Euroopa Liidu
Teataja

ET
L-seeria

2025/2462

9.12.2025

KOMISJONI RAKENDUSMÄÄRUS (EL) 2025/2462,

8. detsember 2025,

millega muudetakse rakendusmäärust (EL) 2024/482 seoses määratluste, IKT-toodete seeriate sertifitseerimise, usaldusväärsuse järjepidevuse ja tehnika taset käsitlevate dokumentidega

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrust (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus), ([1]) eriti selle artikli 49 lõiget 7,

ning arvestades järgmist:

(1) Komisjoni rakendusmäärusega (EL) 2024/482 ([2]) on kindlaks määratud Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kavaga (EUCC) ette nähtud rollid, eeskirjad ja kohustused ning kava struktuur vastavalt määruses (EL) 2019/881 kindlaks määratud küberturvalisuse sertifitseerimise raamistikule.

(2) Ühiskriteeriumid on infoturbe hindamise rahvusvaheline standard, millega kaasaskäiv ühine hindamismetoodika võimaldab sertifitseerimise eesmärgil hinnata IKT-toodete turvalisust. Mõned IKT-tooted võivad põhineda samal funktsionaalsel alusel, et eri platvormidel või seadmetes saaks pakkuda sarnaseid turvafunktsioone; sellistele toodetele osutatakse ka kui tooteseeriale. Kõnealuste IKT-toodete lahendus, riistvara, püsivara või tarkvara võivad tooteti siiski erineda. Sertifitseerimisasutuse ülesanne on otsustada igal üksikjuhul eraldi, kas tooteseeriat saab sertifitseerida. Tooteseeriate sertifitseerimise tingimusi võiks täiendavalt kirjeldada toetavates EUCC suunistes.

(3) Sertifitseeritud toodete usaldusväärsuse säilitamiseks on oluline määratleda, mida kujutab endast oluline ja väike muudatus hindamisobjektis või selle keskkonnas, muu hulgas selle rakendus- või arenduskeskkonnas. Seepärast on vaja neid mõisteid täpsustada, võttes arvesse olemasolevaid ja laialdaselt kasutatavaid tehnilisi spetsifikatsioone, mille on avaldanud kõrgemate ametnike infosüsteemide turvalisuse rühm (SOG-IS) ja IT-turbe valdkonna ühiskriteeriumide sertifikaatide tunnustamise kokkuleppe (CCRA) osalised.

(4) Väikesed muudatused on tavaliselt sellised, mille mõju väljaantud EUCC sertifikaadis esitatud toote usaldusväärsuse kinnitusele on piiratud. Seega tuleks väikesi muudatusi hallata hooldusprotseduuride raames ja nende korral ei ole vaja toote turvafunktsioone ümber hinnata. Sellised muudatused, millega tuleks tegeleda hoolduse käigus, on näiteks redaktsioonilised muudatused, hindamisobjekti keskkonna muudatused, mis ei muuda sertifitseeritud hindamisobjekti, ja sertifitseeritud hindamisobjekti muudatused, mis ei mõjuta usaldusväärsuse tõendeid. Arenduskeskkonna muudatusi võib samuti pidada väikeseks, tingimusel et need ei avalda olemasolevatele usaldusväärsuse meetmetele järelmõju. Mõnel juhul võib nende muudatuste tõttu olla vaja seotud meetmeid hinnata osaliselt.

([1]) ELT L 151, 7.6.2019, lk 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.
([2]) Komisjoni 31. jaanuari 2024 rakendusmäärus (EL) 2024/482, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 rakenduseeskirjad seoses Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava (EUCC) vastuvõtmisega (ELT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) Oluline muudatus on sertifitseeritud hindamisobjekti või selle keskkonna muudatus, mis võib negatiivselt mõjutada EUCC sertifikaadis esitatud usaldusväärsuse kinnitust, mistõttu tuleb teha ümberhindamine. Olulised muudatused on näiteks muudatused usaldusväärsuse nõuetes, millest on teatatud, välja arvatud usaldusväärsuse nõuded, mis kuuluvad ühiskriteeriumide ALC_FLR-perekonda (puuduste kõrvaldamine), muudatused arenduskeskkonna konfidentsiaalsuse või tervikluse tagamise meetmetes, kui sellised muudatused võivad mõjutada hindamisobjekti turvalist arendamist või tootmist, või muudatused hindamisobjektis, et kõrvaldada ärakasutatav turvanõrkus. Lisaks võib olulise muudatusena käsitada ka seda, kui tehakse mitu väikest muudatust, millel on ühiselt märkimisväärne mõju turvalisusele. Samuti on oluline tunnistada, et kuigi veaparandus võib mõjutada ainult hindamisobjekti konkreetset aspekti, võib see prognoosimatuse ja võimaliku mõju tõttu usaldusväärsusele olla oluline muudatus, kui see vähendab sertifitseerimisega määratud turvalisuse usaldusväärsuse taset.

(6) Kui muutused toimuvad muutmata sertifitseeritud IKT-toote ohukeskkonnas, võib olla vaja ümberhindamist. Sellise ümberhindamise võimalikud tulemused, eelkõige mõju EUCC sertifikaadile, tuleks selgelt kindlaks määrata. Kui ümberhindamisprotsess lõpeb positiivse tulemusega, peaks sertifitseerimisasutus sertifikaadi kinnitama või andma välja uue pikendatud kehtivusajaga sertifikaadi. Kui ümberhindamisprotsess lõpeb negatiivse tulemusega, peaks sertifitseerimisasutus sertifikaadi kehtetuks tunnistama või andma välja uue, muudetud kohaldamisalaga sertifikaadi. Neid sätteid tuleks kohaldada *mutatis mutandis* kaitseprofiilide ümberhindamise suhtes.

(7) Rakendusmääruse (EL) 2024/482 I lisas on loetletud IKT-toodete ja kaitseprofiilide hindamiseks kohaldatavad tehnika taset käsitlevad dokumendid. Neid dokumente tuleks ajakohastada, et need kajastaksid uusimaid arengusuundi, mis on seotud näiteks tehnoloogia arengu, küberohtude maastiku, tööstusharu tavade ja rahvusvaheliste standarditega. Kõnealune ajakohastamine on otstarbekas selliste tehnika taset käsitlevate dokumentide puhul, mis on seotud järgmisega: minimaalsed kohapealsed turvanõuded, ründepotentsiaali rakendamine kiipkaartide suhtes, ründepotentsiaali rakendamine turvaümbrisega riistvaraseadmete suhtes, ühiskriteeriumide kohaldamine kiipide suhtes ning liittoodete hindamine kiipkaartide ja samalaadsete seadmete puhul. Ajakohastamine ei hõlma selliseid tehnika taset käsitlevaid dokumente, mis on seotud järgmisega: liittoodete hindamine ja sertifitseerimine ühiskriteeriumide standardite uusima versiooni põhjal, kohapealsete auditite hindamistulemuste taaskasutamine ning selgitused, mis käsitlevad kvalifitseeritud e-allkirja andmise vahendite, sõidumeerikute ja füüsiliste turvamoodulitega seotud kaitseprofiilide tõlgendamist. Et IKT-tooteid hinnataks EUCC raames ühetaoliselt, tuleks I lisa muuta, et lisada sellesse ajakohastatud ja uued tehnika taset käsitlevad dokumendid pärast seda, kui Euroopa küberturvalisuse sertifitseerimise rühm on need heaks kiitnud.

(8) Lisaks tuleks kavasse lisada tehnika taset käsitlev dokument „ADV_SPM.1 interpretation for CC:2022 transition", et konkreetsetel kaitseprofiilidel põhinevad sertifitseerimisprotsessid saaksid jätkuvalt kasutada ametlikku modelleerimist (ADV_SPM.1), kuni vastavaid kaitseprofiile ajakohastatakse, näiteks lisades CC:2022 nõuetele vastava ja ADV_SPM.1 toetava mitme usaldusväärsustasemega kaitseprofiili konfiguratsiooni. Et anda turule piisavalt aega minna üle ajakohastatud ühiskriteeriumide standarditele, tuleb ette näha konkreetsed üleminekueeskirjad järgmiste kaitseprofiilide puhul: „Security IC Platform PP with Augmentation Packages" (v1.0, BSI-CC-PP-0084-2014), „Java Card System – Closed Configuration" (v3.1, BSI-CC-PP-0101-V2-2020) või „Java Card System – Open Configuration" (v3.1, BSI-CC-PP-0099-V2-2020). Turuhäirete vältimiseks on asjakohane sätestada, et enne käesoleva määruse vastuvõtmist alanud sertifitseerimisprotsesside suhtes kohaldatakse tehnika taset käsitlevat dokumenti „ADV_SPM.1 interpretation for CC:2022 transition". Kõnealuse dokumendi kohaldamine peaks siiski rangelt piirduma sellega, mis on vajalik, võttes arvesse vastavate kaitseprofiilide ajakohastamiseks kuluvat aega. Täpsemalt tuleks nende sertifitseerimisprotsesside puhul, mis kasutavad kaitseprofiile „Security IC Platform PP with Augmentation Packages" (v1.0, BSI-CC-PP-0084-2014) või „Java Card System – Closed Configuration" (v3.1, BSI-CC-PP-0101-V2-2020), tehnika taset käsitlevat dokumenti kohaldada enne 1. oktoobrit 2026 alanud protsesside suhtes. Kaitseprofiili „Java Card System – Open Configuration" (v3.1 BSI-CC-PP-0099-V2-2020) kasutavate sertifitseerimisprotsesside puhul tuleks tehnika taset käsitlevat dokumenti kohaldada enne käesoleva määruse jõustumise kuupäeva alanud protsesside suhtes, kuna kaitseprofiili „Java Card System – Open Configuration" uus versioon on juba kättesaadav.

(9) Tehnika taset käsitlevate dokumentide muutmine sertifitseerimisprotsessi ajal võib toote hindamist häirida ja sertifikaadi väljaandmises võivad tekkida viivitused. Ajakohastatud või uute tehnika taset käsitlevate dokumentide jaoks on seega vaja kehtestada asjakohased üleminekueeskirjad, et võimaldada müüjatel, infotehnoloogia turvalisuse hindamise üksustel, sertifitseerimisasutustel ja muudel sidusrühmadel teha vajalikke kohandusi. Kohaldatavad ajakohastatud ja uued tehnika taset käsitlevad dokumendid peaksid hõlmama sertifitseerimistaotlusi ja ümberhindamise taotlusi ning käimasolevates sertifitseerimisprotsessides peaks olema võimalik jätkuvalt kasutada tehnika taset käsitlevate dokumentide varasemaid versioone.

(10) Rakendusmääruse (EL) 2024/482 II ja III lisas on loetletud kaitseprofiilid, mis on sertifitseeritud tasemel AVA_VAN.4 või AVA_VAN.5, ning soovitatud kaitseprofiilid. Mitu viidet on kaitseprofiilide ajakohastamise tõttu puudulikud või aegunud. Neid viiteid tuleks täiendada ja lisada uued viited, et turvalised kiibid, kiipkaardid ja nendega seotud seadmed ning usaldatav töötlus oleks ulatuslikumalt kaetud.

(11) Rakendusmääruse (EL) 2024/482 artiklit 19 on vaja muuta, selgitades, et IV lisa kohaldatakse kaitseprofiilidele välja antud EUCC sertifikaatide läbivaatamise suhtes koos vajalike muudatustega.

(12) Võttes arvesse, et turvasiht on sertifitseerimisprotsessi ulatuse mõistmiseks määrava tähtsusega, peab ENISA avaldama oma veebisaidil ka igale EUCC sertifikaadile vastava turvasihi.

(13) Lisaks peaksid sertifitseerimisasutused esitama ENISA-le turvasihi ja sertifitseerimisaruande ingliskeelse teksti, et amet saaks teha selle teabe oma veebisaidil kättesaadavaks inglise keeles vastavalt rakendusmääruse (EL) 2024/482 artikli 42 lõikele 2. Sel põhjusel peaksid sertifitseerimise taotlejad esitama sertifitseerimisasutusele nõudmise korral turvasihi ingliskeelse versiooni.

(14) Sertifikaadi kordumatus tunnuses ei ole vaja viidata sertifitseerimisasutuse nimele, sest sertifitseerimisasutuse identifitseerimisnumber on piisav selle asutuse kordumatuks kindlakstegemiseks. Samuti ei pea märkima väljaandmise kuud, kuna sertifikaate loendatakse aastate kaupa. Lihtsustamiseks tuleks need nõuded välja jätta. Kuna sertifikaadi väljaandmise aasta vastab esimese sertifikaadi väljaandmisele, peaks pärast läbivaatamist välja antud sertifikaadi kordumatu tunnus jälgitavuse tagamiseks sisaldama sama kuupäeva.

(15) Seepärast tuleks rakendusmäärust (EL) 2024/482 vastavalt muuta.

(16) Käesoleva määrusega ettenähtud meetmed on kooskõlas määruse (EL) 2019/881 artikli 66 kohaselt asutatud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Rakendusmäärust (EL) 2024/482 muudetakse järgmiselt.

1) Artiklile 2 lisatakse punktid 16, 17 ja 18:

„16) „tooteseeria“ – taotleja IKT-toodete kogum, kuhu kuuluvad samade turvavajaduste rahuldamiseks samal funktsionaalsel alusel põhinevad IT-tooted, mille lahendus, riistvara, püsivara või tarkvara võib tooteti erineda;

17) „väike muudatus“ – sertifitseeritud hindamisobjekti või selle keskkonna muudatus, mis ei mõjuta negatiivselt EUCC sertifikaadis esitatud usaldusväärsuse kinnitust;

18) „oluline muudatus“ – sertifitseeritud hindamisobjekti või selle keskkonna muudatus, mis võib negatiivselt mõjutada EUCC sertifikaadis esitatud usaldusväärsuse taset.“

2) Artiklisse 5 lisatakse lõige 3 järgmises sõnastuses:

„3. Sertifitseerimisasutus võib lubada sertifitseerida tooteseeriat.“

3) Artikli 9 lõike 2 punkt a asendatakse järgmisega:

„a) anda sertifitseerimisasutusele ja infotehnoloogia turvalisuse hindamise üksusele kogu vajalik teave, mis on täielik ja õige, ning esitada taotluse korral vajalikku lisateavet, kaasa arvatud turvasihi ingliskeelne versioon;“.

4) Artikli 11 lõikes 3 asendatakse punkt b järgmisega:

„b) sertifikaadi kordumatu tunnus, mis koosneb järgmisest:

1) kava nimi;

2) sertifikaadi välja andnud sertifitseerimisasutuse identifitseerimisnumber vastavalt rakendusmääruse (EL) 2024/3143 artiklile 3;

3) algse sertifikaadi väljaandmise aasta;

4) sertifikaadi välja andnud sertifitseerimisasutuse määratud identifitseerimisnumber.“

5) Artikli 19 lõige 1 asendatakse järgmisega:

„1. Sertifikaadi omaniku taotluse korral või muul õigustatud põhjusel võib sertifitseerimisasutus otsustada kaitseprofiilile välja antud EUCC sertifikaadi läbi vaadata. Läbivaatamine toimub IV lisa kohaselt. Sertifitseerimisasutus määrab kindlaks läbivaatamise ulatuse. Kui see on läbivaatamise jaoks vajalik, taotleb sertifitseerimisasutus infotehnoloogia turvalisuse hindamise üksuselt sertifitseeritud kaitseprofiili ümberhindamist.“

6) Artiklit 42 muudetakse järgmiselt:

a) lõikesse 1 lisatakse punkt i:

„i) iga EUCC sertifikaadi kohta sellele vastav turvasiht;“;

b) lõige 2 asendatakse järgmisega:

„2. Lõikes 1 osutatud teave tehakse kättesaadavaks vähemalt inglise keeles. Selleks esitavad sertifitseerimisasutused ENISA-le sertifitseerimisaruannete ja turvasihtide algkeelsed versioonid ning lisaks nendele põhjendamatu viivituseta ka nende dokumentide ingliskeelsed versioonid.“

7) Artikli 48 lõige 4 asendatakse järgmisega:

„4. Kui I või II lisas ei ole sätestatud teisiti, kohaldatakse tehnika taset käsitlevaid dokumente nende sertifitseerimisprotsesside, sealhulgas ümberhindamise suhtes, mis algasid alates selle muutmisakti kohaldamise kuupäevast, millega need tehnika taset käsitlevad dokumendid I või II lisasse inkorporeeriti.“

8) I lisa asendatakse käesoleva määruse I lisas esitatud tekstiga.

9) II lisa asendatakse käesoleva määruse II lisas esitatud tekstiga.

10) III lisa asendatakse käesoleva määruse III lisas esitatud tekstiga.

11) IV lisa muudetakse vastavalt käesoleva määruse IV lisale.

12) V lisa muudetakse vastavalt käesoleva määruse V lisale.

13) IX lisa asendatakse käesoleva määruse VI lisas esitatud tekstiga.

Artikkel 2

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 8. detsember 2025

Komisjoni nimel
president
Ursula VON DER LEYEN

I LISA

„*I LISA*

Tehnilisi valdkondi toetavad tehnika taset käsitlevad dokumendid ja muud tehnika taset käsitlevad dokumendid

1. Tehnika taset käsitlevad dokumendid, mis toetavad tehnilisi valdkondi tasemetel AVA_VAN.4 ja AVA_VAN.5:

   a) järgmised tehnilise valdkonna „Kiipkaardid ja samalaadsed seadmed“ ühtlustatud hindamisega seotud dokumendid:

      1) „Minimum ITSEF requirements for security evaluations of smart cards and similar devices“, versioon 1.1;

      2) „Minimum Site Security Requirements“, versioon 2;

      3) „Reusing evaluation results of site audits (STAR)“, versioon 1;

      4) „Application of Common Criteria to integrated circuits“, versioon 2;

      5) „Security Architecture requirements (ADV_ARC) for smart cards and similar devices“, versioon 1.1;

      6) „Certification of ‘open’ smart card products“, versioon 1.1;

      7) „Composite product evaluation for smart cards and similar devices for CC3.1“, versioon 2;

      8) „Composite product evaluation and certification for CC:2022“, versioon 1;

      9) „Application of Attack Potential to Smartcards and Similar Devices“, versioon 2;

      10) „Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices“, versioon 1;

      11) „ADV_SPM.1 interpretation for CC:2022 transition”, versioon 1.1, kohaldatakse sertifitseerimisprotsessides, mis kasutavad järgmisi kaitseprofiile:

         a) kaitseprofiilid „Security IC Platform PP with Augmentation Packages“ (v1.0, BSI-CC-PP-0084-2014) või „Java Card System – Closed Configuration“ (v3.1, BSI-CC-PP-0101-V2-2020), mis on algatatud enne 1. oktoobrit 2026;

         b) kaitseprofiil „Java Card System – Open Configuration“ (v3.1 BSI-CC-PP-0099-V2-2020), mis on algatatud enne 29. detsembrit 2025;

   b) järgmised tehnilise valdkonna „Turvaümbrisega riistvaraseadmed“ ühtlustatud hindamisega seotud dokumendid:

      1) „Minimum ITSEF requirements for security evaluations of hardware devices with security boxes“, versioon 1.1;

      2) „Minimum Site Security Requirements“, versioon 2;

      3) „Reusing evaluation results of site audits (STAR)“, versioon 1;

      4) „Application of Attack Potential to hardware devices with security boxes“, versioon 2;

      5) „Hardware assessment in EN 419221-5 (HSM PP)“, versioon 1;

      6) „JIL Tachograph MS PP Clarification“, versioon 1.

2. Vastavushindamisasutuste ühtlustatud akrediteerimisega seotud tehnika taset käsitlevad dokumendid:

   a) „Accreditation of ITSEFs for the EUCC“, versioon 1.1, akrediteeringute puhul, mis on välja antud enne 8. juulit 2025;

   b) „Accreditation of ITSEFs for the EUCC“, versioon 1.6c, akrediteeringute puhul, mis on uued või läbi vaadatud pärast 8. juulit 2025;

   c) „Accreditation of CBs for the EUCC“, versioon 1.6b.“

II LISA

„II LISA

Kaitseprofiilid, mis on sertifitseeritud tasemel AVA_VAN.4 või AVA_VAN.5

1. Kvalifitseeritud e-allkirja või e-templi kaugloomise vahendite puhul:

   a) EN 419241-2:2019 – Trustworthy Systems Supporting Server Signing – Part 2: Protection Profile for QSCD for Server Signing („Serverallkirjastamist toetavad usaldusväärsed süsteemid. Osa 2: Kvalifitseeritud allkirja andmise vahendi kaitseprofiil serverallkirjastamise jaoks“) (v0.16), ANSSI-CC-PP-2018/02-M01;

   b) EN 419221-5:2018 – Protection profiles for Trust Service Provider Cryptographic modules – Part 5: Cryptographic Module for Trust Services („Kaitseprofiilid usaldusteenuse tarnija krüptomoodulitele. Osa 5: Usaldusteenuste krüptomoodul“) (v0.15), ANSSI-CC-PP-2016/05-M01.

2. Tehnika taset käsitlevate dokumentidena vastu võetud kaitseprofiilid:

   [TÄITMATA].”

III LISA

„III LISA

Soovitatud kaitseprofiilid

Kaitseprofiilid, mida kasutatakse IKT-toodete, sealhulgas tehnilise valdkonna toodete sertifitseerimisel

1. Kiipkaardid ja samalaadsed seadmed:

   a) pass:

      1) PP Machine Readable Travel Document with „ICAO Application" Basic Access Control (v1.10), BSI-CC-PP-0055-2009;

      2) PP Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP) (v1), BSI-CC-PP-0068-V2-2011-MA-01;

      3) PP Machine Readable Travel Document with „ICAO Application" Extended Access Control with PACE (v1.3), BSI-CC-PP-0056-V2-2012-MA-02;

   b) turvalise allkirja andmise vahendid (SSCD):

      1) EN 419211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation (Turvalise allkirja andmise vahendi kaitseprofiil. Osa 2: Võtme genereerimisega vahend) (v1.03), BSI-CC-PP-0059-2009-MA-02;

      2) EN 419211-3:2013 – Protection profiles for secure signature creation device – Part 3: Device with key import (Turvalise allkirja andmise vahendi kaitseprofiil. Osa 3: Võtme importimisega vahend) (v1.0.2), BSI-CC-PP-0075-2012-MA-01;

      3) EN 419211-4:2013 – Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application (Turvalise allkirja andmise vahendi kaitseprofiil. Osa 4: Võtme genereerimisega vahendi ja usaldatava kanali laiendus sertifikaadi genereerimise rakendusele) (v1.0.1), BSI-CC-PP-0071-2012-MA-01;

      4) EN 419211-5:2013 – Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application (Turvalise allkirja andmise vahendi kaitseprofiil. Osa 5: Võtme genereerimisega vahendi ja usaldatava kanali laiendus allkirja andmise rakendusele) (v1.0.1), BSI-CC-PP-0072-2012-MA-01;

      5) EN 419211-6:2014 – Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted channel to signature creation application (Turvalise allkirja andmise vahendi kaitseprofiil. Osa 6: Võtme importimisega vahendi ja usaldatava kanali laiendus allkirja andmise rakendusele) (v1.0.4), BSI-CC-PP-0076-2013-MA-01;

   c) sõidumeerik: Digital Tachograph – Tachograph Card (TC PP) (v1.0), BSI-CC-PP-0091-2017;

   d) turvalised kiibid, Java-kaardi platvorm ja eUICC:

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

      2) Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-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-CC-PP-0104-2019;

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

      6) Configuration Cryptographic Service Provider – Time Stamp Service, Audit and Clustering (PPC-CSP-TS-Au-Cl), versioon 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) usaldatav platvormimoodul: 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. Turvaümbrisega riistvaraseadmed:
   a) interaktsioonipunktid (maksmiseks) ja makseterminalid:
      1) Point of Interaction „POI-CHIP-ONLY“ (v4.0), ANSSI-CC-PP-2015/01;
      2) Point of Interaction „POI-CHIP-ONLY and Open Protocol Package“ (v4.0), ANSSI-CC-PP-2015/02;
      3) Point of Interaction „POI-COMPREHENSIVE“ (v4.0), ANSSI-CC-PP-2015/03;
      4) Point of Interaction „POI-COMPREHENSIVE and Open Protocol Package“ (v4.0), ANSSI-CC-PP-2015/04;
      5) Point of Interaction „POI-PED-ONLY“ (v4.0), ANSSI-CC-PP-2015/05;
      6) Point of Interaction „POI-PED-ONLY and Open Protocol Package“ (v4.0), ANSSI-CC-PP-2015/06;
   b) riistvara turvamoodul:
      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 – 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) sõidumeerik:
      1) Digital Tachograph – Motion Sensor (MS PP) (v1.0), BSI-CC-PP-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. Muud: Trusted Execution Environment Protection Profile – GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.“

IV LISA

Rakendusmääruse (EL) 2024/482 IV lisa muudetakse järgmiselt.

1. IV.2 jaos asendatakse punkt 4 järgmisega:

„4. Sertifitseerimisasutus vaatab hindamise ajakohastatud tehnilise aruande läbi ja koostab ümberhindamise aruande. Seejärel muudetakse algse sertifikaadi seisundit vastavalt artiklile 13 või artiklile 19. Kui ümberhindamisprotsess lõpeb positiivse tulemusega, kohaldatakse toote sertifitseerimise puhul artikli 13 lõike 2 punkti a või c ning kaitseprofiili sertifitseerimise puhul artikli 19 lõike 2 punkte a või c. Kui ümberhindamisprotsess lõpeb negatiivse tulemusega, kohaldatakse toote sertifitseerimise puhul artikli 13 lõike 2 punkti b või d ning kaitseprofiili sertifitseerimise puhul artikli 19 lõike 2 punkti b või d.“

2. IV.3 jagu muudetakse järgmiselt:

a) IV.3 jao pealkiri asendatakse järgmisega:

„IV.3 **Sertifitseeritud IKT-toote muudatused – hooldamine ja ümberhindamine“;**

b) punktid 4 ja 5 asendatakse järgmistega:

„4. Pärast kontrollimist määrab sertifitseerimisasutus kindlaks, kas muudatus on väike või oluline vastavalt selle, milline on selle mõju EUCC sertifikaadis väljendatud usaldusväärsusele.

5. Kui sertifitseerimisasutus on kinnitanud, et muudatus on väike, ei anta muudetud IKT-tootele välja uut sertifikaati kooskõlas artikli 13 lõike 2 punktiga a või artikli 19 lõike 2 punktiga a ja koostatakse algse sertifitseerimisaruande haldusaruanne.“;

c) lisatakse punkt 5a:

„5a) Kui usaldusväärsuse meetmetes tehakse muudatusi arenduskeskkonnas, näiteks lisatakse usaldusväärsuse nõudeid, mis kuuluvad ühiskriteeriumide ALC_FLR-perekonda (puuduste kõrvaldamine), võib sertifitseerimisasutus nõuda, et infotehnoloogia turvalisuse hindamise üksus hindaks mõjutatud usaldusväärsuse meetmeid. Infotehnoloogia turvalisuse hindamise üksus esitab osalise hindamise tehnilise aruande ning sertifitseerimisasutus kinnitab selle põhjal, kas muudatus on väike või oluline. Kui sertifitseerimisasutus on kinnitanud, et muudatus on väike, kohaldatakse IV lisa IV.3 jao punkti 5. Kui sertifitseerimisasutus on kinnitanud, et muudatus on oluline, kohaldatakse IV lisa IV.3 jao punkti 7.“

V LISA

Rakendusmääruse (EL) 2024/482 V lisa V.1 jagu asendatakse järgmisega:

„V.1. **Sertifitseerimisaruanne**

1. Sertifitseerimisasutus koostab infotehnoloogia turvalisuse hindamise üksuse esitatud hindamise tehniliste aruannete alusel sertifitseerimisaruande, mis avaldatakse koos vastava EUCC sertifikaadi ja turvasihiga.

2. Sertifitseerimisaruanne on üksikasjaliku ja praktilise teabe allikas IKT-toote ja IKT-toote turvalise kasutuselevõtu kohta. See peab seetõttu sisaldama kogu avalikult kättesaadavat ja jagatavat teavet, mis on kasutajate ja huvitatud isikute jaoks oluline. Sertifitseerimisaruandes võib viidata avalikult kättesaadavale ja jagatavale teabele.

3. Sertifitseerimisaruanne sisaldab vähemalt järgmist teavet:

   a) kokkuvõte;

   b) IKT-toote kindlaksmääramine;

   c) IKT-toote hindamisega seotud kontaktandmed;

   d) turbepoliitika;

   e) eeldused ja kohaldamisala selgitused;

   f) arhitektuuriline teave;

   g) asjakohasel juhul täiendav küberturvalisuse alane teave;

   h) IKT-toote hindamise kokkuvõte ja hinnatud konfiguratsioon;

   i) hindamise tulemused ja teave sertifikaadi kohta;

   j) märkused ja soovitused, kui neid on;

   k) lisad, kui neid on;

   l) viide sertifitseerimiseks esitatud IKT-toote turvasihile;

   m) kavaga seotud märgis või silt, kui see on olemas;

   n) sõnastik, kui see on olemas;

   o) kasutatud kirjandus.

4. Punkti 3 alapunktis a osutatud kokkuvõttes võetakse lühidalt kokku kogu sertifitseerimisaruanne. See peab andma selge ja kokkuvõtliku ülevaate hindamistulemustest ning sisaldama järgmist teavet:

   a) hinnatud IKT-toote nimetus;

   b) hindamise teinud infotehnoloogia turvalisuse hindamise üksuse nimi;

   c) hindamise lõpetamise kuupäev;

   d) sertifikaadi väljaandmise kuupäev;

   e) algse sertifikaadi väljaandmise kuupäev, kui see on olemas;

   f) kehtivusaeg;

   g) artikli 11 kohane sertifikaadi kordumatu tunnus;

   h) sertifitseerimisaruande tulemuste lühikirjeldus, sealhulgas:

      i) hindamise suhtes kohaldatud ühiskriteeriumide versioon ja vajaduse korral väljalase;

      ii) ühiskriteeriumide usaldusväärsuse pakett ja turvalisuse usaldusväärsuse komponentide loetelu, sealhulgas hindamise käigus rakendatud AVA_VAN-tase ja sellele vastav usaldusväärsuse tase, nagu on kindlaks määratud määruse (EL) 2019/881 artiklis 52, millele EUCC sertifikaat viitab;

      iii) olemasolu korral kaitseprofiil(id), millele vastav IKT-toode väidetakse olevat;

      iv) viide hinnatud IKT-toote turbepoliitikale;

      v) lahtiütlus(ed), kui neid on.

5. Punkti 3 alapunktis b osutatud kindlaksmääramise käigus tuleb IKT-toode selgelt kindlaks määrata, muu hulgas järgmise teabe kaudu:

   a) hinnatud IKT-toote kordumatu tunnus;

   b) hindamise osaks olevate IKT-toote komponentide loend ja iga komponendi versiooni number;

   c) viide sertifitseeritud IKT-toote rakenduskeskkonnale esitatavatele lisanõuetele.

6. Punkti 3 alapunktis c osutatud kontaktandmed peavad sisaldama vähemalt järgmist teavet:

   a) arendaja nimi;

   b) EUCC sertifikaadi omaniku nimi ja kontaktandmed;

   c) sertifikaadi väljastanud sertifitseerimisasutuse nimi;

   d) vastutav riiklik küberturvalisuse sertifitseerimise asutus;

   e) hindamise teinud infotehnoloogia turvalisuse hindamise üksuse nimi ja asjakohasel juhul alltöövõtjate nimekiri.

7. Punkti 3 alapunktis d osutatud turbepoliitika peab sisaldama IKT-toote turbepoliitika kirjeldust, mis hõlmab kõiki turvateenuseid, ning põhimõtteid või norme, mille täitmise hinnatud IKT-toode peab tagama või millele see peab vastama. Turbepoliitika peab sisaldama ka järgmist teavet:

   a) sertifikaadi omaniku turvanõrkuste haldamise ja avalikustamise menetluste kirjeldus, mis sisaldab üksnes sellist teavet, mida võib avalikult kättesaadavaks teha;

   b) sertifikaadi omaniku usaldusväärsuse järjepidevuse põhimõtted, sealhulgas vajaduse korral sertifikaadi omaniku elutsüklijuhtimise või tootmisprotsesside kirjeldus kooskõlas IV lisa IV.1 jaoga;

   c) vajaduse korral IV lisa IV.4 jao kohase paikade haldamise korra olemasolu ja selle hindamise tulemus.

8. Punkti 3 alapunktis e osutatud eeldused ja kohaldamisala selgitused peavad sisaldama teavet artikli 7 lõike 1 punktis c osutatud toote ettenähtud kasutamisega seotud asjaolude ja eesmärkide kohta ning see peab hõlmama järgmist:

   a) eeldused IKT-toote kasutamise ja kasutuselevõtu kohta miinimumnõuete kujul, näiteks nõuetekohase paigaldamise ja konfigureerimise ning riistvara nõuete täitmine;

   b) eeldused IKT-toote nõuetekohase toimimise keskkonna kohta;

   c) selliste IKT-toodet ähvardavate ohtude kirjeldus, mida toote hinnatud turvafunktsioonid ettenähtud kasutamise korral ei tõrju, kui leitakse, et see on võimaliku IKT-toote kasutaja jaoks vajalik.

   Esimeses lõigus loetletud teave peab olema võimalikult selge ja arusaadav, et võimaldada sertifitseeritud IKT-toote kasutajatel teha teadlikke otsuseid toote kasutamisega seotud riskide kohta.

9. Punkti 3 alapunktis f osutatud arhitektuuriline teave peab sisaldama IKT-toote ja selle põhikomponentide üldkirjeldust, mis põhineb tulemustel, mis on kindlaks määratud ühiskriteeriumide usaldusväärsusnõuete perekonnas „Development – TOE Design (ADV_TDS)“.

10. Punkti 3 alapunktis g osutatud täiendav küberturvalisuse alane teave peab määruse (EL) 2019/881 artikli 55 kohaselt sisaldama EUCC sertifikaadi omaniku veebisaidi linki.

11. Punkti 3 alapunktis h osutatud IKT-toote hinnangus ja konfiguratsioonis tuleb kirjeldada nii arendaja kui ka hindaja katsetamistoiminguid, muu hulgas katsemeetodeid, konfiguratsiooni ja põhjalikkust. Kirjeldus peab sisaldama vähemalt järgmist teavet:

    a) artiklis 3 osutatud standardite alusel kasutatud usaldusväärsuse komponentide loetelu;

    b) tehnika taset käsitleva dokumendi versioon ja hindamisel kasutatud täiendavad turvalisuse hindamise kriteeriumid;

    c) katsetamiseks ja turvanõrkuse analüüsiks kasutatava hindamisobjekti seaded ja konfiguratsioon;

    d) kõik kasutatud kaitseprofiilid, sealhulgas järgmine teave: kaitseprofiili nimi, versioon, kuupäev ja sertifikaat.

12. Hindamise tulemused ja punkti 3 alapunktis i osutatud sertifikaati käsitlev teave peavad sisaldama teavet saavutatud usaldusväärsuse taseme kohta, nagu on osutatud käesoleva määruse artiklis 4 ja määruse (EL) 2019/881 artiklis 52.

13. Punkti 3 alapunktis j osutatud märkusi ja soovitusi kasutatakse hindamistulemuste kohta lisateabe andmiseks. Need märkused ja soovitused võivad käsitleda IKT-toote hindamise käigus avastatud puudusi või eriti kasulikke omadusi.

14. Punkti 3 alapunktis k osutatud lisasid kasutatakse selleks, et anda täiendavat teavet, mis võib olla kasulik aruande sihtrühmale, kuid mis ei sobi loogiliselt aruande ettenähtud punktide alla, kaasa arvatud turbepoliitika täieliku kirjelduse puhul.

15. Punkti 3 alapunktis l osutatud turvasihiks on hinnatud turvasiht. Hinnatud turvasiht esitatakse koos sertifitseerimisaruandega avaldamiseks määruse (EL) 2019/881 artikli 50 lõikes 1 osutatud veebisaidil. Kui hinnatud turvasiht tuleb enne avaldamist puhastada, tehakse seda kooskõlas käesoleva määruse V lisa V.2 jaoga.

16. Punkti 3 alapunktis m osutatud EUCC kavaga seotud märgised või sildid tuleb sertifitseerimisaruandesse lisada vastavalt artiklis 11 sätestatud eeskirjadele ja menetlustele.

17. Punkti 3 alapunktis n osutatud sõnastikku kasutatakse aruande loetavuse parandamiseks ning selles esitatakse selliste akronüümide või mõistete määratlused, mille tähendus ei pruugi olla ilmne.

18. Punkti 3 alapunktis o osutatud kasutatud kirjandus peab sisaldama viiteid kõikidele sertifitseerimisaruande koostamisel kasutatud dokumentidele. See teave peab sisaldama vähemalt järgmist:

    a) turvalisuse hindamise kriteeriumid, tehnika taset käsitlevad dokumendid ning kasutatud täiendavad asjakohased spetsifikatsioonid;

    b) hindamise tehniline aruanne;

    c) asjakohasel juhul liittoote hindamise tehniline aruanne;

    d) tehnilised viitedokumendid;

    e) arendaja turvajuhend;

    f) arendaja konfiguratsiooniloend.

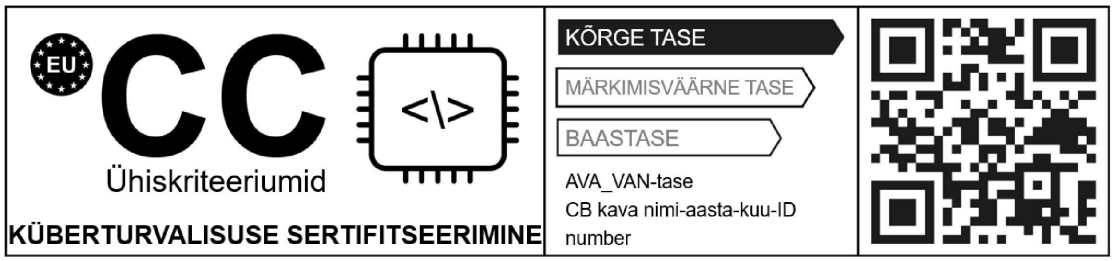
    Hindamise korratavuse tagamiseks tuleb kõik osutatud dokumendid kordumatult identifitseerida avaldamise õige kuupäeva ja õige versiooni numbriga.“

VI LISA

„IX LISA

Märgis ja silt

1. Märgise ja sildi vorm:



2. Märgise ja sildi vähendamise või suurendamise korral tuleb kinni pidada punktis 1 esitatud joonise proportsioonidest.

3. Kui märgis ja silt on füüsiliselt olemas, peavad need olema vähemalt 5 mm kõrgused.“