Europeiska unionens
officiella tidning

SV
L-serien

2025/2462

9.12.2025

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2025/2462

av den 8 december 2025

om ändring av genomförandeförordning (EU) 2024/482 vad gäller definitioner, certifiering av IKT-produktserier, assuranskontinuitet och mönsterdokument

(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) Den gemensamma evalueringsmetod som åtföljer Common Criteria (CC), som är en internationell standard för evaluering av informationssäkerhet, gör det möjligt att evaluera IKT-produkters säkerhet för certifieringsändamål. I detta sammanhang kan vissa IKT-produkter vila på samma funktionella grund, i syfte att erbjuda liknande säkerhetsfunktioner på olika plattformar eller apparater; detta utgör vad som kallas produktserier. Utformningen, maskinvaran, den fasta programvaran eller mjukvaran kan dock variera från en IKT-produkt till en annan. Det ankommer på certifieringsorganet att från fall till fall besluta om huruvida certifiering av en produktserie kan utföras. Villkoren för certifiering av produktserier skulle kunna illustreras ytterligare i EUCC:s stödjande riktlinjer.

(3) För att upprätthålla de certifierade produkternas tillförlitlighet är det viktigt att definiera vad som utgör en större respektive mindre ändring av evalueringsobjektet eller dess miljö, inbegripet dess operativa miljö eller utvecklingsmiljö. Det är därför nödvändigt att specificera dessa begrepp med beaktande av befintliga och allmänt använda tekniska specifikationer från gruppen av högre tjänstemän på informationssäkerhetsområdet (SOG-IS) och deltagarna i *Arrangements on the Recognition of Common Criteria Certificates in the field of IT Security* (CCRA).

(4) Mindre ändringar kännetecknas ofta av deras begränsade inverkan på den produktassurans som tillhandahålls genom det utfärdade EUCC-certifikatet. Mindre ändringar bör därför hanteras inom ramen för underhållsförfaranden och kräver inte en ny evaluering av produktens säkerhetsfunktioner. Exempel på mindre ändringar som bör hanteras genom underhåll är redaktionella ändringar, ändringar av evalueringsobjektsmiljön som inte ändrar det certifierade evalueringsobjektet och ändringar av det certifierade evalueringsobjektet som inte påverkar assuransbevisen. Ändringar med avseende på utvecklingsmiljön kan också betraktas som mindre, förutsatt att de inte har några följdverkningar på befintliga säkerhetsåtgärder. De kan dock i vissa fall kräva en partiell evaluering av de relevanta åtgärderna.

([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).

(5) En större ändring är varje ändring av det certifierade evalueringsobjektet eller dess miljö som kan inverka negativt på den assurans som uttrycks i EUCC-certifikatet, så att en ny evaluering krävs. Exempel på större ändringar är ändringar av uppsättningen med assuranskriterier, med undantag för assuranskriterierna för CC ALC_FLR-familjen (åtgärdande av brister), ändringar av sekretess- eller integritetskontrollerna i utvecklingsmiljön, om sådana ändringar skulle kunna påverka den säkra utvecklingen eller produktionen av evalueringsobjektet eller ändringar av evalueringsobjektet för att avhjälpa en sårbarhet som kan utnyttjas. Dessutom kan en samling mindre ändringar som tillsammans har en betydande inverkan på säkerheten också betraktas som en större ändring. Det är också viktigt att inse att även om en felrättning endast påverkar en specifik aspekt av evalueringsobjektet, kan dess oförutsägbarhet och potentiella inverkan på assuransen göra att den blir till en större ändring om den äventyrar den säkerhetsassurans som certifieringen ger.

(6) Förändringar i hotmiljön för en icke ändrad certifierad IKT-produkt kan medföra att en ny bedömning måste göras. De möjliga resultaten av en sådan ny bedömning bör tydligt fastställas, särskilt dess inverkan på EUCC-certifikatet. Om en ny bedömning har slutförts med avsett resultat bör certifieringsorganet bekräfta certifikatet eller utfärda ett nytt certifikat med förlängd giltighetstid. Om en förfarande för ny bedömning inte slutförs med avsett resultat bör certifieringsorganet återkalla certifikatet och eventuellt utfärda ett nytt certifikat med annat tillämpningsområde. Sådana bestämmelser bör i tillämpliga delar gälla även för nya bedömningar av skyddsprofiler.

(7) I bilaga I till genomförandeförordning (EU) 2024/482 förtecknas tillämpliga mönsterdokument för evaluering av IKT-produkter och skyddsprofiler. Dessa mönsterdokument bör uppdateras för att återspegla den senaste utvecklingen, exempelvis när det gäller teknisk utveckling, cyberhotbilden, branschpraxis eller internationella standarder. En sådan uppdatering är lämplig för mönsterdokumenten om minimikrav för platssäkerhet, tillämpning av angreppspotential på smartkort, tillämpning av angreppspotential på maskinvaruenheter med säkerhetslådor, tillämpning av gemensamma kriterier för integrerade kretsar och sammansatt produktevaluering för smartkort och liknande enheter. Dessutom ingår inte mönsterdokument om sammansatt produktevaluering och certifiering med användning av den senaste versionen av standarderna för gemensamma kriterier, återanvändning av evalueringsresultat från revisioner på plats och förtydliganden om tolkningen av skyddsprofiler för kvalificerade anordningar för skapande av elektroniska signaturer, färdskrivare och säkerhetsmoduler för maskinvara. För att säkerställa en enhetlig evaluering av IKT-produkter inom ramen för EUCC bör bilaga I ändras så att den omfattar dessa uppdaterade och nya mönsterdokument efter det att de godkänts av den europeiska gruppen för cybersäkerhetscertifiering (ECCG).

(8) Dessutom bör mönsterdokumentet ”ADV_SPM.1 interpretation for CC: 2022 transition” läggas till i systemet för att säkerställa att certifieringsprocesser som bygger på specifika skyddsprofiler kan fortsätta att använda formell modellering (ADV_SPM.1) ända till dess att motsvarande skyddsprofiler har uppdaterats, till exempel genom tillägg av en konfiguration av en CC:2022-kompatibel flerassuransskyddsprofil som stöder ADV_SPM.1. För att ge marknaden tillräckligt med tid för att övergå till de uppdaterade standarderna för gemensamma kriterier måste särskilda övergångsregler fastställas för skyddsprofilerna Security IC Platform PP with Augmentation Packages (v1.0), BSI-CCPP-0084–2014, Java Card System – Closed Configuration (v3.1), BSI-CCPP-0101-V2–2020 eller Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2–2020. För att undvika marknadsstörningar bör det fastställas att mönsterdokumentet ”ADV_SPM.1 interpretation for CC:2022 transition” är tillämpligt på certifieringsprocesser som har inletts före antagandet av denna förordning. Tillämpningen av detta dokument bör dock strikt begränsas till vad som är nödvändigt, med tanke på den tid som behövs för att slutföra uppdateringen av motsvarande skyddsprofiler. För certifieringsprocesser som använder skyddsprofilerna Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084–2014 eller Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2–2020, bör mönsterdokumentet tillämpas på de processer som inleddes före den 1 oktober 2026. För certifieringsprocesser som använder skyddsprofilen Java Card System – Open Configuration (v3.1), BSI-CCPP-0099-V2–2020, bör mönsterdokumentet endast tillämpas på de processer som inletts före dagen för denna förordnings ikraftträdande, eftersom en ny version av ”Java Card System – Open Configuration protection profile” redan finns tillgänglig.

(9) En ändring av mönsterdokumenten under en certifieringsprocess skulle kunna störa evalueringen av produkten och försena utfärdandet av certifikatet. Därför är det nödvändigt med lämpliga övergångsregler för nya eller uppdaterade mönsterdokument, så att säljare, ITSEF-er, certifieringsorgan och andra berörda parter kan göra nödvändiga justeringar. Tillämpliga uppdaterade och nya mönsterdokument bör avse ansökningar om certifiering, inbegripet ansökningar om förnyad bedömning och evaluering, samtidigt som det bör vara möjligt för pågående certifieringsprocesser att fortsätta att använda tidigare versioner av mönsterdokumenten.

(10) I bilaga II och bilaga III till genomförandeförordning (EU) 2024/482 förtecknas de skyddsprofiler som certifierats på AVA_VAN-nivå 4 eller 5 respektive de rekommenderade skyddsprofilerna. Flera hänvisningar är ofullständiga eller föråldrade på grund av en uppdatering av skyddsprofilerna. Dessa hänvisningar bör kompletteras och dessutom bör nya hänvisningar införas för att säkerställa en mer fullständig täckning av säkra integrerade kretsar, smartkort och tillhörande enheter samt betrodda datortjänster.

(11) Det är nödvändigt att göra ändringar av artikel 19 i genomförandeförordning (EU) 2024/482 för att klargöra att bilaga IV, med nödvändiga ändringar, är tillämplig på översynen av EUCC-certifikat för skyddsprofiler.

(12) Med hänsyn till att säkerhetsmålsättningen är en nyckelfaktor för att förstå omfattningen av en certifieringsprocess är det också nödvändigt att Enisa offentliggör säkerhetsmålsättningen för varje EUCC-certifikat på sin webbplats.

(13) Dessutom bör certifieringsorganen förse Enisa med en engelsk version av säkerhetsmålsättningen och certifieringsrapporten så att byrån kan göra denna information tillgänglig på engelska på relevant webbplats, i enlighet med artikel 42.2 i genomförandeförordning (EU) 2024/482. Därför bör den som ansöker om certifiering på begäran förse certifieringsorganen med en engelsk version av säkerhetsmålet.

(14) Det är inte nödvändigt att hänvisningen till certifieringsorganets namn framgår av certifikatets unika identifieringsbeteckning, eftersom certifieringsorganets identifieringsnummer är tillräckligt för att identifiera organet på ett unikt sätt. Utfärdandemånaden behöver inte heller visas eftersom certifikaten räknas på årsbasis. Detta krav bör därför strykas i förenklingssyfte. Eftersom utfärdandeåret för intyget motsvarar utfärdandet av det första intyget bör den dateringen, för att säkerställa spårbarhet, anges i den unika identifieringsbeteckningen på certifikat som utfärdas efter en granskning.

(15) Genomförandeförordning (EU) 2024/482 bör därför ändras i enlighet med detta.

(16) 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 följande punkter läggas till som punkterna 16, 17 och 18:

”(16) *produktserie*: en uppsättning av en sökandes IKT-produkter, som vilar på samma funktionella grund för att tillgodose samma säkerhetsbehov och vars konstruktion, maskinvara, fasta programvara eller mjukvara kan variera från en IKT-produkt till en annan.

(17) *mindre ändring*: varje ändring av det certifierade evalueringsobjektet eller dess miljö som inte inverkar negativt på den assurans som uttrycks i EUCC-certifikatet.

(18) *större ändring*: varje ändring av det certifierade evalueringsobjektet eller dess miljö som kan inverka negativt på den assurans som uttrycks i EUCC-certifikatet.”

(2) I artikel 5 ska följande punkt läggas till som punkt 3:

”3. Ett certifieringsorgan får tillåta certifiering av en produktserie.”

(3) I artikel 9.2 ska led a ersättas med följande:

”(a) Förse certifieringsorganet och ITSEF med all den fullständiga och korrekta information som är nödvändig och tillhandahålla ytterligare nödvändig information på begäran, inbegripet en engelsk version av säkerhetsmålsättningen.”

(4) I artikel 11.3 ska led b ersättas med följande:

”(b) Certifikatets unika identifieringsbeteckning som består av

(1) ordningens namn,

(2) identifieringsnummer, i enlighet med artikel 3 i genomförandeförordning (EU) 2024/3143, för det certifieringsorgan som har utfärdat certifikatet,

(3) år för utfärdandet av det ursprungliga certifikatet,

(4) det identifieringsnummer som tilldelats av det certifieringsorgan som har utfärdat certifikatet.”

(5) I artikel 19 ska punkt 1 ersättas med följande:

”1. På certifikatinnehavarens begäran eller av andra motiverade skäl får certifieringsorganet besluta att se över EUCC-certifikatet för en skyddsprofil. Översynen ska utföras i enlighet med bilaga IV. Certifieringsorganet ska fastställa översynens omfattning. När det är nödvändigt för översynen ska certifieringsorganet begära att ITSEF utför en ny evaluering av den certifierade skyddsprofilen.”

(6) Artikel 42 ska ändras på följande sätt:

(a) I punkt 1 ska följande led läggas till som led i:

”(i) Den säkerhetsmålsättning som motsvarar varje EUCC-certifikat.”

(b) Punkt 2 ska ersättas med följande:

”2. Den information som avses i punkt 1 ska tillhandahållas åtminstone på engelska. För det ändamålet ska certifieringsorganen förse Enisa med originalspråkversionerna av certifieringsrapporterna och säkerhetsmålsättningarna, och de ska dessutom utan oskäligt dröjsmål tillhandahålla den engelska versionen av sådana dokument.”

(7) I artikel 48 ska punkt 4 ersättas med följande:

”4. Om inget annat anges i bilaga I eller II ska mönsterdokumenten tillämpas på certifieringsprocesser, inbegripet ny bedömning och ny evaluering, som inleds från och med den dag då den ändringsakt genom vilken mönsterdokumenten har införlivats i bilaga I eller II börjar tillämpas.”

(8) Bilaga I ska ersättas med texten i bilaga I till denna förordning.

(9) Bilaga II ska ersättas med texten i bilaga II till denna förordning.

(10) Bilaga III ska ersättas med texten i bilaga III till denna förordning.

(11) Bilaga IV ska ändras i enlighet med bilaga IV till denna förordning.

(12) Bilaga V ska ändras i enlighet med bilaga V till denna förordning.

(13) Bilaga IX ska ersättas med texten i bilaga VI till denna förordning.

Artikel 2

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

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

Utfärdad i Bryssel den 8 december 2025.

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) ”Minimum ITSEF requirements for security evaluations of smart cards and similar devices”, version 1.1.

      (2) ”Minimum Site Security Requirements”, version 2;

      (3) ”Reusing evaluation results of site audits (STAR)”, version 1;

      (4) ”Application of Common Criteria to integrated circuits”, version 2.

      (5) ”Security Architecture requirements (ADV_ARC) for smart cards and similar devices”, version 1.1.

      (6) ”Certification of ‘open’ smart card products”, version 1.1;

      (7) ”Composite product evaluation for smart cards and similar devices for CC3.1”, version 2.

      (8) ”Composite product evaluation and certification for CC:2022”, version 1.

      (9) ”Application of Attack Potential to Smartcards and Similar Devices”, version 2.

      (10) ”Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices”, version 1.

      (11) ”ADV_SPM.1 interpretation for CC:2022 transition”, version 1.1, för certifieringsprocesser som använder skyddsprofiler enligt följande:

         (a) BSI-CC-PP-0084–2014 [”Security IC Platform PP with Augmentation Packages (v1.0)”], eller BSI-CCPP-0101-V2–2020 [”Java Card System – Closed Configuration (v3.1)”], inledning före den 1 oktober 2026.

         (b) BSI-CC-PP-0099-V2-2020 [“Java Card System – Open Configuration (v3.1)”], inledning före den 29 december 2025.

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

      (1) ”Minimum ITSEF requirements for security evaluations of hardware devices with security boxes”, version 1.1.

      (2) ”Minimum Site Security Requirements”, version 2;

      (3) ”Reusing evaluation results of site audits (STAR)”, version 1;

      (4) ”Application of Attack Potential to hardware devices with security boxes”, version 2.

      (5) ”Hardware assessment in EN 419221-5 (HSM PP)”, version 1.

      (6) ”JIL Tachograph MS PP Clarification”, version 1.

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

   (a) ”Accreditation of ITSEFs for the EUCC”, version 1.1 för ackrediteringar som utfärdats före den 8 juli 2025.

   (b) ”Accreditation of ITSEFs for the EUCC”, version 1.6c för ackrediteringar som utfärdats för första gången eller efter en översyn efter den 8 juli 2025.

   (c) ”Accreditation of CBs for the EUCC’, version 1.6b.”

BILAGA II

”BILAGA II

Skyddsprofiler certifierade på AVA_VAN-nivå 4 eller 5:

1. För skapande av kvalificerade elektroniska underskrifter och kvalificerade stämplar på distans:

   (a) EN 419241-2:2019 – Tillförlitliga system som stöder serversignering – Del 2: Skyddsprofil för QSCD för serversignering (v0.16), ANSSI-CC-PP-2018/02-M01.

   (b) EN 419221-5:2018 – Skyddsprofil för kryptomoduler för leverantörer av betrodda tjänster – Del 5: Kryptomodul för betrodda tjänster (v0.15), ANSSI-CC-PP-2016/05-M01

2. Skyddsprofiler som antagits som mönsterdokument:

   [TOMT].”

BILAGA III

”BILAGA III

Rekommenderade skyddsprofiler

Skyddsprofiler som används vid certifiering av IKT-produkter, inbegripet produkter inom följande teknikdomäner:

1. Smartkort och liknande anordningar

   (a) Pass:

      (1) Skyddsprofil för en maskinläsbar resehandling med grundläggande åtkomstkontroll för ’Icao-applikation’ (v1.10), BSI-CC-PP-0055-2009.

      (2) Skyddsprofil för en maskinläsbar resehandling med användning av standardförfarande för kontroll med PACE (PACE_PP) (v1), BSI-CC-PP-0068-V2-2011-MA-01.

      (3) Skyddsprofil för en maskinläsbar resehandling med utökad åtkomstkontroll för ’Icao-applikation’ med PACE (v1.3), BSI-CC-PP-0056-V2-2012-MA-02.

   (b) Säkra signaturanordningar (SSCD):

      (1) EN 419211-2:2013 – Skyddsprofiler för säker signaturanordning – Del 2: Signaturanordning med nyckelgenerering (v1.03), BSI-CCP-0059-2009-MA-02.

      (2) EN 419211-3:2013 - Skyddsprofiler för säker signaturanordning – Del 3: Nyckelimportanordning (v1.0.2), BSI-CCP-0075-2012-MA-01.

      (3) EN 419211-4:2013 – Skyddsprofiler för säker signaturanordning – Del 4: Anslutning av signaturanordning med nyckelgenerering och säker kommunikation till applikation för certifikatsgenerering (v1.0.1), BSI-CC-PP-0071-2012-MA-01.

      (4) EN 419211-5:2013 – Skyddsprofiler för utrustning för skapande av säkra signaturer – Del 5: Anslutning av signaturanordning med nyckelgenerering och säker kommunikation till applikation för signaturgenerering (v1.0.1), BSI-CC-PP-0072-2012-MA-01.

      (5) EN 419211-6:2014 - Skyddsprofiler för säker signaturanordning – Del 6: Anslutning av signaturanordning med nyckelimport och säker kommunikation till applikation för signaturgenerering (v1.0.4), BSI-CC-PP-0076-2013-MA-01.

   (c) Färdskrivare: Digital färdskrivare – Färdskrivarkort (TC PP) (v1.0), BSI-CCP-0091-2017.

   (d) Säkra integrerade kretsar, Java Card-plattform och eUICC:

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

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

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

      (4) Cryptographic Service Provider – CSP (v0.9.8), BSI-CCP-0104-2019.

      (5) Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) Version 0.9.5, BSI-CC-PP-0107-2019.

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

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

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

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

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

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

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

2. Maskinvara med säkerhetsboxar.
   (a) Interaktionspunkter (betalningspunkter) och betalningsterminaler (POI):
      (1) Interaktionspunkt ’POI-CHIP-ONLY’ (v4.0), ANSSI-CC-PP-2015/01.
      (2) Interaktionspunkt ‘POI-CHIP-ONLY and Open Protocol Package’ (v4.0), ANSSI-CC-PP-2015/02.
      (3) Interaktionspunkt ’POI-COMPREHENSIVE’ (v4.0), ANSSI-CC-PP-2015/03.
      (4) Interaktionspunkt ’POI-COMPREHENSIVE and Open Protocol Package’ (v4.0), ANSSI-CC-PP-2015/04.
      (5) Interaktionspunkt ’POI-PED-ONLY’ (v4.0), ANSSI-CC-PP-2015/05.
      (6) Interaktionspunkt ‘POI-PED-ONLY and Open Protocol Package’ (v4.0), ANSSI-CC-PP-2015/06.
   (b) Säkerhetsmodul i maskinvara:
      (1) Cryptographic Module for CSP Signing Operations with Backup – PP CMCSOB 14167-2 (v0.35), ANSSI-CC-PP-2015/08.
      (2) Cryptographic Module for CSP Key Generation Services (CSP) – PP CMCKG 14167-3 (v0.20), ANSSI-CC-PP-2015/09.
      (3) Cryptographic Module for CSP Signing Operations without Backup – PP CMCSO 14167-4 (v0.32), ANSSI-CC-PP-2015/10.
   (c) Färdskrivare:
      (1) Digital Tachograph – Motion Sensor (MS PP) (v1.0), BSI-CCP-0093-2017.
      (2) Digital Tachograph – Vehicle Unit (VU PP) (v1.15), BSI-CC-PP-0094-V2-2021.
      (3) Digital Tachograph – External GNSS Facility (EGF PP) (v1.10), BSI-CC-PP-0092-V2-2021.
3. Övriga: Trusted Execution Environment Protection Profile – GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.”

BILAGA IV

Bilaga IV till genomförandeförordning (EU) 2024/482 ska ändras på följande sätt:

1. Punkt 4 i avsnitt IV.2 ska ersättas med följande:

"4. Certifieringsorganet ska granska den uppdaterade tekniska evalueringsrapporten och upprätta en rapport om den nya bedömningen. Det ursprungliga certifikatets status ska sedan ändras i enlighet med artikel 13 eller artikel 19. Om den nya bedömningen utfaller positivt är artikel 13.2 a eller c tillämplig vid certifiering av en produkt medan artikel 19.2 a eller c är tillämplig vid certifiering av en skyddsprofil. Om den nya bedömningen inte utfaller positivt är artikel 13.2 b eller d tillämplig vid certifiering av en produkt medan artikel 19.2 b eller d är tillämplig vid certifiering av en skyddsprofil."

2. Avsnitt IV.3 ska ändras på följande sätt:

a) Avsnitt IV.3 ska ersättas med följande:

"IV.3 **Ändringar av en certifierad IKT-produkt – Underhåll och ny evaluering**"

b) Punkterna 4 och 5 ska ersättas med följande:

"4. Efter granskningen fastställer certifieringsorganet omfattningen av en ändring som mindre eller större i förhållande till dess inverkan på den assurans om uttrycks i EUCC-certifikatet..

5. Om certifieringsorganet bekräftar att det rör sig om mindre ändringar, utfärdas i enlighet med artikel 13.2 a eller artikel 19.2 a inget nytt certifikat för den ändrade IKT-produkten och en bibehållanderapport till den första certifieringsrapporten ska upprättas."

c) Följande punkt ska införas som punkt 5a:

"5a. Vid ändringar av assuransåtgärderna i utvecklingsmiljön, inbegripet tillägg av assuranskrav från CC ALC_FLR-familjen (åtgärdande av brister), får certifieringsorganet begära att ITSEF gör en delevaluering av de berörda säkerhetsåtgärderna. ITSEF ska utfärda en partiell teknisk evalueringsrapport, på grundval av vilken certifieringsorganet bekräftar att ändringarna är antingen mindre eller större. Om certifieringsorganet har bekräftat att det rör sig om mindre ändringar ska avsnitt IV.3 punkt 5 tillämpas. Om certifieringsorganet har bekräftat att det rör sig om större ändringar ska avsnitt IV.3 punkt 7 tillämpas."

BILAGA V

Avsnitt V.1 i bilaga V till genomförandeförordning (EU) 2024/482 ska ersättas med följande:

”V.1 **Certifieringsrapport**

1. På grundval av de tekniska evalueringsrapporter som tillhandahålls av ITSEF upprättar certifieringsorganet en certifieringsrapport som ska offentliggöras tillsammans med motsvarande EUCC-certifikat och säkerhetsmål.

2. Certifieringsrapporten är källan till detaljerad och praktisk information om IKT-produkten och om IKT-produktens säkra införande. Den ska därför innehålla all offentligt tillgänglig och delningsbar information som är relevant för användare och berörda parter. Det går att hänvisa till offentligt tillgänglig och delningsbar information i certifieringsrapporten.

3. Certifieringsrapporten ska innehålla åtminstone följande information:

   a) Sammanfattning.

   b) Identifiering av IKT-produkten.

   c) Kontaktuppgifter med avseende på evalueringen av IKT-produkten.

   d) Säkerhetspolicyer.

   e) Antaganden och förtydligande av tillämpningsområdet.

   f) Information om arkitekturen.

   g) Kompletterande cybersäkerhetsinformation, i tillämpliga fall.

   h) Sammanfattning av evalueringen av IKT-produkten och evaluerad konfiguration.

   i) Resultaten av evalueringen och information om certifikatet.

   j) Kommentarer och rekommendationer i tillämpliga fall.

   k) Bilagor, i tillämpliga fall.

   l) Hänvisning till säkerhetsmålsättningen för den IKT-produkt som ska certifieras.

   m) I förekommande fall, den märkning eller etikett som kopplas till systemet.

   n) Ordlista, i tillämpliga fall.

   o) Litteraturförteckning.

4. Sammanfattningen som det hänvisas till i punkt 3 a ska vara en kort sammanfattning av hela certifieringsrapporten. Den ska ge en tydlig och kortfattad översikt över evalueringsresultaten och ska innehålla följande information:

   a) Namn på den evaluerade IKT-produkten.

   b) Namn på den ITSEF som utförde evalueringen.

   c) Slutdatum för evalueringen.

   d) Datum för utfärdande av certifikatet.

   e) I tillämpliga fall, datum för utfärdande av det ursprungliga certifikatet.

   f) Giltighetsperiod.

   g) Unik identifieringsbeteckning för certifikatet i enlighet med artikel 11.

   h) En kort beskrivning av resultaten i certifieringsrapporten, inklusive följande:

      i) Version och i förekommande fall datum för publicering av de Common Criteria som tillämpas på evalueringen.

      ii) Det assuranspaket med Common Criteria eller den förteckning över komponenter för säkerhetsassurans, inbegripet den AVA_VAN-nivå som tillämpats under evalueringen och motsvarande assuransnivå enligt artikel 52 i förordning (EU) 2019/881 som EUCC-certifikatet hänvisar till.

      iii) I tillämpliga fall den eller de skyddsprofiler som IKT-produkten anges uppfylla kriterierna för.

      iv) Hänvisning till den säkerhetspolicy som tillämpats för den evaluerade IKT-produkten.

      v) Ansvarsfriskrivning(-ar), i tillämpliga fall.

5. Den identifiering som avses i punkt 3 b ska tydligt identifiera den evaluerade IKT-produkten, inbegripet följande information:

   a) Den evaluerade IKT-produktens unika identifieringsbeteckning.

   b) Uppräkning av de IKT-produktkomponenter som omfattas av evalueringen med versionsnumret för varje komponent.

   c) Hänvisning till ytterligare krav med avseende på den certifierade IKT-produktens operativa miljö.

6. De kontaktuppgifter som avses i punkt 3 c ska innehålla åtminstone följande information:

   a) Utvecklarens namn.

   b) Namn och kontaktuppgifter för innehavaren av EUCC-certifikatet.

   c) Namn på det certifieringsorgan som utfärdat certifikatet.

   d) Ansvarig nationell myndighet för cybersäkerhetscertifiering

   e) Namnet på den ITSEF som utförde evalueringen och, i tillämpliga fall, en förteckning över underleverantörer.

7. Den säkerhetspolicy som avses i punkt 3 d ska innehålla en beskrivning av IKT-produktens säkerhetspolicy som en samling säkerhetstjänster och de policyer eller regler som den evaluerade IKT-produkten ska följa eller överensstämma med. Den ska även omfatta följande information:

   a) En beskrivning av certifikatinnehavarens förfaranden för sårbarhetshantering och information om sårbarheter, som endast ska omfatta information som kan göras tillgänglig för allmänheten.

   b) Certifikatinnehavarens policy för assuranskontinuitet, i tillämpliga fall inbegripet en beskrivning av certifikatinnehavarens livscykelförvaltning eller produktionsprocesser i enlighet med avsnitt IV.1 i bilaga IV.

   c) I tillämpliga fall, förekomsten av ett förfarande för hantering av programfixar och resultatet av dess bedömning i enlighet med avsnitt IV.4 i bilaga IV.

8. De antaganden och det förtydligande av tillämpningsområdet som avses i punkt 3 e ska innehålla information om de omständigheter och målsättningar kopplade till produktens avsedda användning som avses i artikel 7.1 c. Informationen ska omfatta följande:

   a) Antaganden om IKT-produktens användning och införande i form av minimikrav, såsom att installation och konfiguration ska vara korrekta och maskinvarukraven uppfyllas.

   b) Antaganden om miljön för att IKT-produkten ska fungera enligt kraven.

   c) Beskrivning av eventuella hot mot IKT-produkten som inte hanteras av produktens evaluerade säkerhetsfunktioner vid avsedd användning, om det anses relevant för en potentiell IKT-produktanvändare.

   Den information som avses i första stycket ska vara så tydlig och begriplig som möjligt för att potentiella användare av den certifierade IKT-produkten ska kunna fatta välgrundade beslut om de risker som är förknippade med dess användning.

9. Den information om arkitekturen som avses i punkt 3 f ska innehålla en övergripande beskrivning av IKT-produkten och dess huvudkomponenter, på grundval av de resultat som definieras i de gemensamma kriterierna för assuransfamiljen: Development – TOE Design (ADV_TDS).

10. Den kompletterande cybersäkerhetsinformation som avses i punkt 3 g ska inbegripa en länk till webbplatsen för innehavaren av det EUCC-certifikat som avses i artikel 55 i förordning (EU) 2019/881.

11. Den evaluering och konfiguration av IKT-produkter som avses i punkt 3 h ska beskriva både utvecklarens och evaluerarensens testarbete, med en beskrivning av metod, konfiguration och djup. Den ska åtminstone innehålla följande information:

    a) Identifiering av de använda assuranskomponenterna från de standarder som avses i artikel 3.

    b) Version av mönsterdokumentet och ytterligare säkerhetsevalueringskriterier som används vid evalueringen.

    c) De parametrar för och den konfiguration av evalueringsobjektet som används för testerna och sårbarhetsanalysen.

    d) Alla skyddsprofiler som har använts, inklusive följande information: Skyddsprofilens namn, version, datum och certifikat.

12. De evalueringsresultat och den information om certifikatet som avses i punkt 3 i ska inbegripa uppgifter om den uppnådda assuransnivån enligt artikel 4 i denna förordning och artikel 52 i förordning (EU) 2019/881.

13. De synpunkter och rekommendationer som avses i punkt 3 j används för att tillföra ytterligare information om evalueringsresultaten. Dessa synpunkter och rekommendationer kan röra brister i IKT-produkten som upptäckts under evalueringen eller omnämnande av egenskaper som är särskilt användbara.

14. De bilagor som avses i punkt 3 k används för att beskriva eventuell ytterligare information som kan vara till nytta för rapportens publik men som inte logiskt passar in i de föreskrivna avsnitten i rapporten, inbegripet vid en fullständig beskrivning av säkerhetspolicyn.

15. Den säkerhetsmålsättning som avses i punkt 3 l ska hänvisa till den evaluerade säkerhetsmålsättningen. Den evaluerade säkerhetsmålsättningen ska tillhandahållas tillsammans med certifieringsrapporten för offentliggörande på den webbplats som avses i artikel 50.1 i förordning (EU) 2019/881. Om den evaluerade säkerhetsmålsättningen behöver rensas före offentliggörandet ska detta ske i enlighet med punkt V.2 i bilaga V till denna förordning.

16. De märkningar eller etiketter som kopplas till det EUCC-system som avses i punkt 3 m ska föras in i certifieringsrapporten i enlighet med de regler och förfaranden som fastställs i artikel 11.

17. Den ordlista som avses i punkt 3 n används för att öka rapportens läsbarhet genom att tillhandahålla definitioner av akronymer eller termer vars betydelse kanske inte är omedelbart uppenbar.

18. Avsnittet om litteraturförteckning som avses i punkt 3 o ska innehålla hänvisningar till alla dokument som använts vid sammanställningen av certifieringsrapporten. Den informationen ska omfatta åtminstone följande:

    a) De säkerhetsevalueringskriterier, mönsterdokument och andra relevanta specifikationer som använts.

    b) Den tekniska evalueringsrapporten.

    c) Den tekniska evalueringsrapporten för den sammansatta evalueringen, i tillämpliga fall.

    d) Teknisk referensdokumentation.

    e) Säkerhetsvägledning för utvecklare.

    f) Konfigurationsförteckning för utvecklare.

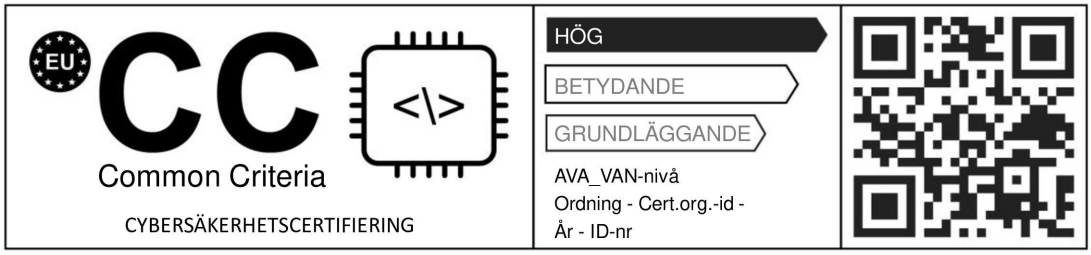
    För att säkerställa att evalueringen kan reproduceras måste all dokumentation som det hänvisas till identifieras på ett unikt sätt med korrekt publiceringsdatum och korrekt versionsnummer.”

BILAGA VI

”BILAGA IX

Märkning och etikett

1. Märkningens och etikettens form:



2. Om märkningen och etiketten förminskas eller förstoras, ska de proportioner som anges i punkt 1 behållas.

3. Om märkningen och etiketten är fysiskt anbringade, ska de vara minst 5 mm höga.”