Europeiska unionens
officiella tidning

SV
L-serien

2024/3144

19.12.2024

# KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2024/3144

**av den 18 december 2024**

**om ändring av genomförandeförordning (EU) 2024/482 vad gäller tillämpliga internationella standarder och om rättelse av den genomförandeförordningen**

**(Text av betydelse för EES)**

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) ([1]), särskilt artikel 49.7, och

av följande skäl:

(1) Genom kommissionens genomförandeförordning (EU) 2024/482 ([2]) specificeras rollerna, reglerna och skyldigheterna samt strukturen för den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC) i enlighet med det europeiska ramverk för cybersäkerhetscertifiering som fastställs i förordning (EU) 2019/881.

(2) Genomförandeförordning (EU) 2024/482 är baserad på etablerade internationella standarder, dvs. Common Criteria och den gemensamma evalueringsmetodik som upprätthålls av Internationella standardiseringsorganisationen (ISO) och Internationella elektrotekniska kommissionen (IEC). Genomförandeförordning (EU) 2024/482 hänvisar till ISO/IEC-standarder, men specificerar inte den tillämpliga versionen av standarderna. Det bör därför specificeras vilken version av standarderna som är tillämplig på certifikat som utfärdas inom ramen för EUCC.

(3) De statliga organisationer som har bidragit till utvecklingen av Common Criteria och den gemensamma evalueringsmetodiken genom Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security (CCRA) är tillsammans med ISO/IEC gemensamma innehavare av upphovsrätten till standarderna. Dessa statliga organisationer behåller rätten att använda dem. Med tanke på betydelsen av dessa dokument som härrör från CCRA bör de också ligga till grund för certifiering inom ramen för EUCC.

(4) Standarderna Common Criteria och den gemensamma evalueringsmetodiken är föremål för tolkningar som görs av CCRA vilka underlättar genomförandet av dem och kan beaktas av faciliteterna för utvärdering av informationsteknologisk säkerhet (ITSEF) och certifieringsorgan.

(5) Internationella standarder med anknytning till Common Criteria kan komma att uppdateras. För att säkerställa en ordnad övergång i rätt tid är det lämpligt att fastställa övergångsregler för att ge säljare, ITSEF:er och certifieringsorgan och andra berörda aktörer tillräckligt med tid för de nödvändiga justeringarna. Övergångsreglerna bör i lämplig utsträckning anpassas till global praxis, såsom den som fastställts av CCRA.

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

([2]) Kommissionens genomförandeförordning (EU) 2024/482 av den 31 januari 2024 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(6) I genomförandeförordning (EU) 2024/482 anges inte hur länge en IKT-produktcertifiering kan baseras på tidigare versioner av standarderna Common Criteria och den gemensamma evalueringsmetodiken. De teknikdomäner och skyddsprofiler som förtecknas i bilagorna I, II och III till den genomförandeförordningen är baserade på tidigare versioner av standarderna ISO/IEC 15408 och 18045. Genomförandeförordning (EU) 2024/482 bör därför specificera under vilka omständigheter den tidigare versionen av Common Criteria och den gemensamma evalueringsmetodiken fortfarande är tillämplig och hur övergången till den senaste versionen av de internationella standarderna kommer att fungera.

(7) Under övergångsperioden bör det vara en prioritering för berörda parter att uppdatera de relevanta teknikdomänerna och skyddsprofilerna. I genomförandeförordning (EU) 2024/482 bör det anges att säkerhetsmål som är baserade på en tidigare version av standarderna kommer att godtas fram till den 31 december 2027 i linje med den övergångspolicy som antagits av CCRA. Det bör dock noteras att CCRA:s övergångspolicy omfattar inledande evalueringar av produkter och skyddsprofiler som skulle inledas senast den 30 juni 2024, ett datum då EUCC ännu inte var tillämpligt. Dessutom bör genomförandeförordning (EU) 2024/482 i enlighet med CCRA:s övergångspolicy föreskriva att säkerhetsmål som överensstämmer med den genomförandeförordningen med åberopande av överensstämmelse med skyddsprofiler som är baserade på en tidigare version av standarderna godtas fram till den 31 december 2027. Om ett nytt certifikat utfärdas enligt genomförandeförordning (EU) 2024/482 i samband med en översyn av ett nationellt certifikat vilken inleds inom två år från det ursprungliga certifikatet bör det dessutom vara möjligt att använda en tidigare version av standarderna. Detta är inte relevant för en översyn som inte kräver utfärdande av ett nytt certifikat enligt genomförandeförordning (EU) 2024/482 och där certifikatet förblir giltigt.

(8) I syfte att säkerställa en ordnad övergång till den senaste versionen av standarderna bör genomförandeförordning (EU) 2024/482 föreskriva särskilda övergångsregler och fortsätta att göra det möjligt att utfärda certifikat enligt den genomförandeförordningen med åberopande av överensstämmelse med skyddsprofiler som är baserade på tidigare versioner av de standarder som offentliggjorts av CCRA när användningen av sådana skyddsprofiler krävs enligt unionslagstiftningen. Detta gäller kommissionens genomförandeförordning (EU) 2016/799 ([3]), Europaparlamentets och rådets förordning (EU) nr 910/2014 ([4]) och kommissionens genomförandebeslut (EU) 2016/650 ([5]).

(9) I bilaga I till genomförandeförordning (EU) 2024/482 förtecknas tillämpliga mönsterdokument för evaluering av IKT-produkter och skyddsprofiler. Där anges dock inte den specifika versionen av dokumenten. Det bör därför specificeras vilken version av dokumenten som är tillämplig på certifikat som utfärdas inom ramen för EUCC. Dessa versioner bygger på dokument som godkänts av den europeiska gruppen för cybersäkerhetscertifiering, och har sedan genomgått ytterligare granskning för att inkluderas i EUCC. Bilaga I bör vidare ändras så att den omfattar uppdaterade och nya mönsterdokument som har godkänts av den europeiska gruppen för cybersäkerhetscertifiering, så att en enhetlig ackreditering av organ för bedömning av överensstämmelse inom ramen för EUCC säkerställs. Ackrediteringskraven i samband med ackreditering av ITSEF:er bör uppdateras för att klargöra tillämpningen av kriterierna oberoende och opartiskhet, och ett nytt mönsterdokument bör fastställas för ackreditering av certifieringsorgan.

(10) Mönsterdokument kan tilläggas till EUCC eller bli föremål för uppdateringar i samband med dess underhållsverksamhet. För nya eller uppdaterade mönsterdokument kan lämpliga övergångsregler behöva fastställas för att göra det möjligt för säljare, ITSEF:er, certifieringsorgan och andra berörda parter att göra nödvändiga anpassningar. För uppdateringen av det mönsterdokument som rör ackreditering av ITSEF:er bör det uppdaterade dokumentet tillämpas på ackrediteringar som utfärdats före den 8 juli 2025 först när de har setts över, till exempel i samband med ett förfarande för bedömning eller ny bedömning. Det uppdaterade dokumentet bör dessutom tillämpas på alla ackrediteringar av ITSEF:er som utfärdats efter den 8 juli 2025.

([3]) Kommissionens genomförandeförordning (EU) 2016/799 av den 18 mars 2016 om genomförande av Europaparlamentets och rådets förordning (EU) nr 165/2014 när det gäller krav för konstruktion, provning, installation, drift och reparation av färdskrivare och deras komponenter (EUT L 139, 26.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

([4]) Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([5]) Kommissionens genomförandebeslut (EU) 2016/650 av den 25 april 2016 om fastställande av standarder för säkerhetsbedömning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplar enligt artiklarna 30.3 och 39.2 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (EUT L 109, 26.4.2016, s. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Ytterligare korrigeringar av artiklarna 5, 8, 16, 29 och 44 i genomförandeförordning (EU) 2024/482 samt bilaga IV till den bidrar till att säkerställa en enhetlig ordalydelse och en tydlig rättslig tolkning.

(12) Reglerna om anmälningar av organen för bedömning av överensstämmelse bör fastställas horisontellt för alla ordningar inom det europeiska ramverket för cybersäkerhetscertifiering. Sådana anmälningsregler finns i kommissionens genomförandeförordning (EU) 2024/3143 ([6]). Artiklarna 23 och 24 i genomförandeförordning (EU) 2024/482 bör därför utgå den dag genomförandeförordning (EU) 2024/3143 blir tillämplig.

(13) Genomförandeförordning (EU) 2024/482 bör därför ändras och rättas i enlighet med detta.

(14) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté som inrättats genom artikel 66 i förordning (EU) 2019/881.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

*Artikel 1*

Genomförandeförordning (EU) 2024/482 ska ändras på följande sätt:

1. I artikel 2 ska leden 1 och 2 ersättas med följande:

"(1) *Common Criteria*: de gemensamma kriterierna för utvärdering av informationsteknologisk säkerhet, enligt standarderna ISO/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 enligt de gemensamma kriterierna för utvärdering av informationsteknologisk säkerhet version CC:2022, delarna 1–5, som offentliggjorts av deltagarna i Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security.

(2) *gemensam evalueringsmetodik*: den gemensamma metoden för utvärdering av informationsteknologisk säkerhet, enligt standarden ISO/IEC 18045:2022, eller den gemensamma metoden för utvärdering av informationsteknologisk säkerhet version CEM:2022, som offentliggjorts av deltagarna i Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security."

2. Artikel 3 ska ersättas med följande:

"*Artikel 3*

**Evalueringsstandarder**

1. Följande standarder ska tillämpas på evalueringar som utförs enligt EUCC-ordningen:

a) Common Criteria.

b) Den gemensamma evalueringsmetodiken.

2. Till och med den 31 december 2027 får ett certifikat utfärdas inom ramen för EUCC-ordningen enligt någon av följande standarder:

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

b) De gemensamma kriterierna för utvärdering av informationsteknologisk säkerhet version 3.1 revision 5, offentliggjord av deltagarna i Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security.

([6]) Kommissionens genomförandeförordning (EU) 2024/3143 av den 18 december 2024 om fastställande av förutsättningar, format och förfaranden för anmälningar enligt artikel 61.5 i Europaparlamentets och rådets förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (EUT L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

c) ISO/IEC 18045:2008.

d) Den gemensamma metoden för utvärdering av informationsteknologisk säkerhet version 3.1 revision 5, offentliggjord av deltagarna i Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security.

3. Till och med den 31 december 2027 får ett certifikat som tillämpar de standarder som avses i punkt 1 utfärdas inom ramen för EUCC-ordningen med åberopande av överensstämmelse med en skyddsprofil som har tillämpat de standarder som förtecknas i punkt 2.

4. Ett certifikat som tillämpar de standarder som avses i punkt 1 får också utfärdas inom ramen för EUCC-ordningen med åberopande av överensstämmelse med en skyddsprofil som har tillämpat någon av följande standarder, förutsatt att användning av en sådan skyddsprofil krävs enligt kommissionens genomförandeförordning (EU) 2016/799 (*), Europaparlamentets och rådets förordning (EU) nr 910/2014 (**) eller kommissionens genomförandebeslut (EU) 2016/650 (***):

a) De gemensamma kriterierna för utvärdering av informationsteknologisk säkerhet version 3.1 revision 1–4, offentliggjord av deltagarna i Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security.

b) Den gemensamma metoden för utvärdering av informationsteknologisk säkerhet version 3.1 revision 1–4, offentliggjord av deltagarna i Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security.

---

(*) Kommissionens genomförandeförordning (EU) 2016/799 av den 18 mars 2016 om genomförande av Europaparlamentets och rådets förordning (EU) nr 165/2014 när det gäller krav för konstruktion, provning, installation, drift och reparation av färdskrivare och deras komponenter (EUT L 139, 26.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Kommissionens genomförandebeslut (EU) 2016/650 av den 25 april 2016 om fastställande av standarder för säkerhetsbedömning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplar enligt artiklarna 30.3 och 39.2 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (EUT L 109, 26.4.2016, s. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).”

3. I kapitel IV ska följande artikel införas som artikel 20a:

”*Artikel 20a*

**Specificering av kraven för ackreditering av organ för bedömning av överensstämmelse**

Vid ackreditering av organ för bedömning av överensstämmelse ska hänsyn tas till specificeringen av krav för ackreditering av certifieringsorgan och ITSEF:er som fastställs i de tillämpliga mönsterdokument som förtecknas i punkt 2 i bilaga I.”

4. Artiklarna 23 och 24 ska utgå.

5. I artikel 48 ska följande punkt läggas till som punkt 4:

”4. Om inget annat anges i bilaga I eller II ska mönsterdokumenten tillämpas från och med den dag då den ändringsakt genom vilken de har införlivats i bilaga I eller II börjar tillämpas.”

6. I artikel 49 ska följande punkt läggas till som punkt 4:

”4. Om den översyn som avses i punkt 3 genomförs inom två år från utfärdandet av det ursprungliga certifikatet och om översynen leder till att ett nytt certifikat utfärdas i enlighet med denna förordning, får de standarder som förtecknas i artikel 3.2 tillämpas. Datumet för utfärdande av det ursprungliga certifikatet ska förstås som datumet för utfärdande av det senaste certifikatet för en IKT-produkt eller IKT-skyddsprofil vilket den nuvarande certifieringen är baserad på.”

7. Bilaga I ska ersättas med texten i bilaga I till den här förordningen.

8. Bilaga IV ska ändras i enlighet med bilaga II till den här förordningen.

*Artikel 2*

Genomförandeförordning (EU) 2024/482 ska rättas på följande sätt:

1. I artikel 5.1 ska led b ersättas med följande:

   ”b) uppges stämma överens med en certifierad skyddsprofil som ett led i IKT-processen, där IKT-produkten ingår i den IKT-produktkategori som omfattas av den skyddsprofilen.”

2. Artikel 8 ska rättas på följande sätt:

   a) Titeln ska ersättas med följande:

   ”Information som är nödvändig för certifieringen och evalueringen”.

   b) Punkt 1 ska ersättas med följande:

   ”1. Den som ansöker om certifiering inom ramen för EUCC ska tillhandahålla eller på annat sätt ge certifieringsorganet och ITSEF tillgång till all information som är nödvändig för certifierings- och evalueringsverksamheten.”

3. Artikel 16 ska ersättas med följande:

”*Artikel 16*

**Information som är nödvändig för certifiering och evaluering av skyddsprofiler**

Den som ansöker om certifiering av en skyddsprofil ska tillhandahålla eller på annat sätt ge certifieringsorganet och ITSEF tillgång till all information som är nödvändig för certifierings- och evalueringsverksamheten i en fullständig och korrekt form. Artikel 8.2, 8.3, 8.4 och 8.7 ska gälla i tillämpliga delar.”

4. I artikel 17 ska punkt 1 utgå.

5. I artikel 29 ska punkt 2 ersättas med följande:

”2. Om innehavaren av EUCC-certifikatet inte föreslår ändamålsenliga korrigerande åtgärder inom den tidsfrist som avses i punkt 1 ska certifikatet tillfälligt upphävas i enlighet med artikel 30 eller återkallas i enlighet med artikel 14 eller 20.”

*Artikel 3*

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 1.4 ska tillämpas från och med den 8 januari 2025.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 18 december 2024.

*På kommissionens vägnar*
Ursula VON DER LEYEN
*Ordförande*

*BILAGA I*

*”BILAGA I*

**Mönsterdokument till stöd för teknikdomäner och andra mönsterdokument**

1. Mönsterdokument till stöd för teknikdomäner på AVA_VAN-nivå 4 eller 5:

   a) Följande dokument som rör den harmoniserade evalueringen av teknikdomänen ’smartkort och liknande anordningar’:

      1) ’Minimikrav enligt ITSEF för säkerhetsevalueringar av smartkort och liknande anordningar’, version 1.1.

      2) ’Minimikrav rörande anläggningssäkerhet’, version 1.1.

      3) ’Tillämpning av Common Criteria på integrerade kretsar’, version 1.1.

      4) ’Krav rörande säkerhetsarkitektur (ADV_ARC) för smartkort och liknande anordningar’, version 1.1.

      5) ’Certifiering av ’öppna’ smartkortsprodukter’, version 1.1.

      6) ’Sammansatt produktevaluering för smartkort och liknande anordningar’, version 1.1.

      7) ’Tillämpning av angreppspotential på smartkort och liknande anordningar’, version 1.2.

   b) Följande dokument som rör den harmoniserade evalueringen av teknikdomänen ’maskinvara med säkerhetsboxar’:

      1) ’Minimikrav enligt ITSEF för säkerhetsevalueringar av maskinvara med säkerhetsboxar’, version 1.1.

      2) ’Minimikrav rörande anläggningssäkerhet’, version 1.1.

      3) ’Tillämpning av angreppspotential på maskinvara med säkerhetsboxar’, version 1.2.

2. Mönsterdokument som rör harmoniserad ackreditering av organ för bedömning av överensstämmelse:

   a) ’Ackreditering av ITSEF:er för EUCC’, version 1.1 för ackrediteringar som utfärdas före den 8 juli 2025.

   b) ’Ackreditering av ITSEF:er för EUCC’, version 1.6c för ackrediteringar som utfärdas för första gången eller efter en översyn efter den 8 juli 2025.

   c) ’Ackreditering av certifieringsorgan för EUCC’, version 1.6b.”

*BILAGA II*

I bilaga IV avsnitt IV.3 till genomförandeförordning (EU) 2024/482 ska punkterna 5 och 6 ersättas med följande:

”5. Om certifieringsorganet bekräftar att ändringarna är mindre, ska inget nytt certifikat utfärdas för den ändrade IKT-produkten och en bibehållanderapport till den första certifieringsrapporten ska upprättas.

Bibehållanderapporten ska ingå som en del av konsekvensanalysrapporten och innehålla följande avsnitt:

a) Inledning.

b) En beskrivning av ändringarna.

c) Den berörda utvecklarbevisningen.

6. Den bibehållanderapport som avses i punkt 5 ska lämnas till Enisa för offentliggörande på Enisas webbplats för cybersäkerhetscertifiering.”