Official Journal
of the European Union

EN
L series

2026/1731

22.7.2026

COMMISSION IMPLEMENTING REGULATION (EU) 2026/1731

of 15 July 2026

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

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ([1]), and in particular Article 5a(23) thereof,

Whereas:

(1) To ensure the highest level of harmonisation among Member States for the development of European Digital Identity Wallets, the technical specifications for the wallets rely on the work carried out on the basis of Commission Recommendation (EU) 2021/946 ([2]) and in particular the architecture and reference framework. As the architecture and reference framework has evolved significantly since Commission Implementing Regulations (EU) 2024/2977 ([3]), (EU) 2024/2979 ([4]), (EU) 2024/2980 ([5]), and (EU) 2024/2982 ([6]), those Implementing Regulations should now be amended to align them with new standards, specifications and procedures.

In accordance with the objectives of Regulation (EU) No 910/2014, a number of standards have been selected to meet these specific requirements. These standards should reflect established practices and be widely recognised within the relevant sectors. For example, as the W3C VCDM format is used as the reference format for attestations in particular in the educational sector, the European Digital Identity Wallets should also support this format when the new profiles on the W3C VCDM format are available. Where necessary, these standards should be adapted or complemented in order to ensure the security and trustworthiness of European Digital Identity Wallets, while facilitating cross-border interoperability and the effective functioning of the internal market.

(2) For any use of the wallet that requires the presentation of the wallet user's portrait, the wallet solutions must support the functionality of selective disclosure and disclosure must be under the full control of the user. To protect the ability to decide upon disclosure, and the portrait against unintended or unauthorised request for disclosure the architectural design of the European Digital Identity Wallets should provide for warning mechanisms and logging all transactions related to the use of the portrait. To ensure that the wallet user is aware of sharing biometric data, the warnings should indicate that the request involves the sharing of biometric data and specifically require the user to confirm disclosure. Where a relying party processes the portrait for the purpose of uniquely identifying a natural person or

([1]) OJ L 257, 28.8.2014, p.73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework (OJ L 210, 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).
([3]) Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets (OJ L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).
([4]) Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets (OJ L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).
([5]) Commission Implementing Regulation (EU) 2024/2980 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards notifications to the Commission concerning the European Digital Identity Wallet ecosystem (OJ L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).
([6]) Commission Implementing Regulation (EU) 2024/2982 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards protocols and interfaces to be supported by the European Digital Identity Framework (OJ L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

for confirming that person's claimed identity, Article 6 and 9 of Regulation (EU) 2016/679 of the European Parliament and of the Council ([7]) apply as well as all other requirements of that Regulation, including that the processing of the portrait by relying parties should be limited to what is necessary for intended use. The intended use should be communicated to the wallet user, together with the request for disclosure, in clear and intelligible language. To duly consider the sensitivity of biometric data, the wallet user should explicitly and specifically confirm the disclosure of the portrait. Silence or pre-ticked boxes should not be considered as confirmation by the wallet user. The explicit confirmation of the wallet user should be a technical safeguard and not in itself provide a legal ground for processing. As set out in paragraph 4 of Article 9 of Regulation (EU) 2016/679 Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

(3) To give Member States sufficient time to adapt their national procedures, the wallet user's portrait may be part of the mandatory person identification data for the natural person only as of 11 August 2028. Where these images are sourced from existing identity documents, such as identity cards or passports, the relevant requirements laid down in Council Regulations (EU) 2025/1208 ([8]) or (EC) No 2252/2004 ([9]) respectively apply.

(4) Regulation (EU) No 910/2014 requires that wallets are capable of displaying an EU Digital Identity Wallet Trust Mark, as a verifiable, simple, and recognisable indication that a wallet has been provided in accordance with the Regulation. The use of such a Trust Mark will support the effective functioning of the internal market, guarantee fair competition and protect consumer interests. To enable the use of such a Trust Mark, the visual and technical characteristics of the Trust Mark should be established.

(5) As set out in Article 12b of Regulation (EU) No 910/2014, gatekeepers are to allow providers of European Digital Identity Wallets and issuers of notified electronic identification means effective interoperability with, and, for the purposes of interoperability, access to, the same operating system, hardware or software features. Such effective interoperability and access are to be provided free of charge and irrespective of whether those hardware or software features form part of the operating system, are available to, or are used by, that gatekeeper when providing such services. As all wallet solutions should support a common set of protocols and interfaces in order to ensure usability, security and interoperability across Member States, gatekeepers should enable the operating system, hardware or software features necessary to implement the protocols and interfaces set out in Annex XII to this Regulation. In this context, in online cross-device flows, for both the physical proximity check and data transfer between the two devices, a local communication channel as enabled by the Client To Authenticator Protocol (CTAP) specification version 2.3 ([10]) should be preferred by gatekeepers to using CTAP Hybrid tunnel services.

(6) To give Member States, providers of wallet-relying party registration certificates and wallet providers sufficient time to enable wallet units to authenticate and validate wallet-relying party registration certificates, this requirement should only apply as of 11 August 2028.

(7) Regulation (EU) 2016/679 and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council ([11]) apply to all personal data processing activities under this Regulation.

([7]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([8]) Council Regulation (EU) 2025/1208 of 12 June 2025 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement (OJ L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (OJ L 385, 29.12.2004, p. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Fido Alliance proposed standard, Client to Authenticator Protocol (CTAP), February 26, 2026.

([11]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(8) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([12]) and delivered its opinion on 17 April 2026 ([13]).

(9) The measures provided for in this Regulation are in accordance with the opinion of the committee established by Article 48 of Regulation (EU) No 910/2014,

HAS ADOPTED THIS REGULATION:

Article 1

Amendments to Implementing Regulation (EU) 2024/2977

Implementing Regulation (EU) 2024/2977 is amended as follows:

(1) The following Article 3a is inserted:

'*Article 3a*

Protection of the portrait

1. In addition to information requirements pursuant to Regulation (EU) 2016/679, wallet providers shall ensure that the wallet solutions they provide issue warnings to wallet users where wallet-relying parties request the disclosure of the portrait, indicating that the request involves the sharing of biometric data and requires confirmation for the selective disclosure of the portrait.

2. For the implementation of selectively disclosing the portrait to a wallet-relying party, the wallet providers shall ensure the wallet solutions require the wallet user to explicitly and specifically confirm the presentation of the portrait.

3. The portrait shall not be retained by wallet-relying parties unless its processing is necessary for the purposes of identification and authentication in compliance with Union data protection law or where this is provided for by Union or national law, in compliance with Union data protection law. The portrait shall not be transferred to third countries or international organisations unless permitted by Union data protection law.';

(2) in Article 4, paragraph 1 is replaced by the following:

'1. Electronic attestations of attributes issued to wallet units shall comply with at least one of the standards set out in Annex II of Implementing Regulation (EU) 2024/2979.';

(3) in Article 5, paragraph 4, point (b) is replaced by the following:

'(b) where the wallet unit attestation of the wallet unit to which the person identification data was issued to has been revoked;';

(4) The Annex is replaced by the text set out in Annex I to this Regulation.

([12]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([13]) EDPS Formal comments on the draft Implementing Regulation as regards applicable standards and specifications and correcting Implementing Regulation (EU) 2024/2980 | European Data Protection Supervisor.

Article 2

Amendments to Implementing Regulation (EU) 2024/2979

Implementing Regulation (EU) 2024/2979 is amended as follows:

(1) in Article 3, paragraph 2 is deleted;

(2) in Article 5, paragraph 1, point (a) is replaced by the following:

'(a) perform wallet cryptographic operations involving critical assets, stored in a wallet secure cryptographic device and not required for the authentication of the wallet user only in cases where those applications have successfully authenticated wallet users;';

(3) the following Article 5a is inserted:

'*Article 5a*

Cryptographic mechanisms

Wallet providers shall, for the purposes of paragraph 2 of Article 4, use only the cryptographic mechanisms referred to in Annex Ia.';

(4) Article 6 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. Wallet providers shall issue wallet unit attestations for each wallet unit. Wallet providers shall sign or seal the wallet unit attestations in a way that the signatures or seals can be validated by means of a certificate listed in accordance with Annex II section 2, point (1), letter (h) of Implementing Regulation (EU) 2024/2980.';

(b) paragraph 2 is replaced by the following:

'2. Wallet providers shall ensure that the wallet unit attestations referred to in paragraph 1 comply with the technical specifications set out in Annex Ib.';

(c) in paragraph 3, point (b) is replaced by the following:

'(b) provide secure identification and authentication mechanisms for wallet users that are independent of wallet units';

(5) in Article 9, paragraph 2, point (b) is replaced by the following:

'(b) the name, contact details, and the unique identifier of the corresponding wallet-relying party and the Member State in which that wallet-relying party is established;';

(6) in Article 10, paragraph 1 is replaced by the following:

'1. Wallet providers shall ensure that electronic attestations of attributes issued in accordance with the technical specifications applicable for common embedded disclosure policies set out in Annex III can be processed by the wallet units that they provide.';

(7) Article 12 is amended as follows:

(a) paragraph 2, point (c) is replaced by the following:

'(c) creating signatures or seals in accordance with at least the mandatory signature or seal format referred to in Annex IV;';

(b) paragraph 3 is replaced by the following:

'3. The signature creation applications may either be integrated into or be external to wallet instances.';

(c) the following paragraph is inserted:

'4. The signature creation applications used by wallet units shall support at least the application programming interface referred to in Annex IV.';

(8) in Article 14, paragraph 1 is deleted;

(9) the following Article 14a is inserted:

'*Article 14a*

EU Digital Identity Wallet Trust Mark

1. Wallet providers shall ensure that wallet units display the EU Digital Identity Wallet Trust Mark. The EU Digital Identity Wallet Trust Mark shall be in the form set out in Annexes VI and VII.

2. Wallet providers shall ensure that wallet units enable wallet users to access information allowing them to verify the certification status of the wallet solution. For that purpose, wallet providers shall ensure that, following the registration of a wallet solution, the corresponding wallet units include the URLs provided by the European Commission for such verification. Wallet providers shall ensure that their wallet units have access to EU Digital Identity Wallet Trust Mark data that comply with the technical specifications set out in Annex VIII.

3. The reference colours for the EU Digital Identity Wallet Trust Mark shall be Pantone No 661 and 116, or blue (100 % cyan + 67 % magenta + 0 % yellow + 40 % black) and yellow (0 % cyan + 20 % magenta + 100 % yellow + 0 % black), when a four colour process is used; when RGB colours are used the reference colours shall be blue (0 red + 51 green + 153 blue) and yellow (255 red + 204 green + 0 blue).

4. Only where the use of colour is not practicable, the EU Digital Identity Wallet Trust Mark may be used in black and white as set out in Annex VII.

5. Where the EU Digital Identity Wallet Trust Mark is used on a dark background, it may be used in negative format using the same background colour. Where the EU Digital Identity Wallet Trust Mark is used in colour on a coloured background that makes it difficult to see it, a delimiting outer line around the EU Digital Identity Wallet Trust Mark may be used to improve contrast with the background colours.

6. The EU Digital Identity Wallet Trust Mark shall have a minimum size of 64 × 85 pixels at 150 dpi.

7. Wallet providers shall ensure that the EU Digital Identity Wallet Trust Mark is used in a manner enabling the clear indication of the wallet unit that the EU Digital Identity Wallet Trust Mark pertains to. The EU Digital Identity Wallet Trust Mark may be associated with graphic or textual elements clearly indicating the wallet unit it is used for, provided that they do not change its recognisability as an EU Digital Identity Wallet Trust Mark, nor alter the association with the list of certified European Digital Identity Wallets referred to in Article 5d of Regulation (EU) No 910/2014.

8. Where wallet providers have revoked a wallet unit attestation, they shall ensure that the EU Digital Identity Wallet Trust Mark is no longer displayed by the corresponding wallet unit.'.

(10) Annexes Ia and Ib are added as set out in Annex II and Annex III to this Regulation.

(11) Annex II is replaced by Annex IV to this Regulation.

(12) Annex III is replaced by Annex V to this Regulation.

(13) Annex IV is amended in accordance with Annex VI to this Regulation.

(14) Annex V is deleted.

(15) The text set out in Annex VII to this Regulation is inserted as Annex VI.

(16) The text set out in Annex VIII to this Regulation is inserted as Annex VII.

(17) The text set out in Annex IX to this Regulation is inserted as Annex VIII.

Article 3

Amendments to Implementing Regulation (EU) 2024/2980

Implementing Regulation (EU) 2024/2980 is amended as follows:

1. in Article 5, paragraph 2 is replaced by the following:

   '2. Where applicable, the Commission shall establish, maintain and publish a list compiling the information notified by Member States on wallet providers, providers of person identification data, providers of wallet-relying party access certificates and providers of wallet-relying party registration certificates, as referred to in Annex II, sections 2, 3, 4 and 5.';

2. Annex II to Implementing Regulation (EU) 2024/2980 is amended as set out in Annex X to this Regulation.

Article 4

Amendments to Implementing Regulation (EU) 2024/2982

Implementing Regulation (EU) 2024/2982 is amended as follows:

(1) in Article 1, paragraph 2 is replaced by the following:

   '(2) the presentation of attributes of person identification data and electronic attestations of attributes to wallet-relying parties;';

(2) Article 3 is amended as follows:

   (a) paragraph (1) is replaced by the following:

      '(1) authenticate and validate the wallet-relying party access certificates where interacting with wallet-relying parties without delegating execution of these processes to an operating system browser or other intermediary application;';

   (b) paragraph (2) is deleted;

   (c) paragraph (3) is replaced by the following:

      '(3) authenticate and validate requests made using wallet-relying party access certificates;';

   (d) paragraph (4) is replaced by the following:

      '(4) authenticate and validate the wallet-relying party registration certificate;';

   (e) paragraph (5) is replaced by the following:

      '(5) display to wallet users information contained in the wallet-relying party access certificates;';

   (f) paragraph (8) is deleted;

   (g) paragraph (9) is replaced by the following:

      '(9) do not present any requested attributes to wallet-relying parties until the following steps have been completed:

         (a) verification that embedded disclosure policies have been processed within the wallet unit in accordance with Article 10 of Implementing Regulation (EU) 2024/2979;

         (b) verification that wallet users have partially or in full approved the presentation.';

(3) in Article 4, paragraph 1 is replaced by the following:

   '1. Wallet providers shall ensure that wallet solutions support the protocols and interfaces set out in Annex I for the issuance of person identification data and electronic attestations of attributes to wallet units.';

(4) Article 5 is amended as follows:

(a) paragraphs 1 and 2 are replaced by the following:

'1. Wallet providers shall ensure that wallet solutions support protocols and interfaces for the presentation of attributes to wallet-relying parties, remotely, and, where appropriate, in proximity, in accordance with the technical specifications set out in Annex II.

2. Wallet providers shall ensure that, at the request of users, wallet units respond to successfully authenticated and validated requests from wallet-relying parties referred to in Article 3, in accordance with the technical specifications set out in Annex II.';

(b) paragraph 5 is deleted.

(5) Article 8 is replaced by the following:

'*Article 8*

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Article 3(4) shall apply from 11 August 2028.

This Regulation shall be binding in its entirety and directly applicable in all Member States.'.

(6) The Annex is deleted.

(7) The text set out in Annex XI to this Regulation is added as Annex I.

(8) The text set out in Annex XII to this Regulation is added as Annex II.

Article 5

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 15 July 2026.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX I

'ANNEX

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

1. Section 1: Set of natural person identification data

Table 1

Mandatory person identification data for the natural person for selective disclosure

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`	Except where the user explicitly opts out, where applicable, the facial image of the user to whom the person identification data relates, compliant with the quality requirements for a full frontal image type as set out in ISO/IEC 39794-5 or, for backward compatibility, ISO/IEC 19794-5, clauses 8.2, 8.3 and 8.4, provided as encoded image data without the headers or blocks as specified in clause 5 of ISO/IEC 19794-5, except for the image data itself (a JPEG) shall apply from 11 August 2028.

— Member States may provide that the user has the option to decline the insertion of the portrait to the person identification data.

— Member States shall ensure that the selective disclosure applies to each data identifier, including the portrait.

— Where the birth date of the natural person is not known, Member States shall choose appropriate values that comply with the specifications set out in sections 4.1 or 4.2 (as appropriate) to this Annex.

— Where the nationality of the natural person is unknown, Member States shall use the value 'QU'.

— Where the natural person does not hold a nationality, Member States shall use the value 'QS'.

— Where the user opts out of the inclusion of the portrait, Member States shall set the value empty.

Table 2

Optional person identification data for the natural person for selective disclosure

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, including the house number and any affix or suffix thereof.
personal_administrative_-number	A value assigned to the user to whom the person identification data relates 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 user to whom the person identification data relates at the time of birth.
given_name_birth	First name(s), including middle name(s), of the user to whom the person identification data relates 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 accordance with RFC 5322 ([1])].

Data identifier	Definition
`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.

([1]) P. Resnick, Ed., 'Internet Message Format,' RFC 5322, October 2008.

2. Section 2: Set of legal person identification data

Table 3

Mandatory person identification data for the legal person

Data identifier
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 identifier 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 identifier
current address
VAT registration number
tax reference number
European unique identifier referred to in Directive (EU) 2017/1132 of the European Parliament and of the Council ([1])
Legal Entity Identifier (LEI) referred to in Commission Implementing Regulation (EU) 2022/1860 ([2])
Economic Operator Registration and Identification (EORI) referred to in Commission Implementing Regulation (EU) No 1352/2013 ([3])
excise number provided in Article 2(12) of Council Regulation (EU) No 389/2012 ([4])

([1]) Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (OJ L 169, 30.6.2017, p. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Commission Implementing Regulation (EU) 2022/1860 of 10 June 2022 laying down implementing technical standards for the application of Regulation (EU) No 648/2012 of the European Parliament and of the Council with regard to the standards, formats, frequency and methods and arrangements for reporting (OJ L 262, 7.10.2022, p. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Commission Implementing Regulation (EU) No 1352/2013 of 4 December 2013 establishing the forms provided for in Regulation (EU) No 608/2013 of the European Parliament and of the Council concerning customs enforcement of intellectual property rights (OJ L 341, 18.12.2013, p. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) C ouncil Regulation (EU) No 389/2012 of 2 May 2012 on administrative cooperation in the field of excise duties and repealing Regulation (EC) No 2073/2004 (OJ L 121, 8.5.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3. Section 3: Set of metadata about person identification data

Table 5

Metadata about the person identification data

Data identifier	Definition	Presence
`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 3166-1, of the country or territory of the provider of the person identification data.	mandatory
`expiry_date`	Date (and if possible time) when the administrative validity period of the person identification data will expire.	optional
`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
`issuance_date`	Date, and if possible time, when the administrative validity period of the person identification data started.	optional

4. Section 4: Encoding of natural person identification data attributes

— Natural person identification data shall be issued in accordance with the standards set out in Annex II to Implementing Regulation (EU) 2024/2979, clauses 5 (SD-JWT VC format) and 6 (ISO/IEC-mdoc format) as applicable to electronic attestations of attributes. Clauses 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3,6.2.4 and 6.2.5 shall not apply.

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

4.1 Encoding of natural 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 set out in this Annex shall be 'eu.europa.ec.eudi.pid.1'.

— Where the person identification data includes data for which data identifiers are not set out in this Annex, these data 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, its scheme, including all data identifiers, their definitions, presence and encoding formats, shall be published in accordance with Article 8 of Commission Implementing Regulation (EU) 2025/1569 ([1]).

— The person identification data and its metadata set out in sections 1 and 3 of this Annex shall be included in person identification data elements within the meaning of ISO/IEC mdoc format specifications.

— The deviceKey member within the deviceKeyInfo member of the instance of MobileSecurityObject type shall contain a public key.

— That public key shall correspond to a private key that is stored in the wallet secure cryptographic device ('WSCD') of the wallet user.

— The Protected Header of the CB-AdES digital signature signing a person identification data in ISO/IEC-mdoc format shall contain the x5u and the x5t header parameters, both specified in RFC 9360 ([2]).

— The digest algorithm used in the x5t header parameter shall be SHA-256.

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

Table 6

Requirements for 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
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

([1]) Commission Implementing Regulation (EU) 2025/1569 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards 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 (OJ L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([2]) J. Schaad, 'CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates' (https://datatracker.ietf.org/doc/rfc9360/).

Data Identifier	Attribute identifier	Encoding format
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
issuance_date	issuance_date	tdate or full-date

— The notation of the encoding format of the attributes specified in Table 6 shall use representation types as specified in RFC 8610 ([3]), 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 ([4]);

(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 ([5]);

(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 and the time-offset specified in RFC 3339 shall be set to 'Z'.

(i) an integer with major types 0 and 1 shall be as small as possible, as specified in RFC 8949 ([6]), 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, as specified in RFC 8949, section 4.2;

([3]) C. Vigano and H. Birkholz, 'Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures', RFC 8610, June 2019.
([4]) M. Jones, A. Nadalin and J. Richter, 'Concise Binary Object Representation (CBOR) Tags for Date', RFC 8943, November 2020.
([5]) G. Klyne and C. Newman, 'Date and Time on the Internet: Timestamps', RFC 3339, July 2002.
([6]) C. Bormann and P. Hoffman, 'Concise Binary Object Representation (CBOR)', RFC 8949, December 2020.

(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 a 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 for encoding person identification data in SD-JWT VC format

— The person identification data and its metadata specified in this section shall be included in a person identification data as claims in the meaning of SD-JWT VC format specifications.

— 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 format.

— 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 Table 8 below or the references therein.

— The JWT claims nbf and exp as defined in RFC 7519 ([7]) shall be used to express the technical validity period of person identification data compliant with SD-JWT VC format.

([7]) J. Jones, et al., 'JSON Web Token (JWT)', RFC 7519, May 2015.

— Person identification data shall incorporate the cnf claim as defined in RFC 7800 ([8]), which shall be a public key generated from a private key stored in the WSCD of the wallet users wallet unit.

— The Protected Header of the digital signature signing a person identification data in SD-JWT VC format shall contain the x5u and the x5t#S256 header parameters, specified in RFC 7515 ([9]).

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
`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

([8]) M. Jones, et al., 'Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)', RFC 7800, April 2016.
([9]) M. Jones, et al., 'JSON Web Signature (JWS)', RFC 7515, May 2015.

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, ISO 8601-1, YYYY-MM-DD format
`issuance_date`	`date_of_issuance`	string, ISO 8601-1, YYYY-MM-DD format
`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

— 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 includes attributes that are not specified in this Annex, these attributes shall be defined within a domestic type.

— Where the domestic type is used, its scheme, including all data identifiers, their definitions, presence and encoding formats, shall be defined in a scheme that is published in accordance with Article 8 of Implementing Regulation (EU) 2025/1569.

5. Section 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 the 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 unit attestations referred to in Article 6(2a)

1. A wallet unit attestation shall comprise one or more wallet instance attestations and one or more key attestations.

2. The wallet instance attestation and the key attestations shall meet the following requirements:

(a) Format requirements

— FR-WIA-1: A wallet instance attestation shall be a JSON Web Token (JWT) as specified in RFC 7519 ([1]), signed or sealed by the wallet provider by means of compact JAdES baseline B signature.

— FR-WIA-1.1: A wallet instance attestation shall be a wallet attestation as specified in Appendix E of OpenID for Verifiable Credential Issuance v1.0 ([2]) ('OID4VCI') and extended as specified in C-WIA-1 and C-WIA-2 below.

— FR-KA-1: A key attestation shall be a JWT as specified in RFC 7519, signed or sealed by the wallet provider by means of compact JAdES baseline B signature.

— FR_KA_1.1: A key attestation shall be a key attestation as specified in Appendix D of OID4VCI, extended as specified in C_KA-1 and C_KA-2 below.

(b) Transport requirements

— TR-WIA-1: A wallet unit shall use a wallet instance attestation during the issuance of person identification data, qualified or non-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.

— TR-WIA-2: A wallet provider shall verify the integrity of the wallet instance and sign or seal the wallet instance attestation.

— TR-WIA-2.1: Where a wallet provider issues a wallet instance attestation, the difference between the time when the wallet provider verified the integrity of the wallet instance and the time they will indicate in the 'exp' header parameter of the issued wallet instance attestation shall be less than 24 hours.

— TR-WIA-2.2: The wallet provider shall ensure that a wallet unit contains wallet instance attestations as needed for issuance of person identification data and electronic attestations of attributes.

— TR-WIA-3: During issuance, a wallet unit shall send a wallet instance attestation to the authorisation server in the pushed authorisation request and the token request, as specified in OID4VCI.

— TR-WIA-3.1: A wallet unit shall send the wallet instance attestation together with a Proof-of-Possession ('PoP') as specified in Appendix E of OID4VCI.

— TR-WIA-3.2: A wallet unit shall send the same wallet instance attestation to only one authorisation server.

([1]) RFC 7519: JSON Web Token (JWT), May 2015.
([2]) OpenID for Verifiable Credential Issuance v1.0, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

- TR-WIA-3.2.1: Where a wallet provider uses the 'per-issuer reuse' option specified in R_WIA_1 below, a wallet unit may send a wallet instance attestation to the same authorisation server multiple times.

- TR-WIA-3.2.2: Where a wallet provider does not use the 'per-issuer reuse' option, a wallet unit shall use a wallet instance attestation in at most one issuance process.

— TR-WIA-4: Where an authorisation server receives a wallet instance attestation, it shall verify the signature of the wallet instance attestation using the public key in the signing certificate included in the 'x5c' parameter in the JOSE header of the wallet instance attestation.

- TR-WIA-4.1: The authorisation server shall also verify that this signing certificate can be verified with a trust anchor on the list of wallet providers referred to in Article 5 of Implementing Regulation (EU) 2024/2980, potentially using intermediate certificates included in the x5c parameter.

- TR-WIA-4.2: The authorisation server shall verify that the wallet instance attestation has not expired.

- TR-WIA-4.3: The authorisation server shall verify the signature of the PoP under the public key present in the 'cnf' claim.

— TR_KA-1: A wallet unit shall use a key attestation during the issuance of person identification data and during the issuance of device-bound qualified or non-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.

- TR_KA-1.1: A wallet unit shall not use a key attestation during the issuance of non-device-bound qualified or non-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.

— TR_KA-2: A wallet provider shall provide a wallet unit with different key attestations for the WSCD of the wallet unit and for each of its keystores.

- TR_KA-2.1: The wallet provider shall sign or seal a key attestation, after the wallet provider has verified that the keys attested to in the key attestation are stored in the WSCD of the wallet unit or keystore described in the key attestation.

- TR_KA-2.2: A key attestation shall contain at least one attested public key. The number of keys in the key attestation sent to a credential issuer should not exceed the maximum batch size specified by that credential issuer in its Credential Issuer metadata; see ETSI TS 119 472-3 ([3]), parameter 'credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size'.

- TR_KA-2.3: A wallet provider shall include a public key (corresponding to a private key stored in the WSCD or keystore of the wallet unit) in at most one key attestation.

- TR_KA-2.4: A wallet unit shall use a key attestation during at most one credential issuance or re-issuance process.

- TR_KA-2.5: A wallet provider shall ensure that a wallet unit is in possession of key attestations as needed for issuance of person identification data and device-bound electronic attestations of attributes.

([3]) ETSI, 'Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 3: JAdES levels and baseline profiles', ETSI TS 119 472-3, V1.1.1, March 2026.

— TR_KA-3: Where needed during issuance, a wallet unit shall include a key attestation in the field 'proofs' of a Credential Request to the credential issuer, as specified in OID4VCI, in a proof of either type 'jwt' or type 'attestation'.

— TR_KA_3.1: Where a wallet unit includes a key attestation in a 'jwt' element, it shall sign or seal the key attestation using the private key corresponding to the public key at index 0 of the 'attested_keys' array within the 'key_attestation' object.

— TR_KA-4: Where a credential issuer issues device-bound credentials, it shall indicate in the 'proof_types_supported' parameter in its Issuer Credential Metadata, as specified in Section 12.2.4 OID4VCI, that it supports both the 'jwt' and the 'attestation' proof type for key attestations that shall include the 'key_attestations_required' object.

— TR_KA-4.1: Where a credential issuer issues non-device-bound credentials, it shall omit the 'proof_types_supported' and the 'cryptographic_binding_methods_supported' parameters in the Credential Issuer Metadata.

— TR_KA-5: Where a credential issuer receives a key attestation in a 'jwt' or an 'attestation' proof type, it shall verify the signature of the key attestation under the public key in the signing certificate included in the 'x5c' parameter in the JOSE header of the key attestation and that this signing certificate with a trust anchor on the list for wallet providers referred to in Article 5 of Implementing Regulation (EU) 2024/2980, potentially using intermediate certificates included in the 'x5c' parameter.

— TR_KA-6: Where a credential issuer receives a key attestation in a 'jwt' proof type, it shall verify the signature of the 'jwt' element under the key at index 0 of the 'attested_keys' array within the 'key_attestation' object included in the 'jwt' element.

— TR_KA-6.1: The credential issuer shall verify that the 'nonce' field of the 'jwt' element includes a valid c_nonce from their nonce_endpoint, as specified in OID4VCI.

— TR_KA-7: Where a credential issuer receives a key attestation in an 'attestation' proof type, it shall verify that the 'key_attestation' object includes a valid c_nonce from their nonce_endpoint.

— TR_KA-8: A provider of person identification data shall ensure that person identification data is bound to a public key that originates from a key attestation mentioning a WSCD.

(c) Content requirements

— C_WIA-1: A wallet instance attestation shall include the following:

— the 'wallet_name' claim specified in Appendix E of OID4VCI, where its value shall be the identifier of the wallet solution that can be found on the list of wallet providers referred to in Article 5 of Implementing Regulation (EU) 2024/2980.

— a 'wallet_version' claim ([4]), that shall be a string whose value shall be the version of the wallet solution.

— a 'wallet_solution_certification_information' claim, that shall be a JSON object containing information about the conformity assessment body that certified the wallet solution, the certification number, as applicable, and other relevant details as regards certification.

([4]) This claim is defined in this CIR as it is not part of the OID4VCI specification.

- a 'client_status' claim, containing two sub-fields:
  - 'status': a status list reference as specified in Appendix E of OID4VCI that represents the revocation status of the wallet instance. See section (e) below for details;
  - 'exp': a NumericDate, as specified in RFC 7519, defining the time until which the wallet provider will maintain the revocation status at the status list index referenced in 'status'.
- the 'exp' claim specified in Appendix E of OID4VCI.

— *NOTE*: The 'client_status.status' claim in a wallet instance attestation represents the revocation status of the wallet instance, not the revocation status of the attestation itself. As described in R_WIA-1 below, a wallet provider can decide to scope each wallet instance attestation to a specific authorisation server based on the fact that all attestations sent to that server contain the same index value in the 'client_status.status' entry.

— *NOTE*: The 'idx' value in the 'status' claim can be used as a (pairwise) unique identifier of the wallet instance and of the wallet unit.

— C_WIA-2: A wallet instance attestation should also include the 'wallet_link' claim specified in Appendix E of OID4VCI and the value of this claim shall be a URI where further information about the wallet solution can be obtained.

— C_WIA-3: An authorization server shall not interpret the 'exp' parameter in the top level of a wallet instance attestation as the end of the revocation maintenance period of the wallet instance.

— *NOTE*: The 'exp' parameter in the top level of a wallet instance attestation denotes when the attestation itself expires.

— C_KA-1: A key attestation shall include:
  - the 'key_storage' and 'user_authentication' claims specified in Appendix D of OID4VCI.
    - The 'key_storage' and 'user_authentication' attributes shall have value 'iso_18045_high' where a key attestation mentions a WSCD,
  - the 'certification' claim specified in Appendix D of OID4VCI, containing a URL where information can be obtained about the certification achieved by the WSCD or keystore, indicatively the scheme such as Common Criteria or GlobalPlatform, the evaluated requirements such as the applicable Protection Profile, and the evaluation level.
    - It shall be possible to determine from this information whether the key storage is a WSCD.
  - a 'key_storage_status' claim, containing two sub-fields:
    - 'status': a status list reference as specified in Appendix D.1 of OID4VCI. The value represents either the revocation status of the WSCD or keystore type used to store the attested keys, or -- under the per-key-attestation index option -- the revocation status of an individual wallet unit's WSCD or keystore. See R_KA_1 below for the available index assignment options;
    - 'exp': a NumericDate, as specified in RFC 7519, defining the time until which the wallet provider will maintain the revocation status at the status list index referenced in 'status'.
  - the 'exp' claim specified in Appendix D of OID4VCI.

— *NOTE* on the 'idx' value in the 'key_storage_status.status' claim in a key attestation: Where the wallet provider uses the 'type-shared index' option (see R_KA_1 below), all key attestations for the same type of WSCD or keystore share the same status list index. Therefore, the 'idx' value is not unique per wallet unit. On the contrary, where the wallet provider uses the 'per-key-attestation index' option, the 'idx' value is unique to the wallet unit (or pairwise unique per credential issuer). In all cases, however, a credential issuer shall not use the 'idx' value in a key attestation as a wallet unit identifier, but shall instead use the 'idx' value in a wallet instance attestation.

— C_KA-2: Where a key attestation is sent in an 'attestation' proof type, it shall also include a valid c_nonce as specified in Appendix F.3 of OID4VCI.

— C_KA-3: A credential issuer shall not interpret the 'exp' parameter in the top level of a key attestation as the end of the revocation maintenance period of the WSCD or keystore.

— *NOTE*: The 'exp' parameter in the top level of a key attestation denotes when the key attestation itself expires.

(d) Life cycle requirements

— This Annex specifies the following Credential Issuer metadata parameters:

  — 'preferred_client_status_period': OPTIONAL. An integer specifying the preferred remaining status maintenance period of the wallet instance attestation to be presented by the wallet unit during issuance, in seconds. The remaining status maintenance period is defined as the value of 'client_status.exp' in the attestation minus the time of reception of the attestation.

  — 'preferred_key_storage_status_period': OPTIONAL. An integer specifying the preferred remaining status maintenance period of the key attestation to be presented by the wallet unit during issuance, in seconds. The remaining status maintenance period is defined as the value 'key_storage_status.exp' in the attestation minus the time of reception of the attestation.

— LC_WIA-1: An authorisation server may communicate its preferences for the remaining status maintenance period in wallet instance attestations by including the 'preferred_client_status_period' metadata parameter in their Credential Issuer metadata endpoint as specified in Section 12.2.2 of OID4VCI.

  — LC_WIA-1.1: This field shall be placed at the top level of the Credential Issuer metadata.

— LC_WIA_2: An authorisation server shall not interpret the 'exp' parameter in the top level of a wallet instance attestation as the end of the revocation maintenance period of the wallet instance.

— LC_WIA_3: Where a wallet provider signs or seals a wallet instance attestation, it shall maintain the revocation status of the relevant wallet instance until the 'wallet_instance_status.exp' indicated in that wallet instance attestation has passed.

— LC_KA-1: Where a key attestation is needed, a credential issuer may communicate its preferences for the remaining status maintenance period in key attestations by including the 'preferred_key_storage_status_period' metadata parameter specified above in their Credential Issuer Metadata endpoint as specified in Section 12.2.2 of OID4VCI.

  — LC_KA-1.1: This field shall be placed within the 'key_attestations_required' object as specified in Section 12.2.4 of OID4VCI.

— LC_KA-2: A wallet provider shall choose the technical validity period of the key attestations it issues.

— LC_KA-3: Where a wallet provider signs or seals a key attestation, it shall maintain the revocation status of the relevant WSCD or keystore until the 'key_storage_status.exp' indicated in that key attestation has passed.

— LC_GEN-1: A wallet provider shall ensure that a wallet unit can always present wallet unit attestations and key attestations whose 'client_status.exp' and 'key_storage_status.exp' (respectively) are at least 31 days in the future at the time of presentation to an authorization server or credential issuer.

— *NOTE*: This guarantees that providers of person identification data can rely on revocation chaining without being forced to issue short-lived person identification data.

— LC_GEN-2: A wallet provider shall ensure that a wallet unit fetches the Credential Issuer metadata during issuance.

  — LC_GEN_2.1: If a 'preferred_key_storage_status_period' field is included in this metadata, then the wallet unit shall send a key attestation with ('key_storage_status.exp' – current time) – 'preferred_-key_storage_status_period' as small as possible but non-negative. If no such key attestation is available to the wallet unit, it shall obtain a new key attestation from the wallet provider that satisfies 'key_storage_status.exp' – current time ≥ 'preferred_key_storage_status_period'.

  — LC_GEN_2.2: If a 'preferred_client_status_period' field is included in this metadata, then the wallet unit shall send a wallet instance attestation with ('client_status.exp' – current time) – 'preferred_-client_status_period' as small as possible but non-negative. If no such wallet instance attestation is available to the wallet unit, it shall request a new wallet instance attestation from the wallet provider that satisfies 'client_status.exp' – current time ≥ 'preferred_client_status_period'.

— LC_GEN-3: The technical validity period of person identification data shall end before both the 'client_status.exp' of the wallet instance attestation and the 'key_storage_status.exp' of the key attestation sent to the provider of person identification data in the issuance process.

— LC_GEN-4: A provider of person identification data having a technical validity period of more than 24 hours shall check the revocation status of both the wallet instance attestation and the key attestation received during issuance at least once every 24 hours, during the technical validity period of the person identification data. Where either is revoked, the provider shall revoke the person identification data.

(e) Revocation requirements

— R_GEN-1: A wallet provider shall use Token Status Lists (specified in IETF Token Status List) as the revocation mechanism for both key attestations and wallet instance attestations, as specified in OID4VCI Appendix D and E, respectively.

— *NOTE*: To improve scalability of its status lists, a wallet provider can use the following optimisations:

  — Dividing the status list into multiple chunks, where the wallet providers have a sizeable number of users and issued attestations. Many chunking strategies exist, for example based on a fixed size or by time period. The strategy for chunking is left to wallet provider discretion. Considerations can include the size of a status list for downloading and the privacy of the user.

  — Having multiple status lists.

  — Compressing a status list to reduce its size.

— R_WIA-1: A wallet provider may assign the same value to the 'idx' claim in the 'client_status.status' claim in all wallet instance attestations that a given wallet unit presents to the same authorization server. This is called the 'per-issuer reuse' option. If this option is used:

  — R_WIA-1.1: The wallet unit shall maintain state on which index value it has used for each authorization server it has previously interacted with, and shall request a wallet instance attestation containing that same index value when interacting with the same authorization server again.

  — R_WIA-1.2: Where a wallet provider receives a request for a wallet instance attestation containing a specific index value, it shall verify that the requesting wallet unit has received that index value previously, before issuing a new wallet instance attestation with that index value.

  — R_WIA-1.3: The wallet unit shall not reuse the same index value for interactions with different authorization servers.

— *NOTE*: If the 'per-issuer reuse' option is used, the wallet provider will be able to determine how many authorization servers a wallet unit has interacted with and how frequently it interacts with each.

— R_WIA-2: In its privacy policy, a wallet provider shall document whether it uses the 'per-issuer reuse' option for wallet instance revocation.

— R_WIA-3: Where a wallet provider does not use the 'per-issuer reuse' option, the wallet provider shall assign a fresh, unlinkable index value to each wallet instance attestation it issues.

— R_WIA-4: Where a wallet unit must be revoked, a wallet provider shall revoke the index values in the 'client_status.status' claim in all wallet instance attestations associated with that wallet unit.

— R_WIA-5: A wallet provider shall take into consideration the scale of its deployment and the underlying architecture when determining the size of its wallet instance attestation status lists, ensuring that they are sufficiently large to prevent correlation and protect user privacy. At a minimum, a status list shall, where possible, relate to at least 10 000 attestations.

— R_KA_1: A wallet provider shall choose one of the following index assignment options for the 'key_storage_status.status' claim in a key attestation:

  — Option 1, called 'type-shared index', in which all key attestations attesting keys stored in the same type of WSCD or keystore contain the same index value in 'key_storage_status.status'.

  — Option 2, called 'per-key-attestion index', in which a key attestation attesting keys stored in an individual WSCD or keystore contains a (pairwise) unique index value in 'key_storage_status.status'.

— *NOTE*: Where a wallet provider uses option 1, a single revocation action invalidates all key attestations of the affected type across all wallet units. Moreover, because all key attestations for the same type of WSCD or keystore share a single status list index, the number of entries in a key attestation status list reflects the number of WSCD or keystore types supported by the wallet provider, not the number of deployed wallet units. The privacy considerations that motivate the minimum status list size for wallet instance status lists therefore do not apply to key attestation status lists under option 1, provided that there are sufficiently many wallet units using the same type of WSCD or keystore.

— *NOTE*: Where a wallet provider uses option 2, each index represents the revocation state of the specific WSCD or keystore attested in that key attestation.

— *NOTE*: Where a wallet provider uses option 2, a specific WSCD or keystore can also be revoked on User request.

— R_KA-2: Where a wallet provider uses option 2, the wallet provider may optionally use the 'per-issuer reuse' option described in R_WIA-1. If the wallet provider uses this option, the requirements R_WIA-1 - R_WIA-3 shall apply mutatis mutandis.

— R_KA-3: Where a wallet provider uses option 2, the wallet provider shall take into consideration the scale of its deployment and the underlying architecture when determining the size of its key attestation status lists, ensuring that they are sufficiently large to prevent correlation and protect user privacy. At a minimum, a status list shall, where possible, relate to at least 10 000 key attestations.

— R_KA-4: Where a wallet provider uses option 1 (type-shared index), the wallet provider shall only revoke a 'key_storage_status.status' entry if the type of WSCD or keystore has a security vulnerability.

(f) Requirements regarding signature algorithms

— SA-1: For signing wallet instance attestations, key attestations, related proof-of-possessions and token status lists, one of the following algorithms shall be used:

  — ES256 (ECDSA with SHA-256 and P-256)

  — ES384 (ECDSA with SHA-384 and P-384)

  — ES512 (ECDSA with SHA-512 and P-521)

— SA-2: A wallet provider shall choose which of the algorithms mentioned in SA-1 it will use.

— SA-3: An authorization server or a credential issuer (as specified in OID4VCI) shall support all of the algorithms mentioned in SA-1.'

ANNEX IV

'ANNEX II

List of standards referred to in Article 8

The technical specifications set out in clauses 2 to 6 of ETSI TS 119 472-1 V1.2.1 (2026-02) apply. They shall be read with the following adaptations:

(1) 2.1 Normative references

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): '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-oauth-status-list-20: 'Token Status List', 20 April 2026.

(2) 4.2.11.1 General requirements

— EAA-4.2.11.1-06: When a 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, it shall only indicate whether the attestation is revoked or not revoked and shall not support any other status values, such as suspension.

— EAA-4.2.11.1-06.1: Where an attestation is revoked, it shall be permanently revoked.

(3) 4.2.13 EAA short-lived

— EAA-4.2.13-03: Where short-lived electronic attestations of attributes with a validity period of 24 hours or less are issued, revocation shall not be required.

(4) 4.6.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (PuB-EAA)

— PuB-EAA-4.6.2-03: void.

— Pub-EAA-4.6.2-04: void.

— PuB-EAA-4.6.3-03: The PuB-EAA digital signature should contain the qualified certificate supporting the PuB-EAA digital signature.

— PuB-EAA-4.6.3-04: The qualified certificate supporting the PuB-EAA digital signature shall meet the requirements of clause 8 of ETSI TS 119 412-6 v1.1.1 and shall contain the QcType qcStatement as defined in ETSI EN 319 412-5 v2.5.1, with the value id-etsi-qct-eidaspsbeaa defined as follows:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } -- Certificate referred to in Art.45f(1)(b) supporting the qualified electronic signature or qualified electronic seal of the public sector body referred to in Article 3, point (46) of Regulation (EU) No 910/2014.

(5) 5.2.10.1 General requirements

— EAA-5.2.10.1-04: void.

— EAA-5.2.10.1-05: void.

— EAA-5.2.10.1-06: The status member may contain the status_list member as specified in clause 6.2 of IETF draft-ietf-oauth-status-list-20 [25].

— EAA-5.2.10.1-07: void.

— EAA-5.2.10.1-08: void.

— EAA-5.2.10.1-09: void.

— EAA-5.2.10.1-10: void.

— EAA-5.2.10.1-11: void.

— EAA-5.2.10.1-12: void.

(6) 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 Mobile Security Object (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 issue short-lived electronic attestations of attributes having a validity period of equal to or less than 24 hours, then revocation shall not be required.

— 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 is specified in the token status list (draft-ietf-oauth-status-list-20) 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 a 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, shall be 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 comply with the verification requirements specified in the token status list specification and the status structure specification 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 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 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 curve NIST P-256 and SHA-256);

(b) 'ES384' (ECDSA with curve NIST P-384 and SHA-384);

(c) 'ES512' (ECDSA with curve NIST P-521 and SHA-512);

(d) 'ESB256' (ECDSA with curve brainpoolP256r1 and SHA-256);

(e) 'ESB384' (ECDSA with curve brainpoolP384r1 and SHA-384);

(f) 'ESB512' (ECDSA with curve brainpoolP512r1 and SHA-512);

— 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 instance attestation (WIA) and for the revocation of a key attestation (KA).

— 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 instance attestation (WIA) and of a key attestation (KA).

— 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 V

'ANNEX III

Technical specifications referred to in Article 10

— Technical specifications:

  — Clause 4.2.5 of ETSI TS 119 472-3 V1.1.1 (2026-03).'

ANNEX VI

Annex IV of Implementing Regulation (EU) 2024/2979 is amended as follows:

1. 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.’;

2. point 3, is replaced by the following:

‘3. Application programming interface:
ETSI TS 119 432 v1.3.1 (2026-03) clauses 6.4.3, A.6, A.7 and A.8.’.

ANNEX VII

'ANNEX VI

EU Digital Identity Wallet Trust Mark in colour



'

ANNEX VIII

‘*ANNEX VII*

EU Digital Identity Wallet Trust Mark in black and white



’

ANNEX IX

'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
ListOfCertifiedWalletsURL	URL of the public list of certified wallet solutions in EU as set out in Commission Implementing Regulation (EU) 2025/849 ([1]).	URL	mandatory
ListOfCertifiedWalletsQRCode	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 solution 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

([1]) Commission Implementing Regulation (EU) 2025/849 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the submission of information to the Commission and to the Cooperation Group for the list of certified European Digital Identity Wallets (OJ L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).'

ANNEX X

Annex II to Implementing Regulation (EU) 2024/2980 is amended as follows:

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

'(i) one or more certificates compliant with standard ETSI EN 319 412-2 V2.4.1 (2025-06) or standard 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;';

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

'(h) one or more certificates compliant with standard ETSI EN 319 412-2 V2.4.1 (2025-06) or standard ETSI EN 319 412-3 V1.3.1 (2023-09) that can be used to authenticate and validate wallet unit attestations the wallet provider has issued, 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;';

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

'(h) one or more certificates compliant with standard ETSI EN 319 412-2 V2.4.1 (2025-06) or standard 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.';

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

'(g) one or more certificates compliant with standard ETSI EN 319 412-2 V2.4.1 (2025-06) or standard 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.';

5. Annex II, Section 5 is added as follows:

'5. Notifications of information on providers of wallet-relying party registration certificates

1. Member States shall provide the following information to the Commission on providers of wallet-relying party registration certificates:

(a) the name of the provider of wallet-relying party registration certificates;

(b) where applicable, a registration number of the provider of wallet-relying party registration certificates;

(c) the Member State in which the provider of wallet-relying party registration certificates is established;

(d) the contact email and contact phone number of the provider of wallet-relying party registration certificates, for matters related to the registration certificates it provides to wallet-relying parties;

(e) where applicable, the URL of the webpage of the provider of wallet-relying party registration certificates that contains additional information about the provider and the registration certificates it provides to wallet-relying parties;

(f) the URL of the webpage that contains the policies, terms and conditions that apply to the provision and use of the registration certificates it provides to wallet-relying parties;

(g) one or more certificates compliant with standard ETSI EN 319 412-2 V2.4.1 (2025-06) or standard 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 registration certificates on the registration certificates it provides to wallet-relying parties, with, where applicable, the information required to distinguish wallet-relying party registration certificates from other certificates.

2. The information referred to in point 1 shall be provided per provider of wallet-relying party registration certificates.'

ANNEX XI

'ANNEX I

Protocols and interfaces referred to in Article 4

The technical specification ETSI TS 119 472-3 V1.1.1 (2026-03) shall apply with the following adaptations:

1. 4.1 General requirements

   — GEN-REQ-4.1-05: Void

   — NOTE: Void

2. 4.2.3 Provision of registration certificates of PID/EAA Provider to EUDI Wallet

   — ISS-MDATA-REG_CERT-4.2.3-04: One of the elements in the issuer_info array parameter shall contain the PID/EAA Provider's registration certificate.

   — ISS-MDATA-REG_CERT-4.2.3-07: void

   — ISS-MDATA-REG_CERT-4.2.3-08: void

   — ISS-MDATA-REG_CERT-4.2.3-09: void

   — ISS-MDATA-REG_CERT-4.2.3-10: void

   — ISS-MDATA-REG_CERT-4.2.3-11: void

   — ISS-MDATA-REG_CERT-4.2.3-12: void

   — ISS-MDATA-REG_CERT-4.2.3-13: void

3. 4.2.4.2 ARF pre-defined PID/EAA reuse policy

   — ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: Where the id member has the value 'arf_annex_ii' and the array mapped to the label 'details' contains the value 'once_only' or the value 'per-relying-party', then the JSON Object that contains this array mapped to the label 'details' shall also contain a JSON number mapped to the label 'reissue_trigger_unused'.

4. Annex A shall not apply.'

ANNEX XII

'ANNEX II

Technical specifications referred to in Article 5

The technical specification in Annex C to ISO/IEC 18013-7:2025 shall apply.

The technical specifications in clauses 4.1, 4.2, 5, and 6 of ETSI TS 119 472-2 V1.2.1 (2026-03), shall apply with the following adaptations, including the insertion of a new clause 4.3:

(1) 1 Scope

— The present document specifies two profiles of protocols for allowing Relying Parties (RP hereinafter) to request EAAPs or Personal Identification Data (PID hereinafter) to the EUDI Wallet, and the EUDI Wallet to send the requested EAAPs/PIDs to the RP. Each of the profiles supports two transmission mechanisms, namely: API-mediated and non-API mediated, as shown below:

(a) A profile is built on:

— ISO/IEC 18013-5 [10] for non-API mediated transmission mechanism only, and

— Annex C of ISO/IEC 18013-7 [16] for API-mediated transmission mechanism.

This profile is named ISO/IEC-mdoc profile and it is defined in clause 5 of the present document.

(b) A profile is built on:

OpenID4VC-HAIP [11] for both API-mediated and non-API mediated transmission mechanisms, as follows:

— Sections 5, 5.1, 5.3, 7, and 8 of [11] for transmission via Redirects or non-API mediated transmission mechanism, and

— Sections 5, 5.2, 5.3, 7, and 8 of [11] for API-mediated transmission mechanism.

This profile is named OpenID4VC-HAIP profile and it is defined in clause 6 of the present document.

(2) 2.1 Normative references

— [15] ISO 639: 'Language code'.

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

(3) 4.1 EAAP implementation based on SD-JWT VC

— EAAP-SD-JWT VC-04: void.

(4) 4.2 EAAP implementation based on ISO/IEC-mdoc

— EAAP-ISO/IEC-mdoc-01: void.

— *Note2*: void.

— EAAP-ISO/IEC-mdoc-02: void.

(5) 4.3 EAAP implementation with mediating API

— EAAP-API-GEN-01: The EUDI Wallet shall support a mediating API that supports both protocols defined in clause 5.2 of [11] and in Annex C of [16].

— *NOTE*: Where the device on which the EUDI Wallet is installed does not support both protocols, this requirement cannot be met and triggers a non-conformity due to underlying operating systems and browsers not implementing the necessary interoperability features.

— EAAP-API-GEN-02: The EUDI Wallet shall support a mediating API at least for PIDs and EAA types registered in the catalogue of schemes as defined in Implementing Regulation (EU) 2025/1569, and at least for all the formats defined in Annex II to Implementing Regulation (EU) 2024/2979.

— *NOTE 1*: Where the underlying operating system, browser, mediating APIs, or any other technical layer outside the control of the EUDI Wallet restricts, filters, preselects, or otherwise constrains the credential formats, and the PID and EAA types registered in the catalogue of schemes, this requirement cannot be met. Where such a restriction prevents the EUDI Wallet from supporting a registered credential type or format, the resulting non-conformity is attributable to the failure of those underlying operating systems, browsers, mediating API, or other relevant technical layer to provide the necessary interoperability features.

(6) 4.4 Wallet-relying party validation and overasking checks

— WRP-VALIDATION-01: The EUDI Wallet shall validate the wallet-relying party registration certificate received in the request before presenting any requested PID or electronic attestation of attributes to the wallet user for approval.

— WRP-VALIDATION-02: Where the validation of the wallet-relying party registration certificate fails, including where the certificate is expired, revoked, not issued by a valid trusted provider of wallet-relying party registration certificates, malformed, or cannot be cryptographically verified, the EUDI Wallet shall warn the wallet user that the wallet-relying party could not be validated and shall not present the request as successfully validated. The wallet user shall explicitly approve the request of the relying party. Silence or pre-ticked boxes shall not suffice for explicit approval.

— WRP-VALIDATION-03: The wallet provider shall determine, based on its risk analysis and security policy, whether and under which conditions specific failed validation checks may be bypassed by the wallet user.

— WRP-OVERASKING-01: The EUDI Wallet shall compare the attestations and attributes requested by the wallet-relying party with the registered attestations and attributes in the wallet-relying party registration certificate.

— WRP-OVERASKING-02: Where the wallet-relying party requests PID or electronic attestations of attributes or claims that are not covered by the wallet-relying party registration certificate, the EUDI Wallet shall clearly warn the wallet user before any disclosure. The warning shall identify that the wallet-relying party is requesting more information than it has registered. The wallet user shall explicitly approve the request of the relying party. Silence or pre-ticked boxes shall not suffice for explicit approval.

— WRP-OVERASKING-03: The wallet provider shall determine, based on its risk analysis, security policy and applicable law, whether the wallet user may continue despite such warning, whether only the subset of requested data covered by the registration certificate may be disclosed, or whether the request shall be rejected.

(7) 5.1 Introduction

— Clause 5 and its subclauses define a profile for a protocol allowing a RP to request EAAPs or PIDs to the EUDI Wallet, and the EUDI Wallet to send the requested EAAPs/PIDs to the RP using either a non-API mediated transmission mechanism, built on ISO/IEC 18013-5 [10] or an API-mediated transmission mechanism built on Annex C of ISO/IEC 18013-7 [16] for transferring the data structures defined in ISO/IEC 18013-5 [10] suitably encapsulated.

— The rest of clause 5 is organised as follows:

  — Clause 5.2 defines requirements on support of the profile and transmission mechanisms by RPs and EUDI Wallet;

  — Clause 5.3 specifies requirements that are specific for the non-API mediated transmission mechanism;

  — Clause 5.4 and its subclauses specify requirements that are specific for the API-mediated transmission mechanism.

(8) 5.2 Requirements on EUDI Wallet and RP support

— ISO/IEC 18013-SUPPORT-01: Wallet Units, PID Providers, Attestation Providers, Wallet Providers, and Relying Parties shall not support server retrieval as specified in ISO/IEC 18013-5 [10] for requesting and presenting PID or attestation attributes.

— ISO/IEC 18013-SUPPORT-02: The EUDI Wallet shall meet the requirements defined in clauses 5.3 and 5.4 of the present document.

— ISO/IEC 18013-SUPPORT-04: A Relying Party should implement the profile defined in clause 5.4 of the present document.

(9) 5.3.2 ISO/IEC-mdoc EAAP Request contents

— ISO/IEC 18013-5-REQ-04: Device requests sent to EUDI Wallets shall contain the 'requestInfo' key-value pair specified in clause 8.3.2.1.2.1 of [10]. The value of this pair shall be of type RequestInfo.

— ISO/IEC 18013-5-REQ-05: The RequestInfo type shall be as the CDDL definition shows below.

```
RequestInfo = {

    'euWrprc': bstr ; contains a registration certificate (see requirements below)

}
```

— ISO/IEC 18013-5-REQ-06: The mentioned requestInfo member shall contain a member with label 'euWrprc'

— ISO/IEC 18013-5-REQ-07: The value of the 'euWrprc' shall be a CBOR-encoded registration certificate.

— ISO/IEC 18013-5-REQ-08: void.

— *NOTE 3*: void.

— ISO/IEC 18013-5-REQ-09: void.

— ISO/IEC 18013-5-REQ-10: void.

— ISO/IEC 18013-5-REQ-11: void.

(10) 5.3.3 ISO/IEC-mdoc EAAP Response profile

— The present clause defines requirements for the DeviceResponse message type, common to the two types of transmission mechanisms (API-mediated and non-API mediated).

— *NOTE 1*: Where a non-API mediated mechanism built on ISO/IEC 18013-5 [10] is used, an EAAP Response is exactly an instance of DeviceResponse as profiled in the present clause, Where an API-mediated mechanism built on Annex C of ISO/IEC 18013-7 [16] is used, the instance of DeviceRequest is encapsulated as specified in Annex C of [16].

— ISO/IEC 18013-5-RESP-02: 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 2*: 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 provided, for example in use cases for secure user authentication.

— *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-03: Providers of person identification data shall not allow the private key of the person identification data to sign data elements that are provided by the wallet-relying party in the transactional data in the mdoc request.

(11) 5.4 Requirements for API mediated mechanism

5.4.1 ISO/IEC 18013-7-related requirements

The present clause defines requirements for API-mediated transmission mechanism related to the requirements defined in Annex C of [16].

— ISO/IEC 18013-7-API-01: The profile supporting API-mediated presentations shall comply with the requirements in Annex C of ISO/IEC 18013-7 [16] as further profiled in clauses 5.3 and 5.4 of the present document.

— ISO/IEC 18013-7-API-02: All the mandatory requirements defined in Annex C of [16] shall apply as further profiled in clauses 5.3 and 5.4 of the present document.

— ISO/IEC 18013-7-API-03: All the optional requirements defined in Annex C of [16] shall remain optional unless stated otherwise in the present document.

(12) 5.4.2 Additional requirements

— The present clause specifies additional requirements for API-mediated transmission mechanism.

— ISO/IEC 18013-ADD-API-01: The EUDI Wallet shall by default disclose the presence of all stored electronic attestations of attributes' type to the mediating API that works in accordance with Annex C of [16], but it shall not disclose the attributes and their values in these electronic attestations of attributes.

— *NOTE 1*: The attribute value restriction applies even if such disclosure would enhance the services provided by the Operating System to the EUDI Wallet, for example, attestation selection in the context of the mediating API.

— There are the considerations related to operating systems and browsers which fall out of the control of implementers, which can be taken into account as indicated in the following notes 2 to 4:

— *NOTE 2*: A presentation request from a Relying Party supporting Annex C of [16] can be processed by the browser and/or the Operating System for searching available EAAs, for preventing fraud targeting the User, or for troubleshooting purposes.

— *NOTE 3*: A presentation request from a Relying Party supporting Annex C of [16] is expected to be processed by the browser and/or the Operating System for User security purposes.

— *NOTE 4*: A presentation request from a Relying Party supporting Annex C of [16] is expected not to be processed by the browser and/or the Operating System for market analysis purposes (including as a secondary purpose) or for the browser's and/or the Operating System's internal purposes.

— ISO/IEC 18013-ADD-API-02: Where an EUDI Wallet deletes on the User's request a PID or EAA previously disclosed to the mediating API that works in accordance with Annex C of [16], the EUDI Wallet shall disclose the fact that it no longer stores this PID or EAA to the mediating API.

— ISO/IEC 18013-ADD-API-03: If the User uninstalls their EUDI Wallet, the EUDI Wallet shall disclose the fact that it no longer stores any previously disclosed PID(s) or EAA(s) to the mediating API that works in accordance with Annex C of [16].

— ISO/IEC 18013-ADD-API-04: The EUDI Wallet shall provide a global user setting to disable the disclosure of stored EAAs via a mediating API that works as is specified in ISO/IEC 18013-ADD-API-01. When this setting is disabled, the EUDI Wallet shall not advertise or respond to the API-mediated presentation or issuance requests.

— ISO/IEC 18013-ADD-API-05: EUDI Wallets shall verify in cross-device flows, using the mediating API, that the interacting device is in close physical proximity to the EUDI Wallet using a secure, direct, and user-mediated local communication channel, such as a short-range wireless communication technology to perform the physical proximity check.

— *NOTE*: CTAP 2.3 enables to use BLE to perform the close physical proximity check and when implemented by both devices, also enables to transport the data between the devices via short-range transmission technologies. Performing both the physical proximity check and data transfer between the two devices using a local communication channel as enabled by CTAP 2.3, should be preferred by underlying operating systems, browsers, mediating APIs, or any other technical layer outside the control of the EUDI Wallet over the use of CTAP Hybrid tunnel services.

(13) 6.2 Requirements on EUDI Wallet and RP support

— OIDFVP-HAIP-SUPPORT-02: The EUDI Wallet shall meet the requirements specified in clause 6.5 of the present Annex.

— OIDFVP-HAIP-SUPPORT-03: The EUDI Wallet should not support the redirects-based mechanism specified in clause 6.4 for cross-device presentation flows.

— *NOTE 3*: Using this mechanism is vulnerable to attacks, such as session fixation. Mitigating such attacks is up to relying parties. Implementing this mechanism should not trigger non-compliance.

— OIDFVP-HAIP-SUPPORT-05: A Relying Party shall meet the requirements specified in clauses 6.5 of the present Annex.

— *NOTE 5*: void.

(14) 6.3.1. General requirements

— OIDFVP-HAIP-GEN-01: All the mandatory requirements specified in clauses 5, 5.3, 7, and 8 of HAIP [11] shall apply.

— *NOTE 1*: 'HAIP [11] Section 5' refers only to the requirements directly under the Section 5 heading. This does not include sections 5.1, 5.2, and 5.3.

— OIDFVP-HAIP-GEN-03: If the present Annex modifies a requirement in OpenID4VC-HAIP [11], the modified requirement specified by the present Annex shall prevail.

— *NOTE 2*: This would allow, for instance, to convert in mandatory an optional requirement from OpenID4VC-HAIP [11] or to extend mandatory requirements.

— OIDFVP-HAIP-GEN-04: When the format of the requested attestation complies with [10] Relying Parties and EUDI Wallets shall comply with the 'ISO mdocs' profile in [11] Section 6.

— *NOTE 3*: For clarity: the 'ISO mdocs profile' in HAIP implies that Relying Parties and EUDI Wallets must comply with the applicable requirements in [7] Annex B.2.

— OIDFVP-HAIP-GEN-05: When the format of the requested attestation complies with [2], Relying Parties and EUDI Wallets shall comply with the 'IETF SD-JWT VCs' profile in [11] Section 6.

— *NOTE 4*: For clarity: the 'IETF SD-JWT VCs profile' implies that Relying Parties and EUDI Wallets must comply with the requirements in [7] Annex B.3, as well as with the requirements in [11] Section 6.1.

(15) 6.3.2.1 General requirements

— OIDFVP-HAIP-COMMON-REQ-01: void.

(16) 6.3.2.2 Requirements for the Request Object

— OIDFVP-HAIP-COMMON-REQ-RO-02: void

— OIDFVP-HAIP-COMMON-REQ-RO-03: void

— OIDFVP-HAIP-COMMON-REQ-RO-04: void

— OIDFVP-HAIP-COMMON-REQ-RO-05: void

— OIDFVP-HAIP-COMMON-REQ-RO-06: void.

— OIDFVP-HAIP-COMMON-REQ-RO-07: void

— OIDFVP-HAIP-COMMON-REQ-RO-08: void

— OIDFVP-HAIP-COMMON-REQ-RO-09: void

— OIDFVP-HAIP-COMMON-REQ-RO-10: void

— OIDFVP-HAIP-COMMON-REQ-RO-11: void

— OIDFVP-HAIP-COMMON-REQ-RO-12: void

— *Note 2*: void

— OIDFVP-HAIP-COMMON-REQ-RO-13: One of the elements of the verifier_info parameter shall include the registration certificate.

— OIDFVP-HAIP-COMMON-REQ-RO-23: The leaf certificate mentioned in OpenID4VP section 5.9.3 for use with the x509_hash Client Identifier Prefix shall be a RP access certificate as specified in ETSI TS 119 475 [14].

(17) 6.3.3 Authorization Response (EAAP response) profile

— OIDFVP-HAIP-COMMON-RESP-01: void.

(18) 6.4.1 General requirements

— OIDFVP-HAIP-REDIRECTS-04: void.

— *NOTE*: void.

(19) 6.5.2 Additional requirements

— OIDFVP-HAIP-ADD-API-01: The EUDI Wallet shall by default disclose the presence of all stored EAA types to the mediating API that works in accordance with clause 5.2 of [11], but it shall not disclose the attributes and their values in these EAAs.

— OIDFVP-HAIP-ADD-API-04: If the EUDI Wallet supports a mediating API that works as is specified in OIDFVP-HAIP-ADD-API-01, it shall provide a global user setting to disable the disclosure of stored EAAs via the mediating API. When this setting is set to disabled disclosure, the EUDI Wallet should subsequently enable the User to select individual attestations to be disclosed to the mediating API.

— OIDFVP-HAIP-ADD-API-05: EUDI Wallets shall verify, in cross-device flows, using the mediating API, that the interacting device is in close physical proximity to the EUDI Wallet using a secure, direct, and user-mediated local communication channel, such as a short-range wireless communication technology to perform the physical proximity check.

— *NOTE 5*: CTAP 2.3, enables to use BLE to perform the close physical proximity check and when implemented by both devices, also enables to transport the data between the devices via short-range transmission technologies. Performing both the physical proximity check and data transfer between the two devices using a local communication channel as enabled by CTAP 2.3, should be preferred by underlying operating systems, browsers, mediating APIs, or any other technical layer outside the control of the EUDI Wallet over the use of CTAP Hybrid tunnel services.

(20) 6.5.3 Specific requirements when requesting ISO/IEC 18013-5 EAAP

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: All requirements specified in this document applicable to Device Request and Device Response structures specified in ISO/IEC 18013-5 also apply when the EUDI Wallet receives a request for ISO/IEC mdoc presentation through an API-transmitted mechanism specified in clause C.1 of [16].'