Publicatieblad
van de Europese Unie

NL
L-serie

2025/1942

30.9.2025

UITVOERINGSVERORDENING (EU) 2025/1942 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 valideringsdiensten voor gekwalificeerde elektronische handtekeningen en gekwalificeerde valideringsdiensten 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 33, lid 2, en artikel 40,

Overwegende hetgeen volgt:

(1) Gekwalificeerde valideringsdiensten voor gekwalificeerde elektronische handtekeningen en voor gekwalificeerde elektronische zegels waarborgen de integriteit, authenticiteit en juistheid van het proces en de resultaten van de validering van respectievelijk gekwalificeerde elektronische handtekeningen en gekwalificeerde elektronische zegels. Deze gekwalificeerde vertrouwensdiensten spelen een cruciale rol in de digitale zakelijke omgeving doordat ze de transitie van traditionele, op papier gebaseerde processen naar elektronische equivalenten bevorderen.

(2) Het in artikel 33, lid 2, en artikel 40 van Verordening (EU) nr. 910/2014 uiteengezette vermoeden van overeenstemming mag alleen worden toegepast wanneer gekwalificeerde valideringsdiensten voor gekwalificeerde elektronische handtekeningen en voor gekwalificeerde elektronische zegels voldoen aan de in deze verordening uiteengezette technische normen. Deze normen moeten vastgestelde praktijken weerspiegelen en algemeen erkend zijn in de desbetreffende sectoren. Ze moeten worden aangepast om aanvullende controles te integreren ter waarborging van zekerheid en betrouwbaarheid van de gekwalificeerde vertrouwensdiensten, evenals het vermogen om de gekwalificeerde status en technische geldigheid van gekwalificeerde handtekeningen en gekwalificeerde elektronische zegels 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 33, 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 referentienormen en specificaties voor gekwalificeerde valideringsdiensten voor gekwalificeerde elektronische handtekeningen en voor gekwalificeerde valideringsdiensten voor gekwalificeerde elektronische zegels

De normen ETSI TS 119 441 V1.2.1 (2023-10) ([1]) ("ETSI TS 119 441"), en ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) ("ETSI TS 119 172-4") zijn van toepassing met de volgende aanpassingen:

1. Voor ETSI TS 119 441

1) 2.1 Normatieve referenties

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

— [3] ETSI EN 319 102-1 V1.4.1 (2024-06) "Elektronische handtekeningen en infrastructuren (ESI); Procedures voor het aanmaken en het valideren van geavanceerde elektronische handtekeningen; Deel 1: Aanmaken en valideren".

— [4] ISO/IEC 15408-1:2022 "Informatiebeveiliging, cyberbeveiliging en privacybescherming — Evaluatiecriteria voor IT-beveiliging".

— [5] ongeldig.

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

— [7] Uitvoeringsverordening (EU) 2024/482 van de Commissie 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) ([3]).

— [8] 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".

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) "Elektronische handtekeningen en infrastructuren (ESI); Procedures voor het aanmaken en het valideren van geavanceerde elektronische handtekeningen; Deel 2: Validatieverslag voor handtekeningen".

— [10] Europese Groep voor cyberbeveiligingscertificering, subgroep inzake cryptografie: "Agreed Cryptographic Mechanisms", gepubliceerd door het Agentschap van de Europese Unie voor cyberbeveiliging ("Enisa") ([4]).

— [11] Uitvoeringsverordening (EU) 2024/3144 van de Commissie tot wijziging van Uitvoeringsverordening (EU) 2024/4822 wat betreft toepasselijke internationale normen en tot rectificatie van die uitvoeringsverordening ([5]).

— [12] ETSI EN 319 411-1 "Elektronische handtekeningen en infrastructuren (ESI); Beleids- en beveiligingseisen voor verleners van vertrouwensdiensten die certificaten afgeven; Deel 1: Algemene eisen".

([1]) ETSI TS 119 441 — Elektronische handtekeningen en infrastructuren (ESI); Policy requirements for TSP providing signature validation services (beleidseisen voor verleners van vertrouwensdiensten die valideringsdiensten voor handtekeningen leveren), V1.2.1 (2023-10).
([2]) ETSI TS 119 172-4 — Elektronische handtekeningen en infrastructuren (ESI); Signature Policies (handtekeningbeleid); Deel 4: Toepasselijkheidsregels voor handtekeningen (validatiebeleid) voor Europese gekwalificeerde elektronische handtekeningen/zegels door middel van vertrouwenslijsten, V1.1.1 (2021-05).
([3]) PB L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([4]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([5]) PB L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 2.2 Verwijzingen ter informatie

— [i.11] ongeldig.

3) 3.3 Afkortingen

— EUCC Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling

4) 4.3.3 Proces

— OPMERKING 10 Zie ETSI EN 319 102-1 [3] voor richtsnoeren en ETSI TS 119 172-4 [8] voor aanvullende richtsnoeren voor de EU-gekwalificeerde handtekening of het EU-gekwalificeerd zegel.

5) 6.1 Praktijkverklaring van de valideringsdienst voor handtekeningen

— OVR-6.1-02 De praktijkverklaring van de valideringsdienst voor handtekeningen wordt gestructureerd conform bijlage A.

— OVR-6.1-03 De praktijkverklaring van de valideringsdienst voor handtekeningen bevat een lijst van of verwijzing naar het ondersteunde beleid van de valideringsdienst voor handtekeningen (bv. via objectidentificatoren) en beschrijft deze kort.

6) 6.3 Informatiebeveiligingsbeleid

— OVR-6.3-02 Het beveiligingsbeleid bevat de ingevoerde beveiligings- en privacycontroles om persoonsgegevens te beschermen.

7) 7.2 Personele middelen

— OVR-7.2-02 Het personeel van de valideringsdienst voor handtekeningen 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, of feitelijke 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.

8) 7.5 Cryptografische beheersmaatregelen

— OVR-7.5-02 [VOORWAARDELIJK] Wanneer validatieverslagen worden ondertekend, wordt het openbare ondertekeningscertificaat van de valideringsdienst voor handtekeningen dat overeenstemt met de privésleutel voor ondertekening van de valideringsdienst voor handtekeningen verleend door een betrouwbare certificaatautoriteit, in overeenstemming met het certificaatbeleid NCP+ als bedoeld in ETSI EN 319 411-1 [12]. Het moet worden verleend in overeenstemming met een gepast certificaatbeleid als bedoeld in ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [VOORWAARDELIJK] Wanneer validatieverslagen worden ondertekend, wordt de privésleutel van de valideringsdienst voor handtekeningen bewaard en gebruikt in een beveiligd cryptografisch apparaat: een betrouwbaar systeem dat is gecertificeerd in overeenstemming met:

a) gemeenschappelijke criteria voor de evaluatie van de beveiliging van informatietechnologie, zoals uiteengezet in ISO/IEC 15408 [4] 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 [7][11] en gecertificeerd tot EAL 4 of hoger, of

c) tot en met 31.12.2030, FIPS PUB 140-3 [6] niveau 3.

Dit certificaat dient voor een beveiligingsdoelstelling of beveiligingsprofiel, of voor een moduleontwerp en beveiligingsdocumentatie, conform 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 [7][11]-certificering, dan zal dit apparaat worden geconfigureerd en gebruikt in overeenstemming met dat certificaat.

— OVR-7.5-04 ongeldig.

— OVR-7.5-06 Een privésleutel van de valideringsdienst voor handtekeningen 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.

9) 7.7 Operationele beveiliging

— OVR-7.7-02 Om te waarborgen dat de systemen waarmee de toepassing is ontwikkeld geschikte beveiligingsmaatregelen toepassen en zich aanpassen aan specifieke toepassingsomgevingen, gebruikt de SVA een toepassingsomgeving die wordt onderhouden met geactualiseerde herstel- en beveiligingsmaatregelen.

— OVR-7.7-03 De volgende in ETSI TS 119 101 [1], clausule 5.2 bedoelde eisen zijn van toepassing op de SVA: GSM 1.3.

10) 7.8 Netwerkbeveiliging

— OVR-7.8-02 Indien externe toegang is toegestaan tot systemen voor het opslaan en verwerken van vertrouwelijke gegevens, dan wordt er een formeel beleid ingevoerd en beschreven als onderdeel van elementen die zijn vereist door OVR-6.3-02.

— OVR-7.8-04 De door REQ-7.8-13 van ETSI EN 319 401 [1] aangevraagde kwetsbaarheidsscan wordt ten minste eenmaal per kwartaal uitgevoerd.

— OVR-7.8-05 De door REQ-7.8-17X van ETSI EN 319 401 [1] aangevraagde penetratietest wordt ten minste eenmaal per jaar uitgevoerd.

— OVR-7.8-06 Firewalls worden geconfigureerd om alle protocollen en toegangen die niet vereist zijn voor de bedrijfsvoering van de valideringsdienst voor handtekeningen te verwijderen.

11) 7.12 Valideringsdienst voor handtekeningen voorziet in beëindiging en beëindigingsplannen

— OVR-7.12-02 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].

12) 7.14 Toeleveringsketen

— OVR-7.14-01 De in ETSI EN 319 401 [2], clausule 7.14 bedoelde eisen zijn van toepassing.

13) 8.1 Validatieproces voor handtekeningen

— VPR-8.1-07 De validatietoepassing (SVA) is in overeenstemming met de in ETSI TS 119 101 [1], clausule 7.4 SIA 1 tot en met SIA 4 bedoelde eisen.

— VPR-8.1-11 [VOORWAARDELIJK] Wanneer de valideringsdienst voor handtekeningen tracht om gekwalificeerde elektronische handtekeningen of gekwalificeerde elektronische zegels te valideren in overeenstemming met artikel 32, lid 1 (of artikel 40 respectievelijk) van Verordening (EU) nr. 910/2014 [i.1], dan volgt het validatieproces de eisen van ETSI TS 119 172-4 [8].

14) 8.2 Validatieprotocol voor handtekeningen

— SVP-8.2-03 De validatierespons voor handtekeningen bestaat uit de objectidentificator van het beleid van de valideringsdienst voor handtekeningen.

15) 8.4 Validatieverslag voor handtekeningen

— SVR-8.4-02 Het validatieverslag is in overeenstemming met ETSI TS 119 102-2 [9].

— SVR-8.4-07 [VOORWAARDELIJK] Wanneer een validatiebeleid voor handtekeningen niet volledig wordt verwerkt door de valideringsdienst voor handtekeningen rapporteert het verslag, naast het rapporteren van gevalideerde beperkingen, over beperkingen die werden genegeerd of overschreven.

— SVR-8.4-15 In het validatieverslag wordt duidelijk de herkomst van elk bewijsstuk vermeld (uit de gegevens die al in de handtekening zitten, van de client, van de server).

— SVR-8.4-16 Het validatierapport moet voorzien zijn van een validatierapporthandtekening, wat de digitale handtekening van de valideringsdienst voor handtekeningen moet zijn.

— SVR-8.4-17 [VOORWAARDELIJK] Wanneer validatieverslagen worden ondertekend, moet het formaat en het doel van de handtekening in overeenstemming zijn met ETSI TS 119 102-2 [9].

16) 9 Kader voor de vaststelling van beleid voor valideringsdiensten die zijn gebaseerd op een in dit document gedefinieerd beleid voor vertrouwensdiensten:

— OVR-9-05 [VOORWAARDELIJK] Wanneer er beleid voor de valideringsdienst voor handtekeningen wordt opgesteld op basis van in onderhavig document vastgesteld beleid voor vertrouwensdiensten, wordt er een risicobeoordeling uitgevoerd om de zakelijke behoeften te beoordelen en de beveiligingseisen te bepalen die moeten worden opgenomen in het beleid voor de genoemde gemeenschap en toepasselijkheid.

— OVR-9-06 [VOORWAARDELIJK] Wanneer er beleid voor de valideringsdienst voor handtekeningen wordt opgesteld op basis van in onderhavig document vastgesteld beleid voor vertrouwensdiensten, wordt het beleid goedgekeurd en gewijzigd in overeenstemming met een vastgesteld beoordelingsproces, met inbegrip van de verantwoordelijkheden voor het handhaven van het beleid.

— OVR-9-07 [VOORWAARDELIJK] Wanneer er beleid voor de valideringsdienst voor handtekeningen wordt opgesteld op basis van in onderhavig document vastgesteld beleid voor vertrouwensdiensten, moet er sprake zijn van een vastgesteld beoordelingsproces om ervoor te zorgen dat het beleid wordt ondersteund door de praktijkverklaringen.

— OVR-9-08 [VOORWAARDELIJK] Wanneer er beleid voor de valideringsdienst voor handtekeningen wordt opgesteld op basis van in onderhavig document vastgesteld beleid voor vertrouwensdiensten, stelt de verlener van vertrouwensdiensten het door de verlener van vertrouwensdiensten ondersteunde beleid ter beschikking aan zijn gebruikersgemeenschap.

— OVR-9-09 [VOORWAARDELIJK] Wanneer er beleid voor de valideringsdienst voor handtekeningen wordt opgesteld op basis van in onderhavig document vastgesteld beleid voor vertrouwensdiensten, worden de door de verlener van vertrouwensdiensten ondersteunde beleidsherzieningen ter beschikking gesteld aan abonnees.

17) Bijlage B (normatief) Gekwalificeerde valideringsdienst voor gekwalificeerde elektronische handtekeningen als bedoeld in artikel 33 van Verordening (EU) nr. 910/2014:

— VPR-B-02 [VOORWAARDELIJK] Indien de valideringsdienst voor handtekeningen een gekwalificeerde valideringsdienst voor handtekeningen is, moet de uitvoering voldoen aan ETSI TS 119 172-4 [8].

— OPMERKING 2 ongeldig.

— OVR-B-04 [VOORWAARDELIJK] Indien de valideringsdienst voor handtekeningen een gekwalificeerde valideringsdienst voor handtekeningen is, moeten de tests in OVR-B-03 verschillende praktijkvoorbeelden controleren, zowel positieve als negatieve.

— VPR-B-11 [VOORWAARDELIJK] Indien de valideringsdienst voor handtekeningen een gekwalificeerde valideringsdienst voor handtekeningen is, controleert de valideringsdienst voor handtekeningen de hash-berekening (hetzij de berekening aan de serverzijde uitvoeren, hetzij de client aansturen indien clientzijde is toegestaan).

— OPMERKING 5 ongeldig.

— OPMERKING 6 ongeldig.

— VPR-B-15 [VOORWAARDELIJK] Indien de valideringsdienst voor handtekeningen een gekwalificeerde valideringsdienst voor handtekeningen is, moet het validatieverslag in overeenstemming zijn met ETSI TS 119 102-2 [9] om te voldoen aan VPR-B-13 tot en met VPR-B-14.

— VPR-B-16 [VOORWAARDELIJK] Indien de valideringsdienst voor handtekeningen een gekwalificeerde valideringsdienst voor handtekeningen is, moet de uitvoering in overeenstemming zijn met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [10] voor gebruik van geschikte cryptografische technieken bij het verlenen van gekwalificeerde valideringsdiensten voor gekwalificeerde elektronische handtekeningen.

18) Bijlage C (informatief) Het in kaart brengen van eisen van Verordening (EU) nr. 910/2014, deel “validering verstrekt overeenkomstig artikel 32, lid 1”, tweede alinea:

— Om te waarborgen dat alle voorwaarden van artikel 32, lid 1, en artikel 40 van Verordening (EU) nr. 910/2014 [i.1] worden nageleefd, is een correct validatie-algoritme nodig. Het levert hetzelfde deterministisch resultaat op voor een handtekening of zegel die voor validatie is ingediend. Het validatiebeleid voor handtekeningen is hiervoor van cruciaal belang. ETSI TS 119 172-4 [8], gebaseerd op het in ETSI EN 319 102-1 [3] bedoelde validatie-algoritme, is met dit perspectief afgegeven.

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 (2024-11) “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):

— 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 24 uur voor het ondertekeningscertificaat. Er wordt geen waarde worden ingesteld voor de RevocationFreshnessConstraints voor certificaten anders dan het handtekeningcertificaat, inclusief certificaten die tijdstempels ondersteunen.

3) 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:

a) stopt het proces;

b) 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;

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