Publicatieblad
van de Europese Unie

NL
L-serie

2025/1943

30.9.2025

UITVOERINGSVERORDENING (EU) 2025/1943 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 referentienormen voor gekwalificeerde certificaten voor elektronische handtekeningen en gekwalificeerde certificaten voor 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 28, lid 6, en artikel 38, lid 6,

Overwegende hetgeen volgt:

(1) Gekwalificeerde certificaten voor elektronische handtekeningen en gekwalificeerde certificaten voor elektronische zegels spelen een cruciale rol in de digitale zakelijke omgeving doordat ze de transitie van traditionele, op papier gebaseerde processen naar elektronische equivalenten bevorderen. Door gegevens voor de validering van elektronische handtekeningen of gegevens voor de validering van elektronische zegels te koppelen aan respectievelijk een natuurlijk persoon of een rechtspersoon en door de naam van die persoon te bevestigen, zorgen certificaten voor meer zekerheid ten aanzien van de identiteit van de ondertekenaar en de zegelaanmaker.

(2) Het in artikel 28, lid 6, en artikel 38, lid 6, van Verordening (EU) nr. 910/2014 uiteengezette vermoeden van overeenstemming mag alleen worden toegepast wanneer gekwalificeerde vertrouwensdiensten voor de verlening van gekwalificeerde certificaten voor elektronische handtekeningen en gekwalificeerde vertrouwensdiensten voor de verlening van gekwalificeerde certificaten voor 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 vertrouwensdiensten en van de inhoud van gekwalificeerde certificaten waarborgen.

(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.

(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.

([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).

([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).

(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 voor gekwalificeerde certificaten voor elektronische handtekeningen en elektronische zegels

1. De in artikel 28, lid 6, van Verordening (EU) nr. 910/2014 bedoelde referentienormen en specificaties worden uiteengezet in bijlage I bij deze verordening.

2. De in artikel 38, lid 6, van Verordening (EU) nr. 910/2014 bedoelde referentienormen en specificaties worden uiteengezet in bijlage II 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

([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 I

Lijst van referentienormen en specificaties voor gekwalificeerde certificaten voor elektronische handtekeningen

De normen ETSI EN 319 411-2 V2.6.1 ("ETSI EN 319 411-2"), ETSI EN 319 412-1 V1.6.1 ("ETSI EN 319 412-1"), ETSI EN 319 412-2 V2.4.1 ("ETSI EN 319 412-2"), en ETSI EN 319 412-5 V2.5.1 ("ETSI EN 319 412-5") zijn van toepassing met de volgende aanpassingen:

1. Voor ETSI EN 319 411-2

   1) 2.1 Normatieve referenties

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

      — [2] ETSI EN 319 411-1 V1.5.1 (2025-04) "Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); Beleids- en beveiligingseisen voor verleners van vertrouwensdiensten die certificaten afgeven; Deel 1: Algemene eisen", met de volgende aanpassingen:

        Clausule 2.1 Normatieve referenties van ETSI EN 319 411-1 V1.5.1 worden als volgt gewijzigd:

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

        — [10] ETSI EN 319 412-2 V2.4.1 "Elektronische handtekeningen en infrastructuren (ESI); Certificaatprofielen; Deel 2: Certificaatprofielen voor aan natuurlijke personen afgegeven certificaten".

        — [14] ETSI EN 319 412-1 V1.6.1 "Elektronische handtekeningen en infrastructuren (ESI); Certificaatprofielen; Deel 1: Overzicht en gemeenschappelijke gegevensstructuren".

      — [3] ETSI EN 319 412-5 V2.5.1 "Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); Certificaatprofielen; Deel 5: KcVermeldingen".

      — [5] ETSI EN 319 412-1 V1.6.1 "Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); Certificaatprofielen; Deel 1: Overzicht en gemeenschappelijke gegevensstructuren".

      — [6] CEN/TS 419261:2015 Beveiligingseisen voor betrouwbare systemen die certificaten en tijdstempels beheren".

      — [7] Europese Groep voor cyberbeveiligingscertificering, subgroep inzake cryptografie: "Agreed Cryptographic Mechanisms", gepubliceerd door het Agentschap van de Europese Unie voor cyberbeveiliging ("Enisa") ([1]).

      — [8] Uitvoeringsverordening (EU) 2024/482 van de Commissie ([2]) 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).

      — [9] Uitvoeringsverordening (EU) 2024/3144 van de Commissie ([3]) tot wijziging van Uitvoeringsverordening (EU) 2024/482 wat betreft toepasselijke internationale normen en tot rectificatie van die uitvoeringsverordening.

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

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

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

2) 5.2 Eisen van certificatiepraktijkverklaring

— OVR-5.2-02 De door de verlener van vertrouwensdiensten vastgestelde certificatiepraktijken vermelden de eisen van de te gebruiken certificaatprofielen.

3) 5.3 Naam en identificatie van certificaatbeleid

— OVR-5.3-01 Als een certificaatbeleid moet worden gewijzigd zoals beschreven in clausule 4.2.2, en een impact heeft op de toepassing, dan moet de beleidsidentificator worden aangepast.

4) 6.1 Verantwoordelijkheden voor publicatie en registratie

— OVR-6.1-02 De in DIS-6.1-04 van ETSI EN 319 411-1 [2] vastgestelde informatie wordt openbaar en internationaal ter beschikking gesteld.

5) 6.2.2 Initiële identiteitsvalidatie

— REG-6.2.2-01A De verzameling van attributen en bewijs inzake de identiteit van de betrokkene gebeurt overeenkomstig de krachtens artikel 24, lid 1, punt c), van Verordening (EU) nr. 910/2014 [i.1] vastgestelde uitvoeringshandelingen.

— REG-6.2.2-02 [QCP-n] en [QCP-n-qscd] De identiteit van de natuurlijke persoon en, indien van toepassing, specifieke attributen van de persoon, worden geverifieerd overeenkomstig de krachtens artikel 24, lid 1, punt c), van Verordening (EU) nr. 910/2014 [i.1] vastgestelde uitvoeringshandelingen.

— OPMERKING 1 ongeldig.

6) 6.3.3 Verlening van certificaten

— GEN-6.3.3-01 De eisen GEN-6.3.3-01 tot en met GEN-6.3.3-10 die zijn vastgesteld in ETSI EN 319 411-1 [2], clausule 6.3.3, zijn van toepassing.

— GEN-6.3.3-02 [VOORWAARDELIJK] Indien een certificaat wordt verleend aan een natuurlijk persoon die werd geïdentificeerd in verband met de rechtspersoon, dan vertegenwoordigen de attributen van de betrokkene die de organisatie in het certificaat identificeren de rechtspersoon of subentiteit van die rechtspersoon en is de identificator van de betrokkene in het certificaat de natuurlijke persoon.

— GEN-6.3.3-03 De identificator van het certificaatbeleid is [KEUZE]:

a) [QCP-n]

— zoals gespecificeerd in clausule 5.3, punt a), en/of

— een door de verlener van vertrouwensdiensten toegewezen objectidentificator, andere belanghebbenden of verdere normalisatie voor een certificaatbeleid dat de overeenstemmende in onderhavig document toepasselijke beleidseisen versterkt.

b) [QCP-n-qscd]

— zoals gespecificeerd in clausule 5.3, punt c), en/of

— een door de verlener van vertrouwensdiensten toegewezen objectidentificator, andere belanghebbenden of verdere normalisatie voor een certificaatbeleid dat de overeenstemmende in onderhavig document toepasselijke beleidseisen versterkt.

7) 6.3.5 Sleutelpaar en certificaatgebruik

— SDP-6.3.5-02A [VOORWAARDELIJK] Als de verlener van vertrouwensdiensten het gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en zegels voor de betrokkene beheert, is de verlener van vertrouwensdiensten een gekwalificeerde verlener van vertrouwensdiensten die een gekwalificeerde vertrouwensdienst verleent voor het beheer van een extern gekwalificeerd middel voor het aanmaken van elektronische handtekeningen, overeenkomstig Verordening (EU) nr. 910/2014 [i.1].

— SDP-6.3.5-11A De verplichtingen van de inschrijver (zie clausule 6.3.4) omvatten, indien de inschrijver of betrokkene de sleutels van de betrokkene genereert:

a) een verplichting om de sleutels van de betrokkene te genereren met behulp van een algoritme dat in overeenstemming is met de door de Europese Groep voor cyberbeveiligingscertificering [7] goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms om de gecertificeerde sleutel te gebruiken zoals vastgesteld in het certificaatbeleid;

b) een verplichting om sleutellengte en algoritme te gebruiken in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering [7] goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms om de gecertificeerde sleutel te gebruiken zoals vastgesteld in het certificaatbeleid tijdens de geldigheidsduur van het certificaat.

8) 6.3.10 Certificaatstatusdiensten

— CSS-6.3.10-08 [VOORWAARDELIJK] Als er certificaatintrekkingslijsten worden geleverd, behoudt de verlener van vertrouwensdiensten de integriteit en de beschikbaarheid van de laatste certificaatintrekkingslijst ten minste voor de in het het certificaatbeleid bedoelde periode, zoals vereist in CSS-6.3.10-12.

9) 6.4.4 Personeelscontroles

— OVR-6.4.4-02 Het personeel van de verlener van vertrouwensdiensten in vertrouwensrollen, en indien van toepassing, zijn onderaannemers in vertrouwensrollen, is in staat om de eis van "deskundigheid, ervaring en kwalificaties" te vervullen, door middel van formele opleiding en referenties, feitelijke ervaring, of een combinatie van beide.

— OVR-6.4.4-03 De overeenstemming met OVR-6.4.4-02 gaat gepaard met regelmatig bijgewerkte informatie (ten minste elke twaalf maanden) over nieuwe dreigingen en actuele beveiligingspraktijken.

— OVR-6.4.4-04 Naast de in ETSI EN 319 401 [1], (clausule 7.2-15) vastgestelde vertrouwensrollen, worden de vertrouwensrollen van de functionarissen voor registratie en intrekking ondersteund met bevoegdheden als bedoeld in TS 419261 [6]. In gevallen waar de gekwalificeerde verlener van vertrouwensdiensten rechtstreeks wordt beheerd of wordt geëxploiteerd namens een lidstaat of openbare instantie, kunnen de aanvullende vertrouwensrollen worden ingevuld door één of meer formele vertegenwoordigers die optreden voor of namens de functionarissen voor registratie en intrekking bij lokale of regionale besturen.

10) 6.4.9 Beëindiging certificaatautoriteit en registratieautoriteit

— OVR-6.4.9-02 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.1].

11) 6.5.1 Generatie en installatie van sleutelpaar

— OVR-6.5.1-01A De generatie van het sleutelpaar door de certificaatautoriteit wordt uitgevoerd aan de hand van een algoritme, in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [7] ter ondertekening door de certificaatautoriteit.

— OVR-6.5.1-01B De geselecteerde sleutellengte en het geselecteerde algoritme voor de sleutel van de certificaatautoriteit wordt uitgevoerd aan de hand van een algoritme, in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [7] ter ondertekening door de certificaatautoriteit.

— OVR-6.5.1-01C [VOORWAARDELIJK] Als de certificaatautoriteit de sleutels van de betrokkene genereert, zijn de door de certificaatautoriteit gegenereerde sleutels van de betrokkene in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [7] voor de in het certificaatbeleid bedoelde doeleinden tijdens de geldigheidsduur van het certificaat.

12) 6.5.2 Beveiliging van privésleutels en technische controles van cryptografische module

— GEN-6.5.2-01 Alle in ETSI EN 319 411-1 [2], clausule 6.5.2, vastgestelde eisen zijn van toepassing, behalve eisen OVR-6.5.2-01, OVR-6.5.2-03 en OVR-6.5.2-04.

— GEN-6.5.2-02 De generatie van het sleutelpaar door de verlener van vertrouwensdiensten, waaronder sleutels die worden gebruikt voor intrekkings- en registratiediensten, wordt uitgevoerd op een beveiligd cryptografisch apparaat: een betrouwbaar systeem dat is gecertificeerd in overeenstemming met:

— 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 2002, 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

— de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC) [8][9] en gecertificeerd tot EAL 4 of hoger; of

— tot 31.12.2030, FIPS PUB 140-3 [11] 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 [8][9]-certificering, dan zal dit apparaat worden geconfigureerd en gebruikt in overeenstemming met dat certificaat.

— GEN-6.5.2-03 De privésleutel voor handtekening van de certificaatautoriteit wordt bewaard en gebruikt in een beveiligd cryptografisch apparaat dat voldoet aan de eisen van GEN-6.5.2-01 en GEN-6.5.2-02.

13) 6.5.7 Netwerkbeveiligingscontroles

— OVR-6.5.7-02 De door REQ-7.8-13 van ETSI EN 319 401 [1] aangevraagde kwetsbaarheidsscan wordt ten minste eenmaal per kwartaal uitgevoerd.

— OVR-6.5.7-03 De door REQ-7.8-17X van ETSI EN 319 401 [1] aangevraagde penetratietest wordt ten minste eenmaal per jaar uitgevoerd.

— OVR-6.5.7-04 Firewalls worden geconfigureerd om alle protocollen en toegangen die niet vereist zijn voor de bedrijfsvoering van de verlener van vertrouwensdiensten te verwijderen.

14) 6.6.1 Certificaatprofiel

— GEN-6.6.1-05 Het certificaat omvat één van de in GEN-6.3.3-03 [KEUZE] vastgestelde beleidsidentificatoren. Het certificaat omvat andere door de verlener van vertrouwensdiensten toegewezen objectidentificatoren.

2. Voor ETSI EN 319 412-2

1) 2.1 Normatieve referenties

— [2] ETSI EN 319 412-5 V2.5.1 “Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); Certificaatprofielen; Deel 5: KcVermeldingen”.

— [9] Europese Groep voor cyberbeveiligingscertificering, subgroep inzake cryptografie: “Agreed Cryptographic Mechanisms”, gepubliceerd door Enisa.

2) 4.2.2 Handtekening

— GEN-4.2.2-2 Het algoritme voor handtekeningen wordt geselecteerd in overeenstemming met de door de Europese groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [9].

— OPMERKING ongeldig.

3) 4.2.3.1 Verleners die rechtspersonen zijn

— GEN-4.2.3.1-3 Indien er een geschikt registratienummer bekend is, dan bevat de identiteit van de verlener de organisatie-identificatiecode met een waarde van dat registratienummer zoals vermeld in het overeenstemmende officiële register waarin dat registratienummer is vastgesteld.

4) 4.2.5 Informatie onderwerp publieke sleutel

— GEN-4.2.5-2 Het onderwerp publieke sleutel wordt geselecteerd in overeenstemming met de door de Europese groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa [9] gepubliceerde Agreed Cryptographic Mechanisms.

— OPMERKING ongeldig.

5) 4.2.6 Serienummer

— GEN-4.2.6-01 Het serienummer van het certificaat (zoals vermeld in IETF RFC 5280 [1], clausule 4.1.2.2) is uniek voor elk door de verlener van vertrouwensdiensten afgegeven certificaat.

BIJLAGE II

Lijst van referentienormen en specificaties voor gekwalificeerde certificaten voor elektronische zegels

De normen ETSI EN 319 411-2 V2.6.1 ("ETSI EN 319 411-2"), ETSI EN 319 412-1 V1.6.1 ("ETSI EN 319 412-1"), ETSI EN 319 412-3 V1.3.1 ("ETSI EN 319 412-3"), ETSI EN 319 412-2 V2.4.1 ("ETSI EN 319 412-2"), en ETSI EN 319 412-5 V2.5.1 ("ETSI EN 319 412-5") zijn van toepassing met de volgende aanpassingen:

1. Voor ETSI EN 319 411-2

1) 2.1 Normatieve referenties

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

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) "Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); Beleids- en beveiligingseisen voor verleners van vertrouwensdiensten die certificaten afgeven; Deel 1: Algemene eisen", met de volgende aanpassingen:

Clausule 2.1 Normatieve referenties van ETSI EN 319 411-1 V1.5.1 worden als volgt gewijzigd:

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

— [10] ETSI EN 319 412-2 V2.4.1 "Elektronische handtekeningen en infrastructuren (ESI); Certificaatprofielen; Deel 2: Certificaatprofielen voor aan natuurlijke personen afgegeven certificaten".

— [14] ETSI EN 319 412-1 V1.6.1 "Elektronische handtekeningen en infrastructuren (ESI); Certificaatprofielen; Deel 1: Overzicht en gemeenschappelijke gegevensstructuren".

— [3] ETSI EN 319 412-5 V2.5.1 "Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); Certificaatprofielen; Deel 5: KcVermeldingen".

— [5] ETSI EN 319 412-1 V1.6.1 "Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); Certificaatprofielen; Deel 1: Overzicht en gemeenschappelijke gegevensstructuren".

— [6] CEN/TS 419261:2015 Beveiligingseisen voor betrouwbare systemen die certificaten en tijdstempels beheren", (geproduceerd door CEN).

— [7] Europese Groep voor cyberbeveiligingscertificering, subgroep inzake cryptografie: "Agreed Cryptographic Mechanisms", gepubliceerd door Enisa.

— [8] Uitvoeringsverordening (EU) 2024/482 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).

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

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

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

2) 5.2 Eisen van certificatiepraktijkverklaring

— OVR-5.2-02 De door de verlener van vertrouwensdiensten vastgestelde certificatiepraktijken vermelden de eisen van de te gebruiken certificaatprofielen.

3) 5.3 Naam en identificatie van certificaatbeleid

— OVR-5.3-01 Als een certificaatbeleid moet worden gewijzigd zoals beschreven in clausule 4.2.2, en een impact heeft op de toepassing, dan moet de beleidsidentificator worden aangepast.

4) 6.1 Verantwoordelijkheden voor publicatie en registratie

— OVR-6.1-02 De in DIS-6.1-04 van ETSI EN 319 411-1 [2] vastgestelde informatie wordt openbaar en internationaal ter beschikking gesteld.

5) 6.2.2 Initiële identiteitsvalidatie

— REG-6.2.2-01A De verzameling van attributen en bewijs inzake de identiteit van de betrokkene gebeurt in overeenstemming met de krachtens artikel 24, lid 1, punt c), van Verordening (EU) nr. 910/2014 [i.1] vastgestelde uitvoeringshandelingen.

— REG-6.2.2-03 [QCP-l] en [QCP-l-qscd] De identiteit van de rechtspersoon en, indien van toepassing, specifieke attributen van de persoon, worden geverifieerd in overeenstemming met de krachtens artikel 24, lid 1, punt c), van Verordening (EU) nr. 910/2014 [i.1] vastgestelde uitvoeringshandelingen.

— Opmerking 3 zie opmerking 2.

6) 6.3.3 Verlening van certificaten

— GEN-6.3.3-01 De eisen GEN-6.3.3-01 tot en met GEN-6.3.3-10 die zijn vastgesteld in ETSI EN 319 411-1 [2], clausule 6.3.3, zijn van toepassing.

— GEN-6.3.3-02 De identificator van het certificaatbeleid is [KEUZE]:

a) [QCP-l]

— zoals gespecificeerd in clausule 5.3, punt b), en/of

— een door de verlener van vertrouwensdiensten toegewezen objectidentificator, andere belanghebbenden of verdere normalisatie voor een certificaatbeleid dat de overeenstemmende in onderhavig document bepaalde toepasselijke beleidseisen versterkt.

b) [QCP-l-qscd]

— zoals gespecificeerd in clausule 5.3, punt d), en/of

— een door de verlener van vertrouwensdiensten toegewezen objectidentificator, andere belanghebbenden of verdere normalisatie voor een certificaatbeleid dat de in onderhavig document toepasselijke beleidseisen versterkt.

7) 6.3.5 Sleutelpaar en certificaatgebruik

— SDP-6.3.5-02A [VOORWAARDELIJK] Als de verlener van vertrouwensdiensten het gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en zegels voor de betrokkene beheert, is de verlener van vertrouwensdiensten een gekwalificeerde verlener van vertrouwensdiensten die een gekwalificeerde vertrouwensdienst verleent voor het beheer van een extern gekwalificeerd middel voor het aanmaken van elektronische zegels, overeenkomstig Verordening (EU) nr. 910/2014 [i.1]

— SDP-6.3.5-11A De verplichtingen van de inschrijver (zie clausule 6.3.4) omvatten, indien de inschrijver of betrokkene de sleutels van de betrokkene genereert:

a) een verplichting om de sleutels van de betrokkene te genereren met behulp van een algoritme dat in overeenstemming is met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [7] om de gecertificeerde sleutel te gebruiken zoals vastgesteld in het certificaatbeleid; en

b) een verplichting om sleutellengte en algoritme te gebruiken in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [7] om de gecertificeerde sleutel te gebruiken zoals vastgesteld in het certificaatbeleid tijdens de geldigheidsduur van het certificaat.

8) 6.3.10 Certificaatstatusdiensten

— CSS-6.3.10-08 [VOORWAARDELIJK] Als er certificaatintrekkingslijsten worden geleverd, behoudt de verlener van vertrouwensdiensten de integriteit en de beschikbaarheid van de laatste certificaatintrekkingslijst ten minste voor de in het certificaatbeleid bedoelde periode, zoals vereist in CSS-6.3.10-12.

9) 6.4.4 Personeelscontroles

— OVR-6.4.4-02 Het personeel van de verlener van vertrouwensdiensten in vertrouwensrollen, en indien van toepassing, zijn onderaannemers in vertrouwensrollen, is in staat om de eis van "deskundigheid, ervaring en kwalificaties" te vervullen, door middel van formele opleiding en referenties, feitelijke ervaring, of een combinatie van beide.

— OVR-6.4.4-03 De overeenstemming met OVR-6.4.4-02 gaat gepaard met regelmatig bijgewerkte informatie (ten minste elke twaalf maanden) over nieuwe dreigingen en actuele beveiligingspraktijken.

— OVR-6.4.4-04 Naast de in ETSI EN 319 401 [1], (clausule 7.2-15) vastgestelde vertrouwensrollen, worden de vertrouwensrollen van de functionarissen voor registratie en intrekking ondersteund met bevoegdheden als bedoeld in TS 419261 [6]. In gevallen waar de gekwalificeerde verlener van vertrouwensdiensten rechtstreeks wordt beheerd of wordt geëxploiteerd namens een lidstaat of openbare instantie, kunnen de aanvullende vertrouwensrollen worden ingevuld door één of meer formele vertegenwoordigers die optreden voor of namens de functionarissen voor registratie en intrekking bij lokale of regionale besturen.

10) 6.4.9 Beëindiging certificaatautoriteit en registratieautoriteit

— OVR-6.4.9-02 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.1]].

11) 6.5.1 Generatie en installatie van sleutelpaar

— OVR-6.5.1-01A De generatie van het sleutelpaar door de certificaatautoriteit wordt uitgevoerd aan de hand van een algoritme, in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [7] ter ondertekening door de certificaatautoriteit.

— OVR-6.5.1-01B De geselecteerde sleutellengte en het geselecteerde algoritme voor de sleutel van de certificaatautoriteit wordt uitgevoerd aan de hand van een algoritme, in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [7] ter ondertekening door de certificaatautoriteit.

— OVR-6.5.1-01C [VOORWAARDELIJK] Als de certificaatautoriteit de sleutels van de betrokkene genereert, zijn de door de certificaatautoriteit gegenereerde sleutels van de betrokkene in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [7] voor de in het certificaatbeleid bedoelde doeleinden tijdens de geldigheidsduur van het certificaat.

12) 6.5.2 Beveiliging van privésleutels en technische controles van cryptografische module

— GEN-6.5.2-01 Alle in ETSI EN 319 411-1 [2], clausule 6.5.2, vastgestelde eisen zijn van toepassing, behalve eisen OVR-6.5.2-01, OVR-6.5.2-03 en OVR-6.5.2-04.

— GEN-6.5.2-02 De generatie van het sleutelpaar door de verlener van vertrouwensdiensten, waaronder sleutels die worden gebruikt voor intrekkings- en registratiediensten, wordt uitgevoerd op een beveiligd cryptografisch apparaat: een betrouwbaar systeem dat is gecertificeerd in overeenstemming met:

  — 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 2002, 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

  — de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC) [8][9] en gecertificeerd tot EAL 4 of hoger; of

  — tot 31.12.2030, FIPS PUB 140-3 [11] 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 [8][9]-certificering, dan zal dit apparaat worden geconfigureerd en gebruikt in overeenstemming met dat certificaat.

— GEN-6.5.2-03 De privésleutel voor handtekening van de certificaatautoriteit wordt bewaard en gebruikt in een beveiligd cryptografisch apparaat dat voldoet aan de eisen van GEN-6.5.2-01 en GEN-6.5.2-02.

13) 6.5.7 Netwerkbeveiligingscontroles

— OVR-6.5.7-02 De door REQ-7.8-13 van ETSI EN 319 401 [1] aangevraagde kwetsbaarheidsscan wordt ten minste eenmaal per kwartaal uitgevoerd.

— OVR-6.5.7-03 De door REQ-7.8-17X van ETSI EN 319 401 [1] aangevraagde penetratietest wordt ten minste eenmaal per jaar uitgevoerd.

— OVR-6.5.7-04 Firewalls worden geconfigureerd om alle protocollen en toegangen die niet vereist zijn voor de bedrijfsvoering van de verlener van vertrouwensdiensten te verwijderen.

14) 6.6.1 Certificaatprofiel

— GEN-6.6.1-05 Het certificaat omvat één van de in GEN-6.3.3-02 [KEUZE] vastgestelde beleidsidentificatoren.

2. Voor ETSI EN 319 412-3

1) 2.1 Normatieve referenties

— [2] ETSI EN 319 412-2 V2.4.1 “Elektronische handtekeningen en infrastructuren (ESI); Certificaatprofielen; Deel 2: Certificaatprofiel voor aan natuurlijke personen uitgegeven certificaten”.

2) 4.2.1 Onderwerp

— LEG-4.2.1-6 Het attribuut organisatie-identificatiecode bevat een identificatie van de betrokken organisatie die verschillend is van de organisatienaam. Indien er een geschikt registratienummer bekend is, dan bevat het attribuut organisatie-identificatiecode een waarde van dat registratienummer zoals vermeld in het overeenstemmende officiële register waarin dat registratienummer is vastgesteld.

3. Voor ETSI EN 319 412-2:

1) 2.1 Normatieve referenties

— [2] ETSI EN 319 412-5 V2.5.1 “Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); Certificaatprofielen; Deel 5: KcVermeldingen”.

— [9] Europese Groep voor cyberbeveiligingscertificering, subgroep inzake cryptografie: “Agreed Cryptographic Mechanisms”, gepubliceerd door Enisa.

2) 2.2 Verwijzingen ter informatie

— [i.7] ongeldig.

3) 4.2.2 Handtekening

— GEN-4.2.2-2 Het algoritme voor handtekeningen wordt geselecteerd in overeenstemming met de door de Europese groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [9].

— OPMERKING ongeldig.

4) 4.2.3.1 Verleners die rechtspersonen zijn

— GEN-4.2.3.1-3 Indien er een geschikt registratienummer bekend is, dan bevat de identiteit van de verlener de organisatie-identificatiecode met een waarde van dat registratienummer zoals vermeld in het overeenstemmende officiële register waarin dat registratienummer is vastgesteld.

5) 4.2.5 Informatie onderwerp publieke sleutel

— GEN-4.2.5-2 Het onderwerp publieke sleutel wordt geselecteerd in overeenstemming met de door de Europese groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa [9] gepubliceerde Agreed Cryptographic Mechanisms.

— OPMERKING ongeldig.

6) 4.2.6 Serienummer

— GEN-4.2.6-01 Het serienummer van het certificaat (zoals vermeld in IETF RFC 5280 [1], clausule 4.1.2.2) is uniek voor elk door de verlener van vertrouwensdiensten afgegeven certificaat.