Official Journal
of the European Union

EN
L series

2026/1735

22.7.2026

COMMISSION IMPLEMENTING REGULATION (EU) 2026/1735

of 15 July 2026

amending Implementing Regulation (EU) 2025/1569 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 Articles 45d(5), 45e(2), 45f(6) and 45f(7) 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 the adoption of Commission Implementing Regulation (EU) 2025/1569 ([3]), Implementing Regulation (EU) 2025/1569 should now be amended accordingly to align it with the new standards and specifications.

(2) In accordance with the objectives of Regulation (EU) No 910/2014, a number of standards have been selected to meet the requirements applicable to the issuance, management and verification of electronic attestations of attributes. These standards should reflect established practices and be widely recognised within the relevant sectors. Where necessary, these standards should be adapted or complemented in order to ensure a high level of security and integrity of electronic attestations of attributes, while facilitating cross-border interoperability and the effective functioning of the internal market. In line with this objective, this Regulation updates the requirements applicable to the issuance and 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 and introduces the requirements for the signing and sealing of verification results against authentic sources.

(3) Regulation (EU) 2016/679 of the European Parliament and of the Council ([4]) and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council ([5]) apply to all personal data processing activities under this Regulation.

([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) 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).

([4]) 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).

([5]) 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).

(4) 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 ([6]) and delivered its opinion on 17 April 2026 ([7]).

(5) 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) 2025/1569

Implementing Regulation (EU) 2025/1569 is amended as follows:

(1) Article 3, paragraph 2, is replaced by the following:

'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 comply 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.'.

(2) Article 4 is amended as follows:

(a) paragraph 1 is deleted;

(b) paragraph 3 is replaced by the following:

'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 request of the person to whom the electronic attestation of attributes was issued or, where applicable, of the subject of the attestation;

(b) where the provider becomes aware 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.'.

(c) paragraph 4 is replaced by the following:

'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. The revocation techniques shall comply with the requirements set out in Annex II.'.

([6]) 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).

([7]) EDPS Formal comments on the draft Commission Implementing Regulation as regards applicable standards and specifications for the registration of wallet-relying parties | European Data Protection Supervisor.

(3) Article 9 is amended as follows:

(a) the following paragraph 2a is inserted after paragraph 2:

'2a. The verification mechanism shall comply with the specifications set out in Annex IV.'.

(b) paragraph 4 is replaced by the following:

'4. The verification result shall state 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.

The verification result shall be signed or sealed by the public sector body responsible for an authentic source, or by the designated intermediary recognised at national level, using at least an advanced electronic signature based on a qualified certificate for electronic signatures or an advanced electronic seal based on a qualified certificate for electronic seals, respectively.'.

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

(5) Annex II is replaced by the text set out in Annex II to this Regulation.

(6) The text set out in Annex III to this Regulation is added as Annex IV.

Article 2

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 1(3) shall apply from 1 January 2027.

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 I

List of reference standards and specifications referred to in Article 3

ETSI TS 119 471 V1.1.1 (2025-05) shall apply with the following adaptations:

(1) 2.1 Normative references:

[1] ETSI EN 319 401 V3.2.1 (2026-01): 'Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers';

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

[3] FIPS PUB 140-3 (2019) 'Security Requirements for Cryptographic Modules';

[4] Commission Implementing Regulation (EU) 2024/482 ([1]);

[5] Commission Implementing Regulation (EU) 2024/3144 ([2]);

[6] ISO/IEC 15408:2022 (parts 1 to 5): 'Information security, cybersecurity and privacy protection – Evaluation criteria for IT security'.

(2) 3.1 Terms:
Following term is added:

— secure cryptographic device: device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user

(3) 4. EAA trust services

— Clause 4.2.2.2 'Verification of attributes against authentic sources' shall not apply.

— REQ-EAASP-4.2.2.3-02: The EAASP shall authenticate to the EUDIW instance implementing mutual authentication mechanisms that use a valid access certificate.

— REQ-EAASP-4.2.2.3-03: The EAASP shall validate the EUDIW unit, and *whether the EUDIW instance is revoked*.

— Clause *4.3.2 'EUDIW Specific' shall not apply*.

(4) 6.1 EAAS practice statement:

— REQ-EAASP-6.1-02: EAASP shall document the revocation mechanism in the EAAS practice statement

(5) 6.3 Information security policy:

— REQ-EAASP-6.3-02: The EAASP shall establish procedures to notify the supervisory body of any changes in the provision of the electronic attestation of attributes trust service and on the intention to cease those activities, in accordance with business requirements and relevant laws and regulations, including in accordance with the requirements of the implementing acts adopted pursuant to Article 24(5) of Regulation (EU) No 910/2014. The EAASP shall notify the supervisory body at least:

— one month before implementing any change;

— three months before the planned cessation of a trust service provision.

([1]) Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) (OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([2]) Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation (OJ L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

(6) 7.5 Cryptographic controls:

— REQ-EAASP-7.5.2-05: void

— REQ-EAASP-7.5.2-06: void

— REQ-EAASP-7.5.3-01A: Appropriate security controls shall be in place for the management of any cryptographic keys, cryptographic algorithms, and cryptographic devices throughout their lifecycle, following, where appropriate, a cryptographic agility approach.

— REQ-EAASP-7.5.3-01B: For the purpose of the provision of its trust services, the EAASP shall select and use suitable cryptographic techniques compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [2].

— REQ-EAASP-7.5.3-02: The EAASP shall ensure that the secure cryptographic device it uses for the digital signature or seal of EAA is a qualified signature or seal creation device and that all other digital signatures or seals used to provide the corresponding electronic attestation of attributes trust service, or part thereof, are created by means of a secure cryptographic device that is a trustworthy system certified in accordance with:

(a) Common Criteria for Information Technology Security Evaluation, as set out in Common Criteria for Information Technology Security Evaluation, version 3.1 (CC3.1) until 31.08.2027 or in version CC:2022 , Parts 1 through 5, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security, or as set out in ISO/IEC 15408 [6], and certified to EAL 4 or higher or

(b) the European Common Criteria-based cybersecurity certification scheme (EUCC) [4][5], and certified to EAL 4 or higher; or

(c) FIPS-140-2level 3 to be used until 31.08.2027 for existing certified systems or FIPS PUB 140-3 [3] level 3 until 31.12.2030.

This certification shall be to a security target or protection profile, or to a module design and security documentation, which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

If the secure cryptographic device benefits from an EUCC [4][5] certification, then this device shall be configured and used in accordance with that certification.

— REQ-EAASP-7.5.5-01: void

— REQ-EAASP-7.5.5-02: void

— REQ-EAASP-7.5.5-04: void

(7) 7.9 Vulnerabilities and Incident management:

— REQ-EAASP-7.9-02: Monitoring activities shall take account of the sensitivity of any information collected or analysed.

(8) 7.12 EAASP and EAAS termination and termination plans:

— REQ-EAASP-7.12-04: The EAASP's termination plan shall comply with the requirements set out in the implementing acts adopted pursuant to Article 24(5) of Regulation (EU) No 910/2014 [i.1].'.

ANNEX II

'ANNEX II

Technical specifications referred to in Article 3 and Article 4

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 compliance with at least one of the standards set out in Annex II to Commission Implementing Regulation (EU) 2024/2979 [1] and apply the relevant revocation techniques, also set out in Annex II to Commission Implementing Regulation (EU) 2024/2979.'.

---

[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

'*ANNEX IV*

List of standards and technical specifications referred to in Article 9

The verification mechanisms referred to in Article 9 shall comply with one or both of the following with the following adaptations:

(a) the technical specifications set out in clause 6.1.1 of ETSI TS 119 478 V1.1.1 (2026-01) - Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources;

— REQ-ASIP-6.1.1.2-04-01 [CONDITIONAL]: In case the attributeVerificationResult is either http://uri.etsi.org/19478/VerificationResult/Match or http://uri.etsi.org/19478/VerificationResult/MatchWithVariation the attributeVerificationResult may contain an attributeValue element.

— REQ-ASIP-6.1.1.2-04-02 [CONDITIONAL]: In case the returned attributeVerificationResult is http://uri.etsi.org/19478/VerificationResult/Match, and the attributeVerificationResult contains an attributeValue element, then the attributeValue element shall contain the value as in the request.

— REQ-ASIP-6.1.1.2-04-03 [CONDITIONAL]: In case the returned attributeVerificationResult is http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, and the attributeVerificationResult contains an attributeValue element, then the attributeValue element shall contain the value of the attribute as stored in the authentic source.

— REQ-ASIP-6.1.1.2-06-04-01 [CONDITIONAL]: In case the fragmentVerificationResult is either http://uri.etsi.org/19478/VerificationResult/Match or http://uri.etsi.org/19478/VerificationResult/MatchWithVariation the attributeVerificationResult may contain a fragmentValue element.

— REQ-ASIP-6.1.1.2-06-04-02 [CONDITIONAL]: In case the returned fragmentVerificationResult is http://uri.etsi.org/19478/VerificationResult/Match, and the attributeVerificationResult contains a fragmentValue element, then the fragmentValue element shall contain the value as in the request.

— REQ-ASIP-6.1.1.2-06-04-03 [CONDITIONAL]: In case the returned fragmentVerificationResult is http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, and the attributeVerificationResult contains a fragmentValue element, then the fragmentValue element shall contain the value of the fragment of the attribute as stored in the authentic source.

(b) the technical specifications set out in clause 6.2.3 of ETSI TS 119 478 V1.1.1 (2026-01)- Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources.

— REQ-ASIP-6.2.3.2.1-08-04: The AttributeVerificationResponse element may include exactly one child element of the choice TextValue, XMLValue or AttributeProperties.'.