Publicatieblad
van de Europese Unie

NL
L-serie

2025/1946

30.9.2025

UITVOERINGSVERORDENING (EU) 2025/1946 VAN DE COMMISSIE

van 29 september 2025

tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad inzake gekwalificeerde bewaardiensten voor gekwalificeerde elektronische handtekeningen en voor gekwalificeerde elektronische zegels

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 34, lid 2, en artikel 40,

Overwegende hetgeen volgt:

(1) Kwalificeerde bewaardiensten voor gekwalificeerde elektronische handtekeningen en gekwalificeerde elektronische zegels zorgen voor de langetermijnintegriteit, de authenticiteit, het bestaansbewijs en de toegankelijkheid van het bewaarbewijs van die elektronische handtekeningen en elektronische zegels. Dit maakt het mogelijk om de rechtsgeldigheid ervan gedurende langere tijd te bewijzen en garandeert dat ze kunnen worden gevalideerd, ongeacht toekomstige technologische veranderingen. Deze diensten worden onafhankelijk verleend, of als onderdeel van een andere gekwalificeerde vertrouwensdienst zoals gekwalificeerde elektronische archiveringsdiensten.

(2) Het in artikel 34, lid 1 bis, en artikel 40 van Verordening (EU) nr. 910/2014 uiteengezette vermoeden van overeenstemming mag alleen worden toegepast wanneer gekwalificeerde bewaardiensten voor gekwalificeerde elektronische handtekeningen en voor gekwalificeerde elektronische zegels voldoen aan de in deze verordening uiteengezette normen. Deze normen moeten vaste praktijken weerspiegelen en in de betrokken sectoren algemeen erkend worden. Ze moeten worden aangepast om er aanvullende controles in op te nemen die de veiligheid en betrouwbaarheid van de gekwalificeerde vertrouwensdienst waarborgen, evenals het vermogen om de gekwalificeerde status en technische geldigheid van de handtekeningen en zegels na verloop van tijd te verifiëren.

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

(4) De Commissie voert regelmatig beoordelingen van nieuwe technologieën, praktijken, normen of technische specificaties uit. Overeenkomstig overweging 75 van Verordening (EU) 2024/1183 van het Europees Parlement en de Raad ([2]) moet de Commissie deze verordening indien nodig evalueren en actualiseren om deze in overeenstemming te houden met de mondiale ontwikkelingen, de nieuwe technologieën, de 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).

(5) 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.

(6) De Europese Toezichthouder voor gegevensbescherming is overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([5]) geraadpleegd en heeft op 6 juni 2025 een advies uitgebracht.

(7) 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 34, lid 2, en artikel 40 van Verordening (EU) nr. 910/2014 genoemde referentienormen en specificaties 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, 29 september 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]) 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).

BIJLAGE

Lijst van de in artikel 2 bedoelde referentienormen en specificaties

De normen ETSI TS 119 511 V1.1.1 (2019-06) ("ETSI TS 119 511"), en ETSI TS 119 172-4 V1.1.1 (2021-05) ("ETSI TS 119 172-4") zijn van toepassing met de volgende aanpassingen:

1. Voor ETSI TS 119 511

   1) 2.1 Normatieve referenties:

      — [1] ETSI EN 319 401 V3.1.1 (2024-06) "Elektronische handtekeningen en infrastructuren (ESI); Algemene beleidseisen voor verleners van vertrouwensdiensten".

      — [2] ETSI TS 119 612 (V2.3.1) "Elektronische handtekeningen en infrastructuren (ESI); Vertrouwenslijsten".

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

      — [6] Uitvoeringsverordening (EU) 2024/482 van de Commissie ([1]) 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).

      — [7] Uitvoeringsverordening (EU) 2024/3144 van de Commissie ([2]) tot wijziging van Uitvoeringsverordening (EU) 2024/482 wat betreft toepasselijke internationale normen en tot rectificatie van die uitvoeringsverordening.

      — [8] Europese Groep voor cyberbeveiligingscertificering, subgroep inzake cryptografie: "Agreed Cryptographic Mechanisms", gepubliceerd door het Agentschap van de Europese Unie voor cyberbeveiliging ("Enisa") ([3]).

      — [9] ETSI TS 119 172-4 V1.1.1 (2021-05) "Elektronische handtekeningen en infrastructuren (ESI); Handtekeningbeleid; Deel 4: Toepasselijkheidsregels voor handtekeningen (validatiebeleid) voor Europese gekwalificeerde elektronische handtekeningen/zegels door middel van vertrouwenslijsten".

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

   2) 3.1 Definities

      — beveiligd cryptografisch apparaat: apparaat dat de privésleutel van de gebruiker bevat, deze sleutel tegen inbreuk beschermt en namens de gebruiker ondertekening of ontcijferingsfuncties uitvoert.

   3) 6.4 Bewaarprofielen

      — OVR-6.4-08A [WTS][WOS] De verwachte bewaartermijn van bewijsmateriaal moet in overeenstemming zijn met de door de Europese groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa[8] gepubliceerde Agreed Cryptographic Mechanisms.

      — OPMERKING 3 ongeldig.

   4) 6.5 Beleid voor het bewaren van bewijsmateriaal

      — OVR-6.5-04A De gebruikte cryptografische algoritmen moeten in overeenstemming zijn met de door de Europese groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa[8] gepubliceerde Agreed Cryptographic Mechanisms.

      — OPMERKING 1 ongeldig.

([1]) PB L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([2]) PB L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

5) 7.2 Personele middelen

— OVR-7.2-02 Het personeel van betalingsdienstaanbieders in vertrouwensrollen, en indien van toepassing zijn onderaannemers in vertrouwensrollen, is in staat om de eis van "deskundigheid, ervaring en kwalificaties" te vervullen, via formele opleiding en referenties, of daadwerkelijke ervaring, of een combinatie van beide.

— OVR-7.2-03 De overeenstemming met OVR-7.2-02 gaat gepaard met regelmatig bijgewerkte informatie (ten minste elke twaalf maanden) over nieuwe dreigingen en actuele beveiligingspraktijken.

6) 7.5 Cryptografische beheersmaatregelen

— OVR-7.5-05 [VOORWAARDELIJK] Wanneer de betalingsdienstverlener (een deel van) bewaringsbewijs ondertekent, wordt de privésleutel voor ondertekening van de betalingsdienstaanbieder 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 [10] 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) EUCC [6][7] en gecertificeerd tot EAL 4 of hoger; of

c) tot 31.12.2030, FIPS PUB 140-3 [5] 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 baat heeft bij een EUCC [6][7]-certificering, dan zal dit apparaat worden geconfigureerd en gebruikt in overeenstemming met dat certificaat.

— OVR-7.5-06 [VOORWAARDELIJK] ongeldig.

— OVR-7.5-07 [VOORWAARDELIJK] Wanneer de betaaldienstverlener (deel van) een bewaarbewijs ondertekent, worden reservekopieën van de privésleutels voor ondertekening van de betaaldienstverlener door het beveiligd cryptografisch apparaat beveiligd ter waarborging van de integriteit en vertrouwelijkheid ervan, voordat het wordt bewaard buiten dat apparaat.

— OVR-7.5-08 Een privésleutel van de betaaldienstverlener wordt alleen geëxporteerd en geïmporteerd naar een ander beveiligd cryptografisch apparaat waar deze export en import beveiligd worden uitgevoerd en in overeenstemming met de certificering van deze apparaten.

7) 7.8 Netwerkbeveiliging

— OVR-7.8-03 De door REQ-7.8-13 van ETSI EN 319.401 [1] aangevraagde kwetsbaarheidsscan wordt ten minste eenmaal per kwartaal uitgevoerd.

— OVR-7.8-04 De door REQ-7.8-17X van ETSI EN 319.401 [1] aangevraagde penetratietest wordt ten minste eenmaal per jaar uitgevoerd.

— OVR-7.8-05 Firewalls worden geconfigureerd om alle protocollen en toegangen die niet vereist zijn voor de bedrijfsvoering van de betaaldienstverlener te verwijderen.

8) 7.14 Cryptografisch toezicht

— OVR-7.14-03A De evaluatie van de cryptografische algoritmen in OVR-7.14.01 en OVR-7.14.02 is in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [8].

— OPMERKING ongeldig.

9) 7.12 Beëindiging en beëindigingsplannen van de verlener van vertrouwensdiensten

— OVR-7.12-01A Het beëindigingsplan van de verlener van vertrouwensdiensten voldoet aan de eisen van de overeenkomstig artikel 24, lid 5, van Verordening (EU) nr. 910/2014 vastgestelde uitvoeringshandelingen [i.2].

10) 7.17 Toeleveringsketen

— OVR-7.17-01 De in ETSI EN 319 401 [1], clausule 7.14 bedoelde eisen zijn van toepassing.

11) Bijlage A (normatief): Gekwalificeerde bewaardiensten voor gekwalificeerde elektronische handtekeningen zoals gedefinieerd door artikel 34 van Verordening (EU) nr. 910/2014.

— OVR-A-02 [PDS][PDS+PGD]

a) de bewaardienst bewaart alle vereiste informatie om de gekwalificeerde status van de elektronische handtekening of het elektronisch zegel te controleren die niet openbaar beschikbaar zou zijn tot het einde van de bewaarperiode;

b) de bewaardienst zorgt ervoor dat op elk moment tijdens de bewaarperiode de bewaarde informatie van dien aard is dat, wanneer deze wordt verstrekt als input voor het in clausule 4.4 van ETSI TS 119 172-4 [9] bedoelde proces, de output van dit proces duidelijk bepaalt of de digitale handtekening of het digitale zegel op het moment van bewaring technisch geschikt was om een EU-gekwalificeerde elektronische handtekening of EU-gekwalificeerd elektronisch zegel uit te voeren.

— OVR-A-03 [PDS][PDS+PGD] Tijdstempels die worden gebruikt binnen het bewaarbewijs zijn gekwalificeerde tijdstempels in overeenstemming met Verordening (EU) nr. 910/2014 [i.2].

2. Voor ETSI TS 119 172-4

1) 2.1 Normatieve referenties:

— [1] ETSI EN 319.102-1 V1.4.1 (2024-06) “Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); Procedures voor het aanmaken en het valideren van geavanceerde elektronische handtekeningen; Deel 1: Aanmaken en valideren”.

— Alle verwijzingen naar “ETSI TS 119 102-1 [1]” worden begrepen als verwijzingen naar “ETSI EN 319 102-1 [1]”.

— [2] ETSI TS 119 612 (V2.3.1) “Elektronische handtekeningen en infrastructuren (ESI); Vertrouwenslijsten”.

— [13] ETSI TS 119 101 V1.1.1 (2016-03) “Elektronische handtekeningen en infrastructuren (ESI); Beleids- en beveiligingseisen voor toepassingen voor het aanmaken en valideren van handtekeningen”.

2) 4.2 Validatiebeperkingen en validatieprocedures, vereiste REQ-4.2-03, punt “X.509 validatiebeperkingen”, punt c):

— i) Indien een eindgebruikerscertificaat een vertrouwensanker is, mogen de RevocationCheckingConstraints (beperkingen voor intrekkingscontrole) niet worden gebruikt.

— ii) Indien een eindgebruikerscertificaat geen vertrouwensanker is, mogen de RevocationCheckingConstraints (beperkingen voor intrekkingscontrole) worden ingesteld op “eitherCheck” (controle via één van beide methodes) als bedoeld in ETSI TS 119 172-1 [3], clausule A.4.2.1, tabel A.2, rijen (m)2.1.

— iii) Indien een eindgebruikerscertificaat een vertrouwensanker is, mogen de RevocationFreshnessConstraints (vereisten voor de actualiteit van de intrekkingsstatus) als bedoeld in ETSI TS 119 172-1 [3], clausule A.4.2.1, tabel A.2, rijen (m)2.2, niet worden gebruikt.

— iv) Indien een eindgebruikerscertificaat geen vertrouwensanker is, mogen de RevocationFreshnessConstraints (vereisten voor de actualiteit van de intrekkingsstatus) als bedoeld in ETSI TS 119 172-1 [3], clausule A.4.2.1, tabel A.2, rijen (m)2.2, worden gebruikt met een maximumwaarde van 0 uur voor het ondertekeningscertificaat. Dit garandeert dat de intrekkingsinformatie alleen wordt aanvaard, als het wordt verleend na de beste tijd voor ondertekening. Er wordt geen waarde worden ingesteld voor de RevocationFreshnessConstraints voor certificaten anders dan het handtekeningcertificaat, inclusief certificaten die tijdstempels ondersteunen.

3) 4.3 Eisen inzake de validering van handtekeningen en controlepraktijken van toepasselijkheidsregels

— REQ-4.3-02 Toepassingen voor validering van handtekeningen zijn in overeenstemming met ETSI TS 119 101 [13].

4) 4.4 Proces voor de controle van de technische toepasselijkheid (regels)

— REQ-4.4.2-03 als één van de in REQ-4.4.2-01 bedoelde controles mislukt, dan:

— stopt het proces:

— wordt de handtekening technisch geclassificeerd als onbepaald, dat wil zeggen: noch als een gekwalificeerde elektronische handtekening van de EU, noch als een gekwalificeerd elektronisch zegel van de EU;

— worden het bovenstaande resultaat en de procesresultaten van alle tussenliggende processen weergegeven in het controleverslag over de toepasselijkheid van de handtekeningregels.