



2025/1567

30.7.2025

COMMISSION IMPLEMENTING REGULATION (EU) 2025/1567

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 the management of remote qualified electronic signature creation devices and of remote qualified electronic seal creation devices as qualified trust services

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 29a(2) and Article 39a thereof,

Whereas:

- (1) Qualified trust services for the management of remote qualified electronic signature creation devices and for the management of remote qualified electronic seal creation devices play a crucial role in the digital business environment by promoting the transition from traditional paper-based processes to electronic equivalents. Those qualified trust services contribute to a secure and trustworthy management of those remote devices on behalf of the signatories and creators of the seals, in a manner that guarantees that the conditions for qualified electronic signatures and qualified electronic seals are met.
- (2) To enhance the legal certainty and trustworthiness of qualified trust services for the management of remote qualified electronic signature creation devices and qualified trust services for the management of remote qualified electronic seal creation devices, qualified trust service providers providing those qualified services should comply with the standards set out in this Regulation.
- (3) These standards should reflect established practices and be widely recognised within the relevant sectors. They should be adapted to include controls ensuring the security and trustworthiness of the qualified trust services, as well as ensuring that the signatories have sole control, with a high level of confidence, over the use of their electronic signature creation data, and that the creators of the seal have control over the use of their electronic seal creation data, respectively.
- (4) With a view to ensuring an adequate timeframe for the audit of trust service providers as regards compliance with the new requirements, this Regulation should apply from 24 months after its entry into force.
- (5) 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>).

- (6) 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⁾ should apply to all personal data processing activities under this Regulation.
- (7) 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 06 June 2025.
- (8) 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 for the management of remote qualified electronic signature creation devices and of remote qualified electronic seal creation devices as qualified trust services referred to in Article 29a(2) and Article 39a of Regulation (EU) No 910/2014 are set out in the Annex to this Regulation.

Article 2

Entry into force and applicability

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 apply from 19 August 2027.

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

⁽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 the management of remote qualified electronic signature creation devices and of remote qualified electronic seal creation devices

The standard ETSI TS 119 431-1 V1.3.1 (2024-12) ('ETSI TS 119 431-1') applies for the purpose of assessing conformance with the EU Server Signing Application Service v2 Policy in compliance with Annex A of that standard, with the following adaptations:

- (1) 2.1 Normative references
 - [1] ETSI EN 319 401 V3.1.1 (2024-06): 'Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers';
 - [7] European Cybersecurity Certification Group, Sub-group on Cryptography: 'Agreed Cryptographic Mechanisms' published by the European Union Agency for Cybersecurity ('ENISA') ⁽¹⁾.
- (2) 6.1 Publication and repository responsibilities
 - OVR-6.1-04: The information identified in OVR-6.1-01 above shall be publicly and internationally available.
- (3) 6.4.4 Personnel controls
 - OVR-6.4.4-02: SSASP's shall employ personnel in trusted roles and, if applicable, subcontractors in trusted roles, who possess the necessary expert knowledge, experience and qualifications through formal training and credentials, or experience, or a combination of the two.
 - OVR-6.4.4-03: Compliance with OVR-6.4.4-02 shall include regular (at least every 12 months) updates on new threats and current security practices.
- (4) 6.4.9 SSASP service termination
 - OVR-6.4.9-02: The SSASP's termination plan shall comply with the implementing acts adopted pursuant to Article 24(5) of Regulation (EU) No 910/2014 [i.1].
- (5) 6.5.5 Network security controls
 - OVR-6.5.5-02: The vulnerability scan requested by REQ-7.8-13 of ETSI EN 319 401 [1] shall be performed at least once per quarter.
 - OVR-6.5.5-03: Firewalls shall be configured to prevent all protocols and accesses not required for the operation of the TSP.
- (6) 6.8.5 Cryptographic controls
 - OVR-6.8.5-01: Appropriate security controls shall be in place for the management of any cryptographic techniques of the SSASP throughout their lifecycle.
 - OVR-6.8.5-02: As regards OVR-6.8.5-01, the SSASP shall select and use suitable cryptographic techniques compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [7].
- (7) Annex A, section A.3 General requirements
 - OVR-A.3-02 [EUSPv2]: The TSP's practice statement shall include the reference to the certification of the employed QSCD in accordance with the requirements of Regulation (EU) No 910/2014 [i.1], Annex II.

⁽¹⁾ https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.