Publicatieblad
van de Europese Unie

NL
L-serie

2024/3144

19.12.2024

# 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**

**(Voor de EER relevante tekst)**

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) ([1]), en met name artikel 49, lid 7,

Overwegende hetgeen volgt:

(1) Uitvoeringsverordening (EU) 2024/482 van de Commissie ([2]) (hierna "de verordening") specificeert de rollen, regels en verplichtingen, alsook de structuur van de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC) overeenkomstig het Europees kader voor cyberbeveiligingscertificering dat is vastgesteld in Verordening (EU) 2019/881.

(2) De verordening is gebaseerd op gevestigde internationale normen, te weten de gemeenschappelijke criteria en de gemeenschappelijke evaluatiemethodologie van de Internationale Organisatie voor normalisatie (ISO) en de Internationale Elektrotechnische Commissie (IEC). Ze verwijst naar ISO/IEC-normen, maar specificeert niet de toepasselijke versie ervan. Daarom moet worden gespecificeerd welke versie van de normen van toepassing is op certificaten die zijn afgegeven in het kader van de EUCC.

(3) De overheidsorganisaties die hebben bijgedragen tot de ontwikkeling van de gemeenschappelijke criteria en de gemeenschappelijke evaluatiemethodologie via de regeling ter erkenning van certificaten van gemeenschappelijke criteria op het gebied van IT-beveiliging (CCRA), zijn samen met de ISO/IEC houder van de auteursrechten. Deze overheidsorganisaties behouden het recht om ze te gebruiken. Vanwege het belang van deze documenten die afkomstig zijn van de CCRA, moeten zij ook een basis vormen voor certificering in het kader van de EUCC.

(4) De normen van de gemeenschappelijke criteria en de gemeenschappelijke evaluatiemethodologie zijn onderhevig aan interpretaties door de CCRA die hun toepassing vergemakkelijken en die door faciliteiten voor de evaluatie van de beveiliging van informatietechnologie (ITSEF's) en certificeringsinstanties in overweging kunnen worden genomen.

(5) Internationale normen met betrekking tot de gemeenschappelijke criteria kunnen worden bijgewerkt. Om een ordelijke en tijdige overgang te waarborgen, moeten overgangsregels worden vastgesteld om verkopers, ITSEF's, certificeringsinstanties en andere belanghebbenden voldoende tijd te geven voor de nodige aanpassingen. Dergelijke overgangsregels moeten passend worden afgestemd op mondiale praktijken, zoals die van de CCRA.

([1]) PB L 151 van 7.6.2019, blz. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) 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).

(6) In de verordening wordt niet gespecificeerd tot wanneer een ICT-productcertificering kan worden gebaseerd op de vorige versies van de normen voor de gemeenschappelijke criteria en de gemeenschappelijke evaluatiemethodologie. De in de bijlagen I, II en III bij de verordening vermelde technische domeinen en beveiligingsprofielen zijn gebaseerd op eerdere versies van de normen ISO/IEC 15408 en 18045. In de verordening moet daarom worden gespecificeerd onder welke omstandigheden de vorige versie van de gemeenschappelijke criteria en de gemeenschappelijke evaluatiemethodologie van toepassing blijft en hoe de overgang naar de nieuwste versie van de internationale normen moet verlopen.

(7) Tijdens de overgangsperiode moet de bijwerking van de technische domeinen en beveiligingsprofielen voor de belanghebbenden een prioriteit zijn. In de verordening moet worden bepaald dat beveiligingsdoelstellingen op basis van een eerdere versie van de normen tot en met 31 december 2027 worden aanvaard, conform het CCRA-overgangsbeleid. Er zij echter op gewezen dat dat beleid betrekking heeft op de eerste evaluaties van producten en beveiligingsprofielen die uiterlijk 30 juni 2024 zijn ingegaan, toen de EUCC nog niet van toepassing was. Conform het CCRA-overgangsbeleid moet in de verordening ook worden bepaald dat beveiligingsdoelstellingen die in overeenstemming zijn met de verordening en op basis van een eerdere versie van de normen aan beveiligingsprofielen zouden voldoen, tot en met 31 december 2027 worden aanvaard. Indien uit hoofde van de verordening een nieuw certificaat wordt afgegeven bij een herzieningsproces van een nationaal certificaat dat binnen twee jaar na het oorspronkelijke certificaat wordt gestart, moet het bovendien mogelijk zijn een eerdere versie van de normen te gebruiken. Dit geldt niet voor een herzieningsproces waarbij geen nieuw certificaat uit hoofde van de verordening hoeft te worden afgegeven en waarbij het certificaat geldig blijft.

(8) Om een ordelijke overgang naar de nieuwste versie van de normen te waarborgen, moeten in de verordening specifieke overgangsregels worden bepaald en moet uit hoofde van de verordening de afgifte mogelijk blijven van certificaten die zouden voldoen aan beveiligingsprofielen die gebaseerd zijn op eerdere versies van de normen van de CCRA, indien het gebruik van dergelijke beveiligingsprofielen krachtens de Uniewetgeving vereist is. Dat is zo voor Uitvoeringsverordening (EU) 2016/799 van de Commissie ([3]), Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad ([4]) en Uitvoeringsbesluit (EU) 2016/650 van de Commissie ([5]).

(9) Bijlage I bij de verordening bevat een lijst van toepasselijke documenten over de huidige stand van de techniek voor de evaluatie van ICT-producten en beveiligingsprofielen. De versie van de documenten wordt echter niet gespecificeerd. Daarom moet worden gespecificeerd welke versie van de documenten van toepassing is op certificaten die zijn afgegeven in het kader van de EUCC. Die versies bouwen voort op documenten die zijn goedgekeurd door de Europese Groep voor cyberbeveiligingscertificering (EGC), maar zijn verder herzien om ze in de EUCC op te nemen. Bovendien moet bijlage I worden gewijzigd om bijgewerkte en nieuwe documenten over de huidige stand van de techniek op te nemen na de goedkeuring ervan door de EGC, zodat een uniforme accreditatie van conformiteitsbeoordelingsinstanties in het kader van de EUCC wordt gewaarborgd. De accreditatie-eisen met betrekking tot de accreditatie van ITSEF's moeten worden bijgewerkt om de toepassing van de onafhankelijkheids- en onpartijdigheidscriteria te verduidelijken, en er moet een nieuw document over de huidige stand van de techniek worden opgesteld voor de accreditatie van certificeringsinstanties.

(10) Documenten over de huidige stand van de techniek kunnen aan de EUCC worden toegevoegd of in het kader van zijn onderhoudsactiviteiten worden bijgewerkt. Mogelijk moeten voor nieuwe of bijgewerkte documenten over de huidige stand van de techniek passende overgangsregels worden vastgesteld, zodat verkopers, ITSEF's, certificeringsinstanties en andere belanghebbenden de nodige aanpassingen aan kunnen brengen. Voor de bijwerking van het document over de huidige stand van de techniek met betrekking tot de accreditatie van ITSEF's mag het bijgewerkte document alleen van toepassing zijn op accreditaties die vóór 8 juli 2025 zijn afgegeven, bijvoorbeeld in het kader van een beoordelings- of herbeoordelingsprocedure. Bovendien moet het bijgewerkte document van toepassing zijn op alle accreditaties voor ITSEF's die na 8 juli 2025 zijn afgegeven.

([3]) Uitvoeringsverordening (EU) 2016/799 van de Commissie van 18 maart 2016 tot uitvoering van Verordening (EU) nr. 165/2014 van het Europees Parlement en de Raad tot vaststelling van de eisen voor de constructie, het testen, de installatie, de exploitatie en de reparatie van tachografen en tachograafonderdelen (PB L 139 van 26.5.2016, blz. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

([4]) 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 (PB L 257 van 28.8.2014, blz. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([5]) Uitvoeringsbesluit (EU) 2016/650 van de Commissie van 25 april 2016 tot vaststelling van normen inzake de veiligheidsbeoordeling van gekwalificeerde middelen voor het aanmaken van handtekeningen en zegels overeenkomstig artikel 30, lid 3, en artikel 39, lid 2, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (PB L 109 van 26.4.2016, blz. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Verdere rectificaties van de artikelen 5, 8, 16, 29 en 44 van en bijlage IV bij de verordening moeten bijdragen tot een eenduidige formulering en een duidelijke juridische interpretatie.

(12) De regels voor de aanmelding van de conformiteitsbeoordelingsinstanties moeten horizontaal worden vastgesteld voor alle regelingen onder het Europees kader voor cyberbeveiligingscertificering. In Uitvoeringsverordening (EU) 2024/3143 van de Commissie ([6]) zijn die aanmeldingsregels bepaald. Daarom moeten de artikelen 23 en 24 van de verordening worden geschrapt met ingang van de datum waarop Uitvoeringsverordening (EU) 2024/3143 van toepassing wordt.

(13) De verordening moet daarom dienovereenkomstig worden gewijzigd en gerectificeerd.

(14) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 66 van Verordening (EU) 2019/881 opgerichte comité,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

*Artikel 1*

Uitvoeringsverordening (EU) 2024/482 wordt als volgt gewijzigd:

1) In artikel 2 worden de punten 1) en 2) vervangen door:

"1) "gemeenschappelijke criteria": de gemeenschappelijke criteria voor de evaluatie van de beveiliging van informatietechnologie, zoals in de normen ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 en ISO/IEC 15408-5:2022 is uiteengezet, alsook in de gemeenschappelijke criteria voor de evaluatie van de beveiliging van informatietechnologie, versie CC:2022, delen 1 tot en met 5, gepubliceerd door de deelnemers aan de regeling ter erkenning van certificaten van gemeenschappelijke criteria op het gebied van IT-beveiliging;

2) "gemeenschappelijke evaluatiemethodologie": de gemeenschappelijke methodologie voor de evaluatie van de beveiliging van informatietechnologie, zoals in norm ISO/IEC 18045:2022 is uiteengezet, alsook in de gemeenschappelijke methodologie voor de evaluatie van de beveiliging van informatietechnologie, versie CEM:2022, gepubliceerd door de deelnemers aan de regeling ter erkenning van certificaten van gemeenschappelijke criteria op het gebied van IT-beveiliging;".

2) Artikel 3 wordt vervangen door:

"*Artikel 3*

**Evaluatienormen**

1. De volgende normen zijn van toepassing op evaluaties die in het kader van de EUCC-regeling worden uitgevoerd:

a) de gemeenschappelijke criteria;

b) de gemeenschappelijke evaluatiemethodologie.

2. Tot en met 31 december 2027 kan een certificaat worden afgegeven in het kader van de EUCC-regeling waarbij een van de volgende normen wordt toegepast:

a) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 of ISO/IEC 15408-3:2008;

b) de gemeenschappelijke criteria voor de evaluatie van de beveiliging van informatietechnologie, versie 3.1, herziening 5, gepubliceerd door de deelnemers aan de regeling ter erkenning van certificaten van gemeenschappelijke criteria op het gebied van IT-beveiliging;

([6]) Uitvoeringsverordening (EU) 2024/3143 van de Commissie van 18 december 2024 tot vaststelling van de omstandigheden, vormen en procedures van aanmeldingen overeenkomstig artikel 61, lid 5, van Verordening (EU) 2019/881 van het Europees Parlement en de Raad inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie (PB L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

c) ISO:IEC 18045:2008;

d) de gemeenschappelijke methodologie voor de evaluatie van de beveiliging van informatietechnologie, versie 3.1, herziening 5, gepubliceerd door de deelnemers aan de regeling ter erkenning van certificaten van gemeenschappelijke criteria op het gebied van IT-beveiliging.

3. Tot en met 31 december 2027 kan een certificaat met toepassing van de in lid 1 bedoelde normen worden afgegeven in het kader van de EUCC-regeling dat zou voldoen aan een beveiligingsprofiel dat de in lid 2 vermelde normen heeft toegepast.

4. Een certificaat met toepassing van de in lid 1 bedoelde normen kan ook worden afgegeven in het kader van de EUCC-regeling indien dat zou voldoen aan een beveiligingsprofiel dat een van de volgende normen heeft toegepast, mits het gebruik van een dergelijk beveiligingsprofiel vereist is op grond van Uitvoeringsverordening (EU) 2016/799 van de Commissie (*), Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad (**) of Uitvoeringsbesluit (EU) 2016/650 van de Commissie (***):

a) de gemeenschappelijke criteria voor de evaluatie van de beveiliging van informatietechnologie, versie 3.1, herzieningen 1 tot en met 4, gepubliceerd door de deelnemers aan de regeling ter erkenning van certificaten van gemeenschappelijke criteria op het gebied van IT-beveiliging;

b) de gemeenschappelijke methodologie voor de evaluatie van de beveiliging van informatietechnologie, versie 3.1, herzieningen 1 tot en met 4, gepubliceerd door de deelnemers aan de regeling ter erkenning van certificaten van gemeenschappelijke criteria op het gebied van IT-beveiliging.

_____

(*) Uitvoeringsverordening (EU) 2016/799 van de Commissie van 18 maart 2016 tot uitvoering van Verordening (EU) nr. 165/2014 van het Europees Parlement en de Raad tot vaststelling van de eisen voor de constructie, het testen, de installatie, de exploitatie en de reparatie van tachografen en tachograafonderdelen (PB L 139 van 26.5.2016, blz. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) 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 (PB L 257 van 28.8.2014, blz. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Uitvoeringsbesluit (EU) 2016/650 van de Commissie van 25 april 2016 tot vaststelling van normen inzake de veiligheidsbeoordeling van gekwalificeerde middelen voor het aanmaken van handtekeningen en zegels overeenkomstig artikel 30, lid 3, en artikel 39, lid 2, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (PB L 109 van 26.4.2016, blz. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).".

3) In hoofdstuk IV wordt het volgende artikel 20 bis ingevoegd:

"*Artikel 20 bis*

**Specificatie van de eisen voor de accreditatie van conformiteitsbeoordelingsinstanties**

Bij de accreditatie van conformiteitsbeoordelingsinstanties wordt rekening gehouden met de specificatie van de eisen voor de accreditatie van certificeringsinstanties en ITSEF's zoals vastgesteld in de in punt 2 van bijlage I vermelde toepasselijke documenten over de huidige stand van de techniek.".

4) De artikelen 23 en 24 worden geschrapt.

5) Aan artikel 48 wordt het volgende lid 4 toegevoegd:

"4. Tenzij in bijlage I of bijlage II anders is bepaald, zijn de documenten over de huidige stand van de techniek van toepassing vanaf de datum van toepassing van de wijzigingshandeling waarbij zij in bijlage I of bijlage II zijn opgenomen.".

6) Aan artikel 49 wordt het volgende lid 4 toegevoegd:

"4. Bij de uitvoering van de in lid 3 bedoelde herziening binnen twee jaar na de afgifte van het oorspronkelijke certificaat en indien die herziening leidt tot de afgifte van een nieuw certificaat overeenkomstig deze verordening, kunnen de in artikel 3, lid 2, vermelde normen worden toegepast. De datum van afgifte van het oorspronkelijke certificaat is de datum van afgifte van het laatste certificaat voor een ICT-product of beveiligingsprofiel waarop de huidige certificering is gebaseerd.".

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

8) Bijlage IV wordt gewijzigd overeenkomstig bijlage II bij deze verordening.

*Artikel 2*

Uitvoeringsverordening (EU) 2024/482 wordt als volgt gerectificeerd:

1) In artikel 5, lid 1, wordt punt b) vervangen door:

"b) door aan een gecertificeerd beveiligingsprofiel als onderdeel van het ICT-proces te zouden voldoen, wanneer het ICT-product behoort tot de ICT-productcategorie die onder dat beveiligingsprofiel valt.".

2) Artikel 8 wordt als volgt gerectificeerd:

a) de titel wordt vervangen door:

"Voor de certificering en herziening benodigde gegevens";

b) lid 1 wordt vervangen door:

"1. Een aanvrager van certificering in het kader van de EUCC verstrekt de certificeringsinstantie en de ITSEF alle informatie die nodig is voor de certificerings- en herzieningsactiviteiten, of stelt deze anderszins ter beschikking.".

3) Artikel 16 wordt vervangen door:

"*Artikel 16*

**Informatie die nodig is voor de certificering en herziening van beveiligingsprofielen**

Een aanvrager van certificering van een beveiligingsprofiel verstrekt de certificeringsinstantie en de ITSEF alle informatie die nodig is voor de certificerings- en herzieningsactiviteiten, of stelt deze anderszins ter beschikking, en dit volledig en op correcte wijze. Artikel 8, leden 2, 3, 4 en 7, zijn van overeenkomstige toepassing.".

4) In artikel 17 wordt lid 1 geschrapt.

5) In artikel 29 wordt lid 2 vervangen door:

"2. Wanneer de houder van het EUCC-certificaat tijdens het in lid 1 bedoelde tijdsbestek geen passende corrigerende maatregelen voorstelt, wordt het certificaat overeenkomstig artikel 30 geschorst of overeenkomstig artikel 14 of artikel 20 ingetrokken.".

*Artikel 3*

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 4, is van toepassing met ingang van 8 januari 2025.

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

Gedaan te Brussel, 18 december 2024.

*Voor de Commissie*
*De voorzitter*
Ursula VON DER LEYEN

*BIJLAGE I*

*““BIJLAGE I*

**Documenten over de huidige stand van de techniek ter ondersteuning van technische domeinen en andere documenten over de huidige stand van de techniek**

1. Documenten over de huidige stand van de techniek ter ondersteuning van technische domeinen op AVA_VAN-niveau 4 of 5:

   a) de volgende documenten met betrekking tot de geharmoniseerde evaluatie van het technische domein “smartcards en soortgelijke componenten”:

      1) “Minimale ITSEF-vereisten voor evaluatie van de beveiliging van smartcards en soortgelijke componenten”, versie 1.1;

      2) “Minimumeisen voor de beveiliging van locaties”, versie 1.1;

      3) “Toepassing van gemeenschappelijke criteria op geïntegreerde schakelingen”, versie 1.1;

      4) “Vereisten inzake beveiligingsarchitectuur (ADV_ARC) voor smartcards en soortgelijke componenten”, versie 1.1;

      5) “Certificering van “open” smartcardproducten”, versie 1.1;

      6) “Beoordeling van samengestelde producten voor smartcards en soortgelijke componenten”, versie 1.1;

      7) “Toepassing van aanvalspotentieel op smartcards en soortgelijke componenten”, versie 1.2;

   b) de volgende documenten met betrekking tot de geharmoniseerde evaluatie van het technische domein “hardwarecomponenten met beveiligingsboxen”:

      1) “Minimale ITSEF-vereisten voor evaluatie van de beveiliging van hardwarecomponenten met beveiligingsboxen”, versie 1.1;

      2) “Minimumeisen voor de beveiliging van locaties”, versie 1.1;

      3) “Toepassing van aanvalspotentieel op hardwarecomponenten met beveiligingsboxen”, versie 1.2.

2. Documenten over de huidige stand van de techniek met betrekking tot de geharmoniseerde accreditatie van conformiteitsbeoordelingsinstanties:

   a) “Accreditatie van ITSEF’s voor de EUCC”, versie 1.1, voor accreditaties die zijn afgegeven vóór 8 juli 2025;

   b) “Accreditatie van ITSEF’s voor het EUCC”, versie 1.6c, voor accreditaties die nieuw zijn afgegeven of herzien na 8 juli 2025;

   c) “Accreditatie van certificeringsinstanties voor de EUCC”, versie 1.6b.”.”

*BIJLAGE II*

In deel IV.3 van bijlage IV bij Uitvoeringsverordening (EU) 2024/482 worden de punten 5 en 6 vervangen door:

"5. Wanneer de wijzigingen door de certificeringsinstantie als gering zijn bevestigd, wordt voor het gewijzigde ICT-product geen nieuw certificaat afgegeven en wordt bij het oorspronkelijke certificeringsverslag een handhavingsverslag opgesteld.

Het handhavingsverslag wordt als een subset van het effectbeoordelingsverslag opgenomen en omvat de volgende delen:

a) inleiding;

b) beschrijving van wijzigingen;

c) getroffen bewijsmateriaal van de ontwikkelaar.

6. Het handhavingsverslag zoals bedoeld in punt 5 wordt aan Enisa verstrekt met het oog op bekendmaking op haar website voor cyberbeveiligingscertificering."