure defined in EAA-6.2.10.1-11 shall be present as a claim in the CWT claims set using the key 65530.

– EAA-6.2.10.1-10: The IdentifierList structure shall be a CBOR structure with the following CDDL:

```
IdentifierList = {
"identifiers": { * Identifier => IdentifierInfo },
? "aggregation_uri": Aggregation_uri
* tstr => RFU
}

IdentifierInfo = { tstr/int => RFU }
Identifier = bstr
Aggregation_uri = tstr
```

– EAA-6.2.10.1-10.1: Where the identifier in the IdentifierList is present, the MSO that contains the identifier in the status element is revoked.

– EAA-6.2.10.1-10.2: The Aggregation_uri claim is specified in section 9.2 of the token status list specification.

– EAA-6.2.10.1-10.3: The identifier list content-type shall be “application/identifierlist+cwt” set out in the requirements specified in section 8.2 of token status list specification.

– EAA-6.2.10.1-11: The following requirements apply to the identifier_list element in the MSO (see EAA-6.2.10.1-17).

– EAA-6.2.10.1-11.1: The identifier_list element is a CBOR structure with the following CDDL:

IdentifierListInfo = {

"id": Identifier ,

"uri": URI,

? "certificate": Certificate

* tstr => RFU

}

URI = tstr

Certificate = bstr

– EAA-6.2.10.1-11.2: REV-11.2: To prevent the identifier from being used as a correlation across presentations, it shall be unique per MSO.

– EAA-6.2.10.1-12: The following requirements apply to the status list:

– EAA-6.2.10.1-12.1: The bits element in the StatusList structure shall be set to 1.

– EAA-6.2.10.1-13: The following requirements apply to the status_list element in the MSO (see EAA-6.2.10.1-17):

– EAA-6.2.10.1-13.1: The status list element shall follow the requirements for the StatusListInfo structure as specified in the token status list specification and the optional certificate element defined in EAA-6.2.10.1-06 shall be added.

– EAA-6.2.10.1-13.2: To prevent the status index from being a correlation across presentations, the combination of status index and URI shall be unique per MSO.

– EAA-6.2.10.1-14: The wallet provider shall use the second (EAA-6.2.10.1-02.2) or the third (EAA-6.2.10.1-02.3) of the methods specified in EAA-6.2.10.1-02 for the revocation of a wallet unit attestation.

– EAA-6.2.10.1-15: The wallet provider shall implement the attestation revocation mechanisms specified in EAA-6.2.10.1-02 in their wallet solution.

– EAA-6.2.10.1-16: The provider of person identification data and the provider of electronic attestations of attributes shall support both the attestation status list mechanism and the attestation revocation list mechanism specified in EAA-6.2.10.1-02 for verifying the revocation status of a wallet unit attestation.

– EAA-6.2.10.1-17: The status structure in the MSO shall be a CBOR structure with the following CDDL:

Status = {

? "identifier_list”: IdentifierListInfo,

? "status_list”: StatusListInfo,

* tstr => RFU

}’

ANNEX VI

‘ANNEX III

Technical specifications referred to in Article 10

– Technical specifications:

  – Clause 4.2.5 in [tbc ETSI TS 119 472-3 V0.0.12 (2026-1)].’

ANNEX VII

Annex IV, point 1, is replaced by the following:

‘1. Mandatory signature or seal format:

(a) PAdES (PDF Advanced Electronic Signature) as specified in ETSI EN 319 142-1 V1.2.1 (2024-01); Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures.’

ANNEX VIII

‘ANNEX V

Technical specifications for pseudonym generation referred to in Article 14

REQ-1: A wallet unit shall enable the user to store and generate a pseudonym by using any WebAuthn Authenticator of the user's choice.

NOTE: WebAuthn is specified in Web Authentication: An API for accessing Public Key Credentials Level 2 – W3C Recommendation, 8 April 2021, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.

ANNEX IX

‘ANNEX VI

EU Digital Identity Wallet Trust Mark in colour

’

ANNEX X

‘ANNEX VII

EU Digital Identity Wallet Trust Mark in black and white

’

ANNEX XI

'ANNEX VIII

EU Digital Identity Wallet Trust Mark data

Data	Description	Encoding	Status
TrustMarkResourceURL	URL of the EU Digital Identity Wallet Trust Mark graphics and user info resources in the wallet user interface.	URL	mandatory
ListOfCerfifiedWalletsURL	URL of the public list of certified wallet solutions in EU as set out in Implementing Regulation (EU) 2025/849.	URL	mandatory
ListOfCerfifiedWalletsQRCode	QR Code containing the information of ListOfCertifiedWalletsURL	ISO-8859-1 Byte mode QR code	optional
WalletSolutionInfoPageURL	URL to the information page of the certified wallet solution in the list of certified wallet solutions page from the ListOfCertifiedWalletsURL URL appended with a '?' and the WalletSolutionID identifier of the wallet solution.	URL	mandatory
WalletSolutionInfoPageQRCode	QR Code containing the information of WalletSolutionInfoPageURL	ISO-8859-1 Byte mode QR code	optional
WalletVerifierToolURL*	URL pointing to the wallet verification tool */.well-known/openid-credential-issuer* endpoint used for retrieval of the attestation provider metadata.	URL	optional

ANNEX XII

Annex II, Section 1, point 1(i), is replaced by the following:

‘(i) one or more certificates compliant with ETSI EN 319 412-2 V2.4.1 (2025-06) or ETSI EN 319 412-3 V1.3.1 (2023-09) which can be used to verify the signature or seal created by the registrar on the register data and for which the certified identity data include the name of the registrar, and where applicable, the registration number of the registrar, as provided in points (c) and (d), respectively;’

Annex II, Section 2, point 1(h), is replaced by the following:

‘(h) one or more certificates compliant with ETSI EN 319 412-2 V2.4.1 (2025-06) or ETSI EN 319 412-3 V1.3.1 (2023-09) that can be used to authenticate and validate the components of the wallet unit the wallet provides, and for which the certified identity data includes the name, and where applicable, the registration number of the wallet provider, as specified in points (a) and (b), respectively;’

Annex II, Section 3, point 1(h), is replaced by the following:

‘(h) one or more certificates compliant with ETSI EN 319 412-2 V2.4.1 (2025-06) or ETSI EN 319 412-3 V1.3.1 (2023-09) that can be used to verify the signature or seal created by the provider of person identification data on the person identification data it provides, and for which the certified identity data include the name, and where applicable, the registration number of the person identification data provider, as specified in points (a) and (b), respectively.’

Annex II, Section 4, point 1(g), is replaced by the following:

‘(g) one or more certificates compliant with ETSI EN 319 412-2 V2.4.1 (2025-06) or ETSI EN 319 412-3 V1.3.1 (2023-09) that can be used to verify the signature or seal created by the provider of wallet-relying party access certificates on the access certificate it provides to wallet-relying parties, with, where applicable, the information required to distinguish wallet-relying party access certificates from other certificates.

ANNEX XIII

‘ANNEX I

Protocols and interfaces referred to in Article 4

The technical specification [tbc ETSI TS 119 472-3 V0.0.12 (2026-1)] applies with the following adaptations:

(1) 2.1. Normative references

[1] OpenID4VC-HAIP: "OpenID4VC High Assurance Interoperability Profile 1.0, 24 December 2025

[3] ETSI TS 119 471 v1.1.1 (2025-05): "Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services".

[4] Annex II to Implementing Regulation (EU) 2024/2979.

[5] 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".

3.1 TermsnWallet instance attestation (WIA): A wallet instance attestation as defined in Implementing Regulation (EU) 2024/2979.

– NOTE 1: void.

(2) 4.2.3. Provision of registration certificates of the provider of person identification data or the provider of electronic attestations of attributes to the wallet solution

– ISS-MDATA-REG_CERT-4.2.3-04: One of the elements in the issuer_info array parameter may contain the PID/EAA Provider’s registration certificate NOTE 1: Where the registration certificate is not available, the wallet unit contacts the registrar indicated in registrar_dataset element specified in ISS-MDATA-REG_REG_CERT-4.2.3-08 to ISS-MDATA-REG_REG_CERT-4.2.3-016.

– ISS-MDATA-REG_CERT-4.2.3-15: Shall contain the “trade name” member specified in Annex B.2.1 of ETSI TS 119 475 [5], whose value shall be the trade name of the PID/EAA Provider’s Registrar.

(3) 4.6.1.2. Using proofs

– CRED-REQ-4.6.1.2-05: The wallet unit attestation shall be a key attestation in JWT format as specified in Clause D.1 of OpenID4VCI [2] with content as specified in requirement C-WUA-1 of Annex III of Implementing Regulation (EU) 2024/2979.

(4) Annex A

This Annex shall not apply.’

ANNEX XIV

'ANNEX II

Technical specifications referred to in Article 5

The technical specifications in Annex A and Annex C to ISO/IEC 18013-7:2025 apply.

The technical specifications in clauses 4.1, 4.2, 4.3, 5, 6 and 7 of ETSI TS 119 472-2 V1.1.1 (2025-12), apply with the following adaptations:

(1) 2.1. Normative references

[3] IETF SD-JWT VC: "SD-JWT-based Verifiable Credentials (SD-JWT VC) draft-ietf-oauth-sd-jwt-vc-13", 6 November 2025.

[5] Annex II to Implementing Regulation (EU) 2024/2979.

[11] OpenID4VC-HAIP: "OpenID4VC High Assurance Interoperability Profile 1.0., 24 December 2025, "

[12] ETSI TS 119 612 V2.4.1 (2025-08) "Electronic Signatures and Trust Infrastructures (ESI); Trusted Lists"

[13] ETSI 119 475 V1.1.1 (2025-10): "Electronic Signatures and Trust Infrastructures (ESI); Relying party attributes supporting EUDI Wallet user's authorisation decisions".

[14] ISO 639: "Language code"

[15] ISO/IEC 18013-7:2025" Personal identification – ISO – compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions".

[16] Client to Authenticator Protocol (CTAP) Review Draft, March 21, 2023

(2) 5.2. General requirements

– ISO/IEC 18013-5-GEN-05: The wallet solution shall comply with the requirements from mDLs and mdocs specified in ISO/IEC 18013-5: "Personal identification – ISO – compliant driving licence – Part 5: Mobile driving licence (mDL) application" [10]. The wallet-relying party supporting proximity presentation shall comply with the requirements mDL readers and mdoc readers in ISO/IEC 18013-5 [10]. The wallet unit, the provider of person identification data, the provider of electronic attestations of attributes, the wallet provider, and the wallet-relying parties shall not support server retrieval as specified in ISO/IEC 18013-5 [10] for the request of and presentation of person identification data or electronic attestations of attributes.

(3) 5.3. ISO/IEC-mdoc proximity EAAP Request profile

– ISO/IEC 18013-5-REQ-01: void.

– ISO/IEC 18013-5-REQ-02: void.

– ISO/IEC 18013-5-REQ-04: void.

– ISO/IEC 18013-5-REQ-06: void.

– ISO/IEC 18013-5-REQ-09: Where a registration certificate is available, it shall be included in the mentioned requestInfo map in a key-value pair with key "euWrprc", that is enclosed in a bstr.

– ISO/IEC 18013-5-REQ-09a: The mentioned requestInfo map shall contain a key-value pair with key "euWrpRegistrarInfo"; its value shall be a map EUWrpRegistrarInfo structured as (using CDDL notation as specified in RFC 8610):

EUWrpRegistrarInfo = {

"tradeName" : tstr, ; The RP's user-friendly name as defined in Annex B.2.1 of [13]

"identifier": [+ Identifier], ; The RP's identifier as defined in Annex B2.2 of [13]

"srvDescription" : ServiceDescription, ; A description of the RP's service as defined in Annex B.2.1 of [13]

"registryURI" : tstr, ; The URI of the RP's Registrar APIas defined in Annex B.2.1 of [13]

"intendedUseIdentifier" : tstr; The Registrar-provided identifier of the RP's intended use, as defined in Annex B.2.7 of [13]

}

Identifier = {

"type" : tstr, ; For possible values, see Annex B.2.5 of [13]

"identifier": tstr ; The identifier which identifies the RP.

}

ServiceDescription = [+ MultiLangString] ; 1 or more localized text describing the same service

MultiLangString = {

"lang" : tstr, ; The country code of the localized text. A two-letter Alpha-2 language code according to ISO 639 [14](Set 1).

"content" : tstr ; The localized text as a string.
}

– NOTE 3a: The information in EUWrpRegistrarInfo is required by the wallet unit to be able to verify the registration information of the wallet-relying party for the intended use of the presentation request and present this information to the user. Note that in case the wallet-relying party uses the services of an intermediary, the name and identifier in the first two pairs shall be different from the name and identifier of the intermediary as included in the access certificate of the intermediary.

– NOTE 3b: The RequestInfo structure specified in ISO/IEC 18013-5-REQ-09 and ISO/IEC 18013-5-REQ-09a shall use CDDL notation as specified in RFC 8610 and shall be the following:

```
RequestInfo = {
? "euWrprc"            : bstr, ; contains a registration certificate (encoded as a CWT) if available.
"euWrpRegistrarInfo"   : EUWrpRegistrarInfo
}
```

(4) 5.4. ISO/IEC 18013-5 proximity EAAP Response profile

– ISO/IEC 18013-5-RESP-02: void.

– ISO/IEC 18013-5-RESP-03: The provider of person identification data and electronic attestations of attributes shall not include any data elements in the KeyAuthorizations map in the Mobile Security Object of the person identification data and electronic attestations of attributes they issue, except for data elements that are provided by the wallet-relying party in the transactional data in the mdoc request to be signed or sealed by the wallet unit using the private key of the person identification data or electronic attestations of attributes.

– NOTE 1: As a result, wallet units cannot present any device-signed data elements to wallet-relying parties, except to signing data that the wallet-relying party providesd data, for example in use cases for secure user authentication.

– NOTE 2: Person identification data cannot be used by wallet units to sign any data that a wallet-relying party provides.

– NOTE 3: ISO/IEC 18013-5:2021 does not specify how wallet-relying parties can include transactional data in an mdoc request. The inclusion of transactional data in an mdoc request shall take place with the addition of technical specifications.

– ISO/IEC 18013-5-RESP-04: void.

– ISO/IEC 18013-5-RESP-05: void.

– ISO/IEC 18013-5-RESP-06: void.

(5) 6.2 General requirements

– GEN-REQ-01: A wallet solution shall implement the profiles of the protocol specified in OpenID4VC-HAIP: "OpenID4VC High Assurance Interoperability Profile 1.0" [11] clause 5.1 and clause 5.2.

– GEN-REQ-02: Wallet-relying parties shall implement the profile of the protocol specified in OpenID4VC-HAIP: "OpenID4VC High Assurance Interoperability Profile 1.0" [11] clause 5.1 and shall, where appropriate, implement the profile of the protocol specified in OpenID4VC-HAIP: "OpenID4VC High Assurance Interoperability Profile 1.0" [11] clause 5.2.

– GEN-REQ-05: A wallet solution shall support the cross-device remote flow via the profile of the protocol specified in OpenID4VC-HAIP: "OpenID4VC High Assurance Interoperability Profile 1.0" [11] clause 5.2.

(6) 6.3.1.2 General requirements

– OIDFVP-HAIP_COMMON_GEN_REQ-03: The possible values for the `format` claim within the `dcql_query` shall be: "`dc+sd-jwt`", "`mso_mdoc`", "`jwt_vc_json`", and "`vp+jwt`".

(7) 6.3.1.3 Requirements for the Authorization Request message

– OIDFVP-HAIP_COMMON_AR_REQ-01: When the authorisation request is used with profile of the protocol specified in OpenID4VC-HAIP: "OpenID4VC High Assurance Interoperability Profile 1.0" [11] clause 5.1, it shall contain the request_uri parameter, and shall not contain the request object (RO).

NOTE 1: The request object is passed by reference to the wallet unit.

– OIDFVP-HAIP_COMMON_AR_REQ-02: A wallet solution shall not support authorisation requests of type "openid4vp-v1-unsigned" specified in clause A.1, Annex A of OpenID4 VP: "OpenID for Verifiable Presentations 1.0" [7].

– OIDFVP-HAIP_COMMON_AR_REQ-03: void.

(8) 6.3.1.4 Requirements for the request object

– OIDFVP-HAIP_COMMON_RO_REQ-01: void.

– OIDFVP-HAIP_COMMON_RO_REQ-02: void.

– OIDFVP-HAIP_COMMON_RO_REQ-03: void.

– OIDFVP-HAIP_COMMON_RO_REQ-04: void

– OIDFVP-HAIP_COMMON_RO_REQ-05: void.

– OIDFVP-HAIP_COMMON_RO_REQ-06: The verifier_info parameter shall be present within the RO JWT body to carry the registrar-provided data specified in OIDFVP-HAIP_COMMON_RO_REQ-09a, and, where available, the wallet-relying party registration certificate.

– OIDFVP-HAIP_COMMON_RO_REQ-07: The element in the verifier_info array that encloses the registration information and, where available, the wallet-relying party registration certificate shall be a JSON Object excluding the credential_ids member.

– OIDFVP-HAIP_COMMON_RO_REQ-08a: The value of the format member of the element in the verifier_info array that encloses the wallet-relying party registration information shall be "registrar_dataset".

– OIDFVP-HAIP_COMMON_RO_REQ-09: The value of the data member of the element in the verifier_info array that encloses the registration certificate shall be a signed or sealed JSON-encoded wallet-relying party registration certificate.

– OIDFVP-HAIP_COMMON_RO_REQ-09a: The value of the data member of the element in the verifier_info array that contains the wallet-relying party registration information shall be a non-empty JSON object that contains the following registration data of the wallet-relying party:

  – the RP's user-friendly name (tradeName) of the wallet-relying party as defined in Annex B.2.1 of [13],

  – the RP's identifier (identifier) of the wallet-relying party as specified in Annex B.2.2 of [13],

  - The registered user-friendly descriptions of the service provided of the wallet-relying party as an array of JSON objects (srvDescription) specified in Annex B.2.1 of [13],
  - the URI of the Registrar API (registryURI) of the wallet-relying parties as specified in Annex B.2.1 of [13] and
  - the registrar-provided identifier of the intended use (intendedUseIdentifier) of the wallet-relying party as specified in Annex B.2.7 of [13].
- NOTE 3a: This information is required by the wallet unit to be able to verify the wallet-relying party registration information for the intended use of the presentation request and present this information to the user. Note that in case the wallet-relying party uses the services of an intermediary, the user-friendly name (tradeName) and identifier shall be different from the name and identifier of the intermediary as included in the access certificate of the intermediary.
- OIDFVP-HAIP_COMMON_RO_REQ-10: void.
- OIDFVP-HAIP_COMMON_RO_REQ-11: void.
- OIDFVP-HAIP_COMMON_RO_REQ-12: void.
- OIDFVP-HAIP_COMMON_RO_REQ-14: void.
- OIDFVP-HAIP_COMMON_RO_REQ-15: void.
- OIDFVP-HAIP_COMMON_RO_REQ-16: void.
- OIDFVP-HAIP_COMMON_RO_REQ-17: void.
- OIDFVP-HAIP_COMMON_RO_REQ-22: void.
- OIDFVP-HAIP_COMMON_RO_REQ-23: void.

(9) 6.3.2 Specific requirements when requesting ISO/IEC 18013-5 EAAP

- OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: The requirements specified in ISO/IEC 18013-7 [15] Annex C, shall apply for Device Request and Device Response structures specified in ISO/IEC 18013-5 when a wallet unit receives a request for ISO/IEC mdoc presentation through an API-transmitted mechanism defined in clause C.1 of [15].

(10) 6.3.4 Specific requirements for API-mediated EAAP requests

- OIDFVP-HAIP-API_REQ-01: The wallet solution shall by default disclose the presence of all stored electronic attestations of attributes to the mediating API that works in accordance with clause 5.2 of [11] or Annex C of [15], but it shall not disclose the attributes and their values in these electronic attestations of attributes.
- NOTE 1: The restriction of attribute value shall apply even where such disclosure would enhance the services provided by the operating system to the wallet unit, for example, selection of attestations in the context of the mediating API.
- OIDFVP-HAIP-API_REQ-02: The browser and/or the operating system for searching available electronic attestations of attributes shall process a presentation request from a wallet-relying party supporting the clause 5.2 of

[11] or Annex C of [15] for the purposes of preventing fraud targeting the user or of troubleshooting.

– OIDFVP-HAIP-API_REQ-03: The browser and/or the operating system shall, where appropriate, process a presentation request from a wallet-relying party supporting the clause of [11] or Annex C of [15] for the purposes of user security.

– OIDFVP-HAIP-API_REQ-04: The browser and/or the operating system shall not process a presentation request from a wallet-relying party supporting the clause 5.2 of [11] or Annex C of [15] for the purposes of market analysis purposes, including as a secondary purpose, or of internal purposes of the browser and/or the operating system.

– OIDFVP-HAIP-API_REQ-05: Where a wallet unit deletes the request of the user on person identification data or electronic attestations of attributes previously disclosed to the mediating API that works in accordance with clause 5.2 of [11] or Annex C of [15], the wallet unit shall disclose that it no longer stores this person identifications data or electronic attestations of attributes in the mediating API.

– OIDFVP-HAIP-API_REQ-06: Where the user uninstalls their wallet unit, the wallet unit shall disclose that it no longer stores any previously disclosed person identification data or electronic attestations of attributes in the mediating API that works in accordance with clause 5.2 of [11] or Annex C of [15].

– OIDFVP-HAIP-API_REQ-07: The wallet unit shall provide a global user setting to disable the disclosure of stored electronic attestations of attributes through the mediating API that works as specified in OIDFVP-HAIP-API_REQ-01. When the global user setting is disabled, the wallet unit shall not advertise or respond to API-mediated requests from wallet-relying parties for presentation or issuances.

– OIDFVP-HAIP-API_REQ-08: Where supported by the browser and operating system of the device of the wallet unit, the wallet unit shall use the CTAP 2.2 hybrid flow as specified in section 11.5 of [16] for cross-device communication between a browser and the device that the wallet unit is installed in.

(11) 6.4.1 Common requirements

– OIDFVP-HAIP_COMMON_RESP-02: void

– OIDFVP-HAIP_COMMON_RESP-03: void

– OIDFVP-HAIP_COMMON_RESP-04: void

– OIDFVP-HAIP_COMMON_RESP-06: void

– OIDFVP-HAIP_COMMON_RESP-07: void

– OIDFVP-HAIP_COMMON_RESP-08: void

– OIDFVP-HAIP_COMMON_RESP-09: void