



2025/1569

30.7.2025

**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

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 Articles 45d(5), 45e(2), 45f(6) and 45f(7) thereof,

Whereas:

- (1) Regulation (EU) No 910/2014 creates a legal framework for the issuance and validation of electronic attestations of attributes, including an obligation for providers of electronic attestations of attributes to provide European Digital Identity Wallet ('wallet') users with the possibility to request, obtain, store and manage the electronic attestation of attributes irrespective of the Member State where the wallets are provided. Electronic attestations of attributes are crucial components for the establishment of a secure and interoperable European Digital Identity Wallet ecosystem ('wallet ecosystem'). They enable users to share information with relying parties in a trusted manner in a variety of use cases.
- (2) The interfaces with European Digital Identity Wallets to be provided by providers of qualified electronic attestations of attributes as set out in Article 45g of Regulation (EU) No 910/2014 underline the importance of the electronic attestations of attributes for the wallet ecosystem and facilitate their swift take up.
- (3) The Commission regularly assesses new technologies, practices, standards and technical specifications. To ensure the highest level of harmonisation among Member States for the development and certification of the wallets, the technical specifications set out in this Regulation rely on the work carried out under Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework (²) and in particular the Architecture and Reference Framework which is part of it. In accordance with Recital 75 of Regulation 2024/1183 of the European Parliament and of the Council (³), the Commission should review and, if necessary, update this Regulation, to keep it in line with global developments, the Architecture and Reference Framework and to follow the best practices on the internal market in particular regarding the issuance of electronic attestations of attributes and verification of attributes against authentic sources or designated intermediaries.
- (4) Where providers of qualified electronic attestations of attributes and electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source issue attestations that claim to comply with the requirements of schemes for the attestation of attributes registered in the catalogue, policies and procedures for compliance with the requirements of those schemes should be part of the conformity assessment established in Regulation (EU) No 910/2014.

(¹) OJ L 257, 28.8.2014, p.73, ELI: <http://data.europa.eu/eli/reg/2014/910/oj>.

(²) OJ L 210, 14.6.2021, p. 51, ELI: <http://data.europa.eu/eli/reco/2021/946/oj>.

(³) Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (OJ L, 2024/1183, 30.4.2024, ELI: <http://data.europa.eu/eli/reg/2024/1183/oj>).

- (5) Protecting against untrustworthy information is of high significance for the digitalisation of attestations. Therefore, qualified electronic attestations of attributes and electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source should be able to be revoked, or alternative measures should be implemented to compensate for the risks related to non-revocability. Certain circumstances, such as the explicit request of the person to whom the electronic attestation of attributes was issued, or where it is known to the provider that there has been a compromise of the security or trustworthiness of the qualified electronic attestations of attributes, or where required by Union or national law, should lead to revocation by the provider of an electronic attestation of attributes. To safeguard the fundamental rights to privacy and data protection of the user, notably by appropriately minimising risks of linkability and traceability, providers of qualified electronic attestations of attributes and electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source, should set up revocation management policies that are privacy preserving.
- (6) In order to facilitate cooperation among Member States and the establishment of a secure and interoperable digital identity ecosystem, including the cross-border recognition and interoperability of 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, simplified administrative communication procedures need to be established among the relevant stakeholders, including the publication of information to swiftly identify the relevant public sector bodies. Member States should notify the relevant attributes to the Commission. Therefore, to ensure the timely, efficient, and interoperable verification of these attributes, the relevant notifications to the Commission should be at least in English as this facilitates its wide accessibility, assessment, and comprehension and at the same time enhances cooperation among the relevant stakeholders. However, translation of already existing documentation should not cause unreasonable administrative or financial burdens.
- (7) To enable users and service providers to verify that electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source were indeed issued by or on behalf of that public sector body, Member States should notify those public sector bodies to the Commission. When notifying public sector bodies that issue electronic attestations of attributes in accordance with Article 45f and Annex VII of Regulation (EU) No 910/2014, Member States are to provide a conformity assessment report confirming a level of reliability and trustworthiness equivalent to qualified trust service providers. However, unlike qualified trust service providers issuing qualified electronic attestations of attributes, for these public sector bodies, it is up to Member States how they ensure that the providers meet the requirements over time. To maintain a high level of trust in public sector attestations across the Union, Member States are therefore encouraged to share their best practices on how they ensure the continued reliability and trustworthiness through the European Digital Identity Cooperation Group established pursuant to Article 46e(1) of Regulation (EU) No 910/2014 ('Cooperation Group'). The Commission should establish, maintain, and publish a list of providers and ensure that this list is easily accessible by the public.
- (8) The Commission should establish a catalogue of attributes with the assistance of the Cooperation Group to facilitate the verification of attributes against authentic sources by qualified trust service providers issuing qualified electronic attestations of attributes. Registration in the catalogue of attributes should be mandatory for attributes listed in Annex VI to Regulation (EU) No 910/2014. For other attributes, registration would be optional.
- (9) The Commission should establish a catalogue of schemes for the attestation of attributes with the assistance of the Cooperation Group to facilitate the issuance of attestations by qualified trust service providers issuing qualified electronic attestations of attributes and providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source and to facilitate harmonisation and cross border interoperability of these attestations. The registration of schemes in the catalogue of schemes should be optional. Requests of registration or changes in the catalogue should be made by the owner of the scheme for the attestation of attributes and may include attributes not listed in the catalogue of attributes. The Commission should assess those requests taking into account interoperability and harmonisation needs.

- (10) To ensure that the catalogue of attributes provides meaningful information and reaches a high level of interoperability within the electronic attestation of attributes ecosystem, it should provide at least a minimum set of information, such as a semantic description of the attribute, the namespace of its identifier, and the data type of the attribute. For the same purpose, the catalogue of schemes for the attestation of attributes should contain descriptions for common types of electronic attestations of attributes and a description of the trust model and the governance mechanisms applied under the attestation scheme. The information contained in the catalogues should include versioning of attributes and schemes so that attestations issued according to specific versions are not affected by changes in those attributes and schemes.
- (11) To ensure the effectiveness of the verification of attributes against authentic sources by qualified trust service providers issuing qualified electronic attestations of attributes, including via designated intermediaries that provide indirect verification mechanisms to service providers, Member States should set up, within the time limit set out in Article 45e(1) of Regulation (EU) No 910/2014, mechanisms that enable qualified trust service providers issuing qualified electronic attestations of attributes to request the verification of attributes. The mechanisms should allow qualified trust service providers issuing qualified electronic attestations of attributes to determine which attributes can be verified and how to verify them. These mechanisms should include details on access points and service protocols for checking attribute validity and accuracy and consider the possibility of offering a single verification point at national level.
- (12) More specifically, Member States should make available to qualified trust service providers issuing qualified electronic attestations of attributes the mechanisms for accessing and using verification points for each one of the attributes listed in Annex VI of that Regulation (EU) No 910/2014, at national level. These mechanisms should allow qualified trust service providers issuing qualified electronic attestations of attributes to present, at the request of the user, specific attributes to a verification point for the issuance of the attestation and during its lifetime. The verification mechanisms should use electronic means suitable for automatic processing, and for obtaining responses as soon as possible from the verification point. This response should confirm if the attributes presented by the qualified trust service providers issuing qualified electronic attestations of attributes correspond to the attributes stored in relation to that user in the relevant authentic source and should specify the authentic source against which the verification was conducted. To avoid misconduct, such as unlawful or manifestly excessive verification requests, Member States may impose control mechanisms on the use of the verification points, where they deem this appropriate taking into account relevant factors, including whether the authentic sources contain information that should be considered as personal data or that is otherwise confidential or sensitive in nature under Union or national law.
- (13) In accordance with the principles established by the Interoperable Europe Act⁽⁴⁾, in order to facilitate the establishment of catalogue of attributes and catalogue of schemes for the attestation of attributes and reuse, as far as possible, existing catalogues, schemes and information, the Commission should, where appropriate, exploit synergies with the common services of the technical system pursuant to Regulation (EU) 2018/1724 of the Parliament and of the Council establishing a single digital gateway and amending Regulation (EU) No 1024/2012⁽⁵⁾.
- (14) In order to enhance interoperability for electronic attestations of attributes issued by non-qualified trust service providers, the principles and requirements established in this Regulation may be followed by issuers of attestations with regard to non-qualified electronic attestation of attributes.

⁽⁴⁾ Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act) (OJ L, 2024/903, 22.3.2024, ELI: <http://data.europa.eu/eli/reg/2024/903/oj>).

⁽⁵⁾ Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (OJ L 295, 21.11.2018, p. 1, ELI: <http://data.europa.eu/eli/reg/2018/1724/oj>).

- (15) Regulation (EU) 2016/679 of the European Parliament and of the Council (⁽⁶⁾) and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council (⁽⁷⁾) apply to the personal data processing activities under this Regulation.
- (16) With the objective to provide the Commission and Member States with sufficient time to set up the list of providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source, the requirements in this Regulation concerning the catalogue of attributes, the catalogue of schemes for the attestations of attributes, and the verification points for attributes, should become applicable 12 months after the date of entry into force of this Regulation.
- (17) 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 (⁽⁸⁾) and delivered its opinion on 31 January 2025.
- (18) 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

Subject matter and scope

This Regulation lays down the reference standards, specifications, and procedures, to be updated on a regular basis to keep in line with technology and standards developments and with the work carried out on the basis of Recommendation (EU) 2021/946, and in particular the Architecture and Reference Framework, relating to:

- (1) qualified electronic attestations of attributes;
- (2) electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source;
- (3) the list of providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source;
- (4) catalogue of attributes and catalogue of schemes for the attestations of attributes referred to in points (1) and (2);
- (5) the verification of attributes with reference to authentic sources or designated intermediaries.

Article 2

Definitions

For the purpose of this Regulation, the following definitions apply:

- (1) ‘wallet unit’ means a unique configuration of a wallet solution that includes wallet instances, wallet secure cryptographic applications and wallet secure cryptographic devices provided by a wallet provider to an individual wallet user;

⁽⁶⁾ 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>).

⁽⁷⁾ 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⁾ 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>).

- (2) 'wallet user' means a user who is in control of the wallet unit;
- (3) 'catalogue of attributes' means a digital repository of attributes that is maintained and published online by the Commission;
- (4) 'scheme for the attestation of attributes' means a set of rules applicable to one or more types of electronic attestation of attributes;
- (5) 'type of electronic attestation of attributes' means a specifically named and semantically described group of electronic attestation of attributes;
- (6) 'catalogue of schemes for the attestation of attributes' means a digital repository listing schemes for the attestation of attributes registered in accordance with this Regulation and that is maintained [and published online] by the Commission;
- (7) 'wallet solution' means a combination of software, hardware, services, settings, and configurations, including wallet instances, one or more wallet secure cryptographic applications and one or more wallet secure cryptographic devices;
- (8) 'wallet instance' means the application installed and configured on a wallet user's device or environment, which is part of a wallet unit, and which the wallet user uses to interact with the wallet unit;
- (9) 'wallet secure cryptographic application' means an application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the wallet secure cryptographic device;
- (10) 'wallet secure cryptographic device' means a tamper-resistant device that provides an environment that is linked to and used by the wallet secure cryptographic application to protect critical assets and provide cryptographic functions for the secure execution of critical operations;
- (11) 'wallet provider' means a natural or legal person who provides wallet solutions;
- (12) 'critical assets' means assets within or in relation to a wallet unit of such extraordinary importance that where their availability, confidentiality or integrity are compromised, this would have a very serious, debilitating effect on the ability to rely on the wallet unit;
- (13) 'owner of a scheme for the attestation of attributes' means an entity responsible for establishing and maintaining a scheme for the attestation of attributes.

Article 3

Issuance of qualified electronic attestations of attributes and electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source

1. Providers of qualified electronic attestations of attributes and providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source shall comply with the list of reference standards and specifications set out in Annex I and shall ensure that the electronic attestations of attributes they issue comply with the technical specifications set out in Annex II.
2. Where providers of qualified electronic attestations of attributes and providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source issue electronic attestations of attributes which are included in schemes registered in the catalogue of schemes for the attestation of attributes, they shall comply with the requirements of the corresponding scheme for the attestation of attributes. Policies and procedures established by the issuers of attestations in order to grant compliance with the requirements of the schemes for the attestation of attributes shall be part of the conformity assessment established in Regulation (EU) No 910/2014.

Article 4

Revocation of qualified electronic attestations of attributes and electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source

1. Providers of qualified electronic attestations of attributes and providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source shall have written and publicly accessible policies relating to validity or revocation status management. These policies shall include, where applicable, the conditions under which electronic attestations of attributes can be revoked without delay and measures for ensuring the availability of the validity status information.

2. Providers of qualified electronic attestations of attributes and providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source shall be the only entities able to revoke the electronic attestations of attributes they issue.

3. Providers of qualified electronic attestations of attributes and providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source, whenever those attestations are issued with a validity period of more than 24 hours, shall revoke them in at least the following circumstances:

- (a) upon the explicit request of the person to whom the electronic attestation of attributes was issued or, where applicable, of the subject of the attestation;
- (b) where it is known to the provider that there has been a compromise of the security or trustworthiness of the qualified electronic attestations of attributes or electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source;
- (c) in other situations, as required by Union or national law, or as determined by the providers in their policies as referred to in paragraph 1.

4. Providers of qualified electronic attestations of attributes and providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source shall set up revocation techniques and management methods that are privacy preserving and hindering linkability or traceability.

5. Providers of qualified electronic attestations of attributes and providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source shall make available to relying parties information on the validity or revocation status of the electronic attestations of attributes they have issued in a manner that ensures the integrity and authenticity of that information.

Article 5

Notification of public sector bodies

1. Member States shall submit at least the information set out in Annex III on public sector bodies as referred to in Article 45f (3) of Regulation (EU) No 910/2014 through a secure electronic notification system provided by the Commission.

2. Member States shall notify any changes to the notified information.

3. Member States shall make the notifications at least in English. Member States shall not be obliged to translate any document supporting the notifications where this would create an unreasonable administrative or financial burden.

4. The Commission may, where appropriate, ask the Member States to provide additional information.

Article 6

Publication of the list of public sector bodies

1. The Commission shall establish, maintain, and publish a list of providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source on the basis of the information notified by Member States pursuant to Article 5.
2. The Commission shall ensure that the list referred to in paragraph 1 can be accessed:
 - (a) in both electronically signed or sealed form suitable for automated processing, and through a human-readable website;
 - (b) without the need to register or to be authenticated;
 - (c) only by using state of the art transport layer security.
3. The Commission shall publish through a secure channel and without undue delay:
 - (a) the technical specifications of the list;
 - (b) the details of the URL where the list is published;
 - (c) the certificates to be used to verify the electronic signature or seal on the list;
 - (d) details relating to the mechanisms used to validate future changes to the location or to the certificates referred to in points (b) and (c).

Article 7

Creation and maintenance of the catalogue of attributes

1. The Commission shall establish and publish a catalogue of attributes and set up a secure system to enable requests to include or modify attributes in the catalogue of attributes.
2. The Commission shall assess requests made using the system referred to in paragraph 1 to include or modify an attribute in the catalogue of attributes, after considering any advice provided by the Cooperation Group. The Commission's assessment shall, take into account whether the inclusion of the attribute contributes to a common foundation for secure and privacy-aware electronic interaction between citizens, businesses and public authorities and to fostering interoperability. The Commission shall also take into account sector-specific regulations, where applicable.
3. Member States shall request the inclusion of attributes listed in Annex VI to Regulation (EU) No 910/2014 to the catalogue of attributes wherever those attributes rely on authentic sources for the purpose of the verification by qualified trust service providers.
4. In addition, Member States may request the inclusion of attributes not listed in Annex VI to the catalogue of attributes wherever those attributes rely on authentic sources within the public sector. Private entities that are considered to be a primary source of information or recognised as authentic in accordance with Union or national law, including administrative practice, may request the inclusion of attributes not listed in Annex VI to the catalogue of attributes wherever the requesting entity is responsible for those attributes.
5. The request to include or to modify an attribute in the catalogue shall contain at least the following information:
 - (a) identification of the entity making the request;
 - (b) where applicable, a reference to Union or national law or administrative practice under which the entity making the request is considered to be a primary source of information or recognised authentic source;
 - (c) if the request refers to an attribute already existing in the catalogue or is a new attribute;
 - (d) a namespace for the identifier of the attributes, the value of which is unique within the catalogue of attributes;
 - (e) an identifier of the attribute, unique within the namespace, and the version of the attribute;

- (f) semantic description of the attribute;
- (g) the data type of the attribute;
- (h) the verification point for the attribute at national level or a link to a description on how to initiate the verification requests.

6. The request to include or modify an attribute shall be signed or sealed by the requester by means of a qualified electronic signature or seal or an advanced electronic signature or seal based on a qualified certificate.

7. The Commission, following the assessment referred to in paragraph 2 and having verified that the information provided in the request for the inclusion or modification of an attribute includes all the information listed in paragraph 5, may include the requested attribute or modification in the catalogue of attributes.

8. The catalogue of attributes sealed by the Commission shall be publicly accessible, through a secure channel, free of charge and without prior identification or authentication, and shall be published in both machine-readable and human-readable forms. The catalogue shall also include a search function.

9. The Commission shall publish the technical specifications the Commission uses for the catalogue of attributes.

10. The Commission shall issue a unique identifier to each registered attribute.

Article 8

Creation and maintenance of the catalogue of schemes for the attestation of attributes

1. The Commission shall establish and publish a catalogue of schemes for the attestation of attributes and set up a secure system to enable requests to include or modify schemes for the attestation of attributes in the catalogue of schemes for the attestation of attributes.

2. Requests to include or modify schemes for the attestation of attributes in the catalogue of schemes for the attestation of attributes shall be assessed by the Commission, after considering any advice provided by the Cooperation Group. The Commission's assessment shall take into account whether the scheme contributes to a common foundation for secure and privacy-aware electronic interaction between citizens, businesses and public authorities and contributes to fostering interoperability. The Commission shall also take into account sector-specific regulations where applicable.

3. Owners of a scheme for the attestation of attributes may request adding schemes to the catalogue of schemes. A request to include or modify a scheme in the catalogue of schemes for the attestation of attributes shall contain, at least:

- (a) the name of the scheme, chosen by the scheme for the attestation of attributes owner and unique within the catalogue of schemes for the attestation of attributes;
- (b) the name and contact information of the scheme for the attestation of attributes owner;
- (c) the status and version of the scheme;
- (d) a reference to specific laws, standards or guidelines, where the issuance, validation, or use of an electronic attestation of attributes within the scope of the scheme is subject to them;
- (e) the format or formats of electronic attestation of attributes within the scope of the scheme;
- (f) one or more namespaces, attribute identifiers, semantic descriptions and data types of each attribute that is part of an electronic attestation of attributes within the scope of the scheme, either by reference to an attribute in the catalogue of attributes in Article 7, or an attribute defined in an analogue way within the scope of the scheme;
- (g) a description of the trust model and the governance mechanisms applied under the scheme, including the revocation mechanisms;
- (h) any requirements concerning the providers of the electronic attestations of attributes or the sources of information on which those providers rely when issuing electronic attestations of attributes, including any authentic sources, if applicable;

- (i) a statement whether electronic attestations of attributes within the scope of the scheme are to be issued as qualified electronic attestations of attributes, as electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source, or as both.

4. The schemes for which inclusion in the catalogue is requested shall only contain attributes that are identifiable based on unique identifiers. The request to include or modify a scheme for the attestation of attributes shall be signed or sealed by the requester by means of a qualified electronic signature or seal or an advanced electronic signature or seal based on a qualified certificate.

5. The Commission, following the assessment referred to in paragraph 2 and having verified that the information provided in the request for the inclusion or modification of an attestation scheme contains all the information listed in paragraphs 3 and 4 may include the requested scheme or modification in the catalogue of schemes for the attestation of attributes.

6. The catalogue of schemes for the attestation of attributes, sealed by the Commission, shall be publicly accessible, through a secure channel, free of charge and without prior identification or authentication, and shall be machine-readable and human-readable. The catalogue shall also include a search function and shall be in a format that guarantees integrity and authenticity.

7. The Commission shall publish the technical specifications the Commission uses for the catalogue of schemes for the attestation of attributes.

8. The Commission shall issue a unique identifier to each registered scheme for the attestation of attributes.

Article 9

Verification of attributes against authentic sources or designated intermediaries

1. To enable the electronic verification of the attributes referred to in Article 45e(1) of Regulation (EU) No 910/2014 by qualified trust service providers issuing qualified electronic attestations of attributes, at the request of the user, Member States shall establish mechanisms that allow that verification and may make available single points of verification for the attributes listed in Annex VI of that Regulation wherever those attributes rely on authentic sources within the public sector. Member States shall publish information on the procedures for initiating the verification requests and for receiving the verification results.

2. The verification mechanism shall provide an access point where qualified trust service providers issuing qualified electronic attestations of attributes can electronically request the verification against authentic sources or designated intermediaries recognised at national level, of the attributes referred to in Article 45e(1) of Regulation (EU) No 910/2014. Attributes subject to verification will be provided to the verification point by the qualified trust service provider at the user request. The public sector body or designated intermediary shall share, through the verification point, the verification results with the qualified trust service providers issuing qualified electronic attestations of attributes.

3. The verification request shall set out the attributes and the identification data of the subject of the attribute for which the qualified trust service provider requests the verification.

4. The verification result shall state exclusively whether the attribute has been verified or not and specify the public sector body responsible for the authentic source or, where applicable, the public sector body designated to act on behalf of the authentic source against which the attribute has been verified.

5. Member States may impose access controls or other verification mechanisms that provide integrity, authenticity, and confidentiality to determine that the requester is a qualified trust service provider and is acting at the request of a legitimate user. Member States may also impose control mechanisms on the use of the verification methods, where they deem this appropriate, taking into account relevant factors, including whether the authentic sources contain personal confidential or sensitive data. Where Member States establish these control mechanisms, they shall publish information on the extent of the control mechanisms as part of the information referred to in paragraph 1.

Article 10**Interoperability and reuse**

1. For the purpose of Articles 3 to 9, Member States may refer to and re-use the common services of the technical system set out in Article 14 of Regulation (EU) 2018/1724, as well as the national components connected to them.
2. When establishing the secure notification system and the list of public sector bodies referred to in Articles 5 and 6 and the catalogues referred to in Articles 7 and 8 of this Regulation, the European Commission shall refer to and re-use, where appropriate, the common services of the technical system pursuant to Regulation (EU) 2018/1724.

Article 11**Entry into force and application**

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

Article 6 to 9 shall apply from 19 August 2026.

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

Done at Brussels, 29 July 2025.

For the Commission

The President

Ursula VON DER LEYEN

ANNEX I

List of reference standards and specifications referred to in Article 3

Providers of qualified electronic attestations of attributes and providers of electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall issue their attestations to natural or legal persons according to the specifications for trust service providers established in standard ETSI EN 319 401 v3.1.1 (2024-06) ('ETSI EN 319 401').

ANNEX II

Technical specifications for the issuance of qualified electronic attestations of attributes and electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source referred to in Article 3

- (1) Providers of qualified electronic attestations of attributes and providers of electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall issue their attestations in a format according to one of the standards listed in Annex II of Commission Implementing Regulation (EU) 2024/2979 (¹).
- (2) For the issuance of attestations to natural or legal persons, providers of qualified electronic attestation of attributes and providers of electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall:
 - (a) where applicable, verify that the requester of the attestation has the right to act on behalf of the person that is the subject of the attestation;
 - (b) where applicable, verify the identity of the authentic source used as a source for the attributes included in the attestation;
 - (c) process only the minimum set of attributes necessary for the issuance and management of the attestation.
- (3) In addition, where the attestation is issued to a European Digital Identity Wallet, the attestation provider shall:
 - (a) authenticate to the wallet unit;
 - (b) verify that the wallet unit is not revoked or suspended.

(¹) 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).

ANNEX III

Notifications referred to in Article 5

Member States shall notify to the Commission at least:

- (1) the name of the public sector body, and where applicable, the registration number as used in official records; the Member State in which the public sector body is established; the Union or national law under which the public sector body is established as the responsible for the authentic source on the basis of which the electronic attestation of attributes is issued or is designated to act on behalf of the public sector body that is responsible for the authentic source;
 - (2) the contact email and phone number of the public sector body;
 - (3) the URL of the webpage for additional information about the public sector body;
 - (4) conformity assessment report as specified Article 45f (3) of Regulation (EU) No 910/2014.
-