2024/3144

19.12.2024

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2024/3144

af 18. december 2024

om ændring af gennemførelsesforordning (EU) 2024/482 for så vidt angår gældende internationale standarder og om berigtigelse af nævnte gennemførelsesforordning

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

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

ud fra følgende betragtninger:

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

(2) Gennemførelsesforordning (EU) 2024/482 er baseret på etablerede internationale standarder i form af de fælles kriterier og den fælles evalueringsmetode, der forvaltes af Den Internationale Standardiseringsorganisation (ISO) og Den Internationale Elektrotekniske Kommission (IEC). Der henvises i gennemførelsesforordning (EU) 2024/482 til ISO/IEC-standarder, men den gældende version af disse standarder er ikke præciseret. Det bør derfor præciseres, hvilken udgave af standarderne der gælder for attester udstedt i henhold til EUCC.

(3) De statslige organisationer, der har bidraget til udviklingen af de fælles kriterier og den fælles evalueringsmetode gennem ordningen for anerkendelse af attester baseret på fælles kriterier inden for IT-sikkerhed (Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security — CCRA), er sammen med ISO/IEC fælles indehavere af ophavsrettighederne til dem. Disse statslige organisationer bevarer retten til at anvende dem. I lyset af betydningen af de dokumenter, der hidrører fra CCRA, bør de også danne grundlag for certificering i henhold til EUCC.

(4) De fælles kriterier og standarderne i den fælles evalueringsmetode er genstand for fortolkninger foretaget af CCRA, som letter deres gennemførelse, og som kan tages i betragtning af faciliteter til evaluering af informationsteknologisk sikkerhed (ITSEF'er) og certificeringsorganer.

(5) De internationale standarder i forbindelse med de fælles kriterier kan blive ajourført. For at sikre en velordnet og rettidig overgang er det hensigtsmæssigt at fastlægge overgangsregler for at give leverandører, ITSEF'er og certificeringsorganer samt andre relevante aktører tilstrækkelig tid til at foretage de nødvendige tilpasninger. Sådanne overgangsregler bør i passende omfang være i overensstemmelse med global praksis såsom den, der er fastsat af CCRA.

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

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

(6) Gennemførelsesforordning (EU) 2024/482 indeholder ikke nogen præcis angivelse af, hvornår en given IKT-produktcertificering ikke længere kan baseres på de tidligere udgaver af de fælles kriterier og standarderne i den fælles evalueringsmetode. De tekniske områder og beskyttelsesprofiler, der er opført i bilag I, II og III til nævnte gennemførelsesforordning, er baseret på tidligere udgaver af standarderne ISO/IEC 15408 og 18045. Det bør i gennemførelsesforordning (EU) 2024/482 derfor præciseres, under hvilke omstændigheder den tidligere udgave af de fælles kriterier og den fælles evalueringsmetode stadig finder anvendelse, og hvordan overgangen til den seneste udgave af de internationale standarder vil fungere.

(7) I overgangsperioden bør det være en prioritet for relevante interessenter at ajourføre de relevante tekniske områder og beskyttelsesprofiler. Gennemførelsesforordning (EU) 2024/482 bør indeholde bestemmelser om, at sikkerhedsmål baseret på en tidligere udgave af standarderne vil blive accepteret frem til den 31. december 2027 i overensstemmelse med den overgangspolitik, som CCRA har vedtaget. Det skal dog bemærkes, at CCRA's overgangspolitik omfatter indledende evalueringer af produkter og beskyttelsesprofiler, der påbegyndtes senest den 30. juni 2024, og at EUCC endnu ikke fandt anvendelse på denne dato. I overensstemmelse med CCRA's overgangspolitik bør gennemførelsesforordning (EU) 2024/482 desuden indeholde bestemmelser om, at sikkerhedsmål, der er i overensstemmelse med nævnte gennemførelsesforordning, og som påberåbes at være i overensstemmelse med beskyttelsesprofiler baseret på en tidligere udgave af standarderne, vil blive accepteret frem til den 31. december 2027. Hvis en ny attest udstedes i henhold til gennemførelsesforordning (EU) 2024/482 i forbindelse med en revision af en national attest, der påbegyndes senest to år efter udstedelsen af den oprindelige attest, bør det desuden være muligt at anvende en tidligere udgave af standarderne. Dette vil ikke være relevant for en revisionsproces, der ikke kræver udstedelse af en ny attest i henhold til gennemførelsesforordning (EU) 2024/482, og hvor attesten forbliver gyldig.

(8) Med henblik på at sikre en velordnet overgang til den seneste udgave af standarderne bør gennemførelsesforordning (EU) 2024/482 indeholde specifikke overgangsregler og fortsat give mulighed for i henhold til nævnte gennemførelsesforordning at udstede attester, der påberåbes at være i overensstemmelse med beskyttelsesprofiler, som er baseret på tidligere udgaver af de standarder, som CCRA har offentliggjort, hvor anvendelsen af sådanne beskyttelsesprofiler er påkrævet i henhold til EU-lovgivningen. Dette er tilfældet for Kommissionens gennemførelsesforordning (EU) 2016/799 ([3]) samt Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 ([4]) og Kommissionens gennemførelsesafgørelse (EU) 2016/650 ([5]).

(9) Bilag I til gennemførelsesforordning (EU) 2024/482 indeholder en liste over de gældende statusdokumenter til evaluering af IKT-produkter og beskyttelsesprofiler. Det præciseres imidlertid ikke på listen, hvilken version af dokumenterne der skal anvendes. Det bør derfor præciseres, hvilken version af dokumenterne der gælder for attester udstedt i henhold til EUCC. Disse versioner bygger på dokumenter, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe (ECCG), samtidig med at de er blevet revideret yderligere med henblik på deres medtagelse i EUCC. Desuden bør bilag I ændres, så det omfatter ajourførte og nye statusdokumenter efter ECCG's godkendelse heraf, således at der sikres en ensartet akkreditering af overensstemmelsesvurderingsorganer i henhold til EUCC. Akkrediteringskravene i forbindelse med akkreditering af ITSEF'er bør ajourføres for at præcisere anvendelsen af kriterierne om uafhængighed og upartiskhed, og der bør udarbejdes et nyt statusdokument til akkreditering af certificeringsorganer.

(10) Statusdokumenter kan tilføjes EUCC eller ajourføres i forbindelse med dens vedligeholdelsesaktiviteter. For nye eller ajourførte statusdokumenter kan det være nødvendigt at fastsætte passende overgangsregler for at gøre det muligt for leverandører, ITSEF'er, certificeringsorganer og andre interessenter at foretage de nødvendige tilpasninger. Med henblik på ajourføring af statusdokumentet vedrørende akkreditering af ITSEF'er bør det ajourførte dokument først finde anvendelse på akkrediteringer, der er udstedt før den 8. juli 2025, når de revideres, f.eks. i forbindelse med en vurderingsprocedure eller en procedure for fornyet vurdering. Desuden bør det ajourførte dokument finde anvendelse på alle akkrediteringer af ITSEF'er, der er udstedt efter den 8. juli 2025.

([3]) Kommissionens gennemførelsesforordning (EU) 2016/799 af 18. marts 2016 om gennemførelse af Europa-Parlamentets og Rådets forordning (EU) nr. 165/2014 om fastsættelse af forskrifter for konstruktion, afprøvning, installering, brug og reparation af takografer og deres komponenter (EUT L 139 af 26.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

([4]) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([5]) Kommissionens gennemførelsesafgørelse (EU) 2016/650 af 25. april 2016 om fastlæggelse af standarder for sikkerhedsvurdering af kvalificerede signatur- og seglgenereringssystemer, jf. artikel 30, stk. 3, og artikel 39, stk. 2, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (EUT L 109 af 26.4.2016, s. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Yderligere berigtigelser af artikel 5, 8, 16, 29 og 44 i gennemførelsesforordning (EU) 2024/482 og bilag IV hertil bidrager til at sikre en ensartet ordlyd og en klar juridisk fortolkning.

(12) Reglerne for anmeldelse af overensstemmelsesvurderingsorganer bør fastsættes horisontalt for alle ordninger under den europæiske ramme for cybersikkerhedscertificering. Disse regler for anmeldelse fastlægges i Kommissionens gennemførelsesforordning (EU) 2024/3143 ([6]). Derfor bør artikel 23 og 24 i gennemførelsesforordning (EU) 2024/482 udgå på anvendelsesdatoen for Kommissionens gennemførelsesforordning (EU) 2024/3143.

(13) Gennemførelsesforordning (EU) 2024/482 bør derfor ændres og berigtiges.

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

VEDTAGET DENNE FORORDNING:

Artikel 1

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

1) Artikel 2, nr. 1) og 2), affattes således:

»1) »fælles kriterier«: de fælles kriterier for evaluering af informationsteknologisikkerhed som fastsat i ISO-standarderne IISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 eller ISO/IEC 15408-5:2022 eller som fastsat i de fælles kriterier for evaluering af informationsteknologisikkerhed, version CC:2022, del 1-5, offentliggjort af deltagerne i ordningen for anerkendelse af attester baseret på fælles kriterier inden for IT-sikkerhed

2) »fælles evalueringsmetode«: den fælles metode til evaluering af informationsteknologisikkerhed som fastsat i ISO-standarden ISO/IEC 18045:2022 eller den fælles metode til informationsteknologisk sikkerhedsevaluering, version CEM:2022, offentliggjort af deltagerne i ordningen for anerkendelse af attester baseret på fælles kriterier inden for IT-sikkerhed«

2) Artikel 3 affattes således:

»*Artikel 3*

Evalueringsstandarder

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

a) de fælles kriterier

b) den fælles evalueringsmetode.

2. Indtil den 31. december 2027 kan der udstedes attester i henhold til EUCC-ordningen med anvendelse af en af følgende standarder:

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

b) fælles kriterier for evaluering af informationsteknologisikkerhed, version 3.1, revision 5, offentliggjort af deltagerne i ordningen for anerkendelse af attester baseret på fælles kriterier inden for IT-sikkerhed

([6]) Kommissionens gennemførelsesforordning (EU) 2024/3143 af 18. december 2024 om fastlæggelse af vilkår, formater og procedurer for anmeldelser i henhold til artikel 61, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) 2019/881 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed) og om cybersikkerhedscertificering af informations- og kommunikationsteknologi (EUT L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

c) ISO/IEC 18045:2008

d) fælles metode til evaluering af informationsteknologisikkerhed, revision 5, version 3.1, offentliggjort af deltagerne i ordningen for anerkendelse af attester baseret på fælles kriterier inden for IT-sikkerhed.

3. Indtil den 31. december 2027 kan der i henhold til EUCC-ordningen udstedes en attest, der anvender de standarder, der er omhandlet i stk. 1, og som påberåbes at være i overensstemmelse med en beskyttelsesprofil, der har anvendt de standarder, der er anført i stk. 2.

4. Der kan også i henhold til EUCC-ordningen udstedes en attest, der anvender de standarder, der er omhandlet i stk. 1, og som påberåbes at være i overensstemmelse med en beskyttelsesprofil, der har anvendt en af følgende standarder, forudsat at anvendelsen af en sådan beskyttelsesprofil er påkrævet i henhold til Kommissionens gennemførelsesforordning (EU) 2016/799 (*), Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 (**) eller Kommissionens gennemførelsesafgørelse (EU) 2016/650 (***):

a) fælles kriterier for evaluering af informationsteknologisikkerhed, version 3.1, revision 1-4, offentliggjort af deltagerne i ordningen for anerkendelse af attester baseret på fælles kriterier inden for IT-sikkerhed

b) fælles metode til evaluering af informationsteknologisikkerhed, version 3.1, revision 1-4, offentliggjort af deltagerne i ordningen for anerkendelse af attester baseret på fælles kriterier inden for IT-sikkerhed.

_____

(*) Kommissionens gennemførelsesforordning (EU) 2016/799 af 18. marts 2016 om gennemførelse af Europa-Parlamentets og Rådets forordning (EU) nr. 165/2014 om fastsættelse af forskrifter for konstruktion, afprøvning, installering, brug og reparation af takografer og deres komponenter (EUT L 139 af 26.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Kommissionens gennemførelsesafgørelse (EU) 2016/650 af 25. april 2016 om fastlæggelse af standarder for sikkerhedsvurdering af kvalificerede signatur- og seglgenereringssystemer, jf. artikel 30, stk. 3, og artikel 39, stk. 2, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (EUT L 109 af 26.4.2016, s. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).«

3) Følgende indsættes som artikel 20a i kapitel IV:

»*Artikel 20a*

Specifikation af kravene til akkreditering af overensstemmelsesvurderingsorganer

Ved akkrediteringen af overensstemmelsesvurderingsorganer skal der tages hensyn til specifikationen af kravene til akkreditering af certificeringsorganer og ITSEF'er som fastsat i de relevante statusdokumenter, der er anført i punkt 2 i bilag I.«

4) Artikel 23 og 24 udgår

5) I artikel 48 tilføjes følgende som stk. 4:

»4. Medmindre andet er fastsat i bilag I eller II, finder statusdokumenter anvendelse fra anvendelsesdatoen for den ændringsretsakt, ved hvilken de er blevet indarbejdet i bilag I eller II.«

6) I artikel 49 tilføjes følgende som stk. 4:

»4. De i artikel 3, stk. 2, anførte standarder kan anvendes i forbindelse med den revision, der er omhandlet i stk. 3, senest to år efter udstedelsen af den oprindelige attest, hvor en sådan revision fører til udstedelsen af en ny attest i overensstemmelse med denne forordning. Udstedelsesdatoen for den oprindelige attest skal forstås som udstedelsesdatoen for den seneste attest for det pågældende IKT-produkt eller en beskyttelsesprofil, som den nuværende attest er baseret på.«

7) Bilag I erstattes af teksten i bilag I til nærværende forordning

8) Bilag IV ændres i overensstemmelse med bilag II til denne forordning.

Artikel 2

Gennemførelsesforordning (EU) 2024/482 berigtiges således:

1) Artikel 5, stk. 1, litra b), affattes således:

»b) ved at påberåbe overensstemmelse med 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) Artikel 8 berigtiges således:

a) Titlen affattes således:

»Oplysninger, der er nødvendige for certificering og evaluering«

b) Stk. 1 affattes således:

»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 certificerings- og evalueringsaktiviteterne, til rådighed for certificeringsorganet og ITSEF.«

3) Artikel 16 affattes således:

»*Artikel 16*

Oplysninger, der er nødvendige for certificering og vurdering 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 certificerings- og vurderingsaktiviteterne, til rådighed for certificeringsorganet og ITSEF'en i fuldstændig og korrekt form. Artikel 8, stk. 2, 3, 4 og 7, finder tilsvarende anvendelse.«

4) Artikel 17, stk. 1, udgår

5) Artikel 29, stk. 2, affattes således:

»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 eller 20.«.

Artikel 3

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

Artikel 1, stk. 4, finder anvendelse fra den 8. januar 2025.

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

Udfærdiget i Bruxelles, den 18. december 2024.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG I

»»*BILAG I*

Statusdokumenter til støtte for tekniske områder og andre statusdokumenter

1. Statusdokumenter til støtte for tekniske områder på AVA_VAN-niveau 4 eller 5:

   a) følgende dokumenter vedrørende den harmoniserede evaluering af det tekniske område »smartcards og lignende enheder«:

      (1) »Minimum ITSEF requirements for security evaluations of smart cards and similar devices« (minimumskrav til sikkerhedsevalueringer af smartcards og lignende enheder), version 1.1

      (2) »Minimum Site Security Requirements« (minimumssikkerhedskrav til sikkerhed på stedet), version 1.1

      (3) »Application of Common Criteria to integrated circuits« (anvendelse af fælles kriterier på integrerede kredsløb), version 1.1

      (4) »Security Architecture requirements (ADV_ARC) for smart cards and similar devices« (krav til sikkerhedsarkitektur (ADV_ARC) for smartcards og lignende enheder), version 1.1

      (5) »Certification of »open« smart card products« (certificering af »åbne« smartcardprodukter), version 1.1

      (6) »Composite product evaluation for smart cards and similar devices« (evaluering af sammensatte produkter til smartcards og lignende enheder), version 1.1

      (7) »Application of Attack Potential to Smartcards and Similar Devices« (anvendelse af angrebspotentiale på smartcards og lignende enheder), version 1.2.

   b) følgende dokumenter vedrørende den harmoniserede evaluering af det tekniske område »hardwareenheder med sikkerhedsbokse«:

      (1) »Minimum ITSEF requirements for security evaluations of hardware devices with security boxes« (minimumskrav til sikkerhedsevalueringer af hardwareenheder med sikkerhedsbokse), version 1.1

      (2) »Minimum Site Security Requirements« (minimumssikkerhedskrav til sikkerhed på stedet), version 1.1

      (3) »Application of Attack Potential to hardware devices with security boxes« (anvendelse af angrebspotentiale på hardwareenheder med sikkerhedsbokse), version 1.2.

2. Statusdokumenter vedrørende harmoniseret akkreditering af overensstemmelsesvurderingsorganer:

   a) »Accreditation of ITSEFs for the EUCC« (akkreditering af ITSEF'er med henblik på EUCC), version 1.1 for akkrediteringer udstedt før den 8. juli 2025.

   b) »Accreditation of ITSEFs for the EUCC« (akkreditering af ITSEF'er med henblik på EUCC), version 1.6c for nyudstedte akkrediteringer eller akkrediteringer, der revideres efter den 8. juli 2025.

   c) »Accreditation of CBs for the EUCC« (akkreditering af certificeringsorganer med henblik på EUCC), version 1.6b.««

BILAG II

Bilag IV til gennemførelsesforordning (EU) 2024/482, afsnit IV.3, punkt 5 og 6, affattes således:

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

Vedligeholdelsesrapporten skal indgå som en del af konsekvensanalyserapporten med følgende afsnit:

a) indledning

b) beskrivelse af ændringerne

c) hvilken af udviklerens dokumentation, der påvirkes.

6. Den i punkt 5 omhandlede vedligeholdelsesrapport fremsendes til ENISA med henblik på offentliggørelse på dets cybersikkerhedscertificeringswebsted.«