Publicatieblad
van de Europese Unie

NL
L-serie

2025/2531

17.12.2025

UITVOERINGSVERORDENING (EU) 2025/2531 VAN DE COMMISSIE

van 16 december 2025

tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende referentienormen en specificaties voor gekwalificeerde elektronische registers

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG ([1]), en met name artikel 45 terdecies, lid 3,

Overwegende hetgeen volgt:

(1) Bij Verordening (EU) 2024/1183 van het Europees Parlement en de Raad ([2]) is een lijst van nieuwe vertrouwensdiensten en gekwalificeerde vertrouwensdiensten, met inbegrip van de registratie van elektronische gegevens in een gekwalificeerd elektronisch register, in Verordening (EU) nr. 910/2014 ingevoerd. De Commissie moet een lijst van referentienormen en, indien nodig, specificaties voor dergelijke diensten opstellen.

(2) Een elektronisch register is een opeenvolging van elektronische gegevensbestanden die de integriteit van die bestanden en de nauwkeurigheid van de chronologische volgorde van die gegevensbestanden moet waarborgen. Opdat de registratie van gegevens in een gekwalificeerd elektronisch register chronologisch wordt geordend, en consistent en betrouwbaar is, moeten gemeenschappelijke specificaties worden vastgesteld voor de registratie van elektronische gegevens in een gekwalificeerd elektronisch register.

(3) Het in artikel 45 terdecies, lid 2, van Verordening (EU) nr. 910/2014 uiteengezette vermoeden van overeenstemming mag alleen worden toegepast indien gekwalificeerde vertrouwensdiensten voor de registratie van elektronische gegevens in een gekwalificeerd elektronisch register aan de in deze verordening uiteengezette normen voldoen. Deze normen moeten vaste praktijken weerspiegelen en in de betrokken sectoren algemeen erkend worden. Deze normen moeten worden aangepast om er aanvullende controles in op te nemen die de veiligheid en betrouwbaarheid van de gekwalificeerde vertrouwensdienst waarborgen.

(4) Indien een verlener van vertrouwensdiensten aan de in de bijlage bij deze verordening vastgestelde vereisten voldoet, moeten toezichtinstanties aannemen dat hij aan de desbetreffende vereisten van Verordening (EU) nr. 910/2014 voldoet en deze veronderstelling in aanmerking nemen voor de toekenning of bevestiging van de gekwalificeerde status van de vertrouwensdienst. Een gekwalificeerde verlener van vertrouwensdiensten kan zich echter nog steeds op andere praktijken beroepen om aan te tonen dat hij aan de vereisten van Verordening (EU) nr. 910/2014 voldoet.

(5) De Commissie voert regelmatig beoordelingen van nieuwe technologieën, praktijken, normen of technische specificaties uit. Overeenkomstig overweging 75 van Verordening (EU) 2024/1183 moet de Commissie deze verordening indien nodig evalueren en actualiseren om deze in overeenstemming te houden met de mondiale ontwikkelingen, nieuwe technologieën, praktijken, normen of de technische specificaties, en om de beste praktijken op de interne markt te volgen.

([1]) PB L 257 van 28.8.2014, blz. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit (PB L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([3]) en, in voorkomend geval, Richtlijn 2002/58/EG van het Europees Parlement en de Raad ([4]) zijn van toepassing op activiteiten betreffende de verwerking van persoonsgegevens uit hoofde van deze verordening, mede met inachtneming van leidraad 02/2025 betreffende de verwerking van persoonsgegevens door middel van blockchaintechnologie van het Europees Comité voor gegevensbescherming ([5]).

(7) Overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([6]) is de Europese Toezichthouder voor gegevensbescherming geraadpleegd, en op 21 oktober 2025 heeft deze een advies uitgebracht ([7]).

(8) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 48 van Verordening (EU) nr. 910/2014 ingestelde comité,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Referentienormen en specificaties

De in artikel 45 terdecies, lid 3, van Verordening (EU) nr. 910/2014 genoemde referentienormen en specificaties voor gekwalificeerde elektronische registers zijn vastgesteld in de bijlage bij deze verordening.

Artikel 2

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 16 december 2025.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

([3]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) edpb_guidelines_202502_blockchain_en.pdf.

([6]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 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.

BIJLAGE

Lijst van technische specificaties en referentienormen voor gekwalificeerde gedistribueerde elektronische registers

1. Voor de toepassing van deze verordening wordt verstaan onder:

   a) “finaliteit”: de toestand van een gegevensbestand van een elektronisch register waarin die zijn finale toestand heeft verkregen en niet kan worden gewijzigd of verwijderd;

   b) “gedistribueerd elektronisch register”: een elektronisch register dat verdeeld is over een reeks gedistribueerde elektronische registernodes en dat middels een consensusmechanisme tussen de gedistribueerde elektronische registernodes wordt gesynchroniseerd;

   c) “gedistribueerde elektronische registernode”: een apparaat of proces dat deel van een gedistribueerd elektronisch register uitmaakt en een volledige of gedeeltelijke kopie van de gegevensbestanden van een elektronisch register opslaat;

   d) “gedistribueerd elektronisch registernetwerk”: een netwerk van gedistribueerde elektronische registernodes dat een gedistribueerd elektronisch registerstelsel vormt;

   e) “gedistribueerd elektronisch registerstelsel”: een stelsel dat een gedistribueerd elektronisch register implementeert;

   f) “consensus”: een overeenkomst tussen gedistribueerde elektronische registernodes betreffende de geldigheid van transacties en de instandhouding van een consistente en geordende reeks gevalideerde transacties in het gedistribueerd elektronisch registerstelsel;

   g) “consensusmechanisme”: de regels en procedures op basis waarvan consensus wordt bereikt;

   h) “toepasselijke regels”: de protocollen, beleidslijnen en mechanismen die bepalen hoe het gedistribueerd elektronisch registerstelsel werkt, hoe gegevens worden gevalideerd en aan een elektronisch register worden toegevoegd en hoe deelnemers interageren;

   i) “transactie”: de kleinste eenheid van een werkproces in een elektronisch register;

   j) “werkproces”: een of meer reeksen acties om een resultaat te verkrijgen dat aan de toepasselijke regels van een elektronisch register voldoet;

   k) “gevalideerde transactie”: een transactie waarvoor de vereiste integriteit, authenticiteit en protocolspecifieke voorwaarden zijn gecontroleerd overeenkomstig de toepasselijke regels van het gedistribueerd elektronisch registerstelsel;

   l) “cryptografische link”: een verwijzing naar gegevens, vastgesteld met behulp van passende cryptografische technieken om de integriteit, authenticiteit of traceerbaarheid van de referentiegegevens en de correcte volgorde van gegevensbestanden te waarborgen;

   m) “registerverslag”: een gestructureerde voorstelling van verifieerbare informatie uit de gegevensbestanden van een elektronisch register die inzicht verschaft in specifieke activiteiten, toestanden of de naleving van vooraf vastgestelde regels;

   n) “aanbieder van gekwalificeerde elektronische registers”: een gekwalificeerde verlener van vertrouwensdiensten die een gekwalificeerde vertrouwensdienst verleent die bestaat in de registratie van gegevens in een gekwalificeerd elektronisch register;

   o) “gekwalificeerd gedistribueerd elektronisch register”: een gedistribueerd elektronisch register dat aan de voorwaarden voor een gekwalificeerd elektronisch register voldoet.

2. Indien de gekwalificeerde verlener van vertrouwensdiensten een registerverslag moet opstellen, geschiedt dat op geautomatiseerde wijze.

3. Aanbieders van gekwalificeerde elektronische registers creëren, actualiseren en onderhouden een gekwalificeerd elektronisch register en registreren daarin elektronische gegevens, overeenkomstig de volgende specificaties:

   a) voor alle aanbieders van gekwalificeerde elektronische registers, ETSI EN 319 401 v3.1.1 (2024-06), met de volgende aanpassingen:

      — 2.1 Normatieve referenties:

        [1] European Cybersecurity Certification Group, Sub-group on Cryptography: “Agreed Cryptographic Mechanisms”, gepubliceerd door het Agentschap van de Europese Unie voor cyberbeveiliging (“Enisa”);

[2] IETF RFC 7515 (mei 2015): "JSON Web Signature (JWS)";

[3] FIPS PUB 140-3 (2019) "Beveiligingseisen voor cryptografische modules";

[4] Uitvoeringsverordening (EU) 2024/482 van de Commissie van 31 januari 2024 houdende uitvoeringsbepalingen van Verordening (EU) 2019/881 van het Europees Parlement en de Raad wat betreft de vaststelling van de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC);

[5] Uitvoeringsverordening (EU) 2024/3144 van de Commissie van 18 december 2024 tot wijziging van Uitvoeringsverordening (EU) 2024/482 wat betreft toepasselijke internationale normen en tot rectificatie van die uitvoeringsverordening;

[6] ISO/IEC 15408:2022 (delen 1 tot en met 5): "Informatiebeveiliging, cyberbeveiliging en privacybescherming — Evaluatiecriteria voor IT-beveiliging".

— 6.1 Praktijkverklaring van vertrouwensdienst:

  — REQ-6.1-12 De praktijkverklaring inzake het elektronische register bevat ten minste de volgende informatie:

    — de functionele en technische capaciteiten van het platform voor elektronische registers en het gebruik ervan tijdens de registratie van gegevens in een gekwalificeerd elektronisch register als gekwalificeerde vertrouwensdienst;

    — de specifieke authenticatiemechanismen van de gegevensoorsprong die bij het verlenen van de dienst worden gebruikt;

    — de specifieke mechanismen voor chronologische ordening die bij het verlenen van de dienst worden gebruikt;

    — indien van toepassing, de cryptografische link om de volgorde van gegevensbestanden te garanderen;

    — indien van toepassing, het consensusmechanisme dat de finaliteit en de integriteit van in het register opgeslagen gegevensbestanden en transacties garandeert, inclusief de waarschuwingstijd totdat finaliteit en integriteit zijn bereikt;

    — de specifieke mechanismen voor gegevensintegriteit die bij het verlenen van de dienst worden gebruikt.

  — 6.2 Voorwaarden:

    — REQ-6.2-03 Abonnees en partijen die gebruikmaken van de vertrouwensdienst worden, voordat zij een overeenkomst aangaan, op duidelijke, volledige en gemakkelijk toegankelijke wijze, in een publiekelijk toegankelijke ruimte en individueel, in kennis gesteld van de precieze voorwaarden, inclusief de hierboven genoemde punten.

  — 6.3 Informatiebeveiligingsbeleid:

    — REQ-6.3-04X De verlener van vertrouwensdiensten stelt procedures vast om wijzigingen in de verlening van de vertrouwensdienst aan het toezichthoudend orgaan te melden, conform de zakelijke vereisten en de toepasselijke wet- en regelgeving. De verlener van vertrouwensdiensten licht het toezichthoudende orgaan ten minste op de volgende momenten in:

      — één maand voor de invoering van een wijziging;

      — drie maanden voor de geplande stopzetting van de verlening van een vertrouwensdienst.

  — 7.2 Personele middelen:

    — REQ-7.2-04X Het personeel van de verlener van vertrouwensdiensten in vertrouwensrollen is in staat om de eis van "deskundigheid, ervaring en kwalificaties" te vervullen, door middel van formele opleiding en referenties, of feitelijke ervaring, of een combinatie van beide;

— REQ-7.2-05X Dit gaat gepaard met regelmatig bijgewerkte informatie (ten minste elke twaalf maanden) over nieuwe dreigingen en actuele beveiligingspraktijken.

— 7.5 Cryptografische beheersmaatregelen:

— REQ-7.5-01X Er worden passende beveiligingscontroles uitgevoerd voor het beheer van cryptografische sleutels, cryptografische algoritmen en cryptografische apparaten gedurende hun hele levenscyclus, in voorkomend geval volgens een crypto-agility-benadering;

— REQ-7.5-02 Voor het verlenen van vertrouwensdiensten selecteert en gebruikt de verlener van vertrouwensdiensten geschikte cryptografische technieken in overeenstemming met de door de European Cybersecurity Certification Group goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [1].

Met name:

— REQ-7.5-03 Aanbieders van gekwalificeerde elektronische registers stellen de oorsprong van de gegevensbestanden in het elektronische register vast. Daartoe maken zij gebruik van geavanceerde elektronische handtekeningen op basis van gekwalificeerde certificaten of geavanceerde elektronische zegels op basis van gekwalificeerde certificaten die door de gebruikers van de dienst zijn aangemaakt overeenkomstig de volgende normen en specificaties:

a) ETSI EN 319 122-1 V1.3.1 (2023-06). Elektronische handtekeningen en infrastructuren (ESI); CAdES digitale handtekeningen; deel 1: Building blocks and CAdES baseline signatures;

b) ETSI EN 319 132-1 V1.3.1 (2024-07). Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); XAdES digitale handtekeningen; deel 1: Building blocks and CAdES baseline signatures;

c) ETSI TS 119 182-1 V1.2.1 (2024-07). Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); JAdES digitale handtekeningen; deel 1: Building blocks and JAdES baseline signatures, met de volgende aanpassing:

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

— de x5c headerparameter zoals gedefinieerd in punt 4.1.6 van IETF RFC 7515 [2] moet in de JAdES-handtekening aanwezig zijn als een ondertekende of niet-ondertekende headerparameter;

— de X5C-headerparameter moet de semantiek van IETF RFC 7515 [2], punt 4.1.6 hebben;

— de X5C-headerparameter moet de syntaxis van IETF RFC 7515 [2], punt 4.1.6 hebben.

— REQ-7.5-04 Aanbieders van gekwalificeerde elektronische registers garanderen de unieke chronologische volgorde van de gegevensbestanden in het elektronische register. Daartoe maken zij gebruik van cryptografische links op basis van hashlijsten of hashbomen, met cryptografische hashfuncties, overeenkomstig de volgende specificaties en normen:

a) SHA-256 of hogere output hashgrootte in overeenstemming met de door de Europese groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [1];

b) SHA3-256 of hogere output hashgrootte in overeenstemming met de door de Europese groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [1].

Bij wijze van alternatief maken aanbieders van gekwalificeerde elektronische registers gebruik van gekwalificeerde tijdstempels tijdens de tijdsregistratie om de unieke chronologische volgorde van de gegevensbestanden in het elektronische register te garanderen.

— REQ-7.5-05 Aanbieders van gekwalificeerde elektronische registers garanderen de integriteit van gegevensbestanden in een gekwalificeerd elektronisch register. Daartoe maken zij gebruik van geavanceerde elektronische handtekeningen op basis van gekwalificeerde certificaten of geavanceerde elektronische zegels op basis van gekwalificeerde certificaten overeenkomstig de onderstaande normen en specificaties:

  a) alle handtekening- of zegelformaten die in overeenstemming zijn met de door de Europese groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [1];

  b) SHA-256 of hogere output hashgrootte in overeenstemming met de door de Europese groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [1];

  c) SHA3-256 of hogere output hashgrootte in overeenstemming met de door de Europese groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [1];

  d) aanbieders van gekwalificeerde elektronische registers garanderen dat iedere latere wijziging in de gegevensbestanden in een elektronisch register onmiddellijk kan worden gedetecteerd.

— REQ-7.5-06 Indien digitale handtekeningmechanismen worden gebruikt, wordt de privésleutel voor ondertekening van de aanbieder van een gekwalificeerd elektronisch register bewaard en gebruikt in een beveiligd cryptografisch apparaat dat een betrouwbaar systeem is dat is gecertificeerd overeenkomstig:

  a) gemeenschappelijke criteria voor de evaluatie van de beveiliging van informatietechnologie, zoals uiteengezet in ISO/IEC 15408 ([1]) [6] of in gemeenschappelijke criteria voor de evaluatie van de beveiliging van informatietechnologie, versie CC 2022, delen 1 tot en met 5, gepubliceerd door deelnemers aan de regeling ter erkenning van certificaten van gemeenschappelijke criteria op het gebied van IT-beveiliging, en gecertificeerd tot EAL 4 of hoger, of

  b) de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC) ([2]) ([3]) [4][5] en gecertificeerd tot EAL 4 of hoger, of

  c) tot 31.12.2030, FIPS PUB 140-3 ([4]) [3] niveau 3.

Dit certificaat dient voor een beveiligingsdoelstelling of beveiligingsprofiel, of voor een moduleontwerp en beveiligingsdocumentatie, wat voldoet aan de eisen van onderhavig document, op basis van een risicoanalyse en rekening houdend met fysieke en andere niet-technische beveiligingsmaatregelen.

Indien het beveiligd cryptografisch apparaat een EUCC-certificering [4][5] heeft, dan zal dit apparaat worden geconfigureerd en gebruikt in overeenstemming met dat certificaat.

([1]) ISO/IEC 15408:2022 (delen 1 tot en met 5): "Informatiebeveiliging, cyberbeveiliging en privacybescherming — Evaluatiecriteria voor IT-beveiliging".

([2]) Uitvoeringsverordening (EU) 2024/482 van de Commissie van 31 januari 2024 houdende uitvoeringsbepalingen van Verordening (EU) 2019/881 van het Europees Parlement en de Raad wat betreft de vaststelling van de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC) (PB L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/2025-01-08).

([3]) Uitvoeringsverordening (EU) 2024/3144 van de Commissie van 18 december 2024 tot wijziging van Uitvoeringsverordening (EU) 2024/482 wat betreft toepasselijke internationale normen en tot rectificatie van die uitvoeringsverordening (PB L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

([4]) FIPS PUB 140-3 (2019): "Beveiligingseisen voor cryptografische modules".

— 7.8 Netwerkbeveiliging:

— REQ-7.8-14X De door REQ-7.8-13 aangevraagde kwetsbaarheidsscan wordt ten minste eenmaal per kwartaal uitgevoerd;

— REQ-7.8-18X De door REQ-7.8-17X aangevraagde penetratietest wordt ten minste eenmaal per jaar uitgevoerd;

— REQ-7.8-21X Firewalls worden ook geconfigureerd om alle protocollen en toegangen die niet vereist zijn voor de bedrijfsvoering van de verlener van vertrouwensdiensten te verwijderen.

— 7.9.1 Monitoring en logging:

— REQ-7.9.1-02X Bij monitoringactiviteiten moet de gevoeligheid van de verzamelde of geanalyseerde informatie in aanmerking worden genomen.

— 7.12 Beëindiging en beëindigingsplannen van de verlener van vertrouwensdiensten:

— REQ-7.12-02A Het beëindigingsplan van de verlener van vertrouwensdiensten voldoet aan de overeenkomstig artikel 24, lid 5, van Verordening (EU) nr. 910/2014 vastgestelde uitvoeringshandelingen [i.1].

b) Voor alle aanbieders van gekwalificeerde elektronische registers die gebruikmaken van gedistribueerde elektronische registertechnologie geldt verder:

1) ISO 23257: 2022 Blockchain en gedistribueerde registertechnologie — Referentiearchitectuur, punt 9, met een volledige beschrijving van het gedistribueerde elektronische registertechnologiestelsel, het overeenkomstige gedistribueerde elektronische registertechnologienetwerk en gedistribueerde elektronische registertechnologienodes;

2) ISO/TS 23635:2022. Blockchain en gedistribueerde registertechnologie — Richtsnoeren voor governance, met betrekking tot schriftelijk en openbaar toegankelijk beleid en praktijken met betrekking tot de governancestructuur voor de door hen aangeboden elektronische registerdiensten.