2024/482

7.2.2024

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)

(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 nærværende forordning 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. EUCC bygger på Gruppen af Højtstående Embedsmænd vedrørende Informationssystemers Sikkerheds (SOG-IS') aftale om gensidig anerkendelse (MRA) ([2]) under anvendelse af de fælles kriterier, herunder gruppens procedurer og dokumenter.

(2) Ordningen bør baseres på etablerede internationale standarder. Fælles kriterier er en international standard for evaluering af informationssikkerhed, der f.eks. er offentliggjort som ISO/IEC 15408 Informationssikkerhed, cybersikkerhed og beskyttelse af privatlivets fred — Evalueringskriterier for IT-sikkerhed. Den er baseret på tredjepartsevalueringer og arbejder med syv Evaluation Assurance Levels (»EAL«). De fælles kriterier ledsages af den fælles evalueringsmetode, der f.eks. er offentliggjort som ISO/IEC 18045 — Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse — Evalueringskriterier for IT-sikkerhed — Metodik for IT-sikkerhedsevaluering. Specifikationer og dokumenter, der anvender bestemmelserne i denne forordning, kan vedrøre en offentligt tilgængelig standard, der afspejler den standard, der anvendes ved certificering i henhold til denne forordning, såsom fælles kriterier for evaluering af informationsteknologisk sikkerhed og fælles metode til informationsteknologisk sikkerhedsevaluering.

(3) EUCC anvender de fælles kriteriers sårbarhedsvurderingsfamilie (AVA_VAN), komponent 1-5. De fem komponenter omfatter alle de vigtigste determinanter og afhængighedsforhold til analyse af IKT-produkters sårbarheder. Da komponenterne svarer til tillidsniveauerne i denne forordning, giver de mulighed for et velinformeret valg af sikkerhed på grundlag af de evalueringer af sikkerhedskravene, der er foretaget, og den risiko, der er forbundet med den tilsigtede anvendelse af IKT-produktet. Ansøgere om en EUCC-attest bør fremlægge dokumentationen vedrørende den påtænkte anvendelse af IKT-produktet og en analyse af de risikoniveauer, der er forbundet med en sådan anvendelse, for at gøre det muligt for overensstemmelsesvurderingsorganet at vurdere egnetheden af det valgte tillidsniveau. Hvis evaluerings- og certificeringsaktiviteterne udføres af det samme overensstemmelsesvurderingsorgan, bør ansøgeren kun indsende de ønskede oplysninger én gang.

(4) Et teknisk område udgør en referenceramme, der dækker en gruppe IKT-produkter, som har specifikke og ensartede sikkerhedsfunktioner, som afbøder angreb, hvor karakteristikaene er fælles for et givet tillidsniveau. I statusdokumentet for et teknisk område beskrives de specifikke sikkerhedskrav samt yderligere evalueringsmetoder, -teknikker og -værktøjer, der finder anvendelse ved certificering af IKT-produkter, som er omfattet af det pågældende tekniske område. Et teknisk område fremmer derfor også harmoniseringen af evalueringen af de omfattede IKT-produkter. Der anvendes i øjeblikket i vid udstrækning to tekniske områder til certificering på

([1]) EUT L 151 af 7.6.2019, s. 15.

([2]) Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0 fra januar 2010 findes på sogis.eu, godkendt af Gruppen af Højtstående Embedsmænd vedrørende Informationssystemers Sikkerhed under Europa-Kommissionen som svar på punkt 3 i Rådets henstilling 95/144/EF af 7. april 1995 om ensartede kriterier for vurdering af informationsteknologisk sikkerhed (EFT L 93 af 26.4.1995, s. 27).

niveauerne AVA_VAN.4 og AVA_VAN.5. Det første tekniske område er det tekniske område »smartcards og lignende enheder«, hvor betydelige dele af de krævede sikkerhedsfunktioner afhænger af specifikke, skræddersyede og ofte adskillelige hardwareelementer (f.eks. smartcardhardware, integrerede kredsløb, sammensatte produkter til smartcards, Trusted Platform Modules som anvendt i sikre computersystemer eller digitale takografkort). Det andet tekniske område er »hardwareenheder med sikkerhedsbokse«, hvor væsentlige dele af de krævede sikkerhedsfunktioner afhænger af en fysisk hardwareramme (en såkaldt »sikkerhedsboks«), der er udformet til at modstå direkte angreb, f.eks. betalingsterminaler, takografkøretøjsenheder, intelligente målere, adgangskontrolterminaler og hardwaresikkerhedsmoduler).

(5) Ved ansøgning om certificering bør ansøgeren knytte sin begrundelse for valget af et sikringsniveau til de mål, der er fastsat i artikel 51 i forordning (EU) 2019/881, og til udvælgelsen af komponenter fra kataloget over sikkerhedskrav og sikkerhedskrav i de fælles kriterier. Certificeringsorganerne bør vurdere hensigtsmæssigheden af det valgte tillidsniveau og sikre, at det valgte niveau står i et rimeligt forhold til det risikoniveau, der er forbundet med den tilsigtede anvendelse af IKT-produktet.

(6) I henhold til de fælles kriterier foretages certificeringen i forhold til et konkret sikkerhedsmål, der omfatter en definition af IKT-produktets sikkerhedsproblem samt de sikkerhedsmålsætninger, der afhjælper sikkerhedsproblemet. Sikkerhedsproblemet indeholder nærmere oplysninger om den tilsigtede anvendelse af IKT-produktet og de risici, der er forbundet med en sådan anvendelse. Et udvalgt sæt sikkerhedskrav svarer til både sikkerhedsproblemet og sikkerhedsmålsætningerne for et IKT-produkt.

(7) Beskyttelsesprofiler er et effektivt middel til at fastsætte de fælles kriterier, der gælder for en given kategori af IKT-produkter, og derfor også et væsentligt element i certificeringsprocessen for IKT-produkter, der er omfattet af beskyttelsesprofilen. Til at vurdere fremtidige sikkerhedsmål, som falder ind under den pågældende IKT-produktkategori, der er omfattet af denne beskyttelsesprofil, anvendes en beskyttelsesprofil. De strømliner og øger effektiviteten af IKT-produktcertificeringsprocessen yderligere og hjælper brugerne med korrekt og effektivt at specificere et IKT-produkts funktioner. Beskyttelsesprofiler bør derfor betragtes som en integreret del af den IKT-proces, der fører til certificering af IKT-produkter.

(8) For at muliggøre beskyttelsesprofilernes rolle i IKT-processen, som støtter udviklingen og leveringen af et certificeret IKT-produkt, bør de kunne certificeres uafhængigt af en certificering af det specifikke IKT-produkt, som er omfattet af den pågældende beskyttelsesprofil. Det er derfor vigtigt at anvende mindst samme grad af kontrol af beskyttelsesprofiler som af sikkerhedsmål for at sikre et højt cybersikkerhedsniveau. Beskyttelsesprofilerne bør evalueres og certificeres særskilt fra det relaterede IKT-produkt og udelukkende ved anvendelse af de fælles kriteriers og den fælles evalueringsmetodes tillidsklasse for beskyttelsesprofiler og, hvor det er relevant, for konfigurationerne af beskyttelsesprofiler. På grund af deres vigtige og følsomme rolle som benchmark i forbindelse med certificering af IKT-produkter bør de kun certificeres af offentlige organer eller af et certificeringsorgan, der har fået forhåndsgodkendelse til den specifikke beskyttelsesprofil af den nationale cybersikkerhedscertificeringsmyndighed. På grund af deres afgørende rolle med hensyn til certificering på tillidsniveauet »højt«, navnlig uden for tekniske områder, bør beskyttelsesprofiler udarbejdes som statusdokumenter, der bør godkendes af Den Europæiske Cybersikkerhedscertificeringsgruppe.

(9) Certificerede beskyttelsesprofiler bør medtages i de nationale cybersikkerhedscertificeringsmyndigheders EUCC-overensstemmelses- og -overholdelsesovervågning. Hvis metoder, værktøjer og færdigheder, der anvendes i forbindelse med tilgange til evaluering af IKT-produkter, er tilgængelige for specifikke certificerede beskyttelsesprofiler, kan tekniske områder baseres på disse specifikke beskyttelsesprofiler.

(10) For at opnå en høj grad af tillid til certificerede IKT-produkter bør selvvurderinger ikke være tilladt i henhold til denne forordning. Kun overensstemmelsesvurderinger foretaget af ITSEF og certificeringsorganer bør tillades.

(11) SOG-IS-fællesskabet bidrog med fælles fortolkninger og tilgange til anvendelsen af de fælles kriterier og den fælles evalueringsmetode i forbindelse med certificering, navnlig med hensyn til sikringsniveauet »høj«, der forfølges inden for de tekniske områder »smartcards og lignende enheder« og »hardwareenheder med sikkerhedsbokse«. Videreanvendelse af sådanne støttedokumenter i EUCC-ordningen sikrer en gnidningsløs overgang fra de nationalt gennemførte SOG-IS-ordninger til den harmoniserede EUCC-ordning. Derfor bør harmoniserede evalueringsmetoder, som generelt er relevante for alle certificeringsaktiviteter, medtages i denne forordning. Kommissionen bør desuden kunne anmode Den Europæiske Cybersikkerhedscertificeringsgruppe om at vedtage en udtalelse, der godkender og anbefaler anvendelsen af de evalueringsmetoder, der er angivet i statusdokumenterne, til certificering af IKT-produktet eller beskyttelsesprofilen under EUCC-ordningen. Bilag I til denne forordning indeholder derfor en liste over statusdokumenter til de evalueringsaktiviteter, der udføres af overensstemmelsesvurderingsorganer. Den Europæiske Cybersikkerhedscertificeringsgruppe bør godkende og vedligeholde statusdokumenterne. Statusdokumenterne bør anvendes i forbindelse med certificering. Kun i ekstraordinære og behørigt begrundede tilfælde må et overensstemmelsesvurderingsorgan undlade at anvende dem på særlige betingelser, navnlig den nationale cybersikkerhedscertificeringsmyndigheds godkendelse.

(12) Certificering af IKT-produkter på AVA_VAN-niveau 4 eller 5 bør kun være mulig på særlige betingelser, og hvis der findes en specifik evalueringsmetode. Den specifikke evalueringsmetode kan være nedfældet i statusdokumenter, der er relevante for det tekniske område, eller i specifikke beskyttelsesprofiler, der er vedtaget som statusdokument, og som er relevante for den pågældende produktkategori. Kun i ekstraordinære og behørigt begrundede tilfælde bør certificering på disse tillidsniveauer være mulig på særlige betingelser, navnlig den nationale cybersikkerhedscertificeringsmyndigheds godkendelse, herunder af den gældende evalueringsmetode. Sådanne ekstraordinære og behørigt begrundede tilfælde kan forekomme, hvor EU-lovgivning eller national lovgivning kræver certificering af et IKT-produkt på AVA_VAN-niveau 4 eller 5. Tilsvarende kan beskyttelsesprofiler i ekstraordinære og behørigt begrundede tilfælde certificeres uden anvendelse af de relevante statusdokumenter på særlige betingelser, navnlig med den nationale cybersikkerhedscertificeringsmyndigheds godkendelse, herunder af den gældende evalueringsmetode.

(13) De mærker og etiketter, der anvendes under EUCC, har til formål tydeligt at dokumentere det certificerede IKT-produkts troværdighed over for brugerne og sætte dem i stand til at træffe et informeret valg, når de køber IKT-produkter. Brugen af mærker og etiketter bør også være underlagt de regler og betingelser, der er fastsat i ISO/IEC 17065 og, hvor det er relevant, ISO/IEC 17030 med den gældende vejledning.

(14) Certificeringsorganerne bør træffe afgørelse om attesternes gyldighedsperiode under hensyntagen til det pågældende IKT-produkts livscyklus. Gyldighedsperioden bør ikke overstige fem år. De nationale cybersikkerhedscertificeringsmyndigheder bør arbejde på at harmonisere gyldighedsperioden i Unionen.

(15) Hvis anvendelsesområdet for en eksisterende EUCC-attest indskrænkes, tilbagekaldes attesten, og der bør udstedes en ny attest med det nye anvendelsesområde for at sikre, at brugerne er klart informeret om det nuværende anvendelsesområde og tillidsniveau for attesten for et givet IKT-produkt.

(16) Certificeringen af beskyttelsesprofiler adskiller sig fra certificeringen af IKT-produkter, da den vedrører en IKT-proces. Eftersom en beskyttelsesprofil dækker en kategori af IKT-produkter, kan evaluering og certificering heraf ikke foretages på grundlag af et enkelt IKT-produkt. Da en beskyttelsesprofil forener de generelle sikkerhedskrav vedrørende en kategori af IKT-produkter og uafhængigt af, hvordan IKT-produktet kommer til udtryk ved leverandøren, bør gyldighedsperioden for en EUCC-attest til en beskyttelsesprofil i princippet gælde i mindst fem år og kunne forlænges til beskyttelsesprofilens levetid.

(17) Et overensstemmelsesvurderingsorgan defineres som et organ, der udfører overensstemmelsesvurderingsaktiviteter, herunder kalibrering, afprøvning, certificering og inspektion. For at sikre tjenester af høj kvalitet præciseres det i denne forordning, at prøvningsaktiviteter på den ene side og certificerings- og inspektionsaktiviteter på den anden bør udføres af enheder, der opererer uafhængigt af hinanden, nemlig henholdsvis informationsteknologisikkerhedsvurderingsfaciliteter (»ITSEF«) og certificeringsorganer. Begge typer overensstemmelsesvurderingsorganer bør akkrediteres og i visse situationer godkendes.

(18) Et certificeringsorgan bør akkrediteres i overensstemmelse med ISO/IEC 17065 af det nationale akkrediteringsorgan for tillidsniveauet »betydeligt« og »højt«. Ud over akkrediteringen i overensstemmelse med forordning (EU) 2019/881 sammenholdt med forordning (EF) nr. 765/2008 bør overensstemmelsesvurderingsorganerne opfylde specifikke krav for at garantere deres tekniske kompetence til at evaluere cybersikkerhedskravene på tillidsniveauet »højt« i EUCC, hvilket bekræftes af en »bemyndigelse«. For at støtte bemyndigelsesprocessen bør der udvikles relevante statusdokumenter, som ENISA offentliggør efter godkendelse fra Den Europæiske Cybersikkerhedscertificeringsgruppe.

(19) En ITSEF's tekniske kompetencer bør vurderes gennem akkreditering af prøvningslaboratoriet i overensstemmelse med ISO/IEC 17025 suppleret med ISO/IEC 23532-1 for alle evalueringsaktiviteter, der er relevante for tillidsniveauet og specificeret i ISO/IEC 18045 sammenholdt med ISO/IEC 15408. Både certificeringsorganet og ITSEF'en bør etablere og vedligeholde et passende kompetencestyringssystem for personalet, der er baseret på ISO/IEC 19896-1, for så vidt angår kompetenceelementerne og -niveauerne og for så vidt angår bedømmelsen af kompetencerne. For så vidt angår niveauet af viden, færdigheder, erfaring og uddannelse bør de gældende krav til bedømmerne baseres på ISO/IEC 19896-3. Tilsvarende bestemmelser og foranstaltninger vedrørende afvigelser fra sådanne kompetenceforvaltningssystemer bør påvises i overensstemmelse med systemets mål.

(20) For at blive godkendt bør en ITSEF dokumentere, at den kan fastslå, at der ikke foreligger kendte sårbarheder, at de nyeste sikkerhedsfunktioner for den pågældende specifikke teknologi gennemføres korrekt og konsekvent, og at det pågældende IKT-produkt er modstandsdygtigt over for drevne angribere. For så vidt angår bemyndigelser på det tekniske område »smartcards og lignende enheder« bør en ITSEF desuden dokumentere den tekniske kapacitet, der er nødvendig for evalueringsaktiviteterne og de dermed forbundne opgaver som defineret i støttedokumentet »Minimum ITSEF requirements for security evaluations of smart cards and similar devices« ([3]) i henhold til de fælles kriterier. For så vidt angår bemyndigelser på det tekniske område »hardwareenheder med sikkerhedsbokse« bør en ITSEF desuden dokumentere de tekniske minimumskrav, der er nødvendige for at udføre evalueringsaktiviteter og relaterede opgaver på hardwareudstyr med sikkerhedsbokse som anbefalet af ECCG. I forbindelse med minimumskravene bør ITSEF kunne udføre de forskellige typer angreb, der er fastsat i støttedokumentet »Application of Attack Potential to Hardware Devices with Security Boxes« i henhold til de fælles kriterier. Disse kapaciteter omfatter evaluatorens viden og færdigheder samt det udstyr og de evalueringsmetoder, der er nødvendige for at fastlægge og vurdere de forskellige typer angreb.

(21) Den nationale cybersikkerhedscertificeringsmyndighed bør overvåge certificeringsorganernes, ITSEF og attestindehaveres overholdelse af deres forpligtelser i henhold til nærværende forordning og forordning (EU) 2019/881. Den nationale cybersikkerhedscertificeringsmyndighed bør anvende alle relevante informationskilder til dette formål, herunder oplysninger modtaget fra deltagere i certificeringsprocessen og egne undersøgelser.

(22) Certificeringsorganerne bør samarbejde med relevante markedsovervågningsmyndigheder og tage hensyn til eventuelle sårbarhedsoplysninger, der kan være relevante for IKT-produkter, som de har udstedt attester for. Certificeringsorganerne bør overvåge de beskyttelsesprofiler, de har certificeret, for at fastslå, om de sikkerhedskrav, der er fastsat for en kategori af IKT-produkter, fortsat afspejler den seneste udvikling i trusselsbilledet.

(23) Til støtte for overensstemmelsesovervågningen bør de nationale cybersikkerhedscertificeringsmyndigheder samarbejde med de relevante markedsovervågningsmyndigheder i overensstemmelse med artikel 58 i forordning (EU) 2019/881 og Europa-Parlamentets og Rådets forordning (EU) 2019/1020 ([4]). Erhvervsdrivende i Unionen er forpligtet til at udveksle oplysninger og samarbejde med markedsovervågningsmyndighederne i henhold til artikel 4, stk. 3, i forordning (EU) 2019/1020.

([3]) Joint Interpretation Library: Minimum ITSEF Requirements for Security Evaluations of Smart cards and similar devices, version 2.1 fra februar 2020 findes på sogis.eu.

([4]) Europa-Parlamentets og Rådets forordning (EU) 2019/1020 af 20. juni 2019 om markedsovervågning og produktoverensstemmelse og om ændring af direktiv 2004/42/EF og forordning (EF) nr. 765/2008 og (EU) nr. 305/2011 (EUT L 169 af 25.6.2019, s. 1).

(24) Certificeringsorganerne bør overvåge, at indehavere af en attest overholder kravene, og at alle attester, der er udstedt under EUCC, er i overensstemmelse med bestemmelserne. Ved overvågningen bør det sikres, at alle evalueringsrapporter fra et ITSEF organ og konklusionerne deri samt evalueringskriterierne og -metoderne anvendes konsekvent og korrekt i alle certificeringsaktiviteter.

(25) Hvis der konstateres potentielle problemer med manglende overholdelse, som påvirker et certificeret IKT-produkt, er det vigtigt at sikre en forholdsmæssig reaktion. Attester kan derfor suspenderes. Suspensionen bør medføre visse begrænsninger med hensyn til fremme og anvendelse af det pågældende IKT-produkt, men bør ikke berøre attestens gyldighed. Indehaveren af EU-attesten bør underrette køberne af de berørte IKT-produkter om suspensionen, mens de relevante markedsovervågningsmyndigheder bør underrettes af den relevante nationale cybersikkerhedscertificeringsmyndighed. For at informere offentligheden bør ENISA offentliggøre oplysninger om en suspension på et særligt websted.

(26) Indehaveren af en EUCC-attest bør gennemføre de nødvendige procedurer for sårbarhedsstyring og sikre, at disse procedurer er integreret i deres organisation. Når indehaveren af EUCC-attesten bliver opmærksom på en potentiel sårbarhed, bør vedkommende foretage en sårbarhedskonsekvensanalyse. Hvis sårbarhedsanalysen bekræfter, at sårbarheden kan udnyttes, bør attestindehaveren sende en rapport om vurderingen til certificeringsorganet, som derefter bør underrette den nationale cybersikkerhedscertificeringsmyndighed. Rapporten bør indeholde oplysninger om virkningen af sårbarheden, de nødvendige ændringer eller afhjælpende løsninger, der er nødvendige, herunder eventuelle bredere konsekvenser af sårbarheden samt afhjælpende løsninger for andre produkter. Om nødvendigt bør standarden EN ISO/IEC 29147 supplere proceduren for offentliggørelse af sårbarheder.

(27) Med henblik på certificering indhenter overensstemmelsesvurderingsorganer og nationale cybersikkerhedscertificeringsmyndigheder fortrolige og følsomme data og forretningshemmeligheder, også vedrørende intellektuel ejendomsret eller overvågning af overholdelse, der kræver tilstrækkelig beskyttelse. De bør derfor have den nødvendige tekniske kompetence og viden og bør etablere systemer til beskyttelse af oplysninger. Kravene og betingelserne for beskyttelse af oplysninger bør opfyldes i forbindelse med både akkreditering og bemyndigelse.

(28) ENISA bør fremlægge listen over certificerede beskyttelsesprofiler på sit websted for cybersikkerhedscertificering og angive deres status i overensstemmelse med forordning (EU) 2019/881.

(29) I nærværende forordning fastsættes betingelserne for aftaler om gensidig anerkendelse med tredjelande. Sådanne aftaler om gensidig anerkendelse kan være bi- eller multilaterale og bør erstatte lignende eksisterende aftaler. For at lette en gnidningsløs overgang til sådanne aftaler om gensidig anerkendelse kan medlemsstaterne fortsætte de eksisterende samarbejdsordninger med tredjelande i en begrænset periode.

(30) Certificeringsorganer, der udsteder EUCC-attester på tillidsniveauet »højt«, samt de relevante tilknyttede ITSEF bør underkastes peervurderinger. Formålet med peervurderinger bør være at fastslå, om et peervurderet certificeringsorgans vedtægter og procedurer fortsat er i overensstemmelse med kravene i EUCC-ordningen. Peervurderinger adskiller sig fra peerreviews blandt nationale cybersikkerhedscertificeringsmyndigheder, jf. artikel 59 i forordning (EU) 2019/881. Med peervurderinger bør det sikres, at certificeringsorganerne arbejder på en harmoniseret måde og producerer attester af samme kvalitet, og de bør identificere enhver potentiel styrke eller svaghed i certificeringsorganernes præstationer, også med henblik på at udveksle bedste praksis. Eftersom der er forskellige typer certificeringsorganer, bør forskellige typer peervurderinger tillades. I mere komplekse tilfælde, f.eks. ved certificeringsorganer, der udsteder attester på forskellige AVA_VAN-niveauer, kan der anvendes forskellige typer peervurderinger, forudsat at alle krav er opfyldt.

(31) Den Europæiske Cybersikkerhedscertificeringsgruppe bør spille en vigtig rolle i forbindelse med vedligeholdelse af ordningen. Ordningen bør bl.a. gennemføres i samarbejde med den private sektor, oprettelse af specialiserede undergrupper og relevant forberedende arbejde og bistand, som Kommissionen anmoder om. Den Europæiske Cybersikkerhedscertificeringsgruppe spiller en vigtig rolle i godkendelsen af statusdokumenter. Ved godkendelse og vedtagelse af statusdokumenter bør der tages behørigt hensyn til de elementer, der er omhandlet i artikel 54, stk. 1, litra c), i forordning (EU) 2019/881. Tekniske områder og statusdokumenter bør offentliggøres i bilag I til

nærværende forordning. Beskyttelsesprofiler, der er vedtaget som statusdokumenter, bør offentliggøres i bilag II. For at sikre, at disse bilag er dynamiske, kan Kommissionen ændre dem i overensstemmelse med proceduren i artikel 66, stk. 2, i forordning (EU) 2019/881 og under hensyntagen til udtalelsen fra Den Europæiske Cybersikkerhedscertificeringsgruppe. Bilag III indeholder anbefalede beskyttelsesprofiler, som på tidspunktet for nærværende forordnings ikrafttræden ikke er statusdokumenter. De bør offentliggøres på ENISA's websted, jf. artikel 50, stk. 1, i forordning (EU) 2019/881.

(32) Nærværende forordning bør finde anvendelse 12 måneder efter dens ikrafttræden. Kravene i kapitel IV og bilag V kræver ikke en overgangsperiode og bør derfor finde anvendelse fra nærværende forordnings ikrafttræden.

(33) Foranstaltningerne i nærværende forordning er i overensstemmelse med udtalelsen fra Det Europæiske Udvalg for Cybersikkerhed, der er nedsat ved artikel 66 i forordning (EU) 2019/881 —

VEDTAGET DENNE FORORDNING:

KAPITEL I

GENERELLE BESTEMMELSER

Artikel 1

Genstand og anvendelsesområde

I denne forordning fastsættes den europæiske ordning for cybersikkerhedscertificering baseret på fælles kriterier (EUCC).

Denne forordning finder anvendelse på alle informations- og kommunikationsteknologiprodukter (»IKT«), herunder deres dokumentation, som indgives med henblik på certificering i henhold til EUCC, og på alle beskyttelsesprofiler, som indgives med henblik på certificering som led i den IKT-proces, der fører til certificering af IKT-produkter.

Artikel 2

Definitioner

I denne forordning forstås ved:

1) »fælles kriterier«: de fælles kriterier for evaluering af informationsteknologisikkerhed som fastsat i ISO-standarden ISO/IEC 15408

2) »fælles evalueringsmetode«: den fælles metode til evaluering af informationsteknologisikkerhed som fastsat i ISO/IEC-standarden ISO/IEC 18045

3) »evalueringsmål«: et IKT-produkt eller en del heraf eller en beskyttelsesprofil som led i en IKT-proces, som underkastes en cybersikkerhedsevaluering med henblik på at opnå EUCC-certificering

4) »sikkerhedsmål«: en påstand om implementeringsafhængige sikkerhedskrav for et specifikt IKT-produkt

5) »beskyttelsesprofil«: en IKT-proces, der fastsætter sikkerhedskrav for en specifik kategori af IKT-produkter, imødekommer implementeringsuafhængige sikkerhedsbehov, og som kan anvendes til at vurdere IKT-produkter, der er omfattet af denne specifikke kategori, med henblik på certificering heraf

6) »rapport om teknisk evaluering«: et dokument udarbejdet af en ITSEF med henblik på at fremlægge de resultater, bedømmelser og begrundelser, der er fremkommet under evalueringen af et IKT-produkt eller en beskyttelsesprofil i overensstemmelse med de regler og forpligtelser, der er fastsat i denne forordning

7) »ITSEF«: en facilitet til evaluering af informationsteknologisk sikkerhed, som er et overensstemmelsesvurderingsorgan som defineret i artikel 2, nr. 13), i forordning (EF) nr. 765/2008, der udfører evalueringsopgaver

8) »AVA_VAN-niveau«: et tillids- og sårbarhedsanalyseniveau, der angiver graden af cybersikkerhedsevalueringsaktiviteter, der er udført for at bestemme graden af modstandsdygtighed over for potentiel udnyttelse af fejl eller svagheder i evalueringsmålet i det operationelle miljø som fastsat i de fælles kriterier

9) »EUCC-attest«: en cybersikkerhedsattest udstedt i henhold til EUCC for IKT-produkter eller for beskyttelsesprofiler, der udelukkende kan anvendes i IKT-certificeringsprocessen for IKT-produkter

10) »sammensat produkt«: et IKT-produkt, der evalueres sammen med et andet underliggende IKT-produkt, som allerede har modtaget en EUCC-attest, og hvis sikkerhedsfunktion det sammensatte IKT-produkt afhænger af

11) »national cybersikkerhedscertificeringsmyndighed«: en myndighed, der er udpeget af en medlemsstat i henhold til artikel 58, stk. 1, i forordning (EU) 2019/881

12) »certificeringsorgan«: et overensstemmelsesvurderingsorgan som defineret i artikel 2, nr. 13), i forordning (EF) nr. 765/2008, som udfører certificeringsaktiviteter

13) »teknisk område«: en fælles teknisk ramme vedrørende en bestemt teknologi for harmoniseret certificering med en række karakteristiske sikkerhedskrav

14) »statusdokument«: et dokument, der specificerer de evalueringsmetoder, -teknikker og -værktøjer, der gælder for certificering af IKT-produkter, eller sikkerhedskravene til en generisk IKT-produktkategori eller andre krav, der er nødvendige for certificering, med henblik på at harmonisere evalueringen, navnlig af tekniske områder eller beskyttelsesprofiler

15) »markedsovervågningsmyndighed«: en myndighed som defineret i artikel 3, nr. 4), i forordning (EU) 2019/1020.

Artikel 3

Evalueringsstandarder

Følgende standarder finder anvendelse på evalueringer, der foretages under EUCC-ordningen:

a) de fælles kriterier

b) den fælles evalueringsmetode.

Artikel 4

Tillidsniveauer

1. Certificeringsorganerne udsteder EUCC-attester på tillidsniveauet »væsentligt« eller »højt«.

2. EUCC-attester på tillidsniveauet »væsentligt« skal svare til attester, der dækker AVA_VAN-niveau 1 eller 2.

3. EUCC-attester på tillidsniveauet »højt« skal svare til attester, der dækker AVA_VAN-niveau 3, 4 eller 5.

4. Det sikkerhedsniveau, der bekræftes i en EUCC-attest, skal skelne mellem overensstemmende og udvidet anvendelse af sikkerhedskomponenterne som angivet i de fælles kriterier i overensstemmelse med bilag VIII.

5. Overensstemmelsesvurderingsorganerne anvender de tillidskomponenter, som det valgte AVA_VAN-niveau afhænger af, i overensstemmelse med de standarder, der er omhandlet i artikel 3.

Artikel 5

Metoder til certificering af IKT-produkter

1. Certificering af et IKT-produkt foretages i forhold til dets sikkerhedsmål:

a) som defineret af ansøgeren eller

b) ved at indarbejde en certificeret beskyttelsesprofil som en del af IKT-processen, hvor IKT-produktet falder ind under den IKT-produktkategori, der er omfattet af den pågældende beskyttelsesprofil.

2. Beskyttelsesprofiler certificeres udelukkende med henblik på certificering af IKT-produkter, der falder ind under den specifikke kategori af IKT-produkter, der er omfattet af beskyttelsesprofilen.

Artikel 6

Selvvurdering af overensstemmelse

Selvvurdering af overensstemmelse som omhandlet i artikel 53 i forordning (EU) 2019/881 er ikke tilladt.

KAPITEL II

CERTIFICERING AF IKT-PRODUKTER

AFDELING I

Specifikke standarder og krav til evaluering

Artikel 7

Evalueringskriterier og -metoder for IKT-produkter

1. Et IKT-produkt, som indgives med henblik på certificering, evalueres som minimum i overensstemmelse med følgende:

a) de relevante elementer i de standarder, der er omhandlet i artikel 3

b) sikkerhedskravene til sårbarhedsvurdering og uafhængig funktionstest som fastsat i de evalueringsstandarder, der er omhandlet i artikel 3

c) det risikoniveau, der er forbundet med den tilsigtede anvendelse af de pågældende IKT-produkter i henhold til artikel 52 i forordning (EU) 2019/881, og deres sikkerhedsfunktioner, der understøtter de sikkerhedsmål, der er fastsat i artikel 51 i forordning (EU) 2019/881

d) de i bilag I anførte relevante statusdokumenter og

e) de i bilag II anførte relevante certificerede beskyttelsesprofiler.

2. I ekstraordinære og behørigt begrundede tilfælde kan et overensstemmelsesvurderingsorgan anmode om at undlade at anvende det relevante statusdokument. I sådanne tilfælde underretter overensstemmelsesvurderingsorganet den nationale cybersikkerhedscertificeringsmyndighed med en behørigt begrundet begrundelse for sin anmodning. Den nationale cybersikkerhedscertificeringsmyndighed vurderer begrundelsen for en undtagelse og godkender den, hvis det er berettiget. Overensstemmelsesvurderingsorganet udsteder ingen attest, før den nationale cybersikkerhedscertificerin-

gsmyndighed har truffet afgørelse. Den nationale cybersikkerhedscertificeringsmyndighed underretter uden unødigt ophold Den Europæiske Cybersikkerhedscertificeringsgruppe, som kan afgive en udtalelse, om den godkendte undtagelse. Den nationale cybersikkerhedscertificeringsmyndighed tager størst muligt hensyn til udtalelsen fra Den Europæiske Cybersikkerhedscertificeringsgruppe.

3. Certificering af IKT-produkter på AVA_VAN-niveau 4 eller 5 er kun mulig i følgende scenarier:

a) hvis IKT-produktet er omfattet af et af de tekniske områder, der er opført i bilag I, evalueres det i overensstemmelse med de gældende statusdokumenter på disse tekniske områder

b) hvis IKT-produktet hører under en IKT-produktkategori, der er omfattet af en certificeret beskyttelsesprofil, som omfatter AVA_VAN-niveau 4 eller 5, og som er opført som en avanceret beskyttelsesprofil i bilag II, evalueres det i overensstemmelse med den evalueringsmetode, der er angivet for den pågældende beskyttelsesprofil

c) hvis litra a) og b) i dette stykke ikke finder anvendelse, og det er usandsynligt, at et teknisk område i bilag I eller en certificeret beskyttelsesprofil i bilag II vil blive optaget i en overskuelig fremtid, og kun i ekstraordinære og behørigt begrundede tilfælde på de betingelser, der er fastsat i stk. 4.

4. Hvis et overensstemmelsesvurderingsorgan vurderer, at det befinder sig i en ekstraordinær og behørigt begrundet situation som omhandlet i stk. 3, litra c), underretter det den nationale cybersikkerhedscertificeringsmyndighed om den påtænkte certificering med en begrundelse og en foreslået evalueringsmetode. Den nationale cybersikkerhedscertificeringsmyndighed vurderer begrundelsen for, at der skulle være tale om en undtagelse, og godkender eller ændrer den evalueringsmetode, som overensstemmelsesvurderingsorganet skal anvende, hvis det er berettiget. Overensstemmelsesvurderingsorganet udsteder ingen attest, før den nationale cybersikkerhedscertificeringsmyndighed har truffet afgørelse. Den nationale cybersikkerhedscertificeringsmyndighed indberetter uden unødigt ophold den planlagte certificering til Den Europæiske Cybersikkerhedscertificeringsgruppe, som kan afgive en udtalelse. Den nationale cybersikkerhedscertificeringsmyndighed tager størst muligt hensyn til udtalelsen fra Den Europæiske Cybersikkerhedscertificeringsgruppe.

5. Hvis et IKT-produkt underkastes en evaluering af et sammensat produkt i overensstemmelse med de relevante statusdokumenter, skal den ITSEF, der foretog evalueringen af det underliggende IKT-produkt, dele de relevante oplysninger med den facilitet, der foretager evalueringen af det sammensatte IKT-produkt.

AFDELING II

Udstedelse, fornyelse og tilbagekaldelse af eucc-attester

Artikel 8

Nødvendige oplysninger ved certificering

1. En ansøger, der ansøger om certificering i henhold til EUCC, skal forelægge eller på anden måde stille alle de oplysninger, der er nødvendige for certificeringsaktiviteterne, til rådighed for certificeringsorganet og ITSEF.

2. De oplysninger, der er omhandlet i stk. 1, omfatter al relevant dokumentation i overensstemmelse med afsnittene om »Developer action elements« (aktionselementer for udviklere) i det relevante format som fastsat i afsnittene om »Content and presentation of evidence element« (indhold og fremlæggelse af dokumentationselement) i de fælles kriterier og den fælles evalueringsmetode for det valgte sikkerhedstillidsniveau og de tilhørende sikkerhedstillidskrav. Dokumentationen skal om nødvendigt omfatte oplysninger om IKT-produktet og dets kildekode i overensstemmelse med denne forordning med forbehold af sikkerhedsforanstaltninger mod uautoriseret videregivelse.

3. Ansøgere om certificering kan forelægge certificeringsorganet og ITSEF relevante evalueringsresultater fra forudgående certificering i henhold til:

a) denne forordning

b) en anden europæisk cybersikkerhedscertificeringsordning vedtaget i henhold til artikel 49 i forordning (EU) 2019/881

c) en national ordning som omhandlet i nærværende forordnings artikel 49.

4. Hvis evalueringsresultaterne er relevante for ITSEF's opgaver, kan den genanvende evalueringsresultaterne, forudsat at resultaterne er i overensstemmelse med de gældende krav, og at deres ægthed bekræftes.

5. Hvis certificeringsorganet tillader, at produktet underkastes certificering af et sammensat produkt, skal ansøgeren om certificering stille alle nødvendige elementer til rådighed for certificeringsorganet og ITSEF'en, hvis det er relevant, i overensstemmelse med statusdokumentet.

6. Ansøgere om certificering skal også give certificeringsorganet og ITSEF'en følgende oplysninger:

a) linket til deres websted, som indeholder de supplerende cybersikkerhedsoplysninger, der er omhandlet i artikel 55 i forordning (EU) 2019/881

b) en beskrivelse af ansøgerens procedurer for sårbarhedsstyring og offentliggørelse af sårbarheder.

7. Al relevant dokumentation, som er omhandlet i denne artikel, skal opbevares af certificeringsorganet, ITSEF'en og ansøgeren i en periode på fem år efter attestens udløb.

Artikel 9

Betingelser for udstedelse af en EUCC-attest

1. Certificeringsorganerne udsteder en EUCC-attest, hvis alle følgende betingelser er opfyldt:

a) kategorien af IKT-produkter er omfattet af akkrediteringens anvendelsesområde og, hvor det er relevant, bemyndigelsen af det certificeringsorgan og den ITSEF, der er involveret i certificeringen

b) ansøgeren om en certificering har underskrevet en erklæring, hvori denne påtager sig alle de forpligtelser, der er anført i stk. 2

c) ITSEF'en har afsluttet evalueringen uden indsigelse i overensstemmelse med de evalueringsstandarder, -kriterier og -metoder, der er omhandlet i artikel 3 og 7

d) certificeringsorganet har afsluttet gennemgangen af evalueringsresultaterne uden indsigelser

e) certificeringsorganet har kontrolleret, at ITSEF'ens tekniske evalueringsrapporter er i overensstemmelse med den fremlagte dokumentation, og at de evalueringsstandarder, -kriterier og -metoder, der er omhandlet i artikel 3 og 7, er anvendt korrekt.

2. Ansøgere om en certificering skal påtage sig følgende forpligtelser:

a) at give certificeringsorganet og ITSEF'en alle de nødvendige fuldstændige og korrekte oplysninger og give yderligere nødvendige oplysninger, hvis der anmodes herom

b) at undlade at markedsføre IKT-produktet som certificeret i henhold til EUCC, før EUCC-attesten er udstedt

c) udelukkende at markedsføre IKT-produktet som certificeret med hensyn til det anvendelsesområde, der er fastsat i EUCC-attesten

d) straks at ophøre med at markedsføre IKT-produktet som certificeret i tilfælde af suspension, tilbagekaldelse eller udløb af EUCC-attesten

e) at sikre, at de IKT-produkter, der sælges med henvisning til EUCC-attesten, er fuldstændig identiske med det IKT-produkt, der er omfattet af certificeringen

f) at overholde reglerne for anvendelse af mærkningen og etiketten, der er fastsat for EUCC-attesten i overensstemmelse med artikel 11.

3. I tilfælde af, at et IKT-produkt er omfattet af en certificering af et sammensat produkt i overensstemmelse med de relevante statusdokumenter, deler det certificeringsorgan, der har foretaget certificeringen af det underliggende IKT-produkt, de relevante oplysninger med det certificeringsorgan, der udfører certificeringen af det sammensatte IKT-produkt.

Artikel 10

EUCC-attestens indhold og format

1. En EUCC-attest skal mindst indeholde de oplysninger, der er fastsat i bilag VII.

2. Omfanget af og grænserne for det certificerede IKT-produkt angives utvetydigt i EUCC-attesten eller certificeringsrapporten med angivelse af, om hele IKT-produktet er blevet certificeret eller kun dele heraf.

3. Certificeringsorganet fremsender EUCC-attesten til ansøgeren i det mindste i elektronisk form.

4. Certificeringsorganet udarbejder en certificeringsrapport i overensstemmelse med bilag V for hver EUCC-attest, det udsteder. Certificeringsrapporten baseres på den rapport om teknisk evaluering, der er udarbejdet af ITSEF. I rapporten om teknisk evaluering og certificeringsrapporten angives de specifikke evalueringskriterier og -metoder, der er omhandlet i artikel 7, og som er anvendt til evalueringen.

5. Certificeringsorganet fremsender alle EUCC-attester og alle certificeringsrapporter til den nationale cybersikkerheds-certificeringsmyndighed og ENISA i elektronisk form.

Artikel 11

Mærkning og etiketter

1. En attestindehaver kan anbringe en mærkning og en etiket på et certificeret IKT-produkt. Mærkningen og etiketten viser, at IKT-produktet er certificeret i overensstemmelse med denne forordning. Mærkningen og etiketten anbringes i overensstemmelse med denne artikel og bilag IX.

2. Mærkningen og etiketten skal anbringes synligt, letlæseligt og uudsletteligt på det certificerede IKT-produkt eller dets dataskilt. Hvis produktet er af en sådan art, at dette ikke er muligt eller berettiget, skal mærkningen og etiketten anbringes på emballagen og i følgedokumenterne. Hvis det certificerede IKT-produkt leveres i form af software, skal mærkningen og etiketten fremgå tydeligt, letlæseligt og uudsletteligt i den ledsagende dokumentation, eller denne dokumentation skal gøres let og direkte tilgængelig for brugerne via et websted.

3. Mærkningen og etiketten skal være i overensstemmelse med bilag IX og indeholde:

a) tillidsniveauet og AVA_VAN-niveauet for det certificerede IKT-produkt

b) den entydige identifikation af attesten bestående af:

   1) ordningens navn

   2) navnet og referencenummeret på akkrediteringen af det certificeringsorgan, der har udstedt attesten

   3) udstedelsesår og -måned

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

4. Mærkningen og etiketten skal ledsages af en QR-kode med et link til et websted, der som minimum indeholder:

a) oplysninger om attestens gyldighedsperiode

b) de nødvendige certificeringsoplysninger, jf. bilag V og VII

c) de oplysninger, som attestindehaveren skal gøre offentligt tilgængelige i henhold til artikel 55 i forordning (EU) 2019/881, og

d) hvis det er relevant, historiske oplysninger vedrørende den specifikke certificering eller de specifikke certificeringer af IKT-produktet for at muliggøre sporbarhed.

Artikel 12

EUCC-attestens gyldighedsperiode

1. Certificeringsorganet fastsætter en gyldighedsperiode for hver EUCC-attest, der udstedes, under hensyntagen til det certificerede IKT-produkts karakteristika.

2. EUCC-attestens gyldighedsperiode må ikke overstige fem år.

3. Uanset stk. 2 må denne periode overstige fem år med forbehold af forudgående godkendelse fra den nationale cybersikkerhedscertificeringsmyndighed. Den nationale cybersikkerhedscertificeringsmyndighed underretter uden unødigt ophold Den Europæiske Cybersikkerhedscertificeringsgruppe om den meddelte godkendelse.

Artikel 13

Revision af en EUCC-attest

1. Efter anmodning fra attestindehaveren eller af andre begrundede årsager kan certificeringsorganet beslutte at revidere EUCC-attesten for et IKT-produkt. 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 det certificerede IKT-produkt.

2. Efter resultaterne af revisionen og, hvor det er relevant, af den fornyede evaluering skal certificeringsorganet:

a) bekræfte EUCC-attesten

b) tilbagekalde EUCC-attesten i henhold til artikel 14

c) tilbagekalde EUCC-attesten i henhold til artikel 14 og udstede en ny EUCC-attest med samme anvendelsesområde og en forlænget gyldighedsperiode eller

d) tilbagekalde EUCC-attesten i henhold til artikel 14 og udstede en ny EUCC-attest med et andet anvendelsesområde.

3. Certificeringsorganet kan uden unødigt ophold beslutte at suspendere EUCC-attesten i henhold til artikel 30, indtil indehaveren af EUCC-attesten har truffet afhjælpende foranstaltninger.

Artikel 14

Tilbagekaldelse af en EUCC-attest

1. Med forbehold af artikel 58, stk. 8, litra e), i forordning (EU) 2019/881 tilbagekaldes en EUCC-attest af det certificeringsorgan, der udstedte attesten.

2. Certificeringsorganet i stk. 1 underretter den nationale cybersikkerhedscertificeringsmyndighed om tilbagekaldelsen af attesten. Det underretter også ENISA om tilbagekaldelsen med henblik på at lette udførelsen af dets opgaver i henhold til artikel 50 i forordning (EU) 2019/881. Den nationale cybersikkerhedscertificeringsmyndighed underretter andre relevante markedsovervågningsmyndigheder.

3. Indehaveren af en EUCC-attest kan anmode om tilbagekaldelse af attesten.

KAPITEL III

CERTIFICERING AF BESKYTTELSESPROFILER

AFDELING I

SPECIFIKKE STANDARDER OG KRAV TIL EVALUERING

Artikel 15

Evalueringskriterier og -metoder

1. En beskyttelsesprofil vurderes som minimum i overensstemmelse med følgende:

a) de relevante elementer i de standarder, der er omhandlet i artikel 3

b) det risikoniveau, der er forbundet med den tilsigtede anvendelse af de pågældende IKT-produkter i henhold til artikel 52 i forordning (EU) 2019/881, og de sikkerhedsfunktioner, der understøtter de sikkerhedsmål, som er fastsat i nævnte forordnings artikel 51, og

c) de relevante statusdokumenter, som er anført i bilag I. En beskyttelsesprofil, der er omfattet af et teknisk område, skal certificeres efter kravene på det pågældende tekniske område.

2. I ekstraordinære og behørigt begrundede tilfælde kan et overensstemmelsesvurderingsorgan certificere en beskyttelsesprofil uden at anvende de relevante statusdokumenter. I sådanne tilfælde underretter det den kompetente nationale cybersikkerhedscertificeringsmyndighed og giver en begrundelse for den påtænkte certificering uden anvendelse af de relevante statusdokumenter samt den foreslåede evalueringsmetode. Den nationale cybersikkerhedscertificeringsmyndighed vurderer begrundelsen og godkender, hvor det er berettiget, den manglende anvendelse af de relevante statusdokumenter og godkender eller ændrer, hvor det er relevant, den evalueringsmetode, som overensstemmelsesvurderingsorganet skal anvende. Overensstemmelsesvurderingsorganet udsteder ingen attest til beskyttelsesprofilen, før den nationale cybersikkerhedscertificeringsmyndighed har truffet afgørelse. Den nationale cybersikkerhedscertificeringsmyndighed underretter uden unødigt ophold Den Europæiske Cybersikkerhedscertificeringsgruppe, som kan afgive en udtalelse, om den tilladte manglende anvendelse af de relevante statusdokumenter. Den nationale cybersikkerhedscertificeringsmyndighed tager størst muligt hensyn til udtalelsen fra Den Europæiske Cybersikkerhedscertificeringsgruppe.

AFDELING II

Udstedelse, fornyelse og tilbagekaldelse af eucc-attester for beskyttelsesprofiler

Artikel 16

Oplysninger, der er nødvendige for certificering af beskyttelsesprofiler

En ansøger, der ansøger om certificering af en beskyttelsesprofil, skal forelægge eller på anden måde stille alle de oplysninger, der er nødvendige for certificeringsaktiviteterne, til rådighed for certificeringsorganet og ITSEF'en. Artikel 8, stk. 2, 3, 4 og 7 finder tilsvarende anvendelse.

Artikel 17

Udstedelse af EUCC-attester for beskyttelsesprofiler

1. Ansøgere om en certificering skal give certificeringsorganet og ITSEF'en alle de nødvendige fuldstændige og korrekte oplysninger.

2. Artikel 9 og 10 finder tilsvarende anvendelse.

3. ITSEF'en vurderer, om en beskyttelsesprofil er fuldstændig, konsekvent, teknisk forsvarlig og effektiv i forhold til den tilsigtede brug og sikkerhedsmålene for den kategori af IKT-produkter, der er omfattet af beskyttelsesprofilen.

4. En beskyttelsesprofil certificeres udelukkende af:

a) en national cybersikkerhedscertificeringsmyndighed eller et andet offentligt organ, der er akkrediteret som certificeringsorgan, eller

b) et certificeringsorgan efter forudgående godkendelse fra den nationale cybersikkerhedscertificeringsmyndighed for hver enkelt beskyttelsesprofil.

Artikel 18

Gyldighedsperiode for en EUCC-attest for beskyttelsesprofiler

1. Certificeringsorganet fastsætter en gyldighedsperiode for hver EUCC-attest.

2. Gyldighedsperioden kan være op til beskyttelsesprofilens levetid.

Artikel 19

Revision af en EUCC-attest for beskyttelsesprofiler

1. Efter anmodning fra attestindehaveren eller af andre begrundede årsager kan certificeringsorganet beslutte at revidere EUCC-attesten for en beskyttelsesprofil. Revisionen foretages under anvendelse af betingelserne i artikel 15. 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.

2. Efter resultaterne af revisionen og, hvor det er relevant, af den fornyede evaluering skal certificeringsorganet:

a) bekræfte EUCC-attesten

b) tilbagekalde EUCC-attesten i henhold til artikel 20

c) tilbagekalde EUCC-attesten i henhold til artikel 20 og udstede en ny EUCC-attest med samme anvendelsesområde og en forlænget gyldighedsperiode

d) tilbagekalde EUCC-attesten i henhold til artikel 20 og udstede en ny EUCC-attest med et andet anvendelsesområde.

Artikel 20

Tilbagekaldelse af en EUCC-attest for beskyttelsesprofiler

1. Med forbehold af artikel 58, stk. 8, litra e), i forordning (EU) 2019/881 tilbagekaldes en EUCC-attest til en beskyttelsesprofil af det certificeringsorgan, der udstedte attesten. Artikel 14 finder tilsvarende anvendelse.

2. En attest for en beskyttelsesprofil, der er udstedt i overensstemmelse med artikel 17, stk. 4, litra b), trækkes tilbage af den nationale cybersikkerhedscertificeringsmyndighed, der godkendte attesten.

KAPITEL IV

OVERENSSTEMMELSESVURDERINGSORGANER

Artikel 21

Yderligere eller specifikke krav til et certificeringsorgan

1. Et certificeringsorgan bemyndiges af den nationale cybersikkerhedscertificeringsmyndighed til at udstede EUCC-attester på tillidsniveauet »højt«, hvis dette organ ud over at opfylde kravene i artikel 60, stk. 1, og bilaget til forordning (EU) 2019/881 vedrørende akkreditering af overensstemmelsesvurderingsorganer dokumenterer følgende:

a) det har den ekspertise og de kompetencer, der er nødvendige for afgørelsen om certificering på tillidsniveauet »højt«

b) det udfører sine certificeringsaktiviteter i samarbejde med et organ, der er bemyndiget i henhold til artikel 22 og

c) det har de nødvendige kompetencer og træffer passende tekniske og operationelle foranstaltninger for effektivt at beskytte fortrolige og følsomme oplysninger med sikringsniveauet »høj« ud over de krav, der er fastsat i artikel 43.

2. Den nationale cybersikkerhedscertificeringsmyndighed vurderer, om et certificeringsorgan opfylder alle kravene i stk. 1. Denne vurdering skal som minimum omfatte strukturerede interviews og en gennemgang af mindst én pilotcertificering udført af certificeringsorganet i overensstemmelse med denne forordning.

Den nationale cybersikkerhedscertificeringsmyndighed kan i sin vurdering genanvende relevant dokumentation fra forudgående bemyndigelse eller lignende aktiviteter, der er fremlagt i henhold til:

a) denne forordning

b) en anden europæisk cybersikkerhedscertificeringsordning vedtaget i henhold til artikel 49 i forordning (EU) 2019/881

c) en national ordning som omhandlet i nærværende forordnings artikel 49.

3. Den nationale cybersikkerhedscertificeringsmyndighed udarbejder en bemyndigelsesrapport, som er genstand for peerevaluering i overensstemmelse med artikel 59, stk. 3, litra d), i forordning (EU) 2019/881.

4. Den nationale cybersikkerhedscertificeringsmyndighed angiver de IKT-produktkategorier og beskyttelsesprofiler, som bemyndigelsen omfatter. Bemyndigelsen er gyldig i en periode, der ikke er længere end akkrediteringens gyldighedsperiode. Den kan forlænges efter anmodning, forudsat at certificeringsorganet stadig opfylder kravene i denne artikel. Der kræves ingen pilotevalueringer i forbindelse med bemyndigelsens fornyelse.

5. Den nationale cybersikkerhedscertificeringsmyndighed tilbagekalder certificeringsorganets bemyndigelse, hvis det ikke længere opfylder betingelserne i denne artikel. Når bemyndigelsen tilbagekaldes, ophører certificeringsorganet straks med at markedsføre sig som et bemyndiget certificeringsorgan.

Artikel 22

Yderligere eller specifikke krav til en ITSEF

1. En ITSEF bemyndiges af den nationale cybersikkerhedscertificeringsmyndighed til at udføre evaluering af IKT-produkter, der er genstand for certificering på tillidsniveauet »højt«, hvis den pågældende ITSEF ud over at opfylde kravene i artikel 60, stk. 1, og bilaget til forordning (EU) 2019/881 vedrørende akkreditering af overensstemmelsesvurderingsorganer dokumenterer, at den overholder alle følgende betingelser:

a) den har den nødvendige ekspertise til at udføre evalueringsaktiviteterne med henblik på at fastslå modstandsdygtigheden over for de mest avancerede cyberangreb, der udføres af aktører med betydelige færdigheder og ressourcer

b) for så vidt angår de tekniske områder og beskyttelsesprofiler, som er en del af IKT-processen for disse IKT-produkter, har den:

1) ekspertisen til at udføre de specifikke evalueringsaktiviteter, der er nødvendige for metodisk at fastlægge et mål for evalueringens resistens over for kvalificerede angribere i det operationelle miljø, idet det antages, at angrebspotentialet er »moderat« eller »højt« som fastsat i de standarder, der er omhandlet i artikel 3

2) de tekniske kompetencer, der fremgår af de statusdokumenter, der er anført i bilag I

c) den har de nødvendige kompetencer og har truffet passende tekniske og operationelle foranstaltninger til effektivt at beskytte fortrolige og følsomme oplysninger med tillidsniveauet »højt« ud over de krav, der er fastsat i artikel 43.

2. Den nationale cybersikkerhedscertificeringsmyndighed vurderer, om en ITSEF opfylder alle kravene i stk. 1. Denne vurdering skal som minimum omfatte strukturerede interviews og en gennemgang af mindst én pilotevaluering udført af udvalget i overensstemmelse med denne forordning.

3. Den nationale cybersikkerhedscertificeringsmyndighed kan i sin vurdering genanvende relevant dokumentation fra forudgående bemyndigelse eller lignende aktiviteter, der er fremlagt i henhold til:

a) denne forordning

b) en anden europæisk cybersikkerhedscertificeringsordning vedtaget i henhold til artikel 49 i forordning (EU) 2019/881

c) en national ordning som omhandlet i nærværende forordnings artikel 49.

4. Den nationale cybersikkerhedscertificeringsmyndighed udarbejder en bemyndigelsesrapport, som er genstand for peerevaluering i overensstemmelse med artikel 59, stk. 3, litra d), i forordning (EU) 2019/881.

5. Den nationale cybersikkerhedscertificeringsmyndighed angiver de IKT-produktkategorier og beskyttelsesprofiler, som bemyndigelsen omfatter. Bemyndigelsen er gyldig i en periode, der ikke er længere end akkrediteringens gyldighedsperiode. Den kan forlænges efter anmodning, forudsat at den pågældende ITSEF stadig opfylder kravene i denne artikel. Der kræves ingen pilotevalueringer i forbindelse med bemyndigelsens fornyelse.

6. Den nationale cybersikkerhedscertificeringsmyndighed tilbagekalder en ITSEF's bemyndigelse, hvis den ikke længere opfylder betingelserne i denne artikel. Når bemyndigelsen tilbagekaldes, ophører ITSEF'en med at promovere sig som en bemyndiget ITSEF.

Artikel 23

Anmeldelse af certificeringsorganer

1. Den nationale cybersikkerhedscertificeringsmyndighed underretter Kommissionen om, hvilke certificeringsorganer på dens område der er kompetente til at certificere på tillidsniveauet »væsentligt« på grundlag af deres akkreditering.

2. Den nationale cybersikkerhedscertificeringsmyndighed underretter Kommissionen om, hvilke certificeringsorganer på dens område der er kompetente til at certificere på tillidsniveauet »højt« på grundlag af deres akkreditering og afgørelsen om bemyndigelse.

3. Den nationale cybersikkerhedscertificeringsmyndighed skal som minimum give følgende oplysninger, når den underretter Kommissionen om certificeringsorganerne:

a) det eller de tillidsniveauer, som certificeringsorganet har kompetence til at udstede EUCC-attester for

b) følgende oplysninger vedrørende akkreditering:

1) akkrediteringsdatoen

2) certificeringsorganets navn og adresse

3) certificeringsorganets registrerede hjemland

4) akkrediteringens referencenummer

5) akkrediteringens anvendelsesområde og gyldighedsperiode

6) adresse, beliggenhed og link til det nationale akkrediteringsorgans relevante websted og

c) følgende oplysninger vedrørende bemyndigelse for niveauet »høj«:

1) bemyndigelsesdatoen

2) bemyndigelsens referencenummer

3) bemyndigelsens gyldighedsperiode

4) bemyndigelsens anvendelsesområde, herunder det højeste AVA_VAN-niveau og det omfattede tekniske område, hvor det er relevant.

4. Den nationale cybersikkerhedscertificeringsmyndighed sender en kopi af den underretning, der er omhandlet i stk. 1 og 2, til ENISA med henblik på offentliggørelse af nøjagtige oplysninger på webstedet for cybersikkerhedscertificering om certificeringsorganernes bemyndigelse.

5. Den nationale cybersikkerhedscertificeringsmyndighed undersøger uden unødigt ophold alle oplysninger fra det nationale akkrediteringsorgan om ændring af status for akkrediteringen. Hvis akkrediteringen eller bemyndigelsen er blevet tilbagekaldt, underretter den nationale cybersikkerhedscertificeringsmyndighed Kommissionen herom og kan indgive en anmodning til Kommissionen i overensstemmelse med artikel 61, stk. 4, i forordning (EU) 2019/881.

Artikel 24

Anmeldelse af en ITSEF

De nationale cybersikkerhedscertificeringsmyndigheders anmeldelsesforpligtelser, jf. artikel 23, finder også anvendelse på ITSEF. Meddelelsen skal indeholde adressen på den pågældende enhed, den gyldige akkreditering og, hvor det er relevant, den pågældende ITSEF's gyldige bemyndigelse.

KAPITEL V

OVERVÅGNING, MANGLENDE OVERENSSTEMMELSE OG MANGLENDE OVERHOLDELSE

AFDELING I

Overvågning af overholdelse

Artikel 25

Den nationale cybersikkerhedscertificeringsmyndigheds overvågningsaktiviteter

1. Med forbehold af artikel 58, stk. 7, i forordning (EU) 2019/881 overvåger den nationale cybersikkerhedscertificeringsmyndighed:

a) at certificeringsorganet og ITSEF'en overholder deres forpligtelser i henhold til nærværende forordning og forordning (EU) 2019/881

b) at EUCC-attestindehavere overholder deres forpligtelser i henhold til nærværende forordning og forordning (EU) 2019/881

c) at de certificerede IKT-produkter overholder de krav, der er fastsat i EUCC-attesten

d) at det tillidsniveau, der er anført i EUCC-attesten, overholder kravene i overensstemmelse med det skiftende trusselsbillede.

2. Den nationale cybersikkerhedscertificeringsmyndighed udfører sine overvågningsaktiviteter på grundlag af især:

a) oplysninger fra certificeringsorganer, nationale akkrediteringsorganer og relevante markedsovervågningsmyndigheder

b) oplysninger fra dens egne eller en anden myndigheds revisioner og undersøgelser

c) stikprøvekontrol gennemført i overensstemmelse med stk. 3

d) indkomne klager.

3. Den nationale cybersikkerhedscertificeringsmyndighed udtager i samarbejde med andre markedsovervågningsmyndigheder årligt prøver af mindst 4 % af EUCC-attesterne som fastsat ved en risikovurdering. Efter anmodning og på vegne af den kompetente nationale cybersikkerhedscertificeringsmyndighed bistår certificeringsorganerne og om nødvendigt ITSEF den pågældende myndighed med at overvåge overholdelsen.

4. Den nationale cybersikkerhedscertificeringsmyndighed udvælger stikprøven af certificerede IKT-produkter, der skal kontrolleres ved hjælp af objektive kriterier, herunder:

a) produktkategori

b) produkternes tillidsniveauer

c) attestindehaver

d) certificeringsorgan og, hvis det er relevant, den relevante ITSEF

e) alle andre oplysninger, som myndigheden har fået kendskab til.

5. Den nationale cybersikkerhedscertificeringsmyndighed underretter indehaverne af EUCC-attesten om de udvalgte IKT-produkter og udvælgelseskriterierne.

6. Det certificeringsorgan, der har certificeret det IKT-produkt, der er udtaget prøver af, foretager efter anmodning fra den nationale cybersikkerhedscertificeringsmyndighed og med bistand fra den pågældende ITSEF yderligere gennemgang i overensstemmelse med proceduren i afsnit IV.2 i bilag IV og underretter den nationale cybersikkerhedscertificeringsmyndighed om resultaterne.

7. Hvis den nationale cybersikkerhedscertificeringsmyndighed har tilstrækkelig grund til at tro, at et certificeret IKT-produkt ikke længere er i overensstemmelse med denne forordning eller forordning (EU) 2019/881, kan den foretage undersøgelser eller gøre brug af andre overvågningsbeføjelser, der er fastsat i artikel 58, stk. 8, i forordning (EU) 2019/881.

8. Den nationale cybersikkerhedscertificeringsmyndighed underretter certificeringsorganet og ITSEF'en om igangværende undersøgelser vedrørende udvalgte IKT-produkter.

9. Hvis den nationale cybersikkerhedscertificeringsmyndighed konstaterer, at en igangværende undersøgelse vedrører IKT-produkter, der er certificeret af certificeringsorganer, som er etableret i andre medlemsstater, underretter den de nationale cybersikkerhedscertificeringsmyndigheder i de relevante medlemsstater herom med henblik på at samarbejde om undersøgelserne, hvor det er relevant. Den nationale cybersikkerhedscertificeringsmyndighed underretter Den Europæiske Cybersikkerhedscertificeringsgruppe om de grænseoverskridende undersøgelser og de efterfølgende resultater.

Artikel 26

Certificeringsorganets overvågningsaktiviteter

1. Certificeringsorganet overvåger:

a) at attestindehavere overholder deres forpligtelser i henhold til nærværende forordning og forordning (EU) 2019/881 i forhold til den EUCC-attest, der er udstedt af certificeringsorganet

b) at de IKT-produkter, som det har certificeret, overholder deres respektive sikkerhedskrav

c) at det tillidsniveau, der er anført i de certificerede beskyttelsesprofiler, overholdes.

2. Certificeringsorganet udfører sine overvågningsaktiviteter på grundlag af:

a) de oplysninger, der er givet på grundlag af de forpligtelser, som ansøgeren om certificering har påtaget sig, jf. artikel 9, stk. 2

b) oplysninger, der følger af andre relevante markedsovervågningsmyndigheders aktiviteter

c) indkomne klager

d) sårbarhedsoplysninger, der kan påvirke de IKT-produkter, det har certificeret.

3. Den nationale cybersikkerhedscertificeringsmyndighed kan udarbejde regler for en regelmæssig dialog mellem certificeringsorganer og EUCC-attestindehavere for at kontrollere og rapportere om overholdelsen af de forpligtelser, der er indgået i henhold til artikel 9, stk. 2, uden at dette berører aktiviteter vedrørende andre relevante markedsovervågningsmyndigheder.

Artikel 27

Overvågningsaktiviteter udført af attestindehaveren

1. EUCC-attestindehavere udfører følgende opgaver med henblik på at overvåge, at certificerede IKT-produkt er i overensstemmelse med dets sikkerhedskrav:

a) overvåge sårbarhedsoplysninger vedrørende det certificerede IKT-produkt, herunder kendt afhængighed, med egne midler, men også under hensyntagen til:

   1) en offentliggørelse eller et indlæg vedrørende sårbarhedsoplysninger fra en bruger eller sikkerhedsforsker som omhandlet i artikel 55, stk. 1, litra c), i forordning (EU) 2019/881

   2) oplysninger fra enhver anden kilde

b) overvåge tillidsniveauet som anført i EUCC-attesten.

2. Indehaveren af en EUCC-attest samarbejder med certificeringsorganet, ITSEF og, hvor det er relevant, den nationale cybersikkerhedscertificeringsmyndighed for at støtte deres overvågningsaktiviteter.

AFDELING II

Overensstemmelse og overholdelse

Artikel 28

Konsekvenser af et certificeret IKT-produkts eller en certificeret beskyttelsesprofils manglende overensstemmelse

1. Hvis et certificeret IKT-produkt eller en certificeret beskyttelsesprofil ikke er i overensstemmelse med kravene i nærværende forordning og forordning (EU) 2019/881, underretter certificeringsorganet indehaveren af EUCC-attesten om den konstaterede manglende overensstemmelse og anmoder om afhjælpende foranstaltninger.

2. Hvis et tilfælde af manglende overensstemmelse med bestemmelserne i nærværende forordning kan påvirke overholdelsen af anden relevant EU-lovgivning, som giver mulighed for at påvise formodningen om overensstemmelse med kravene i den pågældende retsakt ved hjælp af EUCC-attesten, underretter certificeringsorganet straks den nationale cybersikkerhedscertificeringsmyndighed herom. Den nationale cybersikkerhedscertificeringsmyndighed underretter straks den markedsovervågningsmyndighed, der er ansvarlig for en sådan anden relevant EU-lovgivning, om den konstaterede manglende overensstemmelse.

3. Efter modtagelsen af de oplysninger, der er omhandlet i stk. 1, foreslår EUCC-attestindehaveren inden for den frist, som certificeringsorganet har fastsat, og som ikke må overstige 30 dage, certificeringsorganet de afhjælpende foranstaltninger, som er nødvendige for at afhjælpe den manglende overensstemmelse.

4. Certificeringsorganet kan uden unødigt ophold suspendere EUCC-attesten i henhold til artikel 30 i nødsituationer, eller hvis EUCC-attestindehaveren ikke samarbejder behørigt med certificeringsorganet.

5. Certificeringsorganet foretager en gennemgang i henhold til artikel 13 og 19 og vurderer, om de afhjælpende foranstaltninger afhjælper den manglende overensstemmelse.

6. Hvis indehaveren af EUCC-attesten ikke foreslår passende afhjælpende foranstaltninger i den periode, der er omhandlet i stk. 3, suspenderes attesten i overensstemmelse med artikel 30 eller tilbagekaldes i overensstemmelse med artikel 14 eller 20.

7. Denne artikel finder ikke anvendelse på tilfælde af sårbarheder, der påvirker et certificeret IKT-produkt, som håndteres i overensstemmelse med kapitel VI.

Artikel 29

Konsekvenser af manglende overensstemmelse fra attestindehaverens side

1. Hvis certificeringsorganet finder, at:

a) EUCC-attestindehaveren eller ansøgeren om certificering ikke opfylder sine forpligtelser som fastsat i artikel 9, stk. 2, artikel 17, stk. 2, artikel 27 og 41 eller

b) EUCC-attestindehaveren ikke opfylder artikel 56, stk. 8, i forordning (EU) 2019/881 eller kapitel VI i nærværende forordning

fastsætter det en frist på højst 30 dage, inden for hvilken EUCC-attestindehaveren skal træffe afhjælpende foranstaltninger.

2. Hvis EUCC-attestindehaveren ikke foreslår passende afhjælpende foranstaltninger i den periode, der er omhandlet i stk. 1, suspenderes attesten i overensstemmelse med artikel 30 eller tilbagekaldes i overensstemmelse med artikel 14 og 20.

3. EUCC-attestindehaverens fortsatte eller tilbagevendende overtrædelse af de forpligtelser, der er omhandlet i stk. 1, udløser tilbagekaldelse af EUCC-attesten i overensstemmelse med artikel 14 eller 20.

4. Certificeringsorganet underretter den nationale cybersikkerhedscertificeringsmyndighed om de resultater, der er omhandlet i stk. 1. Hvis den manglende overensstemmelse påvirker overholdelsen af anden relevant EU-lovgivning, underretter den nationale cybersikkerhedscertificeringsmyndighed straks den markedsovervågningsmyndighed, der er ansvarlig for denne anden relevante EU-lovgivning, om det konstaterede tilfælde af manglende overensstemmelse.

Artikel 30

Suspension af EUCC-attesten

1. Hvis der i denne forordning henvises til suspension af en EUCC-attest, suspenderer certificeringsorganet den pågældende EUCC-attest i en periode, der er passende i forhold til de omstændigheder, der udløser suspensionen, og som ikke overstiger 42 dage. Suspensionsperioden begynder dagen efter den dag, hvor certificeringsorganet har truffet sin afgørelse. Suspensionen berører ikke attestens gyldighed.

2. Certificeringsorganet underretter uden unødigt ophold attestindehaveren og den nationale cybersikkerhedscertificeringsmyndighed om suspensionen og angiver årsagerne til suspensionen, de foranstaltninger, der anmodes om, og suspensionsperioden.

3. Attestindehavere underretter køberne af de pågældende IKT-produkter om suspensionen og om certificeringsorganets begrundelse for suspensionen, undtagen de dele af årsagerne, hvis deling ville udgøre en sikkerhedsrisiko, eller som indeholder følsomme oplysninger. Disse oplysninger skal også gøres offentligt tilgængelige af attestindehaveren.

4. Hvis anden relevant EU-lovgivning indeholder bestemmelser om en formodning om overensstemmelse på grundlag af attester, der er udstedt i henhold til bestemmelserne i denne forordning, underretter den nationale cybersikkerhedscertificeringsmyndighed den markedsovervågningsmyndighed, der er ansvarlig for den anden relevante EU-lovgivning, om suspensionen.

5. ENISA underrettes om suspensionen af en attest i overensstemmelse med artikel 42, stk. 3.

6. I behørigt begrundede tilfælde kan den nationale cybersikkerhedscertificeringsmyndighed give tilladelse til en forlængelse af perioden for suspension af en EUCC-attest. Den samlede suspensionsperiode må ikke overstige et år.

Artikel 31

Konsekvenser af overensstemmelsesvurderingsorganets manglende overensstemmelse

1. Hvis et certificeringsorgan eller en ITSEF ikke overholder sine forpligtelser, skal den nationale cybersikkerhedscertificeringsmyndighed uden unødigt ophold:

a) med støtte fra den berørte ITSEF identificere de potentielt berørte EUCC-attester

b) om nødvendigt anmode om, at evalueringsaktiviteter udføres på et eller flere IKT-produkter eller en eller flere beskyttelsesprofiler af enten den enhed, der har foretaget evalueringen, eller enhver anden akkrediteret og, hvor det er relevant, bemyndiget ITSEF, der kan være i en bedre teknisk position med hensyn til at støtte denne identifikation

c) analysere virkningerne af manglende overensstemmelse

d) underrette den EUCC-attestindehaver, der er berørt af den manglende overensstemmelse.

2. På grundlag af de foranstaltninger, der er omhandlet i stk. 1, vedtager certificeringsorganet en af følgende afgørelser for hver berørt EUCC-attest:

a) at opretholde EUCC-attesten uændret

b) at tilbagekalde EUCC-attesten i overensstemmelse med artikel 14 eller 20 og, hvor det er relevant, udstede en ny EUCC-attest.

3. På grundlag af de foranstaltninger, der er omhandlet i stk. 1, skal den nationale cybersikkerhedscertificeringsmyndighed:

a) om nødvendigt indberette certificeringsorganets eller den tilknyttede ITSEF's manglende overensstemmelse til det nationale akkrediteringsorgan

b) hvis det er relevant, vurdere den potentielle indvirkning på bemyndigelsen.

KAPITEL VI

SÅRBARHEDSSTYRING OG OFFENTLIGGØRELSE AF SÅRBARHEDER

Artikel 32

Omfanget af sårbarhedsstyring

Dette kapitel finder anvendelse på IKT-produkter, for hvilke der er udstedt en EUCC-attest.

AFDELING I

Sårbarhedsstyring

Artikel 33

Procedurer for sårbarhedsstyring

1. En EUCC-attestindehaver indfører og opretholder alle nødvendige procedurer for sårbarhedsstyring i overensstemmelse med reglerne i denne afdeling om nødvendigt suppleret med procedurerne i EN ISO/IEC 30111.

2. Indehaveren af en EUCC-attest vedligeholder og offentliggør passende metoder til at modtage oplysninger om sårbarheder i forbindelse med deres produkter fra eksterne kilder, herunder brugere, certificeringsorganer og sikkerhedsforskere.

3. Hvis en indehaver af en EUCC-attest opdager eller modtager oplysninger om en potentiel sårbarhed, der påvirker et certificeret IKT-produkt, registrerer indehaveren dette og foretager en sårbarhedskonsekvensanalyse.

4. Når en potentiel sårbarhed påvirker et sammensat produkt, underretter EUCC-attestindehaveren indehavere af afhængige EUCC-attester om potentiel sårbarhed.

5. Som svar på en rimelig anmodning fra det certificeringsorgan, der udstedte attesten, fremsender EUCC-attestindehaveren alle relevante oplysninger om potentielle sårbarheder til det pågældende certificeringsorgan.

Artikel 34

Sårbarhedskonsekvensanalyse

1. I sårbarhedskonsekvensanalysen henvises til målet for evalueringen og de sikkerhedserklæringer, der er indeholdt i attesten. Sårbarhedskonsekvensanalyser gennemføres inden for en frist, der er passende for det certificerede IKT-produkts risiko for at blive udnyttet og kritiske karakter.

2. Hvis det er relevant, foretages en beregning af angrebspotentialet i overensstemmelse med den relevante metode i de standarder, der er omhandlet i artikel 3, og de relevante statusdokumenter, der er opført i bilag I, med henblik på at fastslå sårbarhedens risiko for at blive udnyttet. Der skal tages hensyn til EUCC-attestens AVA_VAN-niveau.

Artikel 35

Rapport om sårbarhedskonsekvensanalyse

1. Indehaveren udarbejder en rapport om sårbarhedskonsekvensanalysen, hvis konsekvensanalysen viser, at sårbarheden sandsynligvis har en indvirkning på IKT-produktets overensstemmelse med dets attest.

2. Rapporten om sårbarhedskonsekvensanalysen skal indeholde en vurdering af følgende elementer:

a) sårbarhedens indvirkning på det certificerede IKT-produkt

b) mulige risici i forbindelse med et angrebs nærhed eller tilgængelighed

c) hvorvidt sårbarheden kan afhjælpes

d) mulige løsninger på sårbarheden, hvis sårbarheden kan afhjælpes.

3. Rapporten om sårbarhedskonsekvensanalysen skal, hvor det er relevant, indeholde nærmere oplysninger om, hvordan sårbarheden eventuelt kan udnyttes. Oplysninger om, hvordan sårbarheden eventuelt kan udnyttes, behandles i overensstemmelse med passende sikkerhedsforanstaltninger for at beskytte fortroligheden og om nødvendigt sikre, at de kun videregives i begrænset omfang.

4. Indehaveren af en EUCC-attest fremsender uden unødigt ophold en rapport om sårbarhedskonsekvensanalysen til certificeringsorganet eller den nationale cybersikkerhedscertificeringsmyndighed i overensstemmelse med artikel 56, stk. 8, i forordning (EU) 2019/881.

5. Hvis det i rapporten om sårbarhedskonsekvensanalysen fastslås, at sårbarheden ikke udgør en fortsat risiko i henhold til de standarder, der er omhandlet i artikel 3, og at den kan afhjælpes, finder artikel 36 anvendelse.

6. Hvis det i rapporten om sårbarhedskonsekvensanalysen fastslås, at sårbarheden ikke udgør en fortsat risiko, og at den ikke kan afhjælpes, tilbagekaldes EUCC-attesten i overensstemmelse med artikel 14.

7. EUCC-attestindehaveren overvåger eventuelle tilbageværende sårbarheder for at sikre, at de ikke kan udnyttes i tilfælde af ændringer i det operationelle miljø.

Artikel 36

Afhjælpning af sårbarheder

EUCC-attestindehaveren forelægger certificeringsorganet et forslag til passende afhjælpende foranstaltninger. Certificeringsorganet reviderer attesten i overensstemmelse med artikel 13. Revisionens omfang bestemmes af den foreslåede afhjælpning af sårbarheden.

AFDELING II

Offentliggørelse af sårbarheder

Artikel 37

Oplysninger, der deles med den nationale cybersikkerhedscertificeringsmyndighed

1. De oplysninger, som certificeringsorganet giver den nationale cybersikkerhedscertificeringsmyndighed, skal omfatte alle de elementer, der er nødvendige for, at den nationale cybersikkerhedscertificeringsmyndighed kan forstå virkningen af sårbarheden, de ændringer, der skal foretages af IKT-produktet, og eventuelle oplysninger fra certificeringsorganet om de bredere konsekvenser af sårbarheden for andre certificerede IKT-produkter.

2. De oplysninger, der gives i henhold til stk. 1, må ikke indeholde nærmere oplysninger om, hvordan sårbarheden kan udnyttes. Denne bestemmelse berører ikke den nationale cybersikkerhedscertificeringsmyndigheds undersøgelsesbeføjelser.

Artikel 38

Samarbejde med andre nationale cybersikkerhedscertificeringsmyndigheder

1. Den nationale cybersikkerhedscertificeringsmyndighed deler de relevante oplysninger, der er modtaget i overensstemmelse med artikel 37, med andre nationale cybersikkerhedscertificeringsmyndigheder og ENISA.

2. Andre nationale cybersikkerhedscertificeringsmyndigheder kan beslutte at analysere sårbarheden yderligere eller, efter at have underrettet indehaveren af EUCC-attesten, anmode de relevante certificeringsorganer om at vurdere, om sårbarheden kan påvirke andre certificerede IKT-produkter.

Artikel 39

Offentliggørelse af sårbarheden

Efter tilbagekaldelse af en attest offentliggør og registrerer EUCC-attestindehaveren enhver offentligt kendt og afhjulpet sårbarhed i IKT-produktet i den europæiske sårbarhedsdatabase, der er oprettet i overensstemmelse med artikel 12 i

Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 ([5]), eller andre onlinedatabaser som omhandlet i artikel 55, stk. 1, litra d), i forordning (EU) 2019/881.

KAPITEL VII

OPBEVARING, VIDEREGIVELSE OG BESKYTTELSE AF OPLYSNINGER

Artikel 40

Certificeringsorganernes og ITSEF's opbevaring af optegnelser

1. ITSEF og certificeringsorganerne fører et registreringssystem med alle de dokumenter, der er udarbejdet i forbindelse med hver evaluering og certificering, som de udfører.

2. Certificeringsorganerne og ITSEF lagrer registreringerne på en sikker måde og opbevarer disse fortegnelser i det tidsrum, der er nødvendigt med henblik på denne forordning, og i mindst fem år efter tilbagekaldelsen af den relevante EUCC-attest. Når certificeringsorganet har udstedt en ny EUCC-attest i overensstemmelse med artikel 13, stk. 2, litra c), opbevarer det dokumentationen for den tilbagekaldte EUCC-attest sammen med og så længe som dokumentationen for den nye EUCC-attest.

Artikel 41

Oplysninger, der gøres tilgængelige af en attestindehaver

1. De oplysninger, der er omhandlet i artikel 55 i forordning (EU) 2019/881, skal være tilgængelige på et sprog, der er let tilgængeligt for brugerne.

2. EUCC-attestindehaveren opbevarer følgende sikkert i det tidsrum, der er nødvendigt med henblik på denne forordning, og i mindst fem år efter tilbagekaldelsen af den relevante EUCC-attest:

a) optegnelser over de oplysninger, der gives til certificeringsorganet og til ITSEF under certificeringsprocessen,

b) et prøveeksemplar af det certificerede IKT-produkt.

3. Når certificeringsorganet har udstedt en ny EUCC-attest i overensstemmelse med artikel 13, stk. 2, litra c), opbevarer indehaveren dokumentationen for den tilbagekaldte EUCC-attest sammen med og så længe som dokumentationen for den nye EUCC-attest.

4. Efter anmodning fra certificeringsorganet eller den nationale cybersikkerhedscertificeringsmyndighed stiller EUCC-attestindehaveren de optegnelser og prøveeksemplarer, der er omhandlet i stk. 2, til rådighed.

Artikel 42

Oplysninger, der gøres tilgængelige af ENISA

1. ENISA offentliggør følgende oplysninger på det websted, der er omhandlet i artikel 50, stk. 1, i forordning (EU) 2019/881:

a) alle EUCC-attester

b) oplysninger om status for en EUCC-attest, navnlig om den er i kraft, suspenderet, tilbagekaldt eller udløbet

c) certificeringsrapporter svarende til hver EUCC-attest

([5]) Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333 af 27.12.2022, s. 80).

d) en liste over akkrediterede overensstemmelsesvurderingsorganer

e) en liste over bemyndigede overensstemmelsesvurderingsorganer

f) de statusdokumenter, der er anført i bilag I

g) udtalelserne fra Den Europæiske Cybersikkerhedscertificeringsgruppe, jf. artikel 62, stk. 4, litra c), i forordning (EU) 2019/881

h) peervurderingsrapporter udstedt i overensstemmelse med artikel 47.

2. De oplysninger, der er omhandlet i stk. 1, stilles til rådighed på mindst engelsk.

3. Certificeringsorganerne og, hvor det er relevant, de nationale cybersikkerhedscertificeringsmyndigheder underretter straks ENISA om deres afgørelser, der påvirker indholdet af eller status for en EUCC-attest som omhandlet i stk. 1, litra b).

4. ENISA sikrer, at de oplysninger, der offentliggøres i overensstemmelse med stk. 1, litra a), b) og c), klart identificerer de versioner af et certificeret IKT-produkt, der er omfattet af en EUCC-attest.

Artikel 43

Beskyttelse af oplysninger

Overensstemmelsesvurderingsorganer, nationale cybersikkerhedscertificeringsmyndigheder, ECCG, ENISA, Kommissionen og alle andre parter sørger for at sikre og beskytte forretningshemmeligheder og andre fortrolige oplysninger, herunder handelshemmeligheder, og for at beskytte intellektuelle ejendomsrettigheder, og de træffer de nødvendige og passende tekniske og organisatoriske foranstaltninger.

KAPITEL VIII

AFTALER OM GENSIDIG ANERKENDELSE MED TREDJELANDE

Artikel 44

Betingelser

1. Tredjelande, der er villige til at certificere deres produkter i henhold til denne forordning, og som ønsker en sådan certificering anerkendt i Unionen, indgår en aftale om gensidig anerkendelse med Unionen.

2. Aftalen om gensidig anerkendelse skal omfatte de gældende tillidsniveauer for certificerede IKT-produkter og, hvor det er relevant, beskyttelsesprofiler.

3. De i stk. 1 omhandlede aftaler om gensidig anerkendelse kan kun indgås med tredjelande, der opfylder følgende betingelser:

a) har en myndighed, der:

   1) er et offentligt organ, som er uafhængigt af de enheder, det fører tilsyn med og overvåger, med hensyn til organisatorisk og juridisk struktur, finansiel finansiering og beslutningstagning

   2) har passende overvågnings- og tilsynsbeføjelser til at foretage undersøgelser og har beføjelse til at træffe passende korrigerende foranstaltninger for at sikre overensstemmelse

   3) har et sanktionssystem, der er effektivt, står i et rimeligt forhold til overtrædelsen og har afskrækkende virkning, for at sikre overensstemmelse

   4) accepterer at samarbejde med Den Europæiske Cybersikkerhedscertificeringsgruppe og ENISA om at udveksle bedste praksis og relevant udvikling inden for cybersikkerhedscertificering og at arbejde hen imod en ensartet fortolkning af de gældende evalueringskriterier og -metoder, bl.a. ved at anvende harmoniseret dokumentation, der svarer til de statusdokumenter, der er opført i bilag I

b) har et uafhængigt akkrediteringsorgan, der udfører akkrediteringer baseret på standarder, der svarer til de standarder, der er omhandlet i forordning (EF) nr. 765/2008

c) garanterer, at evaluerings- og certificeringsprocesserne og -procedurerne gennemføres på en tilstrækkelig professionel måde under hensyntagen til overholdelsen af de internationale standarder, der er omhandlet i denne forordning, navnlig artikel 3

d) har kapacitet til at indberette tidligere uopdagede sårbarheder og en etableret og passende procedure for sårbarhedsstyring og offentliggørelse

e) har indført procedurer, der sætter det i stand til effektivt at indgive og behandle klager og stille effektive retsmidler til rådighed for klageren

f) opretter en mekanisme for samarbejde med andre EU-organer og medlemsstatsorganer, der er relevante for cybersikkerhedscertificeringen i henhold til denne forordning, herunder udveksling af oplysninger om attesters mulige manglende overensstemmelse, overvågning af relevant udvikling på certificeringsområdet og sikring af en fælles tilgang til vedligeholdelse og revision af certificering.

4. Ud over de betingelser, der er fastsat i stk. 3, kan der kun indgås en aftale om gensidig anerkendelse som omhandlet i stk. 1, der dækker tillidsniveauet »højt«, med tredjelande, hvis følgende betingelser også er opfyldt:

a) tredjelandet har en uafhængig og offentlig cybersikkerhedscertificeringsmyndighed, der udfører eller uddelegerer de evalueringsaktiviteter, der er nødvendige for at muliggøre certificering på tillidsniveauet »højt«, som svarer til de krav og procedurer, der er fastsat for nationale cybersikkerhedsmyndigheder i nærværende forordning og i forordning (EU) 2019/881

b) ved aftalen om gensidig anerkendelse indføres der en fælles mekanisme, som svarer til peervurdering af EUCC-attester med henblik på at forbedre udvekslingen af praksis og i fællesskab løse problemer med evaluering og certificering.

KAPITEL IX

PEERVURDERING AF CERTIFICERINGSORGANER

Artikel 45

Peervurderingsprocedure

1. Et certificeringsorgan, der udsteder EUCC-attester på tillidsniveauet »højt«, skal regelmæssigt og mindst hvert femte år gennemgå en peervurdering. De forskellige typer peervurderinger er anført i bilag VI.

2. Den Europæiske Cybersikkerhedscertificeringsgruppe udarbejder og ajourfører en oversigt over peervurderinger, der sikrer, at dette krav om hyppighed overholdes. Undtagen i behørigt begrundede tilfælde foretages peervurderinger på stedet.

3. Peervurderinger kan baseres på dokumentation, der er indsamlet i forbindelse med tidligere peervurderinger eller tilsvarende procedurer foretaget af det peervurderede certificeringsorgan eller den nationale cybersikkerhedscertificeringsmyndighed, forudsat at:

a) resultaterne ikke er ældre end fem år

b) resultaterne ledsages af en beskrivelse af de peervurderingsprocedurer, der er fastsat for den pågældende ordning, hvis de vedrører en peervurdering foretaget under en anden certificeringsordning

c) det i den peervurderingsrapport, der er omhandlet i artikel 47, angives, hvilke resultater der er genanvendt med eller uden yderligere vurdering.

4. Hvis en peervurdering dækker et teknisk område, skal den pågældende ITSEF også vurderes.

5. Det peervurderede certificeringsorgan og om nødvendigt den nationale cybersikkerhedscertificeringsmyndighed sikrer, at alle relevante oplysninger stilles til rådighed for peervurderingsteamet.

6. Peervurderingen foretages af et peervurderingsteam, der er oprettet i overensstemmelse med bilag VI.

Artikel 46

Faser i peervurdering

1. I den forberedende fase gennemgår medlemmerne af peervurderingsteamet certificeringsorganets dokumentation, der omfatter dets politikker og procedurer, herunder anvendelsen af statusdokumenterne.

2. I fasen for besøg på stedet vurderer peervurderingsteamet organets tekniske kompetence og, hvor det er relevant, kompetencen hos en ITSEF, der har udført mindst én evaluering af IKT-produkter, som er omfattet af peervurderingen.

3. Varigheden af fasen for besøg på stedet kan forlænges eller forkortes afhængigt af faktorer som f.eks. muligheden for at genanvende eksisterende peervurderingsdokumentation og -resultater eller af antallet af ITSEF'er og tekniske områder, som certificeringsorganet udsteder attester for.

4. Hvis det er relevant, fastlægger peervurderingsteamet hver ITSEF's tekniske kompetence ved at besøge dens tekniske laboratorium eller laboratorier og interviewe dens evalueringseksperter for så vidt angår det tekniske område og relaterede specifikke angrebsmetoder.

5. I rapporteringsfasen dokumenterer vurderingsteamet sine resultater i en peervurderingsrapport, som omfatter en bedømmelse og, hvor det er relevant, en liste over observerede afvigelser, der hver er klassificeret efter alvorlighed.

6. Peervurderingsrapporten skal først drøftes med det peervurderede certificeringsorgan. Efter disse drøftelser fastlægger det peervurderede certificeringsorgan en tidsplan for de foranstaltninger, der skal træffes for at afhjælpe resultaterne.

Artikel 47

Rapport om peervurdering

1. Peervurderingsteamet forelægger det peervurderede certificeringsorgan et udkast til peervurderingsrapporten.

2. Det peervurderede certificeringsorgan indgiver bemærkninger vedrørende resultaterne og en liste over tilsagn med henblik på at afhjælpe de mangler, der er identificeret i udkastet til peervurderingsrapporten, til peervurderingsteamet.

3. Peervurderingsteamet indgiver en endelig peervurderingsrapport, som også indeholder det peervurderede certificeringsorgans bemærkninger og tilsagn, til Den Europæiske Cybersikkerhedscertificeringsgruppe. Peervurderingsteamet anfører også sin holdning til bemærkningerne og til, hvorvidt disse tilsagn er tilstrækkelige til at afhjælpe de konstaterede mangler.

4. Hvis der konstateres manglende overensstemmelse i peervurderingsrapporten, kan Den Europæiske Cybersikkerhedscertificeringsgruppe fastsætte en passende frist for, hvornår det peervurderede certificeringsorgan skal have afhjulpet manglerne.

5. Den Europæiske Cybersikkerhedscertificeringsgruppe vedtager en udtalelse om peervurderingsrapporten:

a) hvis peervurderingsrapporten ikke identificerer manglende overensstemmelse, eller hvis det peervurderede certificeringsorgan på passende vis har afhjulpet den manglende overensstemmelse, kan Den Europæiske Cybersikkerhedscertificeringsgruppe afgive en positiv udtalelse, og alle relevante dokumenter offentliggøres på ENISA's certificeringswebsted

b) hvis det peervurderede certificeringsorgan ikke på passende vis afhjælper manglerne inden for den fastsatte frist, kan Den Europæiske Cybersikkerhedscertificeringsgruppe afgive en negativ udtalelse, der offentliggøres på ENISA's certificeringswebsted, inklusive peervurderingsrapporten og alle relevante dokumenter.

6. Forud for offentliggørelsen af udtalelsen fjernes alle følsomme, personlige eller ejendomsretligt beskyttede oplysninger fra de offentliggjorte dokumenter.

KAPITEL X

VEDLIGEHOLDELSE AF ORDNINGEN

Artikel 48

Vedligeholdelse af EUCC

1. Kommissionen kan anmode Den Europæiske Cybersikkerhedscertificeringsgruppe om at vedtage en udtalelse med henblik på at opretholde EUCC og foretage det nødvendige forberedende arbejde.

2. Den Europæiske Cybersikkerhedscertificeringsgruppe kan vedtage en udtalelse om godkendelse af statusdokumenter.

3. Statusdokumenter, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe, offentliggøres af ENISA.

KAPITEL XI

AFSLUTTENDE BESTEMMELSER

Artikel 49

Nationale ordninger, der er omfattet af EUCC

1. I overensstemmelse med artikel 57, stk. 1, i forordning (EU) 2019/881 og med forbehold af denne forordnings artikel 57, stk. 3, ophører alle nationale cybersikkerhedscertificeringsordninger og de relaterede procedurer for IKT-produkter og -processer, der er omfattet af EUCC, med at have virkning fra 12 måneder efter nærværende forordnings ikrafttræden.

2. Uanset artikel 50 kan der indledes en certificeringsproces inden for rammerne af en national cybersikkerhedscertificeringsordning senest 12 måneder efter denne forordnings ikrafttræden, forudsat at certificeringsprocessen er afsluttet senest 24 måneder efter forordningens ikrafttræden.

3. Attester, der er udstedt i henhold til nationale cybersikkerhedscertificeringsordninger, kan revideres. Nye attester, der erstatter de reviderede attester, udstedes i overensstemmelse med denne forordning.

Artikel 50

Ikrafttræden

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

Den finder anvendelse fra den 27. februar 2025.

Kapitel IV og bilag V finder anvendelse fra datoen for denne forordnings ikrafttræden.

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

Udfærdiget i Bruxelles, den 31. januar 2024.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG I

Tekniske områder og statusdokumenter

1. Tekniske områder på AVA_VAN-niveau 4 eller 5:

   a) dokumenter vedrørende harmoniseret evaluering af det tekniske område »smartcards og lignende enheder«, herunder navnlig følgende dokumenter i deres respektive udgaver i kraft den [ikrafttrædelsesdato]:

      1) »Minimum ITSEF requirements for security evaluations of smart cards and similar devices« (minimumskrav til sikkerhedsevalueringer af smartcards og lignende enheder), oprindelig godkendt af ECCG den 20. oktober 2023

      2) »Minimum Site Security Requirements« (minimumskrav til sikkerhed på stedet), oprindelig godkendt af ECCG den 20. oktober 2023

      3) »Application of Common Criteria to integrated circuits« (anvendelse af fælles kriterier på integrerede kredsløb), oprindelig godkendt af ECCG den 20. oktober 2023

      4) »Security Architecture requirements (ADV_ARC) for smart cards and similar devices« (krav til sikkerhedsarkitektur (ADV_ARC) for smartcards og lignende enheder), oprindelig godkendt af ECCG den 20. oktober 2023

      5) »Certification of »open« smart card products« (certificering af »åbne« smartcardprodukter), oprindelig godkendt af ECCG den 20. oktober 2023

      6) »Composite product evaluation for smart cards and similar devices« (evaluering af sammensatte produkter til smartcards og lignende enheder), oprindelig godkendt af ECCG den 20. oktober 2023

      7) »Application of Attack Potential to Smartcards« (anvendelse af angrebspotentiale på smartcards), oprindelig godkendt af ECCG den 20. oktober 2023

   b) dokumenter vedrørende harmoniseret evaluering af det tekniske område »hardwareenheder med sikkerhedsbokse«, herunder navnlig følgende dokumenter i deres respektive udgaver i kraft den [ikrafttrædelsesdato]:

      1) »Minimum ITSEF requirements for security evaluations of hardware devices with security boxes« (minimumskrav til sikkerhedsevalueringer af hardwareenheder med sikkerhedsbokse), oprindelig godkendt af ECCG den 20. oktober 2023

      2) »Minimum Site Security Requirements« (minimumskrav til sikkerhed på stedet), oprindelig godkendt af ECCG den 20. oktober 2023

      3) »Application of Attack Potential to hardware devices with security boxes« (anvendelse af angrebspotentiale på hardwareenheder med sikkerhedsbokse), oprindelig godkendt af ECCG den 20. oktober 2023.

2. Statusdokumenter i deres respektive udgaver i kraft den [ikrafttrædelsesdato]:

   a) dokument vedrørende harmoniseret akkreditering af overensstemmelsesvurderingsorganer: »Accreditation of ITSEFs for the EUCC« (akkreditering af ITSEF'er med henblik på EUCC), oprindelig godkendt af ECCG den 20. oktober 2023.

BILAG II

Beskyttelsesprofiler certificeret på AVA_VAN-niveau 4 eller 5

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

1) 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)

2) EN 419221-5:2018 - Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services Protection profile (beskyttelsesprofiler for tillidstjenesteudbydere — Kryptografiske moduler — Del 5: Kryptografisk modul til trust service-beskyttelsesprofiler), der er vedtaget som statusdokumenter:

2. Protection profiles that have been adopted as state-of-the-art documents:

[TOM]

BILAG III

Anbefalede beskyttelsesprofiler (der illustrerer tekniske områder fra bilag I)

Beskyttelsesprofiler, der anvendes i forbindelse med certificering af IKT-produkter, som er omfattet af nedenstående IKT-produktkategori:

a) for kategorien maskinlæsbare rejsedokumenter:

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

2) beskyttelsesprofil til maskinlæsbare rejsedokumenter med »ICAO Application« Extended Access Control, BSI-CC-PP-0056-2009

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

4) beskyttelsesprofil til maskinlæsbare rejsedokumenter med »ICAO Application« Basic Access Control, BSI-CC-PP-0055-2009

b) for kategorien enheder til generering af sikker signatur:

1) EN 419211-1:2014 - Protection profiles for secure signature creation device - Part 1: Overview (beskyttelsesprofiler til enheder til af sikker signatur — del 1: Oversigt)

2) EN 419211-2:2013 - Protection profiles for secure signature creation device - Part 2: Device with key generation (beskyttelsesprofiler til udstyr til generering af sikker signatur — del 2: udstyr med nøglegenerering)

3) EN 419211-3:2013 - Protection profiles for secure signature creation device - Part 3: Device with key import (beskyttelsesprofiler til generering af sikker signatur — del 3: enheder med nøgleimport)

4) 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)

5) 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)

6) 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)

c) for kategorien digitale takografer:

1) digitale takografer — takografkort som omhandlet i Kommissionens gennemførelsesforordning (EU) 2016/799 af 18. marts 2016 om gennemførelse af forordning (EU) nr. 165/2014 (bilag 1C)

2) digitale takografer — køretøjsenhed som omhandlet i bilag IB til Kommissionens forordning (EF) nr. 1360/2002 bestemt til montering i køretøjer til vejtransport

3) digitale takografer — eksternt GNSS-udstyr (EGF PP) som omhandlet i bilag 1C til Kommissionens gennemførelsesforordning (EU) 2016/799 af 18. marts 2016 om gennemførelse af Europa-Parlamentets og Rådets forordning (EU) nr. 165/2014

4) digitale takografer — bevægelsessensor (MS PP) som omhandlet i bilag 1C til Kommissionens gennemførelsesforordning (EU) 2016/799 af 18. marts 2016 om gennemførelse af Europa-Parlamentets og Rådets forordning (EU) nr. 165/2014

d) for kategorien sikre integrerede kredsløb, smartcards og tilhørende udstyr eller systemer:

1) Security IC Platform PP, BSI-CC-PP-0084-2014

2) Java Card System — Open Configuration, V3.0.5 BSI-CC-PP-0099-2017

3) Java Card System — Closed Configuration, BSI-CC-PP-0101-2017

4) PP til en PC Client Specific Trusted Platform Module Family 2.0 Level 0 Revision 1.16, ANSSI-CC-PP-2015/07

5) Universelt SIM-kort, PU-2009-RT-79, ANSSI-CC-PP-2010/04

6) Embedded UICC (eUICC) til Machine-to-Machine Devices, BSI-CC-PP-0089-2015

e) for kategorien (betalings-)interaktionspunkter og betalingsterminaler:

1) Point of Interaction »POI-CHIP-ONLY«, ANSSI-CC-PP-2015/01

2) Point of Interaction »POI-CHIP-ONLY and Open Protocol Package«, ANSSI-CC-PP-2015/02

3) Point of Interaction »POI-COMPREHENSIVE«, ANSSI-CC-PP-2015/03

4) Point of Interaction »POI-COMPREHENSIVE and Open Protocol Package«, ANSSI-CC-PP-2015/04

5) Point of Interaction »POI-PED-ONLY«, ANSSI-CC-PP-2015/05

6) Point of Interaction »POI-PED-ONLY and Open Protocol Package«, ANSSI-CC-PP-2015/06

f) for kategorien hardwareenheder med sikkerhedsbokse:

1) Cryptographic Module for CSP Signing Operations with Backup — PP CMCSOB, PP HSM CMCSOB 14167-2, ANSSI-CC-PP-2015/08

2) Cryptographic Module for CSP key generation services — PP CMCKG, PP HSM CMCKG 14167-3, ANSSI-CC-PP-2015/09

3) Cryptographic Module for CSP Signing Operations without Backup — PP CMCSO, PP HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10.

BILAG IV

Tillidskontinuitet og revision af attester

IV.1 Tillidskontinuitet: omfang

1. Følgende krav til tillidskontinuitet finder anvendelse på vedligeholdelsesaktiviteter i forbindelse med følgende:
   a) en fornyet vurdering, hvis et uændret certificeret IKT-produkt stadig opfylder sikkerhedskravene
   b) en evaluering af virkningerne af ændringer af et certificeret IKT-produkt på dets certificering
   c) anvendelse af patches i overensstemmelse med en vurderet patchstyringsproces, hvis de indgår i certificeringen
   d) hvis det inkluderes, revision af indehaveren af attestens livscyklusforvaltning eller fremstillingsprocesser.

2. En EUCC-attestindehaver kan anmode om revision af attesten i følgende tilfælde:
   a) EUCC-attesten udløber inden for ni måneder
   b) der er sket en ændring i enten det certificerede IKT-produkt eller i en anden faktor, som kan påvirke dets sikkerhedsfunktioner
   c) attestindehaveren kræver, at sårbarhedsvurderingen foretages igen for at bekræfte EUCC-attestens sikkerhed i forbindelse med IKT-produktets modstandsdygtighed over for aktuelle cyberangreb.

IV.2 Fornyet vurdering

1. Hvis der er behov for at vurdere virkningen af ændringer i trusselsmiljøet for et uændret certificeret IKT-produkt, indgives der en anmodning om fornyet vurdering til certificeringsorganet.

2. Den fornyede vurdering foretages af den samme ITSEF som den, der var involveret i den foregående evaluering, og ved at genbruge alle de resultater, der stadig er gældende. Evalueringen skal fokusere på tillidsaktiviteter, der potentielt påvirkes af det certificerede IKT-produkts ændrede trusselsmiljø, navnlig den relevante AVA_VAN-familie, og desuden tillidslivscyklusfamilien (ALC), hvor der igen indsamles tilstrækkelig dokumentation for vedligeholdelse af udviklingsmiljøet.

3. ITSEF'en beskriver ændringerne og specificerer resultaterne af den fornyede vurdering sammen med en ajourføring af den tekniske rapport fra den foregående evaluering.

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.

5. Rapporten om den fornyede vurdering og den ajourførte attest forelægges den nationale cybersikkerhedscertificeringsmyndighed og ENISA med henblik på offentliggørelse på dets cybersikkerhedscertificeringswebsted.

IV.3 Ændringer af et certificeret IKT-produkt

1. Hvis et certificeret IKT-produkt har været genstand for ændringer, skal den attestindehaver, der ønsker at bevare attesten, indgive en konsekvensanalyserapport til certificeringsorganet.

2. Konsekvensanalyserapporten skal omfatte følgende elementer:
   a) en indledning med de oplysninger, der er nødvendige for at identificere konsekvensanalyserapporten og det ændrede evalueringsmål

b) en beskrivelse af ændringerne af produktet

c) identifikation af, hvilken af udviklerens dokumentation, der påvirkes

d) en beskrivelse af ændringerne af udviklerens dokumentation

e) resultaterne og konklusionerne om hver ændrings indvirkning på tilliden.

3. Certificeringsorganet undersøger de ændringer, der er beskrevet i konsekvensanalyserapporten, med henblik på at validere deres indvirkning på tillidsniveauet for det certificerede evalueringsmål i overensstemmelse med konklusionerne i konsekvensanalyserapporten.

4. Efter undersøgelsen fastlægger certificeringsorganet omfanget af en ændring som mindre eller væsentlig i forhold til dens indvirkning.

5. Hvis ændringerne er blevet bekræftet af certificeringsorganet som ændringer af mindre omfang, udstedes der en ny attest for det ændrede IKT-produkt, og der udarbejdes en vedligeholdelsesrapport til den indledende certificeringsrapport på følgende betingelser:

a) vedligeholdelsesrapporten skal indgå som en del af konsekvensanalyserapporten med følgende afsnit:

1) indledning

2) beskrivelse af ændringerne

3) hvilken af udviklerens dokumentation, der påvirkes

b) den nye attests gyldighedsdato må ikke overskride den oprindelige attests gyldighedsdato.

6. Den nye attest, herunder vedligeholdelsesrapporten, fremsendes til ENISA med henblik på offentliggørelse på dets cybersikkerhedscertificeringswebsted.

7. Hvis det bekræftes, at ændringerne er væsentlige, skal der foretages en fornyet evaluering under hensyntagen til den foregående evaluering og ved at genanvende eventuelle resultater fra den foregående evaluering, der stadig er gældende.

8. Når evalueringen af det ændrede evalueringsmål er afsluttet, udarbejder ITSEF'en en ny rapport om teknisk evaluering. Certificeringsorganet reviderer den ajourførte rapport om teknisk evaluering og udarbejder, hvis det er relevant, en ny attest med en ny certificeringsrapport.

9. Den nye attest og den nye certificeringsrapport indgives til ENISA med henblik på offentliggørelse.

IV.4 **Patchstyring**

1. En patchstyringsprocedure giver mulighed for at indføre en struktureret proces for ajourføring af et certificeret IKT-produkt. Patchstyringsproceduren, herunder den mekanisme, som ansøgeren om certificering har implementeret i IKT-produktet, kan anvendes efter certificeringen af IKT-produktet på overensstemmelsesvurderingsorganets ansvar.

2. En ansøger om certificering kan i certificeringen af IKT-produktet inkludere en patchmekanisme som led i en certificeret styringsprocedure, der er implementeret i IKT-produktet, på en af følgende betingelser:

a) de funktioner, der påvirkes af patchen, ligger uden for evalueringsmålet i det certificerede IKT-produkt

b) patchen vedrører en på forhånd fastlagt mindre ændring af det certificerede IKT-produkt

c) patchen vedrører en bekræftet sårbarhed med kritiske konsekvenser for det certificerede IKT-produkts sikkerhed.

3. Hvis patchen vedrører en væsentlig ændring af evalueringsmålet i det certificerede IKT-produkt i forbindelse med en tidligere uopdaget sårbarhed, der ikke har kritisk virkning for IKT-produktets sikkerhed, finder bestemmelserne i artikel 13 anvendelse.

4. Patchstyringsproceduren for et IKT-produkt består af følgende elementer:

   a) processen for udvikling og frigivelse af patchen til IKT-produktet

   b) den tekniske mekanisme og de tekniske funktioner til implementering af patchen i IKT-produktet

   c) en række evalueringsaktiviteter vedrørende den tekniske mekanismes effektivitet og ydeevne.

5. Under certificeringen af IKT-produktet:

   a) ansøgeren om certificering af IKT-produktet skal fremlægge en beskrivelse af patchstyringsproceduren

   b) kontrollerer ITSEF'en følgende elementer:

      1) de patchmekanismer, som udvikleren har implementeret i IKT-produktet i overensstemmelse med den patchstyringsprocedure, der blev forelagt til certificering

      2) grænserne for evalueringsmålet er adskilt på en sådan måde, at de ændringer, der foretages i de adskilte processer, ikke påvirker evalueringsmålets sikkerhed

      3) den tekniske patchmekanisme fungerer i overensstemmelse med bestemmelserne i dette afsnit og ansøgerens oplysninger

   c) certificeringsorganet medtager resultatet af den vurderede patchstyringsprocedure i certificeringsrapporten.

6. Attestindehaveren kan anvende patchen, som er frembragt i overensstemmelse med den certificerede patchstyrings-procedure, i det pågældende certificerede IKT-produkt og træffer følgende foranstaltninger inden for fem arbejdsdage i følgende tilfælde:

   a) i det tilfælde, der er omhandlet i punkt 2, litra a), indberettes den pågældende patch til certificeringsorganet, som ikke ændrer den tilsvarende EUCC-attest

   b) i det tilfælde, der er omhandlet i punkt 2, litra b), indgives patchen til ITSEF'en med henblik på revision. ITSEF'en underretter certificeringsorganet efter modtagelsen af patchen, hvorefter certificeringsorganet træffer passende foranstaltninger med hensyn til udstedelse af en ny version af den tilsvarende EUCC-attest og ajourføringen af certificeringsrapporten

   c) i det tilfælde, der er omhandlet i punkt 2, litra c), indgives patchen til ITSEF'en med henblik på fornyet vurdering, samtidig med at patchen implementeres. ITSEF'en underretter certificeringsorganet, hvorefter certificeringsorganet påbegynder de tilknyttede certificeringsaktiviteter.

BILAG V

INDHOLDET AF EN CERTIFICERINGSRAPPORT

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.

2. Certificeringsrapporten er kilden til detaljerede og praktiske oplysninger om IKT-produktet eller kategorien af IKT-produkter og om sikker implementering af IKT-produktet og 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 afsnit:

   a) resumé

   b) identifikation af IKT-produktet eller IKT-produktkategorien, hvis der er tale om beskyttelsesprofiler

   c) sikkerhedstjenester

   d) antagelser om og præcisering af anvendelsesområdet

   e) oplysninger om arkitektur

   f) supplerende oplysninger om cybersikkerhed, hvis det er relevant

   g) afprøvning af IKT-produkter, der måtte være foretaget

   h) hvor det er relevant, en identificering af indehaveren af attestens livscyklusforvaltning og fremstillingsfaciliteter

   i) resultaterne af evalueringen og oplysninger om attesten

   j) resumé af sikkerhedsmålet for det IKT-produkt, der skal certificeres

   k) den mærkning eller etiket, der eventuelt er knyttet til ordningen

   l) bibliografi.

4. Resuméet skal være et kort sammendrag af hele certificeringsrapporten. Resuméet skal give et klart og præcist overblik over evalueringsresultaterne og indeholde følgende oplysninger:

   a) navnet på det evaluerede IKT-produkt, opremsning af de af produktets komponenter, der indgår i evalueringen, og IKT-produktversionen

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

   c) dato for evalueringens afslutning

   d) henvisning til rapporten om teknisk evaluering fastlagt af ITSEF

   e) kort beskrivelse af certificeringsrapportens resultater, herunder:

      1) versions- og frigivelsesnummer, hvis det er relevant, for de fælles kriterier, der er anvendt ved evalueringen

      2) tillidspakke og sikkerhedstillidskomponenter under de fælles kriterier, herunder 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

      3) det evaluerede IKT-produkts sikkerhedsfunktioner

      4) en sammenfatning af trusler og organisatoriske sikkerhedspolitikker, som det evaluerede IKT-produkt imødegår

5) særlige konfigurationskrav

6) antagelser om driftsmiljøet

7) hvis det er relevant, tilstedeværelsen af en godkendt patchstyringsprocedure i overensstemmelse med bilag IV, afsnit IV.4

8) ansvarsfraskrivelse.

5. Det evaluerede IKT-produkt skal være klart identificeret, bl.a. ved følgende oplysninger:

a) det evaluerede IKT-produkts navn

b) en opremsning af de af IKT-produktets komponenter, som indgår i evalueringen

c) versionsnummeret for IKT-produktets komponenter

d) identifikation af yderligere krav til det certificerede IKT-produkts driftsmiljø

e) navn og kontaktoplysninger på EUCC-attestindehaveren

f) hvis det er relevant, den anvendte patchstyringsprocedure, som indgår i attesten

g) link til EUCC-attestindehaverens websted, hvor der gives supplerende cybersikkerhedsoplysninger om det certificerede IKT-produkt i overensstemmelse med artikel 55 i forordning (EU) 2019/881.

6. Oplysningerne i dette afsnit skal være så nøjagtige som muligt for at sikre en fuldstændig og nøjagtig gengivelse af IKT-produktet, som kan genanvendes i fremtidige evalueringer.

7. Afsnittet om sikkerhedspolitik skal indeholde en beskrivelse af IKT-produktets sikkerhedspolitik og de politikker eller regler, som det evaluerede IKT-produkt skal håndhæve eller overholde. Det skal indeholde en henvisning til og en beskrivelse af følgende politikker:

a) attestindehaverens politik for håndtering af sårbarheder

b) attestindehaverens politik for tillidskontinuitet.

8. Hvor det er relevant, kan politikken omfatte betingelserne for anvendelse af en patchstyringsprocedure i attestens gyldighedsperiode.

9. Afsnittet om antagelser og præcisering af anvendelsesområdet skal indeholde udtømmende oplysninger om omstændighederne og målene i forbindelse med den påtænkte anvendelse af produktet, jf. artikel 7, stk. 1, litra c). Oplysningerne 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.

10. Oplysningerne i punkt 9 skal være så forståelige som muligt, således at brugerne af det certificerede IKT-produkt kan træffe informerede beslutninger om de risici, der er forbundet med dets anvendelse.

11. Afsnittet med oplysninger om arkitektur skal indeholde en overordnet beskrivelse af IKT-produktet og dets hovedkomponenter i overensstemmelse med ADV_TDS-delsystemernes konstruktion efter de fælles kriterier.

12. Der skal gives en fuldstændig liste over IKT-produktets supplerende cybersikkerhedsoplysninger som omhandlet i artikel 55 i forordning (EU) 2019/881. Al relevant dokumentation skal angives med versionsnumrene.

13. Afsnittet om afprøvning af IKT-produktet skal indeholde følgende oplysninger:

    a) navn og kontaktpunkt for den myndighed eller det organ, der har udstedt attesten, herunder den ansvarlige nationale cybersikkerhedscertificeringsmyndighed

    b) navnet på den ITSEF, der har foretaget evalueringen, hvis denne er forskellig fra certificeringsorganet

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

    d) statusdokumentets version og yderligere sikkerhedsevalueringskriterier, der er anvendt i evalueringen

    e) IKT-produktets fuldstændige og præcise indstillinger og konfiguration under evalueringen, herunder operationelle noter og observationer, hvis sådanne foreligger

    f) alle beskyttelsesprofiler, der er blevet anvendt, herunder følgende oplysninger:

        1) ophavsmanden til beskyttelsesprofilen

        2) beskyttelsesprofilens navn og identifikator

        3) identifikator for beskyttelsesprofilens attest

        4) navn og kontaktoplysninger på certificeringsorganet og den ITSEF, der er involveret i evalueringen af beskyttelsesprofilen

        5) den eller de tillidspakker, der kræves for et produkt, som er i overensstemmelse med beskyttelsesprofilen.

14. Resultaterne af evalueringen og oplysninger vedrørende afsnittet om attesten skal omfatte følgende oplysninger:

    a) bekræftelse af det opnåede tillidsniveau som omhandlet i nærværende forordnings artikel 4 og artikel 52 i forordning (EU) 2019/881

    b) krav til tillid fra de standarder, der er omhandlet i artikel 3, som IKT-produktet eller beskyttelsesprofilen faktisk opfylder, herunder AVA_VAN-niveauet

    c) en detaljeret beskrivelse af kravene til tillid og nærmere oplysninger om, hvordan produktet opfylder hvert enkelt krav

    d) attestens udstedelsesdato og gyldighedsperiode

    e) attestens entydige identifikator.

15. Sikkerhedsmålet skal indgå i certificeringsrapporten eller refereres til og sammenfattes i certificeringsrapporten og indgives sammen med den tilhørende certificeringsrapport med henblik på offentliggørelse.

16. Sikkerhedsmålet kan renses i overensstemmelse med afsnit VI.2.

17. Den mærkning eller etiket, der er knyttet til EUCC, må indsættes i certificeringsrapporten i overensstemmelse med de regler og procedurer, der er fastsat i artikel 11.

18. Bibliografiafsnittet 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, og deres version

    b) rapporten om teknisk evaluering

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

    d) teknisk referencedokumentation

    e) udviklerens dokumentation, som er anvendt i evalueringen.

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

V.2 **Rensning af sikkerhedsmål med henblik på offentliggørelse**

1. Det sikkerhedsmål, der skal indgå i eller henvises til i certificeringsrapporten i henhold til afsnit VI.1, punkt 1, kan renses ved at fjerne eller omskrive ejendomsretligt beskyttede tekniske oplysninger.

2. Det resulterende rensede sikkerhedsmål skal være en reel gengivelse af den fuldstændige originale version. Det betyder, at der i det rensede sikkerhedsmål ikke må udelades oplysninger, der er nødvendige for at forstå sikkerhedsegenskaberne ved evalueringsmålet og evalueringens omfang.

3. Indholdet af det rensede sikkerhedsmål skal opfylde følgende minimumskrav:
   a) indledningen må ikke renses, da den generelt ikke indeholder ejendomsretligt beskyttede oplysninger
   b) det rensede sikkerhedsmål skal have en entydig identifikator, der adskiller det fra den fuldstændige oprindelige version.
   c) beskrivelsen af evalueringsmålet kan forkortes, da den kan omfatte ejendomsretligt beskyttede og detaljerede oplysninger om evalueringsmålets konstruktion, som ikke bør offentliggøres
   d) beskrivelsen af evalueringsmålets sikkerhedsmiljø (antagelser, trusler og organisatoriske sikkerhedspolitikker) må ikke forkortes, for så vidt som disse oplysninger er nødvendige for at forstå evalueringens omfang
   e) sikkerhedsmålsætningerne må ikke begrænses, da alle oplysninger skal offentliggøres for at forstå hensigten med sikkerhedsmålet og evalueringsmålet
   f) alle sikkerhedskrav skal offentliggøres. Bemærkninger i ansøgningen kan indeholde oplysninger om, hvordan funktionskravene i de fælles kriterier, jf. artikel 3, er blevet anvendt til at forstå sikkerhedsmålet
   g) resuméet af specifikationerne for evalueringsmålet skal omfatte alle evalueringsmålets sikkerhedsfunktioner, men yderligere ejendomsretligt beskyttede oplysninger må gerne renses
   h) der skal medtages henvisninger til beskyttelsesprofiler, der er anvendt på evalueringsmålet
   i) rationalet kan renses for at udlade ejendomsretligt beskyttede oplysninger.

4. Selv om det rensede sikkerhedsmål ikke formelt er evalueret i overensstemmelse med de evalueringsstandarder, der er omhandlet i artikel 3, sikrer certificeringsorganet, at det opfylder det fuldstændige og evaluerede sikkerhedsmål, og at der henvises til både det fuldstændige og det rensede sikkerhedsmål i certificeringsrapporten.

BILAG VI

OMFANG OG SAMMENSÆTNING AF TEAM MED HENBLIK PÅ PEERVURDERINGER

VI.1 **Peervurderingens omfang**

1. Følgende typer peervurderinger er omfattet:

   a) Type 1: når et certificeringsorgan udfører certificeringsaktiviteter på AVA_VAN.3-niveau

   b) Type 2: når et certificeringsorgan udfører certificeringsaktiviteter vedrørende et teknisk område, der er opført som statusdokumenter i bilag I

   c) Type 3: når et certificeringsorgan udfører certificeringsaktiviteter over AVA_VAN.3-niveau ved brug af en beskyttelsesprofil, der er opført som statusdokumenter i bilag II eller III.

2. Det peervurderede certificeringsorgan indsender listen over certificerede IKT-produkter, der eventuelt skal revideres af peervurderingsteamet (»kandidatprodukter«), i overensstemmelse med følgende regler:

   a) kandidatprodukterne skal dække det tekniske anvendelsesområde for certificeringsorganets bemyndigelse, hvoraf mindst to forskellige produktevalueringer på tillidsniveauet »højt« vil blive analyseret ved peervurdering, og én beskyttelsesprofil, hvis certificeringsorganet har udstedt en attest på tillidsniveauet »højt«

   b) for en type 2-peervurdering indsender certificeringsorganet mindst ét produkt pr. teknisk område og pr. berørt ITSEF

   c) for en type 3-peervurdering evalueres mindst ét kandidatprodukt i overensstemmelse med en gældende og relevant beskyttelsesprofil.

VI.2 **Peervurderingsteam**

1. Vurderingsteamet skal bestå af mindst to eksperter, der hver udvælges fra et forskelligt certificeringsorgan fra forskellige medlemsstater, der udsteder attester på tillidsniveauet »højt«. Eksperterne bør godtgøre, at de har den relevante ekspertise inden for de standarder, der er omhandlet i artikel 3, og de statusdokumenter, der er omfattet af peervurderingen.

2. Hvis udstedelse af attester eller forudgående godkendelse af attester som omhandlet i artikel 56, stk. 6, i forordning (EU) 2019/881 uddelegeres, skal en ekspert fra den nationale cybersikkerhedscertificeringsmyndighed, som er tilknyttet det pågældende certificeringsorgan, desuden deltage i det ekspertteam, der er udvalgt i overensstemmelse med punkt 1 i dette afsnit.

3. For en type 2-peervurdering udvælges teammedlemmerne blandt certificeringsorganer med bemyndigelse inden for det pågældende tekniske område.

4. Hvert medlem af vurderingsteamet skal have mindst to års erfaring med certificeringsaktiviteter i et certificeringsorgan

5. I forbindelse med en type 2- eller 3-peervurdering skal hvert medlem af vurderingsteamet have mindst to års erfaring med certificeringsaktiviteter inden for det pågældende relevante tekniske område eller den pågældende relevante beskyttelsesprofil og dokumenteret ekspertise og deltagelse i bemyndigelsen af en ITSEF

6. Den nationale cybersikkerhedscertificeringsmyndighed, der overvåger og fører tilsyn med det peervurderede certificeringsorgan, og mindst én national cybersikkerhedscertificeringsmyndighed, hvis certificeringsorgan ikke er underlagt peervurderingen, deltager i peervurderingen som observatør. ENISA kan også deltage i peervurderingen som observatør.

7. Det peervurderede certificeringsorgan forelægges peervurderingsteamets sammensætning. I begrundede tilfælde kan det anfægte peervurderingsteamets sammensætning og anmode om en revision heraf.

BILAG VII

EUCC-attestens indhold

EUCC-attesten skal som minimum indeholde:

a) en entydig identifikator, der er fastlagt af det certificeringsorgan, der udsteder attesten

b) oplysninger vedrørende det certificerede IKT-produkt eller den certificerede beskyttelsesprofil og attestindehaveren, herunder:

   1) navnet på IKT-produktet eller beskyttelsesprofilen og, hvor det er relevant, evalueringsmålet

   2) typen af IKT-produkt eller beskyttelsesprofil og, hvor det er relevant, evalueringsmål

   3) version af IKT-produktet eller beskyttelsesprofilen

   4) navn og kontaktoplysninger på attestindehaveren

   5) link til attestindehaverens websted med de supplerende cybersikkerhedsoplysninger, der er omhandlet i artikel 55 i forordning (EU) 2019/881

c) oplysninger vedrørende evaluering og certificering af IKT-produktet eller beskyttelsesprofilen, herunder:

   1) navn og kontaktoplysninger på det certificeringsorgan, der udstedte attesten

   2) navnet på den ITSEF, der har foretaget evalueringen, hvis denne er forskellig fra certificeringsorganet

   3) navnet på den ansvarlige nationale cybersikkerhedscertificeringsmyndighed

   4) en henvisning til denne forordning

   5) en henvisning til den certificeringsrapport, der er knyttet til den attest, der er omhandlet i bilag V

   6) det relevante tillidsniveau i henhold til artikel 4

   7) en henvisning til den version af standarder, der er anvendt til evalueringen som omhandlet i artikel 3

   8) identifikation af det tillidsniveau eller den pakke, der er anført i de standarder, der er omhandlet i artikel 3, og i overensstemmelse med bilag VIII, herunder de anvendte sikkerhedskomponenter og det AVA_VAN-niveau, der er omfattet

   9) hvis det er relevant, henvisning til en eller flere beskyttelsesprofiler, som IKT-produktet eller beskyttelsesprofilen er i overensstemmelse med

   10) udstedelsesdato

   11) attestens gyldighedsperiode

d) den mærkning og etiket, der er knyttet til attesten, jf. artikel 11.

BILAG VIII

Erklæring om tillidspakke

1. I modsætning til definitionerne i de fælles kriterier:

a) må en forøgelse ikke betegnes med forkortelsen »+«

b) skal en forøgelse beskrives med en liste over alle berørte komponenter

c) skal en forøgelse beskrives i detaljer i certificeringsrapporten.

2. Det tillidsniveau, der bekræftes i en EUCC-attest, kan suppleres med det evalueringstillidsniveau, der er fastsat i denne forordnings artikel 3.

3. Hvis det tillidsniveau, der bekræftes i en EUCC-attest, ikke henviser til en forøgelse, skal EUCC-attesten angive en af følgende pakker:

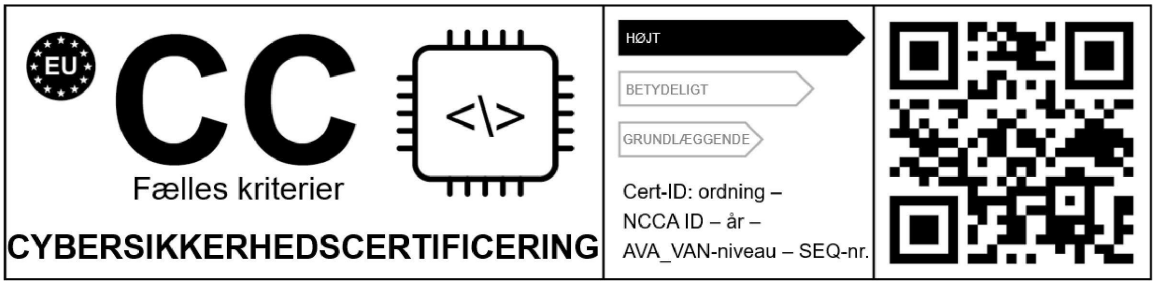
a) »den specifikke tillidspakke«

b) »den tillidspakke, der er i overensstemmelse med en beskyttelsesprofil«, hvis der henvises til en beskyttelsesprofil uden et evalueringstillidsniveau.

BILAG IX

Mærkning og etiketter

1. Mærkningens og etikettens form:



2. Hvis mærkningen og etiketten formindskes eller forstørres, skal størrelsesforhold i tegningen ovenfor overholdes.

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