COMMISSION IMPLEMENTING REGULATION (EU) 2025/1929

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 the binding of date and time to data and establishing the accuracy of the time sources for the provision of qualified electronic time stamps

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 42(2) thereof,

Whereas:

(1) Qualified electronic time stamps play a crucial role in the digital environment by promoting the transition from traditional paper-based processes to electronic equivalents. By binding date and time information to electronic data, qualified electronic time stamps help ensuring the accuracy of date and time they indicate and the integrity of digital documents to which the date and time are bound.

(2) The presumption of compliance laid down in Article 42(1a) of Regulation (EU) No 910/2014 should only apply where qualified trust services for the issuance of qualified time stamps comply with the standards set out in this Regulation. These standards should reflect established practices and be widely recognised within the relevant sectors. These standards should be adapted to include additional controls ensuring the security and trustworthiness of the qualified trust service and of the binding of date and time to data and the accuracy of the time source.

(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 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 Implementing 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.

(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.

[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).

[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.

(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 06 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

The reference standards and specifications referred to in Article 42(2) of Regulation (EU) No 910/2014 are set out in the Annex to this Regulation.

Article 2

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

[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 time stamp services

The standards ETSI EN 319 421 V1.3.1 [1] ('ETSI EN 319 421') and ETSI EN 319 422 V1.1.1 [2] ('ETSI EN 319 422') apply with the following adaptations:

1. For ETSI EN 319 421

(1) 2.1 Normative references:

- [3] ISO/IEC 15408:2022 (parts 1 to 5) 'Information security, cybersecurity and privacy protection – Evaluation criteria for IT security'.
- [4] ETSI EN 319 401 V3.1.1 (2024-06) 'Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers'.
- [5] ETSI EN 319 422 V1.1.1 (2016-03) 'Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles'.
- [6] void.
- [9] European Cybersecurity Certification Group, Sub-group on Cryptography: 'Agreed Cryptographic Mechanisms' published by the European Union Agency for Cybersecurity ('ENISA') [3].
- [10] Commission Implementing Regulation (EU) 2024/482 [4] 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').
- [11] Commission Implementing Regulation (EU) 2024/3144 [5] of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation.

(2) 3.1 Terms

- certificate validity period: time interval from notBefore to notAfter inclusive, during which the certification authority ('CA') warrants that it will maintain information about the status of the certificate.

(3) 3.3 Abbreviations

- EUCC European Common Criteria-based cybersecurity certification scheme

(4) 6.2 Trust Service Practice Statement

- OVR-6.2-03 The TSA shall include statements about the availability of its time-stamping service in its TSA disclosure statement.

(5) 7.3 Personnel security

- OVR-7.3-02 The TSA'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-7.3-03 Compliance with OVR-7.3-02 shall include regular updates (at least every 12 months) on new threats and current security practices.

[1] EN 319 421 – Electronic Signatures and Infrastructures (ESI) – Policy and Security Requirements for Trust Service Providers issuing Time Stamps, V1.3.1.

[2] EN 319 422 – Electronic Signatures and Infrastructures (ESI) – Time-stamping protocol and time-stamp token profiles, V1.1.1 (2016-03), https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.

[3] https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

[4] OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

[5] OJ L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

(6) 7.6.2 TSU key generation

— TIS-7.6.2-03 The generation of the TSU’s key(s) shall be carried out 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 [3] 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 [10][11], and certified to EAL 4 or higher; or

(c) until 31.12.2030, FIPS PUB 140-3 [7] 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 [10][11] certification, then this device shall be configured and used in accordance with that certification.

— TIS-7.6.2-04 void.

— NOTE 3 void.

— TIS-7.6.2-05A The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time-stamps and for signing TSU public key certificates respectively shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group [9] and published by ENISA.

— NOTE 4 void.

— TIS-7.6.2-06 A TSU’s 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) 7.6.3 TSU private key protection

— TIS-7.6.3-02 The TSU private 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 [3] or in Common Criteria for Information Technology Security Evaluation, version CC:2002, 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) the European Common Criteria-based cybersecurity certification scheme (EUCC) [10][11], and certified to EAL 4 or higher; or

(c) until 31.12.2030, FIPS PUB 140-3 [7] 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 [10][11] certification, then this device shall be configured and used in accordance with that certification.

— TIS-7.6.3-03 void.

— NOTE 2 void.

(8) 7.6.7 End of TSU key life cycle

- TIS-7.6.7-03A The expiration date for TSU's private keys shall be compliant with the Agreed Cryptographic Mechanisms [9].

- NOTE 1 void.

(9) 7.10 Network security

- OVR-7.10-05 The vulnerability scan requested by REQ-7.8-13 of ETSI EN 319 401 [1] shall be performed at least once per quarter.

- OVR-7.10-06 The penetration test requested by REQ-7.8-17X of ETSI EN 319 401 [1] shall be performed at least once per year.

- OVR-7.10-07 Firewalls shall be configured to prevent all protocols and accesses not required for the operation of the TSA.

(10) 7.14 TSA termination and termination plans

- OVR-7.14-01A 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.4].

2. For ETSI EN 319 422

(1) 2.1 Normative references

- [5] void.

- [6] void.

- [8] European Cybersecurity Certification Group, Sub-group on Cryptography: 'Agreed Cryptographic Mechanisms'.

- [9] RFC 9110 HTTP Semantics.

(2) 4.1.3 Hash algorithms to be used

- The following clause shall apply:

  Hash algorithms used to hash the information to be time-stamped, the expected duration of the time stamp and selected hash functions versus time shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [8].

- NOTE void.

(3) 4.2.3 Algorithms to be supported

- The following clause shall apply:

  Time-stamp token signature algorithms to be supported shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [8].

- NOTE void.

(4) 4.2.4 Key lengths to be supported

- The following clause shall apply:

  Signature algorithm key lengths for the selected signature algorithm shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA.

- NOTE void.

(5) 5.1.3 Algorithms to be supported

— The following clause shall apply:

Hash algorithms for the time-stamp data to be supported, the expected duration of the time-stamp and selected hash functions versus time shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [8].

— NOTE void.

(6) 5.2.3 Algorithms to be used

— The following clause shall apply:

Hash algorithms used to hash the information to be time-stamped and time-stamp token signature algorithms shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [8].

— NOTE void.

(7) 6.3 Key lengths requirements

— The following clause shall apply:

The key length for the selected signature algorithm of the TSU certificate shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [8].

— NOTE void.

(8) 6.5 Algorithm requirements

— The following clause shall apply:

The TSU public key and the TSU certificate signature shall use the algorithms that are compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [8].

— NOTE void.

(9) 7 Profiles for the transport protocols to be supported

— The time-stamping client and the time-stamping server shall support the time-stamping protocol via HTTPS [9] as defined in clause 3.4 of IETF RFC 3161 [1].

(10) 8 Object identifiers of the cryptographic algorithms

— The following clause shall apply:

The TSU public key and the TSU certificate signature shall use algorithms in compliance with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [8].

(11) 9.1 Regulation compliance statement

— If a time-stamp token is declared by the TSA to be a qualified electronic time stamp in accordance with Regulation (EU) No 910/2014 [i.2], it shall contain one instance of the qcStatements extension in the time stamp token extension field with the syntax as defined in IETF RFC 3739 [i.3], clause 3.2.6.

— The qcStatements extension shall contain one instance of the statement 'esi4-qtstStatement-1' as defined in Annex B.

— The extension qcStatements shall not be marked as critical.