Publicatieblad
van de Europese Unie

NL
L-serie

2025/1929

30.9.2025

UITVOERINGSVERORDENING (EU) 2025/1929 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 de koppeling van datum en tijdstip aan gegevens en tot vaststelling van de nauwkeurigheid van tijdsbronnen voor de verlening van gekwalificeerde elektronische tijdstempels

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 42, lid 2,

Overwegende hetgeen volgt:

(1) Gekwalificeerde elektronische tijdstempels spelen een cruciale rol in de digitale omgeving doordat ze de transitie van traditionele, op papier gebaseerde processen naar elektronische equivalenten bevorderen. Doordat gekwalificeerde elektronische tijdstempels de datum- en tijdsinformatie aan elektronische gegevens koppelen, helpen zij de nauwkeurigheid van de datum en het tijdstip die zij aangeven en de integriteit van de digitale documenten waaraan de datum en het tijdstip zijn gekoppeld, te waarborgen.

(2) Het in artikel 42, lid 1, punt a), van Verordening (EU) nr. 910/2014 uiteengezette vermoeden van overeenstemming mag alleen van toepassing zijn wanneer gekwalificeerde vertrouwensdiensten voor de afgifte van gekwalificeerde tijdstempels voldoen aan de in deze verordening uiteengezette normen. Deze normen moeten vaste praktijken weerspiegelen en in de betrokken sectoren algemeen erkend worden. Deze normen moeten worden aangepast om er aanvullende controles in op te nemen die de veiligheid en betrouwbaarheid van de gekwalificeerde vertrouwensdienst waarborgen en van de koppeling van datum en tijdstip aan gegevens en de nauwkeurigheid van de tijdsbron.

(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 zich echter nog steeds op andere praktijken beroepen om aan te tonen dat hij voldoet aan de vereisten van Verordening (EU) nr. 910/2014.

(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 uitvoeringsverordening indien nodig evalueren en actualiseren om deze in overeenstemming te houden met de mondiale ontwikkelingen, de architectuur en het referentiekader 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

De in artikel 42, lid 2, van Verordening (EU) nr. 910/2014 genoemde referentienormen en specificaties zijn vastgesteld in de bijlage bij deze verordening.

Artikel 2

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

Lijst van referentienormen en specificaties voor gekwalificeerde tijdstempeldiensten

De normen ETSI EN 319 421 V1.3.1 ([1]) ("ETSI EN 319 421") en ETSI EN 319 422 V1.1.1 ([2]) ("ETSI EN 319 422") zijn van toepassing met de volgende aanpassingen:

1. Voor ETSI EN 319 421

1) 2.1 Normatieve referenties:

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

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

— [5] ETSI EN 319 422 V1.1.1 (2016-03) "Elektronische handtekeningen en infrastructuren (ESI); Protocol voor tijdstempels en tokenprofielen voor tijdstempels".

— [6] ongeldig.

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

— [10] 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) ([4]).

— [11] 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 ([5]).

2) 3.1 Definities

— geldigheidsduur van certificaat: het tijdsinterval van "notBefore" tot "notAfter", inclusief, gedurende welke de certificatieautoriteit (CA) garandeert dat zij informatie over de status van het certificaat zal bijhouden.

3) 3.3 Afkortingen

— EUCC Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling.

4) 6.2 Praktijkverklaring van vertrouwensdienst

— OVR-6.2-03 De tijdstempelautoriteit neemt in haar openbaarmakingsverklaring verklaringen op met betrekking tot de beschikbaarheid van haar tijdstempeldienst.

5) 7.3 Personeelsgerelateerde beveiliging

— OVR-7.3-02 Het personeel van de tijdstempelautoriteit in vertrouwensrollen, en indien van toepassing haar 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-7.3-03 De overeenstemming met OVR-7.3-02 gaat gepaard met regelmatig bijgewerkte informatie (ten minste elke twaalf maanden) over nieuwe dreigingen en actuele beveiligingspraktijken.

([1]) EN 319 421 — Elektronische handtekeningen en infrastructuren (ESI) — Beleids- en beveiligingseisen voor verleners van vertrouwensdiensten die tijdstempels afgeven, V1.3.1.
([2]) EN 319 422 — Elektronische handtekeningen en infrastructuren (ESI) — Protocol voor tijdstempels en tokenprofielen voor tijdstempels, V1.1.1 (2016-03). https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([4]) PB L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([5]) PB L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6) 7.6.2 Generatie van sleutel van tijdstempelautoriteit

— TIS-7.6.2-03 Het genereren van de sleutel(s) van de tijdstempelautoriteit wordt uitgevoerd op 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 [3] 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 [10][11], en gecertificeerd tot EAL 4 of hoger, of

c) tot 31.12.2030, FIPS PUB 140-3 [7] 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 [10][11]-certificering, dan zal dit apparaat worden geconfigureerd en gebruikt in overeenstemming met dat certificaat.

— TIS-7.6.2-04 ongeldig.

— OPMERKING 3 ongeldig.

— TIS-7.6.2-05A Het algoritme voor het genereren van sleutels van de tijdstempelautoriteit, de resulterende lengte van de ondertekeningssleutel en het ondertekeningsalgoritme die worden gebruikt voor het ondertekenen van respectievelijk tijdstempels en voor het ondertekenen van certificaten voor openbare sleutels van de tijdstempelautoriteit respectievelijk is in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering [9] goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms.

— OPMERKING 4 ongeldig.

— TIS-7.6.2-06 Een privésleutel van de tijdstempelautoriteit 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) 7.6.3 Beveiliging van de privésleutel van de tijdstempelautoriteit

— TIS-7.6.3-02 De privésleutel van de tijdstempelautoriteit wordt 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 [3] 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

b) de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC) [10][11] en gecertificeerd tot EAL 4 of hoger, of

c) tot 31.12.2030, FIPS PUB 140-3 [7] 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 [10][11]-certificering, dan zal dit apparaat worden geconfigureerd en gebruikt in overeenstemming met dat certificaat.

— TIS-7.6.3-03 ongeldig.

— OPMERKING 2 ongeldig.

8) 7.6.7 Einde van levenscyclus van de sleutel van de tijdstempelautoriteit

— TIS-7.6.7-03A De vervaldatum voor de privésleutels van de tijdstempelautoriteit is in overeenstemming met de “Agreed Cryptographic Mechanisms” [9].

— OPMERKING 1 ongeldig.

9) 7.10 Netwerkbeveiliging

— OVR-7.10-05 De door REQ-7.8-13 van ETSI EN 319.401 [1] aangevraagde kwetsbaarheidsscan wordt ten minste eenmaal per kwartaal uitgevoerd.

— OVR-7.10-06 De door REQ-7.8-17X van ETSI EN 319.401 [1] aangevraagde penetratietest wordt ten minste eenmaal per jaar uitgevoerd.

— OVR-7.10-07 Firewalls worden geconfigureerd om alle protocollen en toegangen die niet vereist zijn voor de bedrijfsvoering van de tijdstempelautoriteit te verwijderen.

10) 7.14 Beëindiging en beëindigingsplannen van de verlener van vertrouwensdiensten

— OVR-7.14-01A 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.4].

2. Voor ETSI EN 319 422

1) 2.1 Normatieve referenties

— [5] ongeldig.

— [6] ongeldig.

— [8] Europese Groep voor cyberbeveiligingscertificering, subgroep inzake cryptografie: “Agreed Cryptographic Mechanisms”.

— [9] RFC 9110 HTTP Semantics.

2) 4.1.3 Te gebruiken hash-algoritmen

— De volgende clausule is van toepassing:

Hash-algoritmen die worden gebruikt om van een tijdstempel te voorziene informatie, de verwachte duur van de tijdstempel en geselecteerde hash-functies ten opzichte van de tijd te hashen, is in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [8].

— OPMERKING ongeldig.

3) 4.2.3 Te ondersteunen algoritmen

— De volgende clausule is van toepassing:

De te ondersteunen algoritmen voor de tokenhandtekening van de tijdstempel is in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [8].

— OPMERKING ongeldig.

4) 4.2.4 Te ondersteunen sleutellengten

— De volgende clausule is van toepassing:

De sleutellengten voor het handtekeningalgoritme voor het geselecteerde handtekeningalgoritme is in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms.

— OPMERKING ongeldig.

5) 5.1.3 Te ondersteunen algoritmen

— De volgende clausule is van toepassing:

Hash-algoritmen voor de te ondersteunen tijdstempelgegevens, de verwachte duur van de tijdstempel en geselecteerde hash-functies ten opzichte van de tijd is in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [8].

— OPMERKING ongeldig.

6) 5.2.3 Te gebruiken algoritmen

— De volgende clausule is van toepassing:

Hash-algoritmen die worden gebruikt om de informatie te hashen die moet worden voorzien van een tijdstempel en de algoritmen voor de tokenhandtekening van de tijdstempel is in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [8].

— OPMERKING ongeldig.

7) 6.3 Eisen van sleutellengten

— De volgende clausule is van toepassing:

De sleutellengte voor het geselecteerde handtekeningalgoritme van het certificaat van de tijdstempelautoriteit is in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [8].

— OPMERKING ongeldig.

8) 6.5 Eisen voor algoritmen

— De volgende clausule is van toepassing:

De publieke sleutel van de tijdstempelautoriteit en de handtekening van het certificaat van de tijdstempelautoriteit gebruiken de algoritmen die in overeenstemming zijn met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [8].

— OPMERKING ongeldig.

9) 7 Profielen voor de te ondersteunen transportprotocollen

— De tijdstempelclient en de tijdstempelserver ondersteunen het tijdstempelprotocol via HTTPS [9] als bedoeld in clausule 3.4 van IETF RFC 3161 [1].

10) 8 Objectidentificatoren van de cryptografische algoritmen

— De volgende clausule is van toepassing:

De publieke sleutel van de tijdstempelautoriteit en de handtekening van het certificaat van de tijdstempelautoriteit gebruiken de algoritmen die in overeenstemming zijn met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [8].

11) 9.1 Verklaring van wettelijke naleving

— Indien een tijdstempeltoken door de tijdstempelautoriteit wordt verklaard als een gekwalificeerd elektronisch tijdstempel in overeenstemming met Verordening (EU) nr. 910/2014 [i.2], bevat het een instantie van de KcVermeldingen-uitbreiding in het uitbreidingsveld van de tijdstempeltoken met de syntax als bedoeld in IETF RFC 3739 [i.3], clausule 3.2.6.

— De extensie qcStatements (KCvermelding) bevat één instantie van de vermelding “esi4-qtstStatement-1” als bedoeld in bijlage B.

— De extensie qcStatements mag niet als kritisch worden gemarkeerd.