Publicatieblad
van de Europese Unie

NL
L-serie

2025/2462

9.12.2025

UITVOERINGSVERORDENING (EU) 2025/2462 VAN DE COMMISSIE

van 8 december 2025

tot wijziging van Uitvoeringsverordening (EU) 2024/482 wat betreft definities, certificering van ICT-productreeksen, continuïteit van de zekerheid en documenten over de huidige stand van de techniek

(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]) 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 gemeenschappelijke evaluatiemethodologie bij de gemeenschappelijke criteria (CC), een internationale norm voor de evaluatie van informatiebeveiliging, maakt het mogelijk de beveiliging van ICT-producten voor certificeringsdoeleinden te evalueren. In dit verband kunnen sommige ICT-producten op dezelfde functionele basis berusten om op verschillende platforms of apparaten soortgelijke beveiligingsfuncties te bieden; dit wordt ook wel productreeks genoemd. Het ontwerp en de hardware, firmware of software kunnen echter per ICT-product verschillen. Het is aan de certificeringsinstantie om per geval te beslissen of een productreeks kan worden gecertificeerd. De voorwaarden voor de certificering van productreeksen kunnen nader worden geïllustreerd in ondersteunende EUCC-richtsnoeren.

(3) Om de betrouwbaarheid van gecertificeerde producten te handhaven, is het van essentieel belang te bepalen wat een belangrijke en wat een geringe wijziging is aan het onderwerp van evaluatie of zijn omgeving, met inbegrip van zijn operationele of ontwikkelomgeving. Daarom moeten die begrippen worden gepreciseerd, waarbij rekening wordt gehouden met bestaande en algemeen gebruikte technische specificaties van de Groep van Hoge Ambtenaren voor de beveiliging van informatiesystemen (SOG-IS) en de deelnemers aan de regeling ter erkenning van certificaten van gemeenschappelijke criteria op het gebied van IT-beveiliging (CCRA).

(4) Geringe wijzigingen worden vaak gekenmerkt door hun beperkte effect op de verklaring met betrekking tot de zekerheid in het afgegeven EUCC-certificaat. Daarom moeten geringe wijzigingen worden beheerd in het kader van onderhoudsprocedures en vereisen zij geen herevaluatie van de beveiligingsfuncties van het product. Voorbeelden van geringe wijzigingen die in het kader van onderhoud moeten worden doorgevoerd, zijn redactionele wijzigingen, wijzigingen aan de omgeving van het onderwerp van evaluatie die het gecertificeerde onderwerp van evaluatie niet wijzigen, en wijzigingen aan het gecertificeerde onderwerp van evaluatie die niet van invloed zijn op de zekerheidsbewijzen. Wijzigingen aan de ontwikkelomgeving kunnen ook als gering worden beschouwd, mits zij niet doorwegen op bestaande zekerheidsmaatregelen. In sommige gevallen kan bij dergelijke wijzigingen echter een gedeeltelijke evaluatie van de relevante maatregelen vereist zijn.

([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).

(5) Een belangrijke wijziging is een wijziging van het gecertificeerde onderwerp van evaluatie of zijn omgeving die een negatief effect kan hebben op de in het EUCC-certificaat gegeven zekerheid en daarom een herevaluatie vereist. Voorbeelden van belangrijke wijzigingen zijn wijzigingen aan de reeks gestelde eisen inzake zekerheid, met uitzondering van de eisen inzake zekerheid van de CC ALC_FLR-familie (herstel van tekortkomingen); wijzigingen aan de vertrouwelijkheids- of integriteitscontroles van de ontwikkelomgeving indien dergelijke wijzigingen van invloed kunnen zijn op de beveiligde ontwikkeling of productie van het onderwerp van evaluatie, of wijzigingen aan het onderwerp van evaluatie om een exploiteerbare kwetsbaarheid op te lossen. Daarnaast kan een verzameling geringe wijzigingen die tezamen aanzienlijke impact op de beveiliging hebben, ook als een belangrijke wijziging worden aangemerkt. Ook moet worden erkend dat een foutcorrectie weliswaar misschien slechts één specifiek aspect van het onderwerp van evaluatie beïnvloedt, maar vanwege de onvoorspelbaarheid en mogelijke gevolgen voor de zekerheid ervan toch een belangrijke wijziging kan zijn als deze de door de certificering geboden beveiligingsborging in gevaar brengt.

(6) Bij wijzigingen aan het dreigingslandschap van een ongewijzigd gecertificeerd ICT-product kan een herbeoordeling vereist zijn. De mogelijke resultaten van een dergelijk herbeoordelingsproces moeten duidelijk worden vastgesteld, met name het effect ervan op het EUCC-certificaat. Als een herbeoordeling met succes wordt afgerond, moet de certificeringsinstantie het certificaat bevestigen of een nieuw certificaat met een verlengde geldigheidsduur afgeven. Als een herbeoordelingsproces niet succesvol is, moet de certificeringsinstantie het certificaat intrekken en mogelijk een nieuw certificaat met een ander toepassingsgebied afgeven. Dergelijke bepalingen moeten van overeenkomstige toepassing zijn op de herbeoordeling van beveiligingsprofielen.

(7) Bijlage I bij Uitvoeringsverordening (EU) 2024/482 bevat een lijst van toepasselijke documenten over de huidige stand van de techniek voor de evaluatie van ICT-producten en beveiligingsprofielen. Die documenten over de huidige stand van de techniek moeten worden geactualiseerd om rekening te houden met de recentste ontwikkelingen, zoals die met betrekking tot technologische ontwikkelingen, het cyberdreigingslandschap, sectorale praktijken of internationale normen. Een dergelijke actualisering is wenselijk voor de documenten over de huidige stand van de techniek met betrekking tot minimumeisen voor de beveiliging van locaties, de toepassing van aanvalspotentieel op smartcards, de toepassing van aanvalspotentieel op hardwarecomponenten met beveiligingsboxen, de toepassing van gemeenschappelijke criteria op geïntegreerde schakelingen en de evaluatie van samengestelde producten voor smartcards en soortgelijke componenten. Bovendien zijn er geen documenten over de huidige stand van de techniek met betrekking tot de evaluatie en certificering van samengestelde producten aan de hand van de nieuwste versie van de gemeenschappelijke criteria, hergebruik van evaluatieresultaten van audits ter plaatse en verduidelijkingen wat betreft de interpretatie van beveiligingsprofielen in verband met gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen, tachografen en hardwarebeveiligingsmodules. Om een uniforme evaluatie van ICT-producten in het kader van de EUCC te waarborgen, moet bijlage I worden gewijzigd om daarin die geactualiseerde en nieuwe documenten over de huidige stand van de techniek op te nemen na de goedkeuring ervan door de Europese Groep voor cyberbeveiligingscertificering (EGC).

(8) Daarnaast moet het document over de huidige stand van de techniek “ADV_SPM.1 interpretation for CC:2022 transition” aan de regeling worden toegevoegd om ervoor te zorgen dat certificeringsprocessen op basis van specifieke beveiligingsprofielen gebruik kunnen blijven maken van formele modellering (ADV_SPM.1) totdat de bijbehorende beveiligingsprofielen worden geactualiseerd, bijvoorbeeld met de toevoeging van een CC:2022-conforme beveiligingsprofielconfiguratie voor meervoudige zekerheid die ADV_SPM.1 ondersteunt. Om de markt voldoende tijd te geven om op de geactualiseerde gemeenschappelijke criteria over te schakelen, moeten specifieke overgangsregels worden vastgesteld voor de beveiligingsprofielen Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, Java Card System — Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, of Java Card System — Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020. Om marktverstoringen te voorkomen, moet worden bepaald dat het document over de huidige stand van de techniek “ADV_SPM.1 interpretation for CC:2022 transition” van toepassing is op certificeringsprocessen die vóór de vaststelling van deze verordening zijn geïnitieerd. De toepassing van dit document moet echter strikt beperkt blijven tot wat nodig is, gezien de tijd die nodig is om de actualisering van de desbetreffende beveiligingsprofielen af te ronden. Meer in het bijzonder moet voor certificeringsprocessen waarbij gebruik wordt gemaakt van beveiligingsprofiel Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, of Java Card System — Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, het document over de huidige stand van de techniek van toepassing zijn op de processen die vóór 1 oktober 2026 zijn geïnitieerd. Voor certificeringsprocessen waarbij gebruik wordt gemaakt van het beveiligingsprofiel Java Card System — Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, mag het document over de huidige stand van de techniek alleen van toepassing zijn op processen die zijn geïnitieerd vóór de datum van inwerkingtreding van deze verordening, aangezien er al een nieuwe versie van het beveiligingsprofiel Java Card System — Open Configuration beschikbaar is.

(9) Een wijziging in de documenten over de huidige stand van de techniek tijdens een certificeringsproces kan de evaluatie van het product verstoren en de afgifte van het certificaat vertragen. Er zijn daarom passende overgangsregels nodig voor nieuwe of geactualiseerde documenten over de huidige stand van de techniek, zodat verkopers, ITSEF's, certificeringsinstanties en andere belanghebbenden de nodige aanpassingen kunnen doorvoeren. Toepasselijke geactualiseerde en nieuwe documenten over de huidige stand van de techniek moeten betrekking hebben op certificeringsaanvragen, met inbegrip van aanvragen voor herbeoordeling en herevaluatie, terwijl het voor lopende certificeringsprocessen mogelijk moet zijn om gebruik te blijven maken van eerdere versies van de documenten over de huidige stand van de techniek.

(10) De bijlagen II en III bij Uitvoeringsverordening (EU) 2024/482 bevatten respectievelijk de op AVA_VAN-niveau 4 of 5 gecertificeerde beveiligingsprofielen en de aanbevolen beveiligingsprofielen. Diverse verwijzingen zijn onvolledig of achterhaald als gevolg van een actualisering van de beveiligingsprofielen. Die verwijzingen moeten worden aangevuld en daarnaast moeten nieuwe verwijzingen worden toegevoegd om te zorgen voor een uitgebreidere dekking van beveiligde geïntegreerde schakelingen, smartcards en aanverwante apparaten en trusted computing.

(11) Artikel 19 van Uitvoeringsverordening (EU) 2024/482 moet worden gewijzigd om te verduidelijken dat bijlage IV, met de nodige wijzigingen, van toepassing is op de herziening van EUCC-certificaten voor beveiligingsprofielen.

(12) Aangezien de beveiligingsdoelstelling van essentieel belang is om het toepassingsgebied van een certificeringsproces te kunnen begrijpen, is het ook noodzakelijk dat Enisa de beveiligingsdoelstelling voor elk EUCC-certificaat op zijn website publiceert.

(13) Voorts moeten de certificeringsinstanties Enisa een Engelse versie van de beveiligingsdoelstelling en het certificeringsverslag verstrekken om het agentschap in staat te stellen die informatie in het Engels beschikbaar te stellen op de desbetreffende website, overeenkomstig artikel 42, lid 2, van Uitvoeringsverordening (EU) 2024/482. Aanvragers van certificering moeten de certificeringsinstanties daarom op verzoek een Engelse versie van de beveiligingsdoelstelling doen toekomen.

(14) De verwijzing naar de naam van de certificeringsinstantie hoeft niet te worden vermeld in de unieke identificatie van het certificaat, aangezien het identificatienummer van de certificeringsinstantie volstaat om deze instantie op unieke wijze te identificeren. De maand van afgifte hoeft evenmin te worden vermeld, aangezien de certificaten jaarlijks worden geteld. Ter vereenvoudiging moet die eis daarom worden geschrapt. Aangezien het jaar van afgifte van het certificaat betrekking heeft op de afgifte van het eerste certificaat, moet diezelfde datum worden vermeld in de unieke identificatie op certificaten die na een herziening worden afgegeven, om de traceerbaarheid te waarborgen.

(15) Uitvoeringsverordening (EU) 2024/482 moet daarom dienovereenkomstig worden gewijzigd.

(16) 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) aan artikel 2 worden de volgende punten 16), 17) en 18) toegevoegd:

"16) "productreeks": een reeks ICT-producten van een aanvrager die, teneinde in dezelfde beveiligingsbehoeften te voorzien, op dezelfde functionele basis berusten, waarbij het ontwerp en de hardware, firmware of software per ICT-product kunnen verschillen;

17) "geringe wijziging": een wijziging aan het gecertificeerde onderwerp van evaluatie of zijn omgeving die geen negatieve invloed heeft op de in het EUCC-certificaat gegeven zekerheid;

18) "belangrijke wijziging": een wijziging aan het gecertificeerde onderwerp van evaluatie of zijn omgeving die een negatieve invloed kan hebben op de in het EUCC-certificaat gegeven zekerheid.";

2) aan artikel 5 wordt het volgende lid 3 toegevoegd:

"3. Een certificeringsinstantie kan de certificering van een productreeks toestaan.";

3) artikel 9, lid 2, punt a), wordt vervangen door:

"a) de certificeringsinstantie en de ITSEF alle nodige volledige en correcte informatie te verstrekken en desgevraagd aanvullende informatie te verstrekken, met inbegrip van een Engelse versie van de beveiligingsdoelstelling;";

4) artikel 11, lid 3, punt b), wordt vervangen door:

"b) de unieke identificatie van het certificaat, bestaande uit:

1) de naam van de regeling;

2) het identificatienummer, overeenkomstig artikel 3 van Uitvoeringsverordening (EU) 2024/3143, van de certificeringsinstantie die het certificaat heeft afgegeven;

3) jaar van afgifte van het oorspronkelijke certificaat;

4) het identificatienummer dat is toegewezen door de certificeringsinstantie die het certificaat heeft afgegeven.";

5) artikel 19, lid 1, wordt vervangen door:

"1. Op verzoek van de houder van het certificaat of om andere gerechtvaardigde redenen kan de certificeringsinstantie besluiten het EUCC-certificaat voor een beveiligingsprofiel te herzien. De herziening wordt in overeenstemming met bijlage IV uitgevoerd. De certificeringsinstantie bepaalt de omvang van de herziening. Wanneer dat voor de herziening nodig is, verzoekt de certificeringsinstantie de ITSEF om het gecertificeerde beveiligingsprofiel opnieuw te evalueren.";

6) artikel 42 wordt als volgt gewijzigd:

a) aan lid 1 wordt het volgende punt i) toegevoegd:

"i) de beveiligingsdoelstelling voor elk EUCC-certificaat;";

b) lid 2 wordt vervangen door:

"2. De in lid 1 bedoelde informatie wordt ten minste in het Engels beschikbaar gesteld. Daartoe doen de certificeringsinstanties Enisa de oorspronkelijke taalversies van de certificeringsverslagen en beveiligingsdoelstellingen toekomen en verstrekken zij bovendien onverwijld de Engelse versie van die documenten.";

7) artikel 48, lid 4, wordt vervangen door:

"4. Tenzij in bijlage I of II anders is bepaald, zijn de documenten over de huidige stand van de techniek van toepassing op certificeringsprocessen, met inbegrip van herbeoordeling en herevaluatie, die zijn gestart op of na de datum van toepassing van de wijzigingshandeling waarbij de documenten over de huidige stand van de techniek in bijlage I of II zijn opgenomen.";

8) bijlage I wordt vervangen door de tekst in bijlage I bij deze verordening;

9) bijlage II wordt vervangen door de tekst in bijlage II bij deze verordening;

10) bijlage III wordt vervangen door de tekst in bijlage III bij deze verordening;

11) bijlage IV wordt gewijzigd overeenkomstig bijlage IV bij deze verordening;

12) bijlage V wordt gewijzigd overeenkomstig bijlage V bij deze verordening;

13) bijlage IX wordt vervangen door de tekst in bijlage VI 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, 8 december 2025.

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) "Minimum ITSEF requirements for security evaluations of smart cards and similar devices", versie 1.1;

      2) "Minimum Site Security Requirements", versie 2;

      3) "Reusing evaluation results of site audits (STAR)", versie 1;

      4) "Application of Common Criteria to integrated circuits", versie 2;

      5) "Security Architecture requirements (ADV_ARC) for smart cards and similar devices", versie 1.1;

      6) "Certification of 'open' smart card products", versie 1.1;

      7) "Composite product evaluation for smart cards and similar devices for CC3.1", versie 2;

      8) "Composite product evaluation and certification for CC:2022", versie 1;

      9) "Application of Attack Potential to Smartcards and Similar Devices", versie 2;

      10) "Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices", versie 1;

      11) "ADV_SPM.1 interpretation for CC:2022 transition", versie 1.1, voor certificeringsprocessen waarbij gebruik wordt gemaakt van de volgende beveiligingsprofielen:

         a) Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, of Java Card System — Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, geïnitieerd vóór 1 oktober 2026;

         b) Java Card System — Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, geïnitieerd vóór 29 december 2025;

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

      1) "Minimum ITSEF requirements for security evaluations of hardware devices with security boxes", versie 1.1;

      2) "Minimum Site Security Requirements", versie 2;

      3) "Reusing evaluation results of site audits (STAR)", versie 1;

      4) "Application of Attack Potential to hardware devices with security boxes", versie 2;

      5) "Hardware assessment in EN 419221-5 (HSM PP)", versie 1;

      6) "JIL Tachograph MS PP Clarification", versie 1.

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

   a) "Accreditation of ITSEFs for the EUCC", versie 1.1, voor accreditaties die zijn afgegeven vóór 8 juli 2025;

   b) "Accreditation of ITSEFs for the EUCC", versie 1.6c, voor accreditaties die nieuw zijn afgegeven of herzien na 8 juli 2025;

   c) "Accreditation of CBs for the EUCC", versie 1.6b."

BIJLAGE II

"BIJLAGE II

Beveiligingsprofielen gecertificeerd op AVA_VAN-niveau 4 of 5

1. Voor middelen voor het aanmaken van gekwalificeerde handtekeningen en zegels op afstand:

   a) EN 419241-2:2019 — Betrouwbare systemen ter ondersteuning van serverhandtekeningen — Deel 2: Beveiligingsprofiel voor QSCD voor serverhandtekeningen (v0.16), ANSSI-CC-PP-2018/02-M01;

   b) EN 419221-5:2018 — Beveiligingsprofielen voor cryptografische modules van verleners van vertrouwensdiensten — Deel 5: Cryptografische module voor vertrouwensdiensten (v0.15), ANSSI-CC-PP-2016/05-M01.

2. Beveiligingsprofielen die als documenten over de huidige stand van de techniek zijn vastgesteld:

   [BLANCO]."

BIJLAGE III

"BIJLAGE III

Aanbevolen beveiligingsprofielen

Beveiligingsprofielen die worden gebruikt bij de certificering van ICT-producten, met inbegrip van producten in de volgende technische domeinen:

1. Smartcards en soortgelijke componenten

   a) paspoort:

      1) PP Machine Readable Travel Document with "ICAO Application" Basic Access Control (v1.10), BSI-CC-PP-0055-2009;

      2) PP Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP) (v1), BSI-CC-PP-0068-V2-2011-MA-01;

      3) PP Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE (v1.3), BSI-CC-PP-0056-V2-2012-MA-02;

   b) beveiligde handtekeningapparatuur (SSCD):

      1) EN 419211-2:2013 — Beveiligingsprofielen voor beveiligde handtekeningapparatuur — Deel 2: middel dat sleutels genereert (v1.03), BSI-CC-PP-0059-2009-MA-02;

      2) EN 419211-3:2013 — Beveiligingsprofielen voor beveiligde handtekeningapparatuur — Deel 3: middel met sleutelinvoer (v1.0.2), BSI-CC-PP-0075-2012-MA-01;

      3) EN 419211-4:2013 — Beveiligingsprofielen voor beveiligde handtekeningapparatuur — Deel 4: uitbreiding voor een middel dat sleutels genereert en met veilige communicatie met een certificaatgenererende applicatie (v1.0.1), BSI-CC-PP-0071-2012-MA-01;

      4) EN 419211-5:2013 — Beveiligingsprofielen voor beveiligde handtekeningapparatuur — Deel 5: uitbreiding voor een middel dat sleutels genereert en met veilige communicatie met een applicatie voor het aanmaken van een handtekening (v1.0.1), BSI-CC-PP-0072-2012-MA-01;

      5) EN 419211-6:2014 — Beveiligingsprofielen voor beveiligde handtekeningapparatuur — Deel 6: uitbreiding voor een middel met sleutelinvoer en veilige communicatie met een applicatie voor het aanmaken van een handtekening (v1.0.4), BSI-CC-PP-0076-2013-MA-01;

   c) tachograaf: Digital Tachograph — Tachograph Card (TC PP) (v1.0), BSI-CC-PP-0091-2017;

   d) beveiligde geïntegreerde schakelingen, Java-card-platform en eUICC:

      1) Universal SIM Java Card Platform Protection Profile Basic and SCWS Configurations (v2.0.2), ANSSI-CC-PP-2010/04 (Basic), ANSSI-CC-PP-2010/05 (Basic and SCWS);

      2) Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014;

      3) Embedded UICC (eUICC) for Machine-to-Machine Devices (v1.1), BSI-CC-PP-0089-2015;

      4) Cryptographic Service Provider — CSP (v0.9.8), BSI-CC-PP-0104-2019;

      5) Cryptographic Service Provider — Time Stamp Service and Audit (PPC-CSP-TS-Au), versie 0.9.5, BSI-CC-PP-0107-2019;

      6) Configuration Cryptographic Service Provider — Time Stamp Service, Audit and Clustering (PPC-CSP-TS-Au-Cl), versie 0.9.4, BSI-CC-PP-0108-2019;

      7) Java Card System — Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020;

      8) Secure Element Protection Profile — GPC_SPE_174 (v1.0), CCN-CC-PP-5-2021;

      9) Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile (v1.8), BSI-CC-PP-0117-V2-2023;

      10) Java Card System — Open Configuration (v3.2), BSI-CC-PP-0099-V3-2024;

      11) Embedded UICC for Consumer Devices Protection Profile (v2.1), BSI-CC-PP-0100-V2-2025;

   e) Trusted Platform Module: Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0; niveau 0; herziening 1.59 (v1.3), ANSSI-CC-PP-2021/02.

2. Hardwarecomponenten met beveiligingsboxen

   a) punten van (betalings)interactie en betaalterminals (POI):

      1) punt van interactie “POI-CHIP-ONLY” (v.4.0), ANSSI-CC-PP-2015/01;

      2) punt van interactie “POI-CHIP-ONLY and Open Protocol Package” (v.4.0), ANSSI-CC-PP-2015/02;

      3) punt van interactie “POI-COMPREHENSIVE” (v.4.0), ANSSI-CC-PP-2015/03;

      4) punt van interactie “POI-COMPREHENSIVE and Open Protocol Package” (v4.0), ANSSI-CC-PP-2015/04;

      5) punt van interactie “POI-PED-ONLY” (v.4.0), ANSSI-CC-PP-2015/05;

      6) punt van interactie “POI-PED-ONLY and Open Protocol Package” (v.4.0), ANSSI-CC-PP-2015/06;

   b) hardware beveiligingsmodule:

      1) Cryptographic Module for CSP Signing Operations with Backup — PP CMCSOB 14167-2 (v0.35), ANSSI-CC-PP-2015/08;

      2) Cryptographic Module for CSP Key Generation Services — PP CMCKG 14167-3 (v0.20), ANSSI-CC-PP-2015/09;

      3) Cryptographic Module for CSP Signing Operations without Backup — PP CMCSO 14167-4 (v0.32), ANSSI-CC-PP-2015/10;

   c) tachograaf:

      1) Digital Tachograph — Motion Sensor (MS PP) (v1.0), BSI-CC-PP-0093-2017;

      2) Digital Tachograph — Vehicle Unit (VU PP) (v1.15), BSI-CC-PP-0094-V2-2021;

      3) Digital Tachograph — External GNSS Facility (EGF PP) (v1.10), BSI-CC-PP-0092-V2-2021.

3. Overige: Trusted Execution Environment Protection Profile — GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.”

BIJLAGE IV

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

1) in punt IV.2 wordt punt 4 vervangen door:

"4. De certificeringsinstantie herziet het bijgewerkte technische evaluatieverslag en stelt een herbeoordelingsverslag op. De status van het oorspronkelijke certificaat wordt dan gewijzigd overeenkomstig artikel 13 of artikel 19. Als het herbeoordelingsproces succesvol is, is artikel 13, lid 2, punt a) of punt c), van toepassing in het geval van de certificering van een product en is artikel 19, lid 2, punt a) of punt c), van toepassing in het geval van de certificering van een beveiligingsprofiel. Als het herbeoordelingsproces niet succesvol is, is artikel 13, lid 2, punt b) of punt d), van toepassing in het geval van de certificering van een product en is artikel 19, lid 2, punt b) of punt d), van toepassing in het geval van de certificering van een beveiligingsprofiel.";

2) punt IV.3 wordt als volgt gewijzigd:

a) titel IV.3 wordt vervangen door:

"IV.3 **Wijzigingen aan een gecertificeerd ICT-product — Onderhoud en herevaluatie**";

b) de punten 4 en 5 worden vervangen door:

"4. Na het onderzoek bepaalt de certificeringsinstantie of de omvang van een wijziging gering of belangrijk is in overeenstemming met de effecten ervan op de in het EUCC-certificaat gegeven zekerheid.

5. Indien de certificeringsinstantie bevestigt dat de wijzigingen gering zijn, wordt voor het gewijzigde ICT-product in overeenstemming met artikel 13, lid 2, punt a), of artikel 19, lid 2, punt a), geen nieuw certificaat afgegeven en wordt bij het oorspronkelijke certificeringsverslag een handhavingsverslag opgesteld.";

c) het volgende punt 5 bis wordt ingevoegd:

"5 bis. In het geval van wijzigingen aan de zekerheidsmaatregelen in de ontwikkelomgeving, met inbegrip van de toevoeging van eisen inzake zekerheid van de CC ALC_FLR-familie (herstel van tekortkomingen), kan de certificeringsinstantie de ITSEF verzoeken een evaluatie van een deel van de betrokken zekerheidsmaatregelen uit te voeren. De ITSEF brengt een technisch verslag van de gedeeltelijke evaluatie uit, op basis waarvan de certificeringsinstantie bevestigt dat de wijzigingen gering of belangrijk zijn. Indien de certificeringsinstantie bevestigt dat de wijzigingen gering zijn, is punt 5 van bijlage IV.3 van toepassing. Indien de certificeringsinstantie bevestigt dat de wijzigingen belangrijk zijn, is punt 7 van bijlage IV.3 van toepassing.".

BIJLAGE V

Punt V.1 van bijlage V bij Uitvoeringsverordening (EU) 2024/482 wordt vervangen door:

"V.1 **Certificeringsverslag**

1. Op basis van de door de ITSEF verstrekte technische evaluatieverslagen stelt de certificeringsinstantie een certificeringsverslag op dat samen met het overeenkomstige EUCC-certificaat en de overeenkomstige beveiligingsdoelstelling moet worden gepubliceerd.

2. In het certificeringsverslag is gedetailleerde en praktische informatie opgenomen over het ICT-product en over de beveiligde uitrol van het ICT-product. Daarom bevat het alle openbaar beschikbare en deelbare informatie bevatten die relevant is voor gebruikers en belanghebbende partijen. In het certificeringsverslag kan naar openbaar beschikbare en deelbare informatie worden verwezen.

3. Het certificeringsverslag bevat ten minste de volgende informatie:
   a) samenvatting;
   b) identificatie van het ICT-product;
   c) contactgegevens met betrekking tot de evaluatie van het ICT-product;
   d) beveiligingsbeleid;
   e) aannames en verduidelijking van het toepassingsgebied;
   f) informatie over architectuur;
   g) aanvullende informatie over cyberbeveiliging, indien van toepassing;
   h) samenvatting van de evaluatie van het ICT-product en geëvalueerde configuratie;
   i) de resultaten van de evaluatie en informatie over het certificaat;
   j) opmerkingen en aanbevelingen, indien van toepassing;
   k) bijlagen, indien van toepassing;
   l) verwijzing naar de beveiligingsdoelstelling van het aan certificering onderworpen ICT-product;
   m) indien beschikbaar, het merkteken of het label dat bij de regeling hoort;
   n) woordenlijst, indien van toepassing;
   o) bibliografie.

4. In de samenvatting als bedoeld in lid 3, punt a), wordt het volledige certificeringsverslag kort samengevat. Deze samenvatting geeft een duidelijk en beknopt overzicht van de evaluatieresultaten en bevat de volgende informatie:
   a) naam van het geëvalueerde ICT-product;
   b) naam van de ITSEF die de evaluatie heeft uitgevoerd;
   c) datum van voltooiing van de evaluatie;
   d) datum van afgifte van het certificaat;
   e) indien van toepassing, datum van afgifte van het oorspronkelijke certificaat;
   f) geldigheidsduur;
   g) unieke identificatie van het certificaat zoals beschreven in artikel 11;
   h) korte beschrijving van de resultaten van het certificeringsverslag, met inbegrip van:
      i) de versie en, indien van toepassing, de release van de gemeenschappelijke criteria die op de evaluatie zijn toegepast,
      ii) het zekerheidspakket gemeenschappelijke criteria of de lijst van onderdelen van de beveiligingsborging, met inbegrip van het tijdens de evaluatie toegepaste AVA_VAN-niveau en het bijbehorende zekerheidsniveau als bedoeld in artikel 52 van Verordening (EU) 2019/881 waarnaar het EUCC-certificaat verwijst,
      iii) in voorkomend geval, het (de) beveiligingsprofiel(en) waaraan het ICT-product beweerdelijk voldoet,
      iv) verwijzing naar het beveiligingsbeleid van het geëvalueerde ICT-product,
      v) disclaimer(s), indien van toepassing.

5. Bij de in lid 3, punt b), bedoelde identificatie wordt het geëvalueerde ICT-product duidelijk geïdentificeerd, onder meer met de volgende informatie:

   a) de unieke identificatie van het geëvalueerde ICT-product;

   b) opsomming van de componenten van het ICT-product die deel uitmaken van de evaluatie, met versienummer van elke component;

   c) verwijzing naar aanvullende eisen voor de operationele omgeving van het gecertificeerde ICT-product.

6. De in lid 3, punt c), bedoelde contactinformatie omvat ten minste de volgende elementen:

   a) naam van de ontwikkelaar;

   b) naam en contactgegevens van de houder van het EUCC-certificaat;

   c) naam van de certificeringsinstantie die het certificaat heeft afgegeven;

   d) verantwoordelijke nationale cyberbeveiligingscertificeringsautoriteit;

   e) naam van de ITSEF die de evaluatie heeft uitgevoerd en, in voorkomend geval, de lijst van onderaannemers.

7. Het in lid 3, punt d), bedoelde beveiligingsbeleid bevat de beschrijving van het beveiligingsbeleid van het ICT-product als een verzameling van beveiligingsdiensten en de beleidslijnen of regels die het geëvalueerde ICT-product moet handhaven of naleven. Daarin wordt ook vermeld:

   a) een beschrijving van de procedures voor het beheer en de openbaarmaking van kwetsbaarheden van de certificaathouder, die uitsluitend informatie bevat die openbaar kan worden gemaakt;

   b) het beleid van de certificaathouder inzake de continuïteit van de zekerheid. met inbegrip van, indien van toepassing, de beschrijving van de levenscyclusbeheer- of productieprocessen van de certificaathouder overeenkomstig afdeling IV.1 van bijlage IV;

   c) indien van toepassing, de aanwezigheid van een procedure voor patchbeheer en het resultaat van de beoordeling ervan overeenkomstig afdeling IV.4 van bijlage IV.

8. De in lid 3, punt e), bedoelde aannames en verduidelijking van het toepassingsgebied bevatten informatie over de omstandigheden en doelstellingen in verband met het beoogde gebruik van het product als bedoeld in artikel 7, lid 1, punt c), en omvatten het volgende:

   a) aannames over het gebruik en de uitrol van het ICT-product in de vorm van minimumeisen waaraan moet zijn voldaan zoals correcte installatie en configuratie, en hardware-eisen;

   b) aannames over de omgeving voor de conforme werking van het ICT-product;

   c) beschrijving van eventuele bedreigingen voor het ICT-product die niet worden ondervangen door de geëvalueerde beveiligingsfuncties van het product overeenkomstig het beoogde gebruik, indien dit relevant wordt geacht voor een potentiële gebruiker van het ICT-product.

   De in de eerste alinea vermelde informatie moet zo duidelijk en begrijpelijk mogelijk zijn zodat potentiële gebruikers van het gecertificeerde ICT-product doordachte beslissingen kunnen nemen over de risico's die aan het gebruik ervan verbonden zijn.

9. De in lid 3, punt f), bedoelde informatie over architectuur bevat een algemene beschrijving van het ICT-product en de belangrijkste onderdelen ervan, op basis van de te produceren elementen die zijn vastgelegd in de zekerheidsfamilie van de gemeenschappelijke criteria: Development — TOE Design (Ontwikkeling — ontwerp van het onderwerp van evaluatie) (ADV_TDS).

10. De in lid 3, punt g), bedoelde aanvullende cyberbeveiligingsinformatie bevat de link naar de website van de houder van het EUCC-certificaat als bedoeld in artikel 55 van Verordening (EU) 2019/881.

11. In de in lid 3, punt h), bedoelde evaluatie en configuratie van het ICT-product worden de testinspanningen van zowel de ontwikkelaar als de beoordelaar beschreven, waarbij de aanpak, configuratie en omvang van de tests worden uiteengezet. Daarin wordt ten minste vermeld:

    a) een identificatie van de gebruikte zekerheidscomponenten uit de in artikel 3 bedoelde normen;

    b) de versie van de documenten over de huidige stand van de techniek en verdere bij de evaluatie gebruikte criteria voor de evaluatie van de beveiliging;

    c) de instellingen en configuratie van het onderwerp van evaluatie die zijn gebruikt voor de tests en de kwetsbaarheidsanalyse;

    d) elk beveiligingsprofiel dat is gebruikt, met inbegrip van de volgende informatie: de naam, de versie, de datum en het certificaat van het beveiligingsprofiel.

12. De resultaten van de evaluatie en de informatie over het certificaat als bedoeld in lid 3, punt i), omvatten informatie over het bereikte zekerheidsniveau als bedoeld in artikel 4 van deze verordening en artikel 52 van Verordening (EU) 2019/881.

13. De in lid 3, punt j), bedoelde opmerkingen en aanbevelingen worden gebruikt om aanvullende informatie over de evaluatieresultaten te verstrekken. Deze opmerkingen en aanbevelingen kunnen de vorm aannemen van tekortkomingen van het ICT-product die tijdens de evaluatie aan het licht zijn gekomen of van bijzonder nuttige kenmerken.

14. De in lid 3, punt k), bedoelde bijlagen worden gebruikt om eventuele aanvullende informatie uiteen te zetten die nuttig kan zijn voor het publiek van het verslag, maar die logischerwijs niet past binnen de voorgeschreven delen van het verslag, ook in geval van een volledige beschrijving van het beveiligingsbeleid.

15. De in lid 3, punt l), bedoelde beveiligingsdoelstelling verwijst naar de geëvalueerde beveiligingsdoelstelling. De geëvalueerde beveiligingsdoelstelling wordt samen met het certificeringsverslag verstrekt voor publicatie op de website als bedoeld in artikel 50, lid 1, van Verordening (EU) 2019/881. Indien de geëvalueerde beveiligingsdoelstelling vóór publicatie moet worden opgeschoond, gebeurt dit overeenkomstig punt V.2 van bijlage V bij deze verordening.

16. De merktekens of labels met betrekking tot de EUCC-regeling als bedoeld in lid 3, punt m), worden overeenkomstig de regels en procedures van artikel 11 in het certificeringsverslag ingevoegd.

17. De in lid 3, punt n), bedoelde woordenlijst wordt gebruikt om de leesbaarheid van het verslag te verbeteren door definities te geven van acroniemen of termen waarvan de betekenis wellicht niet meteen duidelijk is.

18. De bibliografie als bedoeld in lid 3, punt o), bevat verwijzingen naar alle documenten die bij de opmaak van het certificeringsverslag worden gebruikt. Deze informatie omvat ten minste het volgende:

    a) de criteria voor de evaluatie van de beveiliging, documenten over de huidige stand van de techniek en verdere relevante specificaties die worden gebruikt;

    b) het technisch evaluatieverslag;

    c) het technisch evaluatieverslag voor evaluatie van samengestelde producten, indien van toepassing;

    d) technische referentiedocumenten;

    e) beveiligingsrichtsnoeren voor ontwikkelaars;

    f) configuratielijst voor ontwikkelaars.

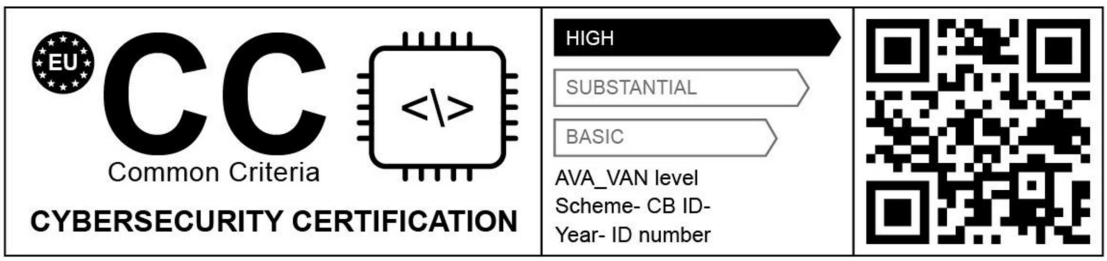
    Om de reproduceerbaarheid van de evaluatie te garanderen, moet alle genoemde documentatie uniek worden geïdentificeerd met de juiste publicatiedatum en het juiste versienummer.”.

BIJLAGE VI

"BIJLAGE IX

Merkteken en label

1. De vorm van het merkteken en het label:



2. Bij vergroting of verkleining van het merkteken en het label worden de verhoudingen onder punt 1 in acht genomen.

3. Indien het merkteken en het label ook effectief zijn aangebracht, moeten zij ten minste 5 mm hoog zijn."