Publicatieblad
van de Europese Unie

NL
L-serie

2026/1735

22.7.2026

UITVOERINGSVERORDENING (EU) 2026/1735 VAN DE COMMISSIE

van 15 juli 2026

tot wijziging van Uitvoeringsverordening (EU) 2025/1569 inzake de toepasselijke normen en specificaties

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 quinquies, lid 5, artikel 45 sexies, lid 2, en artikel 45 septies, leden 6 en 7,

Overwegende hetgeen volgt:

(1) Met het oog op het hoogste niveau van harmonisatie tussen de lidstaten voor de ontwikkeling van Europese portemonnees voor digitale identiteit, zijn de technische specificaties voor de portemonnees geschraagd op de werkzaamheden op basis van Aanbeveling (EU) 2021/946 van de Commissie ([2]), en met name de architectuur en het referentiekader. Aangezien de architectuur en het referentiekader sinds de vaststelling van Uitvoeringsverordening (EU) 2025/1569 van de Commissie ([3]) aanzienlijk zijn geëvolueerd, moet Uitvoeringsverordening (EU) 2025/1569 nu dienovereenkomstig worden gewijzigd om die in overeenstemming te brengen met de nieuwe normen en specificaties.

(2) Conform de doelstellingen van Verordening (EU) nr. 910/2014 is een aantal normen geselecteerd om aan de voor de afgifte, het beheer en de verificatie van elektronische attestering van attributen geldende vereisten te voldoen. Deze normen moeten vaste praktijken weerspiegelen en in de betrokken sectoren algemeen erkend worden. Waar nodig moeten die normen worden aangepast of aangevuld om een hoog niveau van veiligheid en integriteit van elektronische attestering van attributen te waarborgen en de grensoverschrijdende interoperabiliteit en de doeltreffende werking van de interne markt te faciliteren. Conform die doelstelling worden bij deze verordening de vereisten bijgewerkt die van toepassing zijn op de afgifte en de intrekking van gekwalificeerde elektronische attesteringen van attributen en elektronische attesteringen van attributen die zijn afgegeven door of namens een voor een authentieke bron verantwoordelijke openbare instantie, en worden de vereisten voor de ondertekening en de verzegeling van verificatieresultaten aan de hand van authentieke bronnen ingevoerd.

(3) Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([4]) en, in voorkomend geval, Richtlijn 2002/58/EG van het Europees Parlement en de Raad ([5]), zijn van toepassing op alle 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]) Aanbeveling (EU) 2021/946 van de Commissie van 3 juni 2021 betreffende een gemeenschappelijke EU-toolbox voor een gecoördineerde aanpak ten behoeve van een Europees kader voor digitale identiteit (PB L 210 van 14.6.2021, blz. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Uitvoeringsverordening (EU) 2025/1569 van de Commissie van 29 juli 2025 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad inzake door of namens een voor een authentieke bron verantwoordelijke openbare instantie verstrekte gekwalificeerde elektronische attesteringen van attributen en elektronische attesteringen van attributen (PB L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([4]) 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).

([5]) 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).

(4) De Europese Toezichthouder voor gegevensbescherming is overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([6]) geraadpleegd en heeft op 17 april 2026 advies uitgebracht ([7]).

(5) 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

Wijzigingen van Uitvoeringsverordening (EU) 2025/1569

Uitvoeringsverordening (EU) 2025/1569 wordt als volgt gewijzigd:

(1) In artikel 3 wordt lid 2 vervangen door:

"2. Indien aanbieders van gekwalificeerde elektronische attesteringen van attributen en aanbieders van elektronische attesteringen van attributen die zijn afgegeven door of namens een voor een authentieke bron verantwoordelijke openbare instantie, elektronische attesteringen van attributen afgeven die zijn opgenomen in regelingen die zijn geregistreerd in de catalogus van regelingen voor de attestering van attributen, voldoen zij aan de vereisten van de overeenkomstige regeling voor de attestering van attributen. De gedragslijnen en procedures die door de uitgevers van attesteringen zijn vastgesteld om de vereisten van de regelingen voor de attestering van attributen na te leven, maken deel uit van de bij Verordening (EU) nr. 910/2014 vastgestelde conformiteitsbeoordeling.".

(2) Artikel 4 wordt als volgt gewijzigd:

a) lid 1 wordt geschrapt;

b) lid 3 wordt vervangen door:

"3. Aanbieders van gekwalificeerde elektronische attesteringen van attributen en aanbieders van elektronische attesteringen van attributen, afgegeven door of namens een voor een authentieke bron verantwoordelijke openbare instantie, trekken, indien die attesteringen zijn afgegeven met een geldigheidsduur van meer dan 24 uur, die in de volgende gevallen in:

a) op verzoek van de persoon aan wie de elektronische attestering van attributen is afgegeven, of, indien van toepassing, van het onderwerp van de attestering;

b) indien de aanbieder constateert dat inbreuk is gepleegd op de beveiliging of de betrouwbaarheid van de gekwalificeerde elektronische attesteringen van attributen of elektronische attesteringen van attributen die zijn afgegeven door of namens een voor een authentieke bron verantwoordelijke openbare instantie;

c) in andere gevallen overeenkomstig het Unierecht of het nationale recht.".

c) lid 4 wordt vervangen door:

"4. Aanbieders van gekwalificeerde elektronische attesteringen van attributen en aanbieders van elektronische attesteringen van attributen die zijn afgegeven door of namens een voor een authentieke bron verantwoordelijke openbare instantie, zetten intrekkingstechnieken en beheermethoden op die privacybeschermend zijn en koppelbaarheid en traceerbaarheid beletten. De intrekkingstechnieken voldoen aan de voorwaarden van bijlage II.".

([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 Commission Implementing Regulation as regards applicable standards and specifications for the registration of wallet-relying parties" | Europese Toezichthouder voor gegevensbescherming.

(3) Artikel 9 wordt als volgt gewijzigd:

a) na lid 2 wordt het volgende lid 2 bis ingevoegd:

"2 bis.
Het verificatiemechanisme voldoet aan de specificaties van bijlage IV.";

b) lid 4 wordt vervangen door:

"4. Het verificatieresultaat vermeldt of het attribuut al dan niet is geverifieerd en specificeert de openbare instantie die voor de authentieke bron verantwoordelijk is of, in voorkomend geval, de openbare instantie die is aangewezen om op te treden namens de authentieke bron aan de hand waarvan het attribuut is geverifieerd.

Het verificatieresultaat wordt ondertekend of verzegeld door de openbare instantie die voor de authentieke bron verantwoordelijk is, of door de op nationaal niveau erkende aangewezen intermediair, waarbij respectievelijk ten minste gebruik wordt gemaakt van een geavanceerde elektronische handtekening op basis van een gekwalificeerd certificaat voor elektronische handtekeningen of een geavanceerd elektronisch zegel op basis van een gekwalificeerd certificaat voor elektronische zegels.".

(4) Bijlage I wordt vervangen door de tekst in bijlage I bij deze verordening.

(5) Bijlage II wordt vervangen door de tekst in bijlage II bij deze verordening.

(6) De tekst in bijlage III bij deze verordening wordt toegevoegd als bijlage IV.

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*.

Artikel 1, lid 3, is van toepassing met ingang van 1 januari 2027.

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

Gedaan te Brussel, 15 juli 2026.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

BIJLAGE I

"BIJLAGE I

Lijst van de in artikel 3 bedoelde referentienormen en specificaties

ETSI TS 119 471 V1.1.1 (2025-05) geldt met de volgende aanpassingen:

(1) 2.1 Normatieve referenties:

[1] ETSI EN 319 401 V3.2.1 (2026-01): "Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); Algemene beleidseisen voor verleners van vertrouwensdiensten";

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

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

[4] Uitvoeringsverordening (EU) 2024/482 van de Commissie ([1]);

[5] Uitvoeringsverordening (EU) 2024/3144 van de Commissie ([2]);

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

(2) 3.1 Definities:
de volgende definitie wordt toegevoegd:

— 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) 4. Vertrouwensdiensten van de EAA

— Clausule 4.2.2.2 "Verificatie van attributen aan de hand van authentieke bronnen" is niet van toepassing.

— REQ-EAASP-4.2.2.3-02: De aanbieder van EAA-diensten (EAASP) authenticeert zich bij de EUDIW-instantie door toepassing van wederzijdse authenticatiemechanismen die een geldig toegangscertificaat gebruiken.

— REQ-EAASP-4.2.2.3-03: De EAASP valideert de EUDIW-eenheid en *of de EUDIW-instantie wordt ingetrokken*.

— Clausule *4.3.2 "EUDIW-specifiek" is niet van toepassing*.

(4) 6.1 Praktijkverklaring van de EAAS:

— REQ-EAASP-6.1-02: De EAASP documenteert het intrekkingsmechanismen in de praktijkverklaring van de EAAS

(5) 6.3 Informatiebeveiligingsbeleid:

— REQ-EAASP-6.3-02: De EAASP stelt procedures vast om het toezichthoudend orgaan in kennis te stellen van wijzigingen in de verlening van de vertrouwensdienst voor elektronische attestering van attributen en van het voornemen om die activiteiten te beëindigen, conform de bedrijfsvereisten en de toepasselijke wet- en regelgeving, waaronder de overeenkomstig artikel 24, lid 5, van Verordening (EU) nr. 910/2014 vastgestelde uitvoeringshandelingen. De EAASP 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.

([1]) 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/oj).

([2]) 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).

(6) 7.5 Cryptografische beheersmaatregelen:

— REQ-EAASP-7.5.2-05: ongeldig

— REQ-EAASP-7.5.2-06: ongeldig

— REQ-EAASP-7.5.3-01A: 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-EAASP-7.5.3-01B: Voor het verlenen van vertrouwensdiensten selecteert en gebruikt de EAASP geschikte cryptografische technieken in overeenstemming met de door de European Cybersecurity Certification Group goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [2].

— REQ-EAASP-7.5.3-02: De EAASP waarborgt dat het beveiligde cryptografische apparaat, gebruikt voor de digitale ondertekening of zegel van EAA een gekwalificeerd middel voor het aanmaken van handtekeningen of zegels is en dat alle andere digitale handtekeningen of zegels die worden gebruikt voor het verlenen van de overeenkomstige vertrouwensdienst voor elektronische attestering van attributen, of een deel daarvan, worden aangemaakt door middel van een beveiligd cryptografisch apparaat dat een betrouwbaar systeem is dat is gecertificeerd overeenkomstig:

  a) de gemeenschappelijke criteria voor de evaluatie van de beveiliging van informatietechnologie, zoals uiteengezet in de gemeenschappelijke criteria voor de evaluatie van de beveiliging van informatietechnologie, versie 3.1 (CC3.1) to en met 31.8.2027 of 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, of als bepaald in ISO/IEC 15408 [6] en gecertificeerd tot EAL 4 of hoger, of

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

  c) FIPS-140-2-niveau 3 te gebruiken tot en met 31.8.2027 voor bestaande gecertificeerde systemen of FIPS PUB 140-3 [3] niveau 3 tot en met 31.12.2030.

  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 [4][5]-certificering, dan zal dit apparaat worden geconfigureerd en gebruikt in overeenstemming met dat certificaat.

— REQ-EAASP-7.5.5-01: ongeldig

— REQ-EAASP-7.5.5-02: ongeldig

— REQ-EAASP-7.5.5-04: ongeldig

(7) 7.9 Kwetsbaarheden- en incidentenbeheer:

— REQ-EAASP-7.9-02: Bij monitoringactiviteiten moet de gevoeligheid van de verzamelde of geanalyseerde informatie in aanmerking worden genomen.

(8) 7.12 Beëindigings- en beëindigingsplannen van EAASP en EAAS:

— REQ-EAASP-7.12-04: Het beëindigingsplan van de EAASP voldoet aan de overeenkomstig artikel 24, lid 5, van Verordening (EU) nr. 910/2014 vastgestelde uitvoeringshandelingen [i.1].”.

BIJLAGE II

"BIJLAGE II

Technische specificaties als bedoeld in de artikelen 3 en 4

Aanbieders van gekwalificeerde elektronische attesteringen van attributen en aanbieders van elektronische attesteringen van attributen, afgegeven door of namens een voor een authentieke bron verantwoordelijk openbare instantie, geven hun attesteringen af in overeenstemming met ten minste een van de normen volgens bijlage II bij Uitvoeringsverordening (EU) 2024/2979 van de Commissie ([1]), en passen de toepasselijke intrekkingstechnieken toe, ook volgens bijlage II bij Uitvoeringsverordening (EU) 2024/2979 van de Commissie.".

([1]) Uitvoeringsverordening (EU) 2024/2979 van de Commissie van 28 november 2024 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de integriteit en de kernfunctionaliteiten van Europese portemonnees voor digitale identiteit (PB L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

BIJLAGE III

"BIJLAGE IV

Lijst van de in artikel 9 bedoelde normen en technische specificaties

De in artikel 9 bedoelde verificatiemechanismen voldoen aan een of beide van de volgende voorwaarden, met de volgende aanpassingen:

a) de technische specificaties van clausule 6.1.1 van ETSI TS 119 478 V1.1.1 (2026-01) - Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); specificaties van interfaces met betrekking tot authentieke bronnen;

— REQ-ASIP-6.1.1.2-04-01 [VOORWAARDELIJK]: Indien het AttributeVerificationResult hetzij http://uri.etsi.org/19478/VerificationResult/Match hetzij http://uri.etsi.org/19478/VerificationResult/MatchWithVariation is, kan het AttributeVerificationResult een AttributeValue-element omvatten.

— REQ-ASIP-6.1.1.2-04-02 [VOORWAARDELIJK]: Indien het teruggezonden attributeVerificationResult http://uri.etsi.org/19478/VerificationResult/Match is en het attributeVerificationResult een attributeValue element bevat, moet het attributeValue element de waarde bevatten zoals in het verzoek.

— REQ-ASIP-6.1.1.2-04-03 [VOORWAARDELIJK]: Indien het teruggezonden attributeVerificationResult http://uri.etsi.org/19478/VerificationResult/MatchWithVariation is en het attributeVerificationResult een attributeValue element bevat, moet het attributeValue element de waarde van het attribuut bevatten zoals opgeslagen in de authentieke bron.

— REQ-ASIP-6.1.1.2-06-04-01 [VOORWAARDELIJK]: Indien het FragmentVerificationResult hetzij http://uri.etsi.org/19478/VerificationResult/Match hetzij http://uri.etsi.org/19478/VerificationResult/MatchWithVariation is, kan het AttributeVerificationResult een FragmentVerification-element omvatten.

— REQ-ASIP-6.1.1.2-06-04-02 [VOORWAARDELIJK]: Indien het teruggezonden fragmentVerificationResult http://uri.etsi.org/19478/VerificationResult/Match is en het attributeVerificationResult een fragmentValue element bevat, moet het fragmentValue element de waarde bevatten zoals in het verzoek.

— REQ-ASIP-6.1.1.2-06-04-03 [VOORWAARDELIJK]: Indien het teruggezonden fragmentVerificationResult http://uri.etsi.org/19478/VerificationResult/MatchWithVariation is en het attributeVerificationResult een fragmentValue element bevat, moet het fragmentValue element de waarde van het fragment van het attribuut bevatten zoals opgeslagen in de authentieke bron.

b) de technische specificaties van clausule 6.2.3 van ETSI TS 119 478 V1.1.1 (2026-01) - Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); specificaties van interfaces met betrekking tot authentieke bronnen.

— REQ-ASIP-6.2.3.2.1-08-04: Het element AttributeVerificationResponse kan precies één dochterelement van de keuze TextValue, XMLValue of AttributeProperties omvatten.".