2025/2531

17.12.2025

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2025/2531

af 16. december 2025

om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår referencestandarder og specifikationer for kvalificerede elektroniske hovedbøger

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF ([1]), særlig artikel 45l, stk. 3, og

ud fra følgende betragtninger:

(1) Ved Europa-Parlamentets og Rådets forordning (EU) 2024/1183 ([2]) blev der i forordning (EU) nr. 910/2014 indført en liste over nye tillidstjenester og kvalificerede tillidstjenester, herunder registrering af elektroniske data i en elektronisk hovedbog. Kommissionen skal fastsætte en liste over referencestandarder og, hvor det er nødvendigt, specifikationer for disse tjenester.

(2) En elektronisk hovedbog er en sekvens af elektroniske dataposter, der skal sikre integriteten af disse dataposter og nøjagtigheden af deres kronologiske rækkefølge. For at sikre, at registreringen af data i en kvalificeret elektronisk hovedbog følger en kronologisk rækkefølge og er konsekvent og pålidelig, er det nødvendigt at fastsætte et fælles sæt specifikationer for registrering af elektroniske data i en kvalificeret elektronisk hovedbog.

(3) Den formodning om overholdelse, der er fastsat i artikel 45l, stk. 2„ i forordning (EU) nr. 910/2014, bør kun finde anvendelse, hvis kvalificerede tillidstjenester til registrering af elektroniske data i en kvalificeret elektronisk hovedbog er i overensstemmelse med de standarder, der er fastsat i nærværende forordning. Disse standarder bør afspejle etableret praksis og være bredt anerkendte inden for de relevante sektorer. De bør tilpasses, så de omfatter yderligere kontroller, der sikrer den kvalificerede tillidstjenestes sikkerhed og troværdighed.

(4) Hvis en tillidstjenesteudbyder opfylder kravene i bilaget til denne forordning, bør tilsynsorganerne formode, at de relevante krav i forordning (EU) nr. 910/2014 er opfyldt, og tage behørigt hensyn til denne formodning i forbindelse med tildeling eller bekræftelse af tillidstjenestens status som kvalificeret. En kvalificeret tillidstjenesteudbyder kan dog stadig benytte anden praksis til at påvise opfyldelse af kravene i forordning (EU) nr. 910/2014.

(5) Kommissionen vurderer regelmæssigt nye teknologier, praksisser, standarder og tekniske specifikationer. I overensstemmelse med betragtning 75 til forordning (EU) 2024/1183 bør Kommissionen revidere og om nødvendigt ajourføre nærværende forordning for at sikre, at den er i overensstemmelse med den globale udvikling, nye teknologier, praksisser, standarder eller tekniske specifikationer, og for at følge bedste praksis på det indre marked.

([1]) EUT L 257 af 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Europa-Parlamentets og Rådets forordning (EU) 2024/1183 af 11. april 2024 om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af den europæiske ramme for digital identitet (EUT L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([3]) og, hvor det er relevant, Europa-Parlamentets og Rådets direktiv 2002/58/EF ([4]) finder anvendelse på alle behandlingsaktiviteter vedrørende personoplysninger i henhold til nærværende forordning, under hensyntagen til Det Europæiske Databeskyttelsesråds retningslinjer »Guidelines 02/2025 on processing of personal data through blockchain technologies« ([5]).

(7) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([6]) og afgav udtalelse den 21. oktober 2025 ([7]).

(8) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 48 i forordning (EU) nr. 910/2014 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Referencestandarder og specifikationer

De referencestandarder og specifikationer, der er omhandlet i artikel 45l, stk. 3, i forordning (EU) nr. 910/2014, er, for så vidt angår kvalificerede elektroniske hovedbøger, anført i bilaget til nærværende forordning.

Artikel 2

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 16. december 2025.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

([3]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) edpb_guidelines_202502_blockchain_en.pdf.

([6]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse 1247/2002/EF (EUT L 295 af 21.11.2018, s. 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.

BILAG

Liste over tekniske specifikationer og referencestandarder for kvalificerede distribuerede elektroniske hovedbøger

1. I denne forordning forstås ved:

   a) »endegyldighed«: den tilstand, som en datapost i en elektronisk hovedbog er i, når den er blevet irreversibel og ikke kan ændres eller fjernes

   b) »distribueret elektronisk hovedbog«: en elektronisk hovedbog, der deles på tværs af et sæt distribuerede elektroniske hovedbogsknudepunkter, og som synkroniseres mellem de distribuerede elektroniske hovedbogsknudepunkter ved hjælp af en konsensusmekanisme

   c) »distribueret elektronisk hovedbogsknudepunkt«: en enhed eller proces, der er en del af et distribueret elektronisk hovedbogsnet, og som lagrer en fuldstændig eller delvis kopi af dataposterne i en elektronisk hovedbog

   d) »distribueret elektronisk hovedbogsnet«: et net af distribuerede elektroniske hovedbogsknudepunkter, som udgør et distribueret elektronisk hovedbogssystem

   e) »distribueret elektronisk hovedbogssystem«: et system, der gennemfører en distribueret elektronisk hovedbog

   f) »konsensus«: en enighed mellem distribuerede elektroniske hovedbogsknudepunkter om transaktioners gyldighed og opretholdelsen af et sammenhængende og ordnet sæt validerede transaktioner i hele det distribuerede elektroniske hovedbogssystem

   g) »konsensusmekanisme«: det sæt regler og procedurer, der anvendes til at opnå konsensus

   h) »styrende regler«: det sæt protokoller, politikker og mekanismer, der bestemmer, hvordan det distribuerede elektroniske hovedbogssystem fungerer, hvordan data valideres og tilføjes til en elektronisk hovedbog, og hvordan deltagerne interagerer

   i) »transaktion«: den mindste enhed af en arbejdsproces i en elektronisk hovedbog

   j) »arbejdsproces«: en eller flere sekvenser af handlinger, der er nødvendige for at frembringe et resultat, der er i overensstemmelse med de styrende regler for en elektronisk hovedbog

   k) »valideret transaktion«: en transaktion, for hvilken den krævede integritet og autenticitet og protokolspecifikke betingelser er blevet kontrolleret i overensstemmelse med de styrende regler for det distribuerede elektroniske hovedbogssystem

   l) »kryptografisk tilknytning«: en henvisning til data, der etableres ved hjælp af passende kryptografiske teknikker for at sikre integriteten, autenticiteten eller sporbarheden af de data, der henvises til, og den korrekte sekvens af dataposter

   m) »hovedbogsrapport«: en struktureret præsentation af verificerbare oplysninger, der er hentet fra dataposterne i en elektronisk hovedbog, og som giver indsigt i specifikke aktiviteter, tilstande eller overensstemmelse med prædefinerede regler

   n) »udbyder af en kvalificeret elektronisk hovedbog«: en kvalificeret tillidstjenesteudbyder, der udbyder en kvalificeret tillidstjeneste, som består i registrering af data i en kvalificeret elektronisk hovedbog.

   o) »kvalificeret distribueret elektronisk hovedbog«: en distribueret elektronisk hovedbog, der opfylder kravene til en kvalificeret elektronisk hovedbog.

2. Når den kvalificerede tillidstjenesteudbyder skal udarbejde en hovedbogsrapport, skal den udarbejdes på automatiseret vis.

3. Udbydere af kvalificerede elektroniske hovedbøger opretter, registrerer elektroniske data i, ajourfører og vedligeholder en kvalificeret elektronisk hovedbog i overensstemmelse med de specifikationer, der er fastsat i:

   a) For alle udbydere af kvalificerede elektroniske hovedbøger ETSI EN 319 401 v3.1.1 (2024-06) med følgende tilpasninger:

      — 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].

Navnlig:

— 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].

Alternativt, når der anvendes tidsregistrering til at sikre den entydige kronologiske rækkefølge af dataposter i den elektroniske hovedbog, skal udbydere af kvalificerede elektroniske hovedbøger anvende tidsstempler.

— 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.

Denne certificering skal omfatte et sikkerhedsmål eller en beskyttelsesprofil eller et moduldesign og sikkerhedsdokumentation, der opfylder kravene i dette dokument, på grundlag af en risikoanalyse og under hensyntagen til fysiske og andre ikketekniske sikkerhedsforanstaltninger.

Hvis den sikre kryptografiske enhed er omfattet af en certificering under EUCC [4][5], skal enheden konfigureres og anvendes i overensstemmelse med denne certificering.

([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) Ydermere for alle udbydere af kvalificerede elektroniske hovedbøger, der gør brug af distribueret elektronisk hovedbogsteknologi:

(1) ISO 23257:2022 Blockchain og distributed ledger-teknologi — Referencearkitektur, punkt 9, der giver en fuldstændig beskrivelse af det distribuerede elektroniske hovedbogsteknologisystem, det tilsvarende distribuerede elektroniske hovedbogsteknologinet og distribuerede elektroniske hovedbogsteknologiknudepunkter

(2) ISO/TS 23635:2022. Blockchain og distributed ledger-teknologi — Vejledning i governance, med hensyn til skriftlige og offentligt tilgængelige politikker og praksisser vedrørende ledelsesstrukturen for den elektroniske hovedbogstjeneste, som de leverer.