Official Journal
of the European Union

EN
L series

2025/2531

17.12.2025

COMMISSION IMPLEMENTING REGULATION (EU) 2025/2531

of 16 December 2025

laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards and specifications for qualified electronic ledgers

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 45l(3) thereof,

Whereas:

(1) By Regulation (EU) 2024/1183 of the European Parliament and of the Council ([2]), a list of new trust services and qualified trust services, including the recording of electronic data in a qualified electronic ledger, was introduced in Regulation (EU) No 910/2014. The Commission is to establish a list of reference standards and, where necessary, establish specifications for such services.

(2) An electronic ledger is a sequence of electronic data records which is to ensure the integrity of those data records and the accuracy of the chronological ordering of those records. In order to ensure that the recording of data in a qualified electronic ledger is chronologically ordered, consistent and reliable, it is necessary to establish a common set of specifications for the recording of electronic data in a qualified electronic ledger.

(3) The presumption of compliance laid down in Article 45l(2) of Regulation (EU) No 910/2014 should only apply where qualified trust services for the recording of electronic data in a qualified electronic ledger 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.

(4) 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.

(5) The Commission regularly assesses new technologies, practices, standards or technical specifications. In accordance with Recital 75 of Regulation (EU) 2024/1183, the Commission should review and, if necessary, update this Regulation, to keep it in line with global developments, new technologies, practices, 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]) apply to the personal data processing activities under this Regulation, taking also into consideration the European Data Protection Board 'Guidelines 02/2025 on processing of personal data through blockchain technologies' ([5]).

(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 ([6]) and delivered its opinion on 21 October 2025 ([7]).

(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 referred to in Article 45l(3) of Regulation (EU) No 910/2014 are set out, for qualified electronic ledgers, 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, 16 December 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]) edpb_guidelines_202502_blockchain_en.pdf.

([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 Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic ledgers.

ANNEX

List of technical specifications and reference standards for qualified distributed electronic ledgers

1. For the purposes of this Regulation, the following definitions apply:

   (a) 'finality' means the state of a data record of an electronic ledger wherein it has become irreversible and cannot be modified or removed;

   (b) 'distributed electronic ledger' means an electronic ledger that is shared across a set of distributed electronic ledger nodes and which is synchronized between the distributed electronic ledger nodes using a consensus mechanism;

   (c) 'distributed electronic ledger node' means a device or process that is part of a distributed electronic ledger network and stores a complete or partial copy of the data records of an electronic ledger;

   (d) 'distributed electronic ledger network' means a network of distributed electronic ledger nodes which makes up a distributed electronic ledger system;

   (e) 'distributed electronic ledger system' means a system that implements a distributed electronic ledger;

   (f) 'consensus' means an agreement among distributed electronic ledger nodes on the validity of transactions and the maintenance of a consistent and ordered set of validated transactions across the distributed electronic ledger system;

   (g) 'consensus mechanism' means the set of rules and procedures by which consensus is reached;

   (h) 'governing rules' means the set of protocols, policies, and mechanisms that dictates how the distributed electronic ledger system operates, how data is validated and added to an electronic ledger, and how participants interact;

   (i) 'transaction' means the smallest unit of a work process within an electronic ledger;

   (j) 'work process' means one or more sequences of actions required to produce an outcome that complies with governing rules of an electronic ledger;

   (k) 'validated transaction' means a transaction for which the required integrity, authenticity, and protocol-specific conditions have been checked in accordance with the governing rules of the distributed electronic ledger system;

   (l) 'cryptographic link' means a reference to data that is established using suitable cryptographic techniques to ensure the integrity, authenticity, or traceability of the referenced data and the correct sequence of data records;

   (m) 'ledger report' means a structured presentation of verifiable information extracted from the data records of an electronic ledger, and providing insights into specific activities, states, or compliance with predefined rules;

   (n) 'provider of qualified electronic ledger' means a qualified trust service provider that provides a qualified trust service consisting in the recording of data in a qualified electronic ledger.

   (o) 'qualified distributed electronic ledger' means a distributed electronic ledger that meets the requirements of a qualified electronic ledger.

2. Where the qualified trust service provider needs to produce a ledger report, it shall be produced in an automated manner.

3. Providers of qualified electronic ledgers shall create, record electronic data in, update and maintain a qualified electronic ledger in accordance with the specifications established in:

   (a) For all providers of qualified electronic ledgers, ETSI EN 319 401 v3.1.1 (2024-06) with the following adaptations:

      — 2.1 Normative references:

         [1] European Cybersecurity Certification Group, Sub-group on Cryptography: "Agreed Cryptographic Mechanisms" published by the European Network and Information Agency ('ENISA').

[2] IETF RFC 7515 (May 2015): "JSON Web Signature (JWS)".

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

[4] 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).

[5] 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.

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

— 6.1 Trust service practice statement:

  — REQ-6.1-12 The electronic ledger practice statement shall include at least the following information:

    — the functional and technical capabilities of the electronic ledger platform and its use throughout the provision of the recording of data in a qualified electronic ledger as a qualified trust service;

    — the specific data origin authentication mechanisms used when providing the service;

    — the specific sequential chronological ordering mechanisms used when providing the service.

    — where applicable, the cryptographic link used to ensure the sequence of data records;

    — where applicable, the consensus mechanism ensuring finality and integrity of data records and transactions stored in the ledger, including any cautionary time until finality and integrity are achieved;

    — the specific data integrity mechanisms used when providing the service.

  — 6.2 Terms and conditions:

    — REQ-6.2-03 Subscribers and parties relying on the trust service shall be informed, in a clear, comprehensive and easily accessible manner, in a publicly accessible space and individually, of precise terms and conditions, including the items listed above, before entering into a contractual relationship.

  — 6.3 Information security policy:

    — REQ-6.3-04X The TSP shall establish procedures to notify any changes in the provision of the trust service to the supervisory body, in accordance with business requirements and relevant laws and regulations. The TSP shall notify the supervisory body at least:

      — one month before implementing any change;

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

  — 7.2 Human resources:

    — REQ-7.2-04X TSP’s personnel in trusted role 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.

— REQ-7.2-05X This shall include regular (at least every 12 months) updates on new threats and current security practices.

— 7.5 Cryptographic controls:

— REQ-7.5-01X 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-7.5-02 For the purpose of the provision of its trust services, the TSP shall select and use suitable cryptographic techniques compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [1].

In particular:

— REQ-7.5-03 Providers of qualified electronic ledgers shall establish the origin of data records in the electronic ledger. To this extent, they shall use advanced electronic signatures based on qualified certificates or advanced electronic seals based on qualified certificates created by the users of the service in accordance with the following standards and specifications:

(a) ETSI EN 319 122-1 V1.3.1 (2023-06). Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures.

(b) ETSI EN 319 132-1 V1.3.1 (2024-07). Electronic Signatures and Trust Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures.

(c) ETSI TS 119 182-1 V1.2.1 (2024-07). Electronic Signatures and Trust Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures, with the following adaptation:

— 5.1.8 The x5c (X.509 Certificate Chain) header parameter

— The x5c header parameter as defined in clause 4.1.6 of IETF RFC 7515 [2] shall be present in the JAdES signature, either as a signed or unsigned header parameter.

— The x5c header parameter shall have the semantics specified in IETF RFC 7515 [2], clause 4.1.6.

— The x5c header parameter shall have the syntax specified in IETF RFC 7515 [2], clause 4.1.6.

— REQ-7.5-04: Providers of qualified electronic ledgers shall ensure the unique sequential chronological ordering of data records in the electronic ledger. To this extent, they shall use cryptographic links, based in hash lists or hash trees, using cryptographic hash functions, in accordance with the following specifications and standards:

(a) SHA-256 or higher output hash size, in compliance with the "Agreed Cryptographic Mechanisms" endorsed by the European Cybersecurity Certification Group and published by ENISA [1].

(b) SHA3-256 or higher output hash size, in compliance with the "Agreed Cryptographic Mechanisms" endorsed by the European Cybersecurity Certification Group and published by ENISA [1].

Alternatively, when using time recording to ensure the unique sequential chronological order of data records in the electronic ledger, providers of qualified electronic ledgers shall use qualified timestamps.

— REQ-7.5-05 Providers of qualified electronic ledgers shall ensure the integrity of data records recorded in a qualified electronic ledger. To this extent, they shall use advanced electronic signatures based on qualified certificates or advanced electronic seals based on qualified certificates, in accordance with the following standards and specifications:

  (a) any signature or seal formats that are compliant with the "Agreed Cryptographic Mechanisms" endorsed by the European Cybersecurity Certification Group and published by ENISA [1];

  (b) SHA-256 or higher output hash size, in compliance with the "Agreed Cryptographic Mechanisms" endorsed by the European Cybersecurity Certification Group and published by ENISA [1];

  (c) SHA3-256 or higher output hash size, in compliance with the "Agreed Cryptographic Mechanisms" endorsed by the European Cybersecurity Certification Group and published by ENISA [1].

  (d) Providers of qualified electronic ledgers shall ensure the immediate detectability of any subsequent change to data recorded in a qualified electronic ledger.

— REQ-7.5-06 Where digital signature mechanisms are used, signing private keys of the provider of qualified electronic ledger 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 ([1]) [6] 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) the European Common Criteria-based cybersecurity certification scheme (EUCC) ([2]) ([3]) [4][5] and certified to EAL 4 or higher; or

  (c) until 31.12.2030, FIPS PUB 140-3 ([4]) [3] 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 certification [4][5], then this device shall be configured and used in accordance with that certification.

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

([2]) 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/2024/482/2025-01-08).

([3]) 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).

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

— 7.8 Network security:

— REQ-7.8-14X The vulnerability scan requested by REQ-7.8-13 shall be performed at least once per quarter.

— REQ-7.8-18X The penetration test requested by REQ-7.8-17X shall be performed at least once per year.

— REQ-7.8-21X: Firewalls shall also be configured to prevent all protocols and accesses not required for the operation of the TSP.

— 7.9.1 Monitoring and logging:

— REQ-7.9.1-02X Monitoring activities shall take account of the sensitivity of any information collected or analysed.

— 7.12 TSP termination and termination plans:

— REQ-7.12-02A The TSP's termination plan shall comply with the requirements set out in the implementing acts adopted pursuant to Art. 24(5) of Regulation (EU) No 910/2014 [i.1].

(b) Additionally for all providers of qualified electronic ledgers making use of distributed electronic ledger technologies:

(1) ISO 23257:2022 Blockchain and distributed ledger technologies – Reference architecture, clause 9, providing a complete description of the distributed electronic ledger technology system, the corresponding distributed electronic ledger technology network and distributed electronic ledger technology nodes;

(2) ISO/TS 23635:2022. Blockchain and distributed ledger technologies – Guidelines for governance, with respect to written and publicly accessible policies and practices related to the governance structure for the electronic ledger service they provide.