2025/2462

9.12.2025

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2025/2462

af 8. december 2025

om ændring af gennemførelsesforordning (EU) 2024/482 for så vidt angår definitioner, certificering af IKT-produktserier, tillidskontinuitet og statusdokumenter

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) ([1]), særlig artikel 49, stk. 7, og

ud fra følgende betragtninger:

(1) I Kommissionens gennemførelsesforordning (EU) 2024/482 ([2]) præciseres roller, regler og forpligtelser samt strukturen for den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier (EUCC) i overensstemmelse med den europæiske ramme for cybersikkerhedscertificering, der er fastsat i forordning (EU) 2019/881.

(2) Den fælles evalueringsmetode, der ledsager de fælles kriterier (CC), som er en international standard for evaluering af informationssikkerhed, gør det muligt at evaluere sikkerheden af IKT-produkter med henblik på certificering. I denne sammenhæng kan nogle IKT-produkter være baseret på samme funktionsgrundlag for at tilbyde lignende sikkerhedsfunktioner på forskellige platforme eller apparater, hvilket også kaldes en produktserie. Dog kan design, hardware, firmware eller software variere fra det ene IKT-produkt til det andet. Det er certificeringsorganet, der fra sag til sag afgør, om certificering af en produktserie kan gennemføres. Betingelserne for certificering af produktserier kan yderligere illustreres i supplerende EUCC-retningslinjer.

(3) For at opretholde pålideligheden af certificerede produkter er det afgørende at definere, hvad der udgør en væsentlig henholdsvis mindre ændring af evalueringsmålet eller dets miljø, herunder dets drifts- eller udviklingsmiljøer. Det er derfor nødvendigt at præcisere disse begreber under hensyntagen til eksisterende og udbredte tekniske specifikationer fra Gruppen af Højtstående Embedsmænd vedrørende Informationssystemers Sikkerhed (SOG-IS) og deltagerne i ordningerne for anerkendelse af attester baseret på fælles kriterier inden for IT-sikkerhed (CCRA).

(4) Mindre ændringer er ofte kendetegnet ved deres begrænsede indvirkning på den erklæring om produkttillid, som den udstedte EUCC-attest indeholder. Mindre ændringer bør derfor håndteres under vedligeholdelsesprocedurer og kræver ikke en fornyet evaluering af produktets sikkerhedsfunktioner. Eksempler på mindre ændringer, der bør håndteres gennem vedligeholdelse, omfatter, men er ikke begrænset til, redaktionelle ændringer, ændringer af evalueringsmiljøets mål, der ikke ændrer det certificerede evalueringsmål, og ændringer af det certificerede evalueringsmål, der ikke påvirker beviserne for opfyldelse af tillidssikkerheden. Ændringer i udviklingsmiljøet kan også betragtes som mindre, forudsat at de ikke har nogen indvirkning på eksisterende tillidsforanstaltninger. De kan dog i nogle tilfælde kræve en delvis evaluering af de relevante foranstaltninger.

([1]) EUT L 151 af 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) Kommissionens gennemførelsesforordning (EU) 2024/482 af 31. januar 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2019/881 for så vidt angår vedtagelsen af den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier (EUCC) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) En væsentlig ændring er enhver ændring af det certificerede evalueringsmål eller dets miljø, der kan have en negativ indvirkning på det tillidsniveau, der er anført i EUCC-attesten, og den bør derfor kræve en fornyet evaluering. Eksempler på væsentlige ændringer omfatter, men er ikke begrænset til, ændringer af det anmeldte sæt af tillidskrav, bortset fra tillidskravene i CC ALC_FLR-familien (afhjælpning af mangler), ændringer af fortroligheds- eller integritetskontrollerne i udviklingsmiljøet, hvis sådanne ændringer kan påvirke den sikre udvikling eller produktion af evalueringsmålet, eller ændringer af evalueringsmålet for at afhjælpe en sårbarhed, der kan udnyttes. Desuden kan en samling af mindre ændringer, der tilsammen har en betydelig indvirkning på sikkerheden, også kvalificeres som en væsentlig ændring. Det er også vigtigt at erkende, at selv om en fejlrettelse kun kan påvirke et specifikt aspekt af evalueringsmålet, kan dens uforudsigelighed og potentielle indvirkning på tillidsniveauet gøre den til en væsentlig ændring, hvis den bringer de sikkerhedsgarantier, som certificeringen giver, i fare.

(6) Ændringer i trusselsmiljøet for et uændret certificeret IKT-produkt kan kræve en revurdering. De mulige resultater af en sådan revurderingsproces bør fastlægges klart, navnlig dens indvirkning på EUCC-attesten. Hvis en fornyet vurdering afsluttes med et positivt resultat, bør certificeringsorganet bekræfte attesten eller udstede en ny attest med en forlænget udløbsdato. I tilfælde, hvor en fornyet vurdering ikke medfører et positivt resultat, bør certificeringsorganet trække attesten tilbage og eventuelt udstede en ny attest med et andet anvendelsesområde. Sådanne bestemmelser bør med de fornødne ændringer finde anvendelse på fornyet vurdering af beskyttelsesprofiler.

(7) Bilag I til gennemførelsesforordning (EU) 2024/482 indeholder en liste over de gældende statusdokumenter til evaluering af IKT-produkter og beskyttelsesprofiler. Disse statusdokumenter bør opdateres for at afspejle den seneste udvikling, såsom den teknologiske udvikling, cybertrusselsbilledet, brancheprakser eller internationale standarder. En sådan opdatering er hensigtsmæssig for statusdokumenterne vedrørende minimumssikkerhedskrav til sikkerhed på stedet, anvendelse af angrebspotentiale på smartcards, anvendelse af angrebspotentiale på hardwareenheder med sikkerhedsbokse, anvendelse af fælles kriterier på integrerede kredsløb samt evaluering af sammensatte produkter til smartcards og lignende enheder. Desuden er statusdokumenter vedrørende evaluering og certificering af sammensatte produkter ved brug af den seneste version af standarderne for fælles kriterier, genanvendelse af evalueringsresultater fra revisioner på stedet og præciseringer vedrørende fortolkningen af beskyttelsesprofiler for kvalificerede elektroniske signaturgenereringssystemer, takografer og hardwaresikkerhedsmoduler ikke medtaget. For at sikre en ensartet evaluering af IKT-produkter under EUCC bør bilag I ændres, så det omfatter disse opdaterede og nye statusdokumenter efter deres godkendelse af Den Europæiske Cybersikkerhedscertificeringsgruppe (ECCG).

(8) Desuden bør det nyeste dokument »ADV_SPM.1 interpretation for CC:2022 transition« føjes til ordningen for at sikre, at certificeringsprocesser, der er afhængige af specifikke beskyttelsesprofiler, fortsat kan anvende formel modellering (ADV_SPM.1), indtil de tilsvarende beskyttelsesprofiler er opdateret, f.eks. med tilføjelsen af en CC:2022-konform multisikringsbeskyttelsesprofilkonfiguration, der understøtter ADV_SPM.1. For at give markedet tilstrækkelig tid til at overgå til de opdaterede standarder for fælles kriterier skal der fastsættes specifikke overgangsregler for beskyttelsesprofilerne 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 eller Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020. For at undgå markedsforstyrrelser bør det fastsættes, at statusdokumentet om fortolkning af ADV_SPM.1 for CC:2022-overgangen finder anvendelse på certificeringsprocesser, der er indledt før vedtagelsen af denne forordning. Anvendelsen af dette dokument bør dog være strengt begrænset til, hvad der er nødvendigt, under hensyntagen til det tidsrum, der er påkrævet for at færdiggøre opdateringen af de tilsvarende beskyttelsesprofiler. Mere præcist bør statusdokumentet for så vidt angår certificeringsprocesser, der anvender beskyttelsesprofilerne Security IC Platform PP med Augmentation Packages (v1.0), BSI-CC-PP-0084-2014 eller Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, finde anvendelse på de processer, der er indledt inden den 1. oktober 2026. For certificeringsprocesser, der anvender beskyttelsesprofilen Java Card System — Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, bør statusdokumentet kun finde anvendelse på de processer, der er indledt inden datoen for denne forordnings ikrafttræden, da en ny version af beskyttelsesprofilen Java Card System — Open Configuration allerede er tilgængelig.

(9) En ændring i statusdokumenterne under en certificeringsproces kan forstyrre evalueringen af produktet og forsinke udstedelsen af attesten. Der er derfor behov for passende overgangsregler for nye eller ajourførte statusdokumenter for at gøre det muligt for leverandører, ITSEF'er, certificeringsorganer og andre interessenter at foretage de nødvendige tilpasninger. Gældende ajourførte og nye statusdokumenter bør vedrøre ansøgninger om certificering, herunder ansøgninger om fornyet vurdering og fornyet evaluering, mens det bør være muligt for igangværende certificeringsprocesser fortsat at anvende tidligere versioner af statusdokumenterne.

(10) Bilag II og III til gennemførelsesforordning (EU) 2024/482 opregner henholdsvis de beskyttelsesprofiler, der er certificeret på AVA_VAN-niveau 4 eller 5, og de anbefalede beskyttelsesprofiler. Flere referencer er ufuldstændige eller forældede på grund af opdateringer af beskyttelsesprofilerne. Disse referencer bør suppleres, og der bør desuden tilføjes nye referencer for at sikre en mere omfattende dækning af sikre integrerede kredsløb, smartcards og relaterede enheder samt sikre computersystemer.

(11) Det er nødvendigt at ændre artikel 19 i gennemførelsesforordning (EU) 2024/482 for at præcisere, at bilag IV med de nødvendige ændringer finder anvendelse på revisionen af EUCC-attester for beskyttelsesprofiler.

(12) I betragtning af, at sikkerhedsmålet er et centralt element for at forstå omfanget af en certificeringsproces, er det også nødvendigt, at ENISA offentliggør det sikkerhedsmål, der svarer til hver enkelt EUCC-attest, på sit websted.

(13) Certificeringsorganerne bør desuden give ENISA en engelsk udgave af sikkerhedsmålet og certificeringsrapporten, således at agenturet kan stille disse oplysninger til rådighed på engelsk på det relevante websted i henhold til artikel 42, stk. 2, i gennemførelsesforordning (EU) 2024/482. Derfor bør ansøgere om certificering på anmodning forsyne certificeringsorganerne med en engelsk udgave af sikkerhedsmålet.

(14) Det er ikke nødvendigt, at certificeringsorganets navn fremgår af attestens entydige identifikation, da certificeringsorganets identifikationsnummer er tilstrækkeligt til entydigt at identificere dette organ. Udstedelsesmåneden behøver heller ikke at fremgå, da optællingen af attesterne sker på årsbasis. Af forenklingshensyn bør dette krav derfor udgå. Da udstedelsesåret for attesten svarer til udstedelsen af den første attest, bør samme dato fremgå af den entydige identifikation på attester, der udstedes efter en revision, således at sporbarheden kan sikres.

(15) Gennemførelsesforordning (EU) 2024/482 bør derfor ændres.

(16) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 66 i forordning (EU) 2019/881 —

VEDTAGET DENNE FORORDNING:

Artikel 1

I gennemførelsesforordning (EU) 2024/482 foretages følgende ændringer:

1) I artikel 2 indsættes som nr. 16), 17) og 18):

»16) »produktserie«: et sæt af IKT-produkter fra en ansøger, der er bygget på det samme funktionelle grundlag for at opfylde de samme sikkerhedsbehov, og hvis design, hardware, firmware eller software kan variere fra et IKT-produkt til et andet

17) »mindre ændring«: enhver ændring i det certificerede evalueringsmål eller dets miljø, som ikke indvirker negativt på det tillidsniveau, der er anført i EUCC-attesten

18) »væsentlig ændring«: enhver ændring i det certificerede evalueringsmål eller dets miljø, som kan have en negativ indvirkning på det tillidsniveau, der er anført i EUCC-attesten.«

2) I artikel 5 tilføjes følgende som stk. 3:

»3. Et certificeringsorgan kan tillade certificering af en produktserie.«

3) Artikel 9, stk. 2, litra a), affattes således:

»a) at give certificeringsorganet og ITSEF'en alle de nødvendige fuldstændige og korrekte oplysninger og give yderligere nødvendige oplysninger, hvis der anmodes herom, herunder en engelsk version af sikkerhedsmålet«

4) Artikel 11, stk. 3, litra b), affattes således:

»b) entydige identifikation af attesten bestående af:

1) ordningens navn

2) identifikationsnummeret, jf. artikel 3 i gennemførelsesforordning (EU) 2024/3143, for det certificeringsorgan, der har udstedt attesten

3) udstedelsesår for den oprindelige attest

4) identifikationsnummer tildelt af det certificeringsorgan, der har udstedt attesten.«

5) Artikel 19, stk. 1, affattes således:

»1. Efter anmodning fra attestindehaveren eller af andre begrundede årsager kan certificeringsorganet beslutte at revidere EUCC-attesten for en beskyttelsesprofil. Revisionen foretages i overensstemmelse med bilag IV. Certificeringsorganet fastsætter omfanget af revisionen. Hvis det er nødvendigt for revisionen, anmoder certificeringsorganet ITSEF'en om at foretage en fornyet evaluering af den certificerede beskyttelsesprofil.«

6) I artikel 42 foretages følgende ændringer:

a) I stk. 1 tilføjes følgende som nyt litra i):

»i) det sikkerhedsmål, der svarer til hver EUCC-attest.«

b) Stk. 2 affattes således:

»2. De oplysninger, der er omhandlet i stk. 1, stilles til rådighed på mindst engelsk. Med henblik herpå forelægger certificeringsorganerne ENISA de originale sprogversioner af certificeringsrapporterne og sikkerhedsmålene og derudover også den engelske version af sådanne dokumenter uden unødig forsinkelse.«

7) Artikel 48, stk. 4, affattes således:

»4. Medmindre andet er fastsat i bilag I eller II, finder statusdokumenter anvendelse på certificeringsprocesser, herunder fornyet vurdering og fornyet evaluering, der indledes fra anvendelsesdatoen for den ændringsretsakt, ved hvilken statusdokumenterne er blevet indarbejdet i bilag I eller II.«

8) Bilag I erstattes af teksten i bilag I til nærværende forordning.

9) Bilag II erstattes af teksten i bilag II til nærværende forordning.

10) Bilag III erstattes af teksten i bilag III til nærværende forordning.

11) Bilag IV ændres som angivet i bilag IV til nærværende forordning.

12) Bilag V ændres som angivet i bilag V til nærværende forordning.

13) Bilag IX erstattes af teksten i bilag VI til nærværende forordning.

Artikel 2

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 8. december 2025.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG I

»BILAG I

Statusdokumenter til støtte for tekniske områder og andre statusdokumenter

1. Statusdokumenter til støtte for tekniske områder på AVA_VAN-niveau 4 eller 5:
   a) følgende dokumenter vedrørende den harmoniserede evaluering af det tekniske område »smartcards og lignende enheder«:
      1) »Minimum ITSEF requirements for security evaluations of smart cards and similar devices« (minimumskrav til sikkerhedsevalueringer af smartcards og lignende enheder), version 1.1
      2) »Minimum Site Security Requirements« (minimumssikkerhedskrav til sikkerhed på stedet), version 2
      3) »Reusing evaluation results of site audits (STAR)« (genanvendelse af evalueringsresultater fra revisioner på stedet (STAR), version 1
      4) »Application of Common Criteria to integrated circuits« (anvendelse af fælles kriterier på integrerede kredsløb), version 2
      5) »Security Architecture requirements (ADV_ARC) for smart cards and similar devices« (krav til sikkerhedsarkitektur (ADV_ARC) for smartcards og lignende enheder), version 1.1
      6) »Certification of 'open' smart card products« (certificering af »åbne« smartcardprodukter), version 1.1
      7) »Composite product evaluation for smart cards and similar devices for CC3.1« (evaluering af sammensatte produkter til smartcards og lignende enheder for CC3.1), version 2
      8) »Composite product evaluation and certification for CC:2022« (evaluering og certificering af sammensatte produkter for CC:2022), version 1
      9) »Application of Attack Potential to Smartcards and Similar Devices« (anvendelse af angrebspotentiale på smartcards og lignende enheder), version 2.
      10) »Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices« (sikkerhedsevaluering og certificering af kvalificerede elektroniske signatur-/segloprettelsesenheder), version 1
      11) »ADV_SPM.1 interpretation for CC:2022 transition« (ADV_SPM.1-fortolkning for CC:2022-overgang), version 1.1, gældende for certificeringsprocesser, der anvender beskyttelsesprofiler som følger:
         a) beskyttelsesprofilerne Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, eller Java Card System — Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, indledt inden den 1. oktober 2026
         b) beskyttelsesprofil Java Card System — Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, indledt inden 29. december 2025.
   b) følgende dokumenter vedrørende den harmoniserede evaluering af det tekniske område »hardwareenheder med sikkerhedsbokse«:
      1) »Minimum ITSEF requirements for security evaluations of hardware devices with security boxes« (minimumskrav til sikkerhedsevalueringer af hardwareenheder med sikkerhedsbokse), version 1.1
      2) »Minimum Site Security Requirements« (minimumssikkerhedskrav til sikkerhed på stedet), version 2
      3) »Reusing evaluation results of site audits (STAR)« (genanvendelse af evalueringsresultater fra revisioner på stedet (STAR), version 1
      4) »Application of Attack Potential to hardware devices with security boxes« (anvendelse af angrebspotentiale på hardwareenheder med sikkerhedsbokse), version 2.
      5) »Hardware assessment in EN 419221-5 (HSM PP)« (hardwarevurdering i EN 419221-5 (HSM PP), version 1
      6) »JIL Tachograph MS PP Clarification« (præcisering af JIL takograf MS PP), version 1.
2. Statusdokumenter vedrørende harmoniseret akkreditering af overensstemmelsesvurderingsorganer:
   a) »Accreditation of ITSEFs for the EUCC« (akkreditering af ITSEF'er med henblik på EUCC), version 1.1 for akkrediteringer udstedt før den 8. juli 2025.
   b) »Accreditation of ITSEFs for the EUCC« (akkreditering af ITSEF'er med henblik på EUCC), version 1.6c for nyudstedte akkrediteringer eller akkrediteringer, der revideres efter den 8. juli 2025.
   c) »Accreditation of CBs for the EUCC« (akkreditering af certificeringsorganer med henblik på EUCC), version 1.6b.«

BILAG II

»*BILAG II*

Beskyttelsesprofiler certificeret på AVA_VAN-niveau 4 eller 5

1. For kvalificerede systemer til signatur- og seglgenerering på afstand:

   a) EN 419241-2:2019 — Trustworthy Systems Supporting Server Signing — Part 2: Protection Profile for QSCD for Server Signing (pålidelige systemer, der understøtter serversignatur — del 2: beskyttelsesprofil for QSCD-enheder til serversignering), (v0.16), ANSSI-CC-PP-2018/02-M01

   b) EN 419221-5:2018 — Protection profiles for Trust Service Provider Cryptographic modules — Part 5 (beskyttelsesprofiler for tillidstjenesteudbydere — Kryptografiske moduler — Del 5:) Cryptographic Module for Trust Services (kryptografisk modul til trust service-beskyttelsesprofiler) (v0.15), ANSSI-CC-PP-2016/05-M01

2. Beskyttelsesprofiler, der er vedtaget som statusdokumenter:

   [TOM]«

BILAG III

»BILAG III

Anbefalede beskyttelsesprofiler

Beskyttelsesprofiler, der anvendes i forbindelse med certificering af IKT-produkter, herunder produkter inden for de tekniske områder:

1. Smartcards og lignende enheder

   a) rejsepas:

      1) beskyttelsesprofil til maskinlæsbare rejsedokumenter med »ICAO Application« Basic Access Control (v1.10), BSI-CC-PP-0055-2009

      2) beskyttelsesprofil til maskinlæsbare rejsedokumenter ved brug af Standard Inspection Procedure med PACE (PACE_PP) (v1), BSI-CC-PP-0068-V2-2011-MA-01

      3) beskyttelsesprofil til maskinlæsbare rejsedokumenter med »ICAO Application« Extended Access Control med PACE (v1.3), BSI-CC-PP-0056-V2-2012-MA-02

   b) enheder til generering af sikker signatur (SSCD):

      1) EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation (beskyttelsesprofiler til enheder til generering af sikker signatur — del 2: enhed med nøglegenerering) (v1.03), BSI-CC-PP-0059-2009-MA-02

      2) EN 419211-3:2013 — Protection profiles for secure signature creation device — Part 3: Device with key import (beskyttelsesprofiler til enheder til generering af sikker signatur — del 3: enhed med nøgleimport) (v1.0.2), BSI-CC-PP-0075-2012-MA-01

      3) EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application (beskyttelsesprofiler til enheder til generering af sikker signatur — del 4: udvidelse for enheder med nøglegenerering og pålidelig kanal til certifikatgenereringsapplikation) (v1.0.1), BSI-CC-PP-0071-2012-MA-01

      4) EN 419211-5:2013 — Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application (beskyttelsesprofiler til enheder til generering af sikker signatur — del 5: udvidelse til enheder med nøglegenerering og pålidelig kanal til signaturgenereringsapplikation) (v1.0.1), BSI-CC-PP-0072-2012-MA-01

      5) EN 419211-6:2014 — Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted channel to signature creation application (beskyttelsesprofiler til enheder til generering af sikker signatur — del 6: udvidelse til enheder med nøgleimport og pålidelig kanal til signaturgenereringsapplikation) (v1.0.4), BSI-CC-PP-0076-2013-MA-01

   c) takografer: digital takograf — takografkort (TC PP) (v1.0), BSI-CC-PP-0091-2017

   d) sikker IC, Java Card-platform og eUICC:

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

      2) Security IC Platform PP med udvidelsespakker (v1.0), BSI-CC-PP-0084-2014

      3) Indlejret UICC (eUICC) til maskine-til-maskine-enheder, BSI-CC-PP-0089-2015

      4) Kryptografisk tjenesteudbyder — CSP (v0.9.8), BSI-CC-PP-0104-2019

      5) Kryptografisk tjenesteudbyder — tidsstempeltjeneste og revision (PPC-CSP-TS-Au) Version 0.9.5, BSI-CC-PP-0107-2019

      6) Konfiguration af kryptografisk tjenesteudbyder — Tidsstempeltjeneste, revision og klyngedannelse (PPC-CSP-TS-Au-Cl) Version 0.9.4, BSI-CC-PP-0108-2019

      7) Java Card System — lukket konfiguration, BSI-CC-PP-0101-V2-2020

      8) Beskyttelsesprofil til Secure Element — GPC_SPE_174 (v1.0), CCN-CC-PP-5-2021

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

      10) Java Card System — åben konfiguration, v3.2 BSI-CC-PP-0099-V3-2024

      11) Indlejret UICC til forbrugerenheder, beskyttelsesprofil (v2.1), BSI-CC-PP-0100-V2-2025

   e) pålideligt platformmodul: Beskyttelsesprofil for PC-klient specifikt pålideligt platformmodul i specifikationsfamilie 2.0 Niveau 0: Revision 1.59 (v1.3), ANSSI-CC-PP-2021/02.

2. Hardwareenheder med sikkerhedsbokse
   a) (betalings-)interaktionspunkter og betalingsterminaler (POI):
      1) Point of Interaction »POI-CHIP-ONLY« (v4.0), ANSSI-CC-PP-2015/01
      2) Point of Interaction »POI-CHIP-ONLY and Open Protocol Package« (v4.0), ANSSI-CC-PP-2015/02
      3) Point of Interaction »POI-COMPREHENSIVE« (v4.0), ANSSI-CC-PP-2015/03
      4) Point of Interaction»POI-COMPREHENSIVE and Open Protocol Package« (v4.0), ANSSI-CC-PP-2015/04
      5) Point of Interaction »POI-PED-ONLY« (v4.0), ANSSI-CC-PP-2015/05
      6) Point of Interaction »POI-PED-ONLY and Open Protocol Package« (v4.0), ANSSI-CC-PP-2015/06
   b) hardwaresikkerhedsmodul:
      1) Kryptografisk modul til CSP-signeringsoperationer med sikkerhedskopiering — PP CMCSOB 14167-2 (v0.35), ANSSI-CC-PP-2015/08
      2) Kryptografisk modul til CSP-nøglegenereringstjenester — PP CMCKG 14167-3 (v0.20), ANSSI-CC-PP-2015/09
      3) Kryptografisk modul til CSP-signeringsoperationer uden backup — PP CMCSO 14167-4 (v0.32), ANSSI-CC-PP-2015/10
   c) takografer:
      1) Digital takograf — bevægelsessensor (MS PP) (v1.0), BSI-CC-PP-0093-2017
      2) Digital takograf — køretøjsenhed (VU PP) (v1.15), BSI-CC-PP-0094-V2-2021
      3) Digital takograf — eksternt GNSS-udstyr (EGF PP) (v1.10), BSI-CC-PP-0092-V2-2021.
3. Andre: Trusted Execution Environment Protection Profile — GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.«

BILAG IV

Bilag IV til gennemførelsesforordning (EU) 2024/482 ændres således:

1. Punkt IV.2, nr. 4), affattes således:

»4. Certificeringsorganet reviderer den ajourførte rapport om teknisk evaluering og udarbejder en rapport om fornyet vurdering. Status for den oprindelige attest ændres derefter i overensstemmelse med artikel 13 eller artikel 19. Hvis den fornyede vurderingsproces afsluttes med et positivt resultat, finder artikel 13, stk. 2, litra a) eller c), anvendelse i tilfælde af certificering af et produkt, og artikel 19, stk. 2, litra a) eller c), finder anvendelse i tilfælde af certificering af en beskyttelsesprofil. Hvis den fornyede vurderingsproces ikke afsluttes med et positivt resultat, finder artikel 13, stk. 2, litra b) eller d), anvendelse i tilfælde af certificering af et produkt, og artikel 19, stk. 2, litra b) eller d), finder anvendelse i tilfælde af certificering af en beskyttelsesprofil.«

2. I punkt IV.3 foretages følgende ændringer:

a) Overskrift IV.3 affattes således:

»IV.3 **Ændringer af et certificeret IKT-produkt — Vedligeholdelse og fornyet vurdering**«

b) Punkt 4) og 5) affattes således:

»4. Efter undersøgelsen fastlægger certificeringsorganet omfanget af en ændring som mindre eller væsentlig i forhold til dens indvirkning på det tillidsniveau, der er anført i EUCC-attesten.

5. Hvis ændringerne er blevet bekræftet af certificeringsorganet som ændringer af mindre omfang, udstedes der ikke nogen ny attest for det ændrede IKT-produkt i overensstemmelse med artikel 13, stk. 2, litra a), eller artikel 19, stk. 2, litra a), og der udarbejdes en vedligeholdelsesrapport til den indledende certificeringsrapport.«

c) Følgende indsættes som punkt 5a:

»5.a I tilfælde af ændringer af tillidsforanstaltningerne i udviklingsmiljøet, herunder tilføjelse af krav til tillid fra CC ALC_FLR-familien (afhjælpning af fejl), kan certificeringsorganet anmode ITSEF'en om at foretage en delvis evaluering af de berørte tillidsforanstaltninger. ITSEF'en udsteder en teknisk rapport om den delvise evaluering, på grundlag af hvilken certificeringsorganet bekræfter, om ændringerne er mindre eller væsentlige. Hvis certificeringsorganet har bekræftet, at ændringerne er af mindre omfang, finder bilag IV.3, punkt 5, anvendelse. Hvis certificeringsorganet har bekræftet, at ændringerne er væsentlige, finder bilag IV.3, punkt 7, anvendelse.«

BILAG V

Punkt V.1 i bilag V til gennemførelsesforordning (EU) 2024/482 affattes således:

»V.1 **Certificeringsrapport**

1. På grundlag af rapporterne om teknisk evaluering fra certificeringsorganet udarbejder certificeringsorganet en certificeringsrapport, der skal offentliggøres sammen med den tilsvarende EUCC-attest og det tilsvarende sikkerhedsmål.

2. Certificeringsrapporten er kilden til detaljerede og praktiske oplysninger om IKT-produktet og om sikker implementering af IKT-produktet. Den skal derfor indeholde alle offentligt tilgængelige oplysninger, som kan deles, og som er relevante for brugere og interesserede parter. Der kan henvises til offentligt tilgængelige oplysninger, som kan deles, i certificeringsrapporten.

3. Certificeringsrapporten skal som minimum indeholde følgende oplysninger:
   a) resumé
   b) identifikation af IKT-produktet
   c) kontaktoplysninger vedrørende evalueringen af IKT-produktet
   d) sikkerhedspolitikker
   e) antagelser om og præcisering af anvendelsesområdet
   f) oplysninger om arkitektur
   g) supplerende oplysninger om cybersikkerhed, hvis det er relevant
   h) sammenfatning af IKT-produktevaluering og evalueret konfiguration
   i) resultaterne af evalueringen og oplysninger om attesten
   j) bemærkninger og henstillinger, hvis relevant
   k) bilag, hvis relevant
   l) henvisning til sikkerhedsmålet for det IKT-produkt, der skal certificeres
   m) den mærkning eller etiket, der eventuelt er knyttet til ordningen
   n) ordliste, hvis relevant
   o) bibliografi.

4. Det resumé, der er omhandlet i nr. 3), litra a), skal være et kort resumé af hele certificeringsrapporten. Resuméet skal give et klart og præcist overblik over evalueringsresultaterne og indeholde følgende oplysninger:
   a) navnet på det evaluerede IKT-produkt
   b) navnet på den ITSEF, der har foretaget evalueringen
   c) dato for evalueringens afslutning
   d) dato for udstedelse af attesten
   e) hvis det er relevant, udstedelsesdatoen for den indledende attest
   f) gyldighedsperiode
   g) entydig identifikation af attesten som beskrevet i artikel 11
   h) kort beskrivelse af certificeringsrapportens resultater, herunder:
      i) versions- og frigivelsesnummer, hvis det er relevant, for de fælles kriterier, der er anvendt ved evalueringen
      ii) tillidspakke eller sikkerhedstillidskomponenter under de fælles kriterier, det AVA_VAN-niveau, der er anvendt ved evalueringen, og det tilsvarende tillidsniveau som fastsat i artikel 52 i forordning (EU) 2019/881, som EUCC-attesten henviser til
      iii) hvis det er relevant, den eller de beskyttelsesprofiler, som IKT-produktet påberåber overensstemmelse med
      iv) henvisning til sikkerhedspolitikken for det evaluerede IKT-produkt
      v) ansvarsfraskrivelse(r), hvis relevant.

5. Den identifikation, der er omhandlet i nr. 3), litra b), skal klart angive det evaluerede IKT-produkt og omfatte følgende oplysninger:

   a) den entydige identifikation af det evaluerede IKT-produkt

   b) en opremsning af de af IKT-produktets komponenter, som indgår i evalueringen, med versionsnummer for hver komponent

   c) reference til yderligere krav til det certificerede IKT-produkts driftsmiljø.

6. De kontaktoplysninger, der er omhandlet i nr. 3), litra c), skal mindst indeholde følgende oplysninger:

   a) udviklerens navn

   b) navn og kontaktoplysninger på EUCC-attestindehaveren

   c) navnet på det certificeringsorgan, der har udstedt attesten

   d) ansvarlig national cybersikkerhedscertificeringsmyndighed

   e) navnet på den ITSEF, der har foretaget evalueringen, og listen over underleverandører, hvis det er relevant

7. Den sikkerhedspolitik, der er omhandlet i nr. 3), litra d), skal indeholde en beskrivelse af IKT-produktets sikkerhedspolitik som en samling af sikkerhedstjenester samt de politikker eller regler, som det evaluerede IKT-produkt skal håndhæve eller overholde. Den skal ligeledes indeholde følgende oplysninger:

   a) en beskrivelse af attestindehaverens procedurer for sårbarhedsstyring og offentliggørelse af sårbarheder, som udelukkende skal udfyldes med oplysninger, der kan gøres offentligt tilgængelige

   b) attestindehaverens politik for tillidskontinuitet, herunder, hvis det er relevant, en beskrivelse af attestindehaverens livscyklusstyrings- eller produktionsprocesser i overensstemmelse med bilag IV, punkt IV.1

   c) hvis det er relevant, tilstedeværelsen af en patchstyringsprocedure og resultatet af vurderingen heraf i overensstemmelse med bilag IV, punkt IV.4.

8. De antagelser og præciseringer af anvendelsesområdet, der er omhandlet i nr. 3), litra e), skal indeholde oplysninger om omstændighederne og målene i forbindelse med den påtænkte anvendelse af produktet, jf. artikel 7, stk. 1, litra c), og skal omfatte følgende:

   a) antagelser om IKT-produktets anvendelse og implementering i form af minimumskrav, f.eks. korrekt installation og konfiguration, og hardwarekrav, der skal opfyldes

   b) antagelser om miljøet for overensstemmende drift af IKT-produktet.

   c) beskrivelse af eventuelle trusler mod IKT-produktet, som ikke imødegås af produktets evaluerede sikkerhedsfunktioner i henhold til den påtænkte anvendelse, hvis det anses for relevant for en potentiel bruger af IKT-produktet.

   De oplysninger, der er omhandlet i første afsnit, skal være så klare og forståelige som muligt for at sætte potentielle brugere af det certificerede IKT-produkt i stand til at træffe informerede beslutninger om de risici, der er forbundet med dets anvendelse.

9. De arkitektoniske oplysninger, der er omhandlet i nr. 3), litra f), skal omfatte en overordnet beskrivelse af IKT-produktet og dets hovedkomponenter baseret på de leverancer, der er defineret i sikringsfamilien for fælles kriterier: udvikling — TOE Design (ADV_TDS).

10. De supplerende oplysninger om cybersikkerhed, der er omhandlet i nr. 3), litra g), skal omfatte linket til webstedet for indehaveren af EUCC-attesten, jf. artikel 55 i forordning (EU) 2019/881.

11. Den IKT-produktevaluering og -konfiguration, der er omhandlet i nr. 3), litra h), skal beskrive både udviklerens og evaluatorens testindsats og skitsere testtilgangen, konfigurationen og dybden. Den skal mindst indeholde følgende oplysninger:

    a) en identifikation af de anvendte tillidselementer fra de standarder, der er omhandlet i artikel 3

    b) statusdokumenternes version og yderligere sikkerhedsevalueringskriterier, der er anvendt i evalueringen

    c) indstillingerne og konfigurationen af det evalueringsmål, der anvendes til testning og sårbarhedsanalyse

    d) alle beskyttelsesprofiler, der er blevet anvendt, herunder følgende oplysninger: beskyttelsesprofilens navn, version, dato og certifikat.

12. Resultaterne af evalueringen og oplysningerne vedrørende den attest, der er omhandlet i nr. 3), litra i), skal omfatte oplysninger om det opnåede tillidsniveau som omhandlet i denne forordnings artikel 4 og artikel 52 i forordning (EU) 2019/881.

13. De bemærkninger og henstillinger, der er omhandlet i nr. 3), litra j), anvendes til at give supplerende oplysninger om evalueringsresultaterne. Disse bemærkninger og henstillinger kan tage form af mangler ved IKT-produktet, der opdages under evalueringen, eller omtale af funktioner, der er særligt nyttige.

14. De bilag, der er omhandlet i nr. 3), litra k), anvendes til at skitsere eventuelle yderligere oplysninger, der kan være nyttige for rapportens målgruppe, men som logisk set ikke passer ind i de foreskrevne afsnit i rapporten, herunder i tilfælde af en fuldstændig beskrivelse af sikkerhedspolitikken.

15. Det sikkerhedsmål, der er omhandlet i nr. 3), litra l), skal henvise til det evaluerede sikkerhedsmål. Det evaluerede sikkerhedsmål skal fremgå af certificeringsrapporten med henblik på offentliggørelse på det websted, der er omhandlet i artikel 50, stk. 1, i forordning (EU) 2019/881. Hvis det er nødvendigt at rense det evaluerede sikkerhedsmål for følsomme oplysninger inden offentliggørelsen, skal det ske i overensstemmelse med punkt V.2 i bilag V til denne forordning.

16. Den mærkning eller de etiketter, der er knyttet til EUCC-ordningen, jf. nr. 3), litra m), skal indsættes i certificeringsrapporten i overensstemmelse med de regler og procedurer, der er fastsat i artikel 11.

17. Den ordliste, der er omhandlet i nr. 3), litra n), anvendes til at øge rapportens læsbarhed ved at give definitioner af akronymer eller udtryk, hvis betydning måske ikke er umiddelbart indlysende.

18. Den i nr. 3), litra o), omhandlede bibliografi skal indeholde henvisninger til alle dokumenter, der er anvendt ved udarbejdelsen af certificeringsrapporten. Disse oplysninger skal som minimum omfatte følgende:

    a) sikkerhedsevalueringskriterierne, statusdokumenterne og yderligere relevante specifikationer, der er anvendt

    b) rapporten om teknisk evaluering

    c) rapporten om teknisk evaluering for den sammensatte evaluering, hvis det er relevant

    d) teknisk referencedokumentation

    e) sikkerhedsvejledning til udviklere

    f) konfigurationsliste til udviklere.

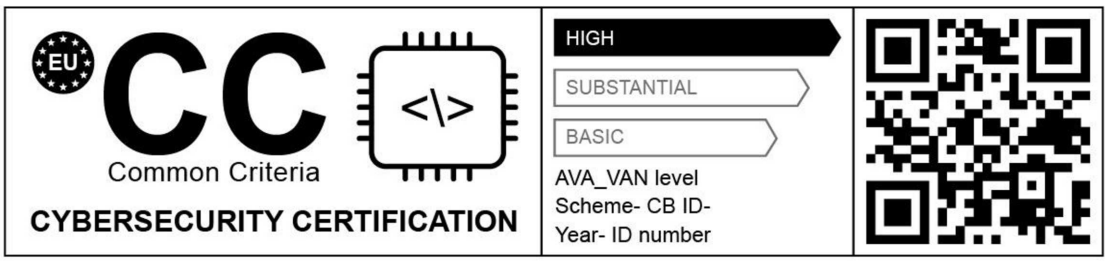
    For at sikre, at evalueringen er reproducerbar, skal al den dokumentation, der henvises til, identificeres entydigt med den korrekte udgivelsesdato og det korrekte versionsnummer.«

BILAG VI

»BILAG IX

Mærkning og etiketter

1. Mærkningens og etikettens form:



2. Hvis mærkningen og etiketten formindskes eller forstørres, skal det størrelsesforhold, der fremgår af punkt 1, overholdes.

3. Hvis mærkningen og etiketten er påført fysisk, skal den være mindst 5 mm høj.«