Official Journal
of the European Union

EN
L series

2025/1942

30.9.2025

# COMMISSION IMPLEMENTING REGULATION (EU) 2025/1942

## 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 validation services for qualified electronic signatures and qualified validation services 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 Article 33(2) and Article 40 thereof,

Whereas:

(1) Qualified validation services for qualified electronic signatures and for qualified electronic seals ensure the integrity, authenticity and correctness of the process and results of the validation of qualified electronic signatures and of qualified electronic seals respectively. Those qualified trust services play a crucial role in the digital business environment by promoting the transition from traditional paper-based processes to electronic equivalent ones.

(2) The presumption of compliance laid down in Article 33(2) and Article (40) of Regulation (EU) No 910/2014 should only apply where qualified validation services for qualified electronic signatures and for qualified electronic seals comply with the technical standards set out in this Regulation. Those 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 services, as well as the ability to verify the qualified status and technical validity of qualified electronic signatures and qualified electronic seals.

(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 33(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 for qualified validation services for qualified electronic signatures and for qualified validation services for qualified electronic seals**

The standards ETSI TS 119 441 V1.2.1 (2023-10) ([1]) ('ETSI TS 119 441'), and ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) ('ETSI TS 119 172-4') apply with the following adaptations:

1. For ETSI TS 119 441

(1) 2.1 Normative references

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

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

— [4] ISO/IEC 15408-1:2022 – Information security, cybersecurity and privacy protection – Evaluation criteria for IT security.

— [5] void.

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

— [7] Commission Implementing Regulation (EU) 2024/482 ([3]) 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).

— [8] 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'.

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) 'Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report'.

— [10] European Cybersecurity Certification Group, Sub-group on Cryptography: 'Agreed Cryptographic Mechanisms' published by the European Union Agency for Cybersecurity ('ENISA') ([4]).

— [11] Commission Implementing Regulation (EU) 2024/3144 ([5]) amending Implementing Regulation (EU) 2024/4822 as regards applicable international standards and correcting that Implementing Regulation.

— [12] ETSI EN 319 411-1 'Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements'

([1]) ETSI TS 119 441 – Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services, V1.2.1 (2023-10).
([2]) ETSI TS 119 172-4 – Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists, V1.1.1 (2021-05).
([3]) OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([4]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([5]) OJ L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

(2) 2.2 Informative references

— [i.11] void.

(3) 3.3 Abbreviations

— EUCC European Common Criteria-based cybersecurity certification scheme

(4) 4.3.3 Process

— NOTE 10 See ETSI EN 319 102-1 [3] for guidance and ETSI TS 119 172-4 [8] for additional guidance for the EU qualified signature or seal case.

(5) 6.1 Signature Validation Service practice statement

— OVR-6.1-02 The SVS practice statement shall be structured as per Annex A.

— OVR-6.1-03 The SVS practice statement shall list or make reference to the supported SVS policies (e.g. through OIDs) and briefly describe them.

(6) 6.3 Information security policy

— OVR-6.3-02 The security policy shall document the security and privacy controls implemented to protect personal data.

(7) 7.2 Human resources

— OVR-7.2-02 SVSP'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.

(8) 7.5 Cryptographic controls

— OVR-7.5-02 [CONDITIONAL] When validation reports are signed, the SVSP public signing certificate corresponding to the SVSP private signing key shall be issued, by a trustworthy CA, in compliance with the NCP+ certificate policy as specified in ETSI EN 319 411-1 [12]. It should be issued in compliance with an appropriate certificate policy specified in ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [CONDITIONAL] When validation reports are signed, the SVSP 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 [4] 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 [7][11] and certified to EAL 4 or higher; or

(c) until 31.12.2030, FIPS PUB 140-3 [6] 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 [7][11] certification, then this device shall be configured and used in accordance with that certification.

— OVR-7.5-04 void.

— OVR-7.5-06 A SVSP'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.

(9) 7.7 Operation security

— OVR-7.7-02 To ensure that the systems on which the application is developed apply appropriate security measures and adapt to specific application environments, the SVA shall use application environment that is maintained with up-to-date security fixes.

— OVR-7.7-03 The following requirements specified in ETSI TS 119 101 [1], clause 5.2 shall apply to the SVA: GSM 1.3.

(10) 7.8 Network security

— OVR-7.8-02 If remote access to systems storing or processing confidential data is allowed, a formal policy shall be adopted and described as part of elements required by OVR-6.3-02.

— OVR-7.8-04 The vulnerability scan requested by REQ-7.8-13 of ETSI EN 319 401 [1] shall be performed at least once per quarter.

— OVR-7.8-05 The penetration test requested by REQ-7.8-17X of ETSI EN 319 401 [1] shall be performed at least once per year.

— OVR-7.8-06 Firewalls shall be configured to prevent all protocols and accesses not required for the operation of the SVSP.

(11) 7.12 Signature Validation Service provisioning termination and termination plans

— OVR-7.12-02 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.1].

(12) 7.14 Supply chain

— OVR-7.14-01 The requirements specified in ETSI EN 319 401 [2], clause 7.14 shall apply.

(13) 8.1 Signature validation process

— VPR-8.1-07 The validation application (SVA) shall comply with the requirements in ETSI TS 119 101 [1], clause 7.4 SIA 1 to SIA 4.

— VPR-8.1-11 [CONDITIONAL] When the SVS aims to validate qualified electronic signatures or qualified electronic seals such in accordance with Article 32(1) (or Article 40 respectively) of Regulation (EU) No 910/2014 [i.1], validation process shall follow the requirements of ETSI TS 119 172-4 [8].

(14) 8.2 Signature validation protocol

— SVP-8.2-03 The signature validation response shall bear the OID of the SVS policy.

(15) 8.4 Signature validation report

— SVR-8.4-02 The validation report shall conform to ETSI TS 119 102-2 [9].

— SVR-8.4-07 [CONDITIONAL] When a signature validation policy is not completely processed by the SVS, the report shall, in addition to reporting on validated constraints, report on constraints that have been ignored or overridden.

— SVR-8.4-15 The validation report shall clearly indicate the origin of each PoE (from within the signature, from the client, from the server).

— SVR-8.4-16 The validation report shall bear a validation report signature, which shall be the SVSP's digital signature.

— SVR-8.4-17 [CONDITIONAL] When validation reports are signed, the format and the target of the signature shall conform to ETSI TS 119 102-2 [9].

(16) 9 Framework for definition of validation service policies built on a trust service policy defined in the present document:

— OVR-9-05 [CONDITIONAL] When building a SVS policy on a trust service policy defined in the present document, a risk assessment shall be carried out to evaluate business requirements and determine the security requirements to be included in the policy for the stated community and applicability.

— OVR-9-06 [CONDITIONAL] When building a SVS policy on a trust service policy defined in the present document, the policy shall be approved and modified in accordance with a defined review process, including responsibilities for maintaining the policy.

— OVR-9-07 [CONDITIONAL] When building a SVS policy on a trust service policy defined in the present document, a defined review process shall exist to ensure that the policy is supported by the practices statements.

— OVR-9-08 [CONDITIONAL] When building a SVS policy on a trust service policy defined in the present document, the TSP shall make available the policies supported by the TSP to its user community.

— OVR-9-09 [CONDITIONAL] When building a SVS policy on a trust service policy defined in the present document, revisions to policies supported by the TSP shall be made available to subscribers.

(17) Annex B (normative) Qualified Validation Service for QES as defined by Article 33 of Regulation (EU) No 910/2014:

— VPR-B-02 [CONDITIONAL] If the SVSP is a QSVSP the implementation shall comply with ETSI TS 119 172-4 [8].

— NOTE 2 void.

— OVR-B-04 [CONDITIONAL] If the SVSP is a QSVSP, the tests in OVR-B-03 shall check different use-cases, positive and negative ones.

— VPR-B-11 [CONDITIONAL] If the SVSP is a QSVSP, the SVSP shall control the hash computation (either perform the computation on the server side or control the client if it is allowed on the client side).

— NOTE 5 void.

— NOTE 6 void.

— VPR-B-15 [CONDITIONAL] If the SVSP is a QSVSP, in order to satisfy VPR-B-13 to VPR-B-14 the validation report shall comply with ETSI TS 119 102-2 [9].

— VPR-B-16 [CONDITIONAL] If the SVSP is a QSVSP, the implementation shall comply with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [10] for use of suitable cryptographic techniques when providing qualified validation services for QES.

(18) Annex C (informative) Mapping of requirements to Regulation (EU) No 910/2014, section 'Providing validation in compliance with Article 32(1)', second paragraph:

— To ensure that all conditions required by Articles 32(1) and 40 of Regulation (EU) No 910/2014 [i.1] are verified, a correct validation algorithm is needed. It provides the same deterministic result for a signature or seal submitted to validation. The signature validation policy is crucial for this purpose. ETSI TS 119 172-4 [8], based on the validation algorithm specified in ETSI EN 319 102-1 [3] has been issued with this perspective.

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 (2024-11) '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 24 hours for the signing certificate. No value shall be set for the RevocationFreshnessConstraints for certificates other than the signing certificate, including certificates supporting time-stamps.

(3) 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:

(a) the process stops;

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

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