Official Journal
of the European Union

EN
L series

2025/1946

30.9.2025

# COMMISSION IMPLEMENTING REGULATION (EU) 2025/1946

## of 29 September 2025

## laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards qualified preservation services for qualified electronic signatures and for qualified electronic seals

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 34(2) and Article 40 thereof,

Whereas:

(1) Qualified preservation services for qualified electronic signatures and for qualified electronic seals ensure the long-term integrity, authenticity, proof of existence and accessibility of preservation evidence of those electronic signatures and electronic seals. This allows the demonstration of their legal validity over extended periods of time and guarantees that they can be validated irrespective of future technological changes. These services are provided independently, or as a part of another qualified trust service such as qualified electronic archiving services.

(2) The presumption of compliance laid down in Article 34(1a) and Article 40 of Regulation (EU) No 910/2014 should only apply where qualified preservation services for qualified electronic signatures and for qualified electronic seals comply with the standards set out in this Regulation. These standards should reflect established practices and be widely recognised within the relevant sectors. They should be adapted to include additional controls ensuring the security and trustworthiness of the qualified trust service, as well as the ability to verify the qualified status and technical validity of the signatures and seals over time.

(3) If a trust service provider adheres to the requirements set out in the Annex to this Regulation, supervisory bodies should presume compliance with the relevant requirements of Regulation (EU) No 910/2014 and duly consider such presumption for granting or confirming the qualified status of the trust service. However, a qualified trust services provider may still rely on other practices to demonstrate compliance with the requirements of the Regulation (EU) No 910/2014.

(4) The Commission regularly assesses new technologies, practices, standards or technical specifications. In accordance with Recital 75 of Regulation (EU) 2024/1183 of the European Parliament and of the Council ([2]), the Commission should review and update this Regulation, if necessary, to keep it in line with global developments, new technologies, standards or technical specifications and to follow the best practices on the internal market.

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

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

(6) 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 ([5]) and delivered its opinion on 6 June 2025.

(7) 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*

**Reference standards and specifications**

The reference standards and specifications referred to in Article 34(2) and Article 40 of Regulation (EU) No 910/2014 are set out in the Annex to this Regulation.

*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*.

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

Done at Brussels, 29 September 2025.

*For the Commission*
*The President*
Ursula VON DER LEYEN

([3]) 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).

([4]) 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).

([5]) 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).

*ANNEX*

**List of reference standards and specifications referred to in Article 2**

The standards ETSI TS 119 511 V1.1.1 (2019-06) ('ETSI TS 119 511'), and ETSI TS 119 172-4 V1.1.1 (2021-05) ('ETSI TS 119 172-4') apply with the following adaptations:

1. For ETSI TS 119 511

(1) 2.1 Normative references:

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

— [2] ETSI TS 119 612 (V2.3.1) 'Electronic Signatures and Infrastructures (ESI); Trusted Lists'.

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

— [6] Commission Implementing Regulation (EU) 2024/482 ([1]) 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).

— [7] Commission Implementing Regulation (EU) 2024/3144 ([2]) amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation.

— [8] European Cybersecurity Certification Group, Sub-group on Cryptography: 'Agreed Cryptographic Mechanisms' published by the European Union Agency for Cybersecurity ('ENISA') ([3]).

— [9] ETSI TS 119 172-4 V1.1.1 (2021-05) 'Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists'.

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

(2) 3.1 Terms

— 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) 6.4 Preservation profiles

— OVR-6.4-08A [WTS][WOS] The expected evidence duration shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA[8].

— NOTE 3 void.

(4) 6.5 Preservation evidence policy

— OVR-6.5-04A The cryptographic algorithms used shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA[8].

— NOTE 1 void.

([1]) OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([2]) OJ L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

(5) 7.2 Human resources

— OVR-7.2-02 PSP's personnel in trusted roles, and if applicable its subcontractors in trusted roles, shall be able to fulfil the requirement of 'expert knowledge, experience and qualifications' through formal training and credentials, or actual experience, or a combination of the two.

— OVR-7.2-03 Compliance with OVR-7.2-02 shall include regular updates (at least every 12 months) on new threats and current security practices.

(6) 7.5 Cryptographic controls

— OVR-7.5-05 [CONDITIONAL] When PSP signs (part of) a preservation evidence, the PSP private signing key shall be held and used within a secure cryptographic device which is a trustworthy system certified in accordance with:

(a) Common Criteria for Information Technology Security Evaluation, as set out in ISO/IEC 15408 [10] or in Common Criteria for Information Technology Security Evaluation, 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, and certified to EAL 4 or higher; or

(b) EUCC [6][7] and certified to EAL 4 or higher; or

(c) until 31.12.2030, FIPS PUB 140-3 [5] level 3.

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 [6][7] certification, then this device shall be configured and used in accordance with that certification.

— OVR-7.5-06 [CONDITIONAL] void.

— OVR-7.5-07 [CONDITIONAL] When PSP signs (part of) a preservation evidence, any backup copies of the PSP private signing keys shall be protected to ensure its integrity and confidentiality by the secure cryptographic device before being stored outside that device.

— OVR-7.5-08 A PSP's private signing key shall only be exported and imported into a different secure cryptographic device where this export and import are implemented securely and in accordance with the certification of those devices.

(7) 7.8 Network security

— OVR-7.8-03 The vulnerability scan requested by REQ-7.8-13 of ETSI EN 319 401 [1] shall be performed at least once per quarter.

— OVR-7.8-04 The penetration test requested by REQ-7.8-17X of ETSI EN 319 401 [1] shall be performed at least once per year.

— OVR-7.8-05 Firewalls shall be configured to prevent all protocols and accesses not required for the operation of the PSP.

(8) 7.14 Cryptographic monitoring

— OVR-7.14-03A The evaluation of the cryptographic algorithms in OVR-7.14.01 and OVR-7.14.02 shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [8].

— NOTE void.

(9) 7.12 TSP termination and termination plans

— OVR-7.12-01A The TSP'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.2].

(10) 7.17 Supply chain

— OVR-7.17-01 The requirements specified in ETSI EN 319 401 [1], clause 7.14 shall apply.

(11) Annex A (normative): Qualified preservation service for QES as defined by article 34 of the Regulation (EU) No 910/2014

— OVR-A-02 [PDS][PDS+PGD]

(a) the preservation service shall preserve all information needed to check the qualified status of the electronic signature or seal that would not be publicly available until the end of the preservation period;

(b) the preservation service shall ensure that, at any given time during the preservation period, the information preserved is such that, when provided as input to the process specified in clause 4.4 of ETSI TS 119 172-4 [9], the output of this process clearly determines whether or not the digital signature or seal was, at the time of its preservation, technically suitable to implement an EU qualified electronic signature or EU qualified electronic seal.

— OVR-A-03 [PDS][PDS+PGD] Time-stamps used within the preservation evidence shall be qualified time-stamps in accordance with Regulation (EU) No 910/2014 [i.2].

2. For ETSI TS 119 172-4

(1) 2.1 Normative references:

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) 'Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation'.

— All references to 'ETSI TS 119 102-1 [1]' shall be understood as references to 'ETSI EN 319 102-1 [1]'.

— [2] ETSI TS 119 612 (V2.3.1) 'Electronic Signatures and Infrastructures (ESI); Trusted Lists'.

— [13] ETSI TS 119 101 V1.1.1 (2016-03) 'Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation'.

(2) 4.2 Validation constraints and validation procedures, requirement REQ-4.2-03, section 'X.509 validation constraints', point c):

— (i) If an end-entity certificate represents a trust anchor, the RevocationCheckingConstraints shall not be used.

— (ii) If an end-entity certificate does not represent a trust anchor, the RevocationCheckingConstraints shall be set to 'eitherCheck' as defined in ETSI TS 119 172-1 [3], clause A.4.2.1, table A.2 rows (m)2.1.

— (iii) If an end-entity certificate represents a trust anchor, the RevocationFreshnessConstraints defined in ETSI TS 119 172-1 [3], clause A.4.2.1, table A.2 rows (m)2.2 shall not be used.

— (iv) If an end-entity certificate does not represent a trust anchor, the RevocationFreshnessConstraints defined in ETSI TS 119 172-1 [3], clause A.4.2.1, table A.2 rows (m)2.2 shall be used with a maximum value of 0 for the signing certificate, ensuring that the revocation information is only accepted if it has been issued after the best signature time. No value shall be set for the RevocationFreshnessConstraints for certificates other than the signing certificate, including certificates supporting time-stamps.

(3) 4.3 Requirements on signature validation and applicability rules checking practices

— REQ-4.3-02 Signature validation applications shall be compliant with ETSI TS 119 101 [13].

(4) 4.4 Technical applicability (rules) checking process

— REQ-4.4.2-03 If any of the checks specified in REQ-4.4.2-01 fails, then:

— the process stops;

— the signature shall be technically determined as indeterminate, i.e. as neither an EU qualified electronic signature, nor as an EU qualified electronic seal;

— the above result and the results of processes of all the intermediate processes shall be reflected in the signature applicability rules checking report.