Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2025/2462

9.12.2025.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2025/2462

(2025. gada 8. decembris),

ar ko Īstenošanas regulu (ES) 2024/482 groza attiecībā uz definīcijām, IKT izstrādājumu sērijas sertifikāciju, apliecinājuma pastāvīgumu un aktuālajiem dokumentiem

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) ([1]), un jo īpaši tās 49. panta 7. punktu,

tā kā:

(1) Komisijas Īstenošanas regulā (ES) 2024/482 ([2]) nosaka vienotos kritērijos balstītas Eiropas kiberdrošības sertifikācijas shēmas (*EUCC*) uzdevumus, noteikumus un pienākumus, kā arī struktūru saskaņā ar Regulā (ES) 2019/881 noteikto Eiropas kiberdrošības sertifikācijas satvaru.

(2) Vienotā izvērtēšanas metodika, kura papildina vienotos kritērijus (VK), kas ir starptautisks standarts informācijas drošības izvērtēšanai, ļauj novērtēt IKT izstrādājumu drošību sertifikācijas vajadzībām. Šajā kontekstā dažus IKT izstrādājumus var veidot uz tā paša funkcionālā pamata, lai piedāvātu līdzīgas drošības funkcijas dažādās platformās vai ierīcēs, ko dēvē arī par izstrādājumu sēriju. Tomēr koncepcija, aparatūra, aparātprogrammatūra vai programmatūra dažādiem IKT izstrādājumiem var atšķirties. Sertifikācijas struktūra katrā atsevišķā gadījumā lemj par to, vai var veikt izstrādājumu sērijas sertifikāciju. Izstrādājumu sērijas sertifikācijas nosacījumus varētu sīkāk ilustrēt, izmantojot atbalsta *EUCC* pamatnostādnes.

(3) Lai saglabātu sertificēto izstrādājumu uzticamību, ir būtiski noteikt, kas ir būtiskas un nebūtiskas izmaiņas izvērtēšanas objektā vai tā vidē, tai skaitā tā darbības vai izstrādes vidē. Tāpēc ir nepieciešams precizēt šos jēdzienus, ņemot vērā esošās un plaši izmantotās tehniskās specifikācijas, ko sagatavojusi Vecāko amatpersonu grupa – informācijas sistēmu drošība (*SOG-IS*) un Vienošanās par vienotu kritēriju sertifikātu atzīšanu IT drošības jomā (*CCRA*) dalībnieki.

(4) Nebūtiskām izmaiņām bieži ir raksturīga ierobežota ietekme uz izdotajā *EUCC* sertifikātā sniegto izstrādājuma apliecinājuma deklarāciju. Tādējādi nebūtiskas izmaiņas būtu jāpārvalda uzturēšanas procedūru ietvaros, un tām nav nepieciešama izstrādājuma drošības funkciju atkārtota novērtēšana. Nebūtisku izmaiņu piemēri, kas būtu jārisina, veicot uzturēšanu, cita starpā ietver redakcionālas izmaiņas, izmaiņas izvērtēšanas objekta vidē, kas nemaina sertificēto izvērtēšanas objektu, un izmaiņas sertificētajā izvērtēšanas objektā, kas neietekmē apliecinājuma pierādījumus. Izmaiņas izstrādes vidē arī var uzskatīt par nebūtiskām, ja tām nav turpmākas ietekmes uz esošajiem apliecinājuma pasākumiem. Tomēr dažos gadījumos tām var būt nepieciešams attiecīgo pasākumu daļējs izvērtējums.

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

([2]) Komisijas Īstenošanas regula (ES) 2024/482 (2024. gada 31. janvāris) par to, kā vienotos kritērijos balstītas Eiropas kiberdrošības sertifikācijas shēmas (*EUCC*) pieņemšanas sakarā piemērojama Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (OV L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) Būtiskas izmaiņas ir jebkādas izmaiņas sertificētajā izvērtēšanas objektā vai tā vidē, kas var negatīvi ietekmēt *EUCC* sertifikātā sniegto apliecinājumu, un tāpēc būtu jāveic atkārtota izvērtēšana. Būtisku izmaiņu piemēri cita starpā ietver izmaiņas pieprasīto apliecinājuma prasību kopumā, izņemot CC ALC_FLR saimes apliecinājuma prasības (trūkumu novēršana); izmaiņas izstrādes vides konfidencialitātes vai integritātes kontrolē, ja šādas izmaiņas varētu ietekmēt izvērtēšanas objekta drošu izstrādi vai ražošanu, vai izmaiņas izvērtēšanas objektā, lai novērstu izmantojamo vārīgo vietu. Turklāt kā būtiskas izmaiņas var klasificēt arī nebūtisku izmaiņu kopumu, kas kopā būtiski ietekmē drošību. Ir svarīgi arī atzīt, ka, lai gan kļūdas izlabošana var ietekmēt tikai konkrētu izvērtēšanas objekta aspektu, šā procesa neparedzamība un iespējamā ietekme uz apliecinājumu var radīt būtiskas izmaiņas, ja tas apdraud sertifikācijas sniegtos drošības apliecinājumus.

(6) Ja tiek veiktas izmaiņas nemainīta sertificēta IKT izstrādājuma apdraudējuma vidē, varētu būt nepieciešams atkārtots novērtējums. Būtu skaidri jānosaka šāda atkārtotas izvērtēšanas procesa iespējamie rezultāti, jo īpaši tā ietekme uz *EUCC* sertifikātu. Ja atkārtota novērtēšana ir sekmīgi pabeigta, sertifikācijas struktūrai būtu jāapstiprina sertifikāts vai jāizdod jauns sertifikāts ar pagarinātu derīguma termiņu. Ja atkārtotās novērtēšanas process netiek sekmīgi pabeigts, sertifikācijas struktūrai būtu jāatsauc sertifikāts un, iespējams, jāizdod jauns sertifikāts ar citu tvērumu. Šādi noteikumi *mutatis mutandis* būtu jāpiemēro aizsardzības profilu atkārtotai novērtēšanai.

(7) Īstenošanas regulas (ES) 2024/482 I pielikumā ir uzskaitīti aktuālie dokumenti, kas piemērojami IKT izstrādājumu un aizsardzības profilu izvērtēšanai. Šie aktuālie dokumenti būtu jāatjaunina, lai atspoguļotu jaunākās norises, piemēram, tās, kas saistītas ar tehnoloģiju attīstību, kiberdraudu ainu, nozares praksi vai starptautiskajiem standartiem. Šāds atjauninājums būtu piemērots aktuālajiem dokumentiem, kas attiecas uz minimālajām drošības prasībām objektā, uzbrukuma potenciāla piemērošanu viedkartēm, uzbrukuma potenciāla piemērošanu aparatūras ierīcēm ar drošības kastēm, vienoto kritēriju piemērošanu integrālajām shēmām un salikto izstrādājumu izvērtēšanu viedkartēm un tamlīdzīgām ierīcēm. Turklāt nav iekļauti aktuālie dokumenti, kas saistīti ar salikto izstrādājumu izvērtēšanu un sertificēšanu, izmantojot vienoto kritēriju standartu jaunāko versiju, objektu revīziju izvērtējuma rezultātu atkalizmantošanu un skaidrojumiem par aizsardzības profilu interpretāciju attiecībā uz kvalificētu elektronisko parakstu radīšanas ierīcēm, tahogrāfiem un aparatūras drošības moduļiem. Lai nodrošinātu IKT izstrādājumu vienotu izvērtēšanu saskaņā ar *EUCC*, I pielikums būtu jāgroza, lai iekļautu šos atjauninātos un jaunos aktuālos dokumentus pēc tam, kad tos būs apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa (*ECCG*).

(8) Turklāt shēmai būtu jāpievieno aktuālais dokuments "ADV_SPM.1 interpretācija CC:2022 pārejai" (*ADV_SPM.1 interpretation for CC:2022 transition*), lai nodrošinātu, ka sertifikācijas procesos, kas balstās uz konkrētiem aizsardzības profiliem, var turpināt izmantot formālu modelēšanu (ADV_SPM.1) līdz attiecīgo aizsardzības profilu atjaunināšanai, piemēram, pievienojot CC:2022 atbilstīgu vairāku apliecinājumu aizsardzības profila konfigurāciju, kas atbalsta ADV_SPM.1. Lai nodrošinātu pietiekamu laiku tirgus pārejai uz atjauninātajiem vienoto kritēriju standartiem, ir jāparedz konkrēti pārejas noteikumi aizsardzības profiliem "Drošas IS platformas PP ar papildinājuma paketēm" (*Security IC Platform PP with Augmentation Packages*) (1.0. vers.), "BSI-CC-PP-0084-2014, Java karšu sistēma – slēgtā konfigurācija" (*Java Card System – Closed Configuration*) (3.1. vers.), "BSI-CC-PP-0101-V2-2020" vai "Java karšu sistēma – atvērtā konfigurācija" (*Java Card System – Open Configuration*) (3.1. vers.), "BSI-CC-PP-0099-V2-2020". Lai izvairītos no tirgus traucējumiem, ir lietderīgi noteikt, ka aktuālais dokuments par ADV_SPM.1 interpretāciju CC:2022 pārejai ir piemērojams sertifikācijas procesiem, kas uzsākti pirms šīs regulas pieņemšanas. Tomēr šis dokuments būtu jāpiemēro tikai tiktāl, cik tas nepieciešams, ņemot vērā laiku, kas vajadzīgs, lai pabeigtu attiecīgo aizsardzības profilu atjaunināšanu. Konkrētāk, attiecībā uz sertifikācijas procesiem, kuros izmanto aizsardzības profilus "Drošas IS platformas PP ar papildinājuma paketēm" (*Security IC Platform PP with Augmentation Packages*) (1.0. vers.), "BSI-CC-PP-0084-2014" vai "Java karšu sistēma – slēgtā konfigurācija" (*Java Card System – Closed Configuration*) (3.1. vers.), "BSI-CC-PP-0101-V2-2020", aktuālais dokuments būtu jāpiemēro tiem procesiem, kas uzsākti pirms 2026. gada 1. oktobra. Attiecībā uz sertifikācijas procesiem, kuros izmanto aizsardzības profilu "Java karšu sistēma – atvērtā konfigurācija" (3.1. vers.), "BSI-CC-PP-0099-V2-2020", aktuālais dokuments būtu jāpiemēro tikai tiem procesiem, kas uzsākti pirms šīs regulas spēkā stāšanās dienas, ņemot vērā to, ka jau ir pieejama jauna aizsardzības profila "Java karšu sistēmas – atvērtā konfigurācija" (*Java Card System – Open Configuration*) versija.

(9) Aktuālo dokumentu izmaiņas sertifikācijas procesā varētu traucēt izvērtēt izstrādājumu un aizkavēt sertifikāta izdošanu. Tāpēc ir vajadzīgi atbilstoši pārejas noteikumi attiecībā uz jauniem vai atjauninātiem aktuālajiem dokumentiem, lai pārdevēji, *ITSEF*, sertifikācijas struktūras un citas ieinteresētās personas varētu veikt vajadzīgos pielāgojumus. Piemērojamajiem atjauninātajiem un aktuālajiem dokumentiem būtu jāattiecas uz sertifikācijas pieteikumiem, tai skaitā atkārtotās novērtēšanas un atkārtotās izvērtēšanas pieteikumiem, savukārt notiekošajos sertifikācijas procesos vajadzētu būt iespējai turpināt izmantot aktuālo dokumentu agrākas versijas.

(10) Īstenošanas regulas (ES) 2024/482 II un III pielikumā ir uzskaitīti attiecīgi AVA_VAN 4. vai 5. līmenī sertificētie aizsardzības profili un ieteicamie aizsardzības profili. Vairākas atsauces ir nepilnīgas vai novecojušas aizsardzības profilu atjaunināšanas dēļ. Minētās atsauces būtu jāpapildina un papildus būtu jāiekļauj jaunas atsauces, lai nodrošinātu plašāku drošu integrālo shēmu, viedkaršu un saistīto ierīču, kā arī uzticamas skaitļošanas segumu.

(11) Īstenošanas regulas (ES) 2024/482 19. pantā ir jāizdara grozījumi, lai precizētu, ka IV pielikumu ar nepieciešamajām izmaiņām piemēro aizsardzības profilu *EUCC* sertifikātu pārskatīšanai.

(12) Ņemot vērā to, ka drošības mērķis ir svarīgs elements, lai izprastu sertifikācijas procesa tvērumu, *ENISA* savā tīmekļa vietnē ir jāpublicē arī katram *EUCC* sertifikātam atbilstošais drošības mērķis.

(13) Turklāt sertifikācijas struktūrām būtu jānodrošina *ENISA* drošības mērķa un sertifikācijas ziņojuma angļu valodas versija, lai aģentūra minēto informāciju varētu darīt pieejamu angļu valodā attiecīgajā tīmekļa vietnē saskaņā ar Īstenošanas regulas (ES) 2024/482 42. panta 2. punktu. Šā iemesla dēļ sertifikācijas pieteikuma iesniedzējiem pēc pieprasījuma būtu jāiesniedz sertifikācijas struktūrām drošības mērķa angļu valodas versija.

(14) Sertifikāta unikālajā identifikācijā nav jānorāda atsauce uz sertifikācijas struktūras nosaukumu, jo ar sertifikācijas struktūras identifikācijas numuru pietiek, lai unikālā veidā identificētu šo struktūru. Nav jānorāda arī izdošanas mēnesis, jo sertifikātu skaitīšanu veic katru gadu. Tāpēc vienkāršošanas nolūkā minētā prasība būtu jāsvītro. Tā kā sertifikāta izdošanas gads atbilst pirmā sertifikāta izdošanai, tas pats datums būtu jānorāda unikālajā identifikācijā sertifikātos, kas izdoti pēc pārskatīšanas, lai nodrošinātu izsekojamību.

(15) Tāpēc Īstenošanas regula (ES) 2024/482 būtu attiecīgi jāgroza.

(16) Šajā regulā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi ar Regulas (ES) 2019/881 66. pantu izveidotā komiteja,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Īstenošanas regulu (ES) 2024/482 groza šādi:

1) regulas 2. pantu papildina ar šādu 16., 17. un 18. punktu:

"16) "izstrādājuma sērija" ir pieteikuma iesniedzēja izstrādāts IKT izstrādājumu kopums, kurš balstās uz to pašu funkcionālo pamatu, lai apmierinātu tās pašas drošības vajadzības, un kura koncepcija, aparatūra, aparātprogrammatūra vai programmatūra dažādiem IKT izstrādājumiem var atšķirties;

17) "nebūtiskas izmaiņas" ir jebkādas izmaiņas sertificētajā izvērtēšanas objektā vai tā vidē, kas neietekmē negatīvi *EUCC* sertifikātā sniegto apliecinājumu;

18) "būtiskas izmaiņas" ir jebkādas izmaiņas sertificētajā izvērtēšanas objektā vai tā vidē, kas var negatīvi ietekmēt *EUCC* sertifikātā sniegto apliecinājumu.";

2) regulas 5. pantam pievieno 3. punktu:

"3. Sertifikācijas struktūra var atļaut sertificēt izstrādājumu sēriju.";

3) regulas 9. panta 2. punkta a) apakšpunktu aizstāj ar šādu:

"a) sniegt sertifikācijas iestādei un *ITSEF* pilnīgu un pareizu visu nepieciešamo informāciju un pēc pieprasījuma sniegt vajadzīgo papildu informāciju, ieskaitot drošības mērķa versiju angļu valodā;";

4) regulas 11. panta 3. punkta b) apakšpunktu aizstāj ar šādu:

"b) sertifikāta unikāla identifikācija, ko veido:

1) shēmas nosaukums;

2) sertifikātu izdevušās sertifikācijas struktūras identifikācijas numurs saskaņā ar Īstenošanas regulas (ES) 2024/3143 3. pantu;

3) sākotnējā sertifikāta izdošanas gads;

4) sertifikātu izdevušās sertifikācijas struktūras piešķirtais identifikācijas numurs.";

5) regulas 19. panta 1. punktu aizstāj ar šādu:

"1. Pēc sertifikāta turētāja pieprasījuma vai citu pamatotu iemeslu dēļ sertifikācijas struktūra var nolemt pārskatīt aizsardzības profila *EUCC* sertifikātu. Pārskatīšanu veic saskaņā ar IV pielikumu. Sertifikācijas struktūra nosaka pārskatīšanas apjomu. Sertifikācijas struktūra pieprasa *ITSEF* sertificēto aizsardzības profilu izvērtēt vēlreiz, ja tas nepieciešams pārskatīšanai.";

6) regulas 42. pantu groza šādi:

a) panta 1. punktam pievieno šādu i) apakšpunktu:

"i) drošības mērķi, kas atbilst katram *EUCC* sertifikātam.";

b) panta 2. punktu aizstāj ar šādu:

"2. Šā panta 1. punktā minēto informāciju dara pieejamu vismaz angļu valodā. Šajā nolūkā sertifikācijas struktūras nodrošina *ENISA* sertifikācijas ziņojumu un drošības mērķu oriģinālvalodas versijas un turklāt bez liekas kavēšanās iesniedz arī šādu dokumentu angļu valodas versiju.";

7) regulas 48. panta 4. punktu aizstāj ar šādu:

"4. Ja I vai II pielikumā nav noteikts citādi, aktuālos dokumentus piemēro sertifikācijas procesiem, tai skaitā atkārtotai novērtēšanai un atkārtotai izvērtēšanai, kas sākti no datuma, kad sāk piemērot grozošo aktu, ar kuru aktuālie dokumenti ir iekļauti I vai II pielikumā.";

8) I pielikumu aizstāj ar šīs regulas I pielikuma tekstu;

9) II pielikumu aizstāj ar šīs regulas II pielikuma tekstu;

10) III pielikumu aizstāj ar šīs regulas III pielikuma tekstu;

11) IV pielikumu groza saskaņā ar šīs regulas IV pielikumu;

12) V pielikumu groza saskaņā ar šīs regulas V pielikumu;

13) IX pielikumu aizstāj ar šīs regulas VI pielikuma tekstu.

2. pants

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī.*

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2025. gada 8. decembrī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

I PIELIKUMS

"I PIELIKUMS

Aktuāli dokumenti, kas atbalsta tehniskās jomas un citādus aktuālus dokumentus

1. Aktuāli dokumenti, kas atbalsta tehniskās jomas AVA_VAN 4. vai 5. līmenī:

   a) šādi dokumenti, kas saistīti ar tehniskās jomas "viedkartes un tamlīdzīgas ierīces" saskaņotu izvērtēšanu:

      1) "Minimālās *ITSEF* prasības viedkaršu un tamlīdzīgu ierīču drošības izvērtēšanai", 1.1. redakcija;

      2) "Minimālās drošības prasības objektā", 2. redakcija;

      3) "Objektu revīziju novērtējuma rezultātu atkārtota izmantošana (*STAR*)", 1. redakcija;

      4) "Vienotu kritēriju piemērošana integrālajām shēmām", 2. redakcija;

      5) "Drošības arhitektūras prasības (ADV_ARC) viedkartēm un tamlīdzīgām ierīcēm", 1.1. redakcija;

      6) ""Atvērto" viedkaršu izstrādājumu sertifikācija", 1.1. redakcija;

      7) "Saliktu izstrādājumu izvērtēšana viedkartēm un tamlīdzīgām ierīcēm CC3.1 vajadzībām", 2. redakcija;

      8) "Saliktu izstrādājumu izvērtēšana un sertifikācija CC:2022 vajadzībām", 1. redakcija;

      9) "Uzbrukuma potenciāla piemērošana viedkartēm un tamlīdzīgām ierīcēm", 2. redakcija;

      10) "Drošības novērtēšana un kvalificētu elektronisko parakstu / zīmogu radīšanas ierīču sertifikācija", 1. redakcija;

      11) "ADV_SPM.1 interpretācija CC:2022 pārejai", 1.1. redakcija, kas piemērojama sertifikācijas procesiem, kuros izmanto šādus aizsardzības profilus:

         a) aizsardzības profili "Drošas IS platformas PP ar papildinājuma paketēm" (*Security IC Platform PP with Augmentation Packages*) (1.0. vers.), "BSI-CC-PP-0084-2014" vai "Java karšu sistēma – slēgta konfigurācija" (*Java Card System – Closed Configuration*) (3.1. vers.), "BSI-CC-PP-0101-V2-2020", kas uzsākti pirms 2026. gada 1. oktobra;

         b) aizsardzības profils "Java karšu sistēma – atvērtā konfigurācija" (*Java Card System – Open Configuration*) (3.1. vers.), "BSI-CC-PP-0099-V2-2020", kas uzsākts pirms 2025. gada 29. decembra;

   b) šādi dokumenti, kas saistīti ar tehniskās jomas "aparatūras ierīces ar drošības kastēm" saskaņotu izvērtēšanu:

      1) "Minimālās *ITSEF* prasības aparatūras ierīču ar drošības kastēm drošības izvērtējumiem", 1.1. redakcija;

      2) "Minimālās drošības prasības objektā", 2. redakcija;

      3) "Objektu revīziju novērtējuma rezultātu atkārtota izmantošana (*STAR*)", 1. redakcija;

      4) "Uzbrukuma potenciāla piemērošana aparatūras ierīcēm ar drošības kastēm", 2. redakcija;

      5) "Aparatūras novērtējums EN 419221-5 (HSM PP)", 1. redakcija;

      6) "*JIL* tahogrāfa *MS PP* precizējums" (*JIL Tachograph MS PP Clarification*), 1. redakcija.

2. Aktuāli dokumenti, kas attiecas uz atbilstības novērtēšanas struktūru saskaņoto akreditāciju:

   a) "*ITSEF* akreditācija *EUCC* vajadzībām", 1.1. redakcija akreditācijai, kas izdota pirms 2025. gada 8. jūlija;

   b) "*ITSEF* akreditācija *EUCC* vajadzībām", 1.6.c redakcija akreditācijai, kas no jauna izdota vai pārskatīta pēc 2025. gada 8. jūlija;

   c) "*CB* akreditācija *EUCC* vajadzībām", 1.6.b redakcija."

II PIELIKUMS

"II PIELIKUMS

Aizsardzības profili, ko sertificē AVA_VAN 4. vai 5. līmenī

1. Attiecībā uz kvalificēta paraksta un zīmoga tālradīšanas ierīcēm:

   a) EN 419241-2:2019. Uzticamas sistēmas, kas atbalsta servera parakstu. 2. daļa: Elektronisko parakstu *QSCD* aizsardzības profili (v0.16), ANSSI-CC-PP-2018/02-M01;

   b) EN 419221-5:2018. Aizsardzības profili uzticamības pakalpojuma sniedzēja kriptogrāfijas moduļiem. 5. daļa: Uzticamības pakalpojumu kriptogrāfijas modulis (v0.15), ANSSI-CC-PP-2016/05-M01

2. Aizsardzības profili, kas pieņemti kā aktuālie dokumenti:

   [BLANK]."

III PIELIKUMS

"III PIELIKUMS

Ieteicamie aizsardzības profili

Aizsardzības profili, ko izmanto IKT izstrādājumu, tai skaitā tehnisko jomu izstrādājumu, sertificēšanā.

1. Viedkartes un līdzīgas ierīces:

   a) pase:

      1) PP mašīnlasāms ceļošanas dokuments ar "*ICAO* lietojumu", pamata piekļuves kontrole (1.10. vers.), BSI-CC-PP-0055-2009;

      2) PP mašīnlasāms ceļošanas dokuments, kas izmanto standarta pārbaudes procedūru ar *PACE* (1. vers.), BSI-CC-PP-0068-V2-2011-MA-01;

      3) PP mašīnlasāms ceļošanas dokuments ar "*ICAO* lietojumu", paplašinātā piekļuves kontrole ar *PACE* (1.3. vers.), BSI-CC-PP-0056-V2-2012-MA-02;

   b) droša paraksta radīšanas ierīces (*SSCD*):

      1) EN 419211-2:2013. Aizsardzības profili drošām paraksta radīšanas ierīcēm. 2. daļa: Atslēgu ģenerēšanas ierīce (1.03. vers.), BSI-CC-PP-0059-2009-MA-02;

      2) EN 419211-3:2013. Aizsardzības profili drošām paraksta radīšanas ierīcēm. 3. daļa: Ierīce ar atslēgas importu (1.0.2. vers.), BSI-CC-PP-0075-2012-MA-01;

      3) EN 419211-4:2013. Aizsardzības profili drošām paraksta radīšanas ierīcēm. 4. daļa: Paplašinājums atslēgu ģenerēšanas ierīcei un uzticams kanāls sertifikāta ģenerēšanas lietotnei (1.0.1. vers.), BSI-CC-PP-0071-2012-MA-01;

      4) EN 419211-5:2013. Aizsardzības profili drošām paraksta radīšanas ierīcēm. 5. daļa: Paplašinājums atslēgu ģenerēšanas ierīcei un uzticams kanāls paraksta radīšanas lietotnei (1.0.1. vers.), BSI-CC-PP-0072-2012-MA-01;

      5) EN 419211-6:2014. Aizsardzības profili drošām paraksta radīšanas ierīcēm. 6. daļa: Paplašinājums atslēgu importēšanas ierīcei un uzticams kanāls paraksta radīšanas lietotnei (1.0.4. vers.), BSI-CC-PP-0076-2013-MA-01;

   c) tahogrāfs: digitālais tahogrāfs – tahogrāfa karte (TC PP) (1.0. vers.), BSI-CC-PP-0091-2017;

   d) droša *IC*, *Java Card* platforma un *eUICC*:

      1) universāls *SIM Java* karšu platformas aizsardzības pamata profils un *SCWS* konfigurācijas (2.0.2. vers.), ANSSI-CC-PP-2010/04 (pamata), ANSSI-CC-PP-2010/05 (pamata un *SCWS*);

      2) drošas IS platformas PP ar papildinājuma paketēm (*Security IC Platform PP with Augmentation Packages*) (1.0. vers.), BSI-CC-PP-0084-2014;

      3) iegultais *UICC* (*eUICC*) mašīnas–mašīnas ierīcēm (*Embedded UICC (eUICC) for Machine-to-Machine Devices*) (1.1. vers.), BSI-CC-PP-0089-2015;

      4) kriptogrāfijas pakalpojumu sniedzējs – *CSP* (0.9.8. vers.), BSI-CC-PP-0104-2019;

      5) kriptogrāfijas pakalpojumu sniedzējs – laika zīmoga pakalpojums un revīzija (PPC-CSP-TS-Au), 0.9.5. vers., BSI-CC-PP-0107-2019;

      6) konfigurācijas kriptogrāfijas pakalpojumu sniedzējs – laika zīmoga pakalpojums, revīzija un kopa (PPC-CSP-TS-Au-Cl), 0.9.4. vers., BSI-CC-PP-0108-2019;

      7) *Java* karšu sistēmas – slēgtā konfigurācija (*Java Card System – Closed Configuration*) (3.1. vers.), BSI-CC-PP-0101-V2-2020;

      8) drošības elementa aizsardzības profils – GPC_SPE_174 (1.0. vers.), CCN-CC-PP-5-2021;

      9) drošas apakšsistēmas mikroshēmas sistēmā (*3S in SoC*) aizsardzības profils (1.8. vers.), BSI-CC-PP-0117-V2-2023;

      10) *Java* karšu sistēmas – atvērtā konfigurācija (*Java Card System – Open Configuration*) (3.2. vers.), BSI-CC-PP-0099-V3-2024;

      11) iegultais *UICC* patērētāju ierīču aizsardzības profilam (2.1. vers.), BSI-CC-PP-0100-V2-2025;

   e) uzticamo platformu modulis: aizsardzības profils "*PC* klienta uzticama platformas moduļa saime 2.0, līmenis 0, redakcija 1.59 (1.3. vers.), ANSSI-CC-PP-2021/02.

2. Aparatūras ierīces ar drošības kastēm:

   a) (maksājumu) mijiedarbības un maksājumu termināļu (*POI*) punkti:

      1) mijiedarbības punkts "POI-CHIP-ONLY" (4.0. vers.), ANSSI-CC-PP-2015/01;

      2) mijiedarbības punkts "POI-CHIP-ONLY un atvērtā protokola pakotne" ("POI-CHIP-ONLY and Open Protocol Package") (4.0. vers.), ANSSI-CC-PP-2015/02;

      3) mijiedarbības punkts "POI-COMPREHENSIVE" (4.0. vers.), ANSSI-CC-PP-2015/03;

      4) mijiedarbības punkts "POI-COMPREHENSIVE un atvērtā protokola pakotne" ("POI-COMPREHENSIVE and Open Protocol Package") (4.0. vers.), ANSSI-CC-PP-2015/04;

      5) mijiedarbības punkts "POI-PED-ONLY" (4.0. vers.), ANSSI-CC-PP-2015/05;

      6) mijiedarbības punkts "POI-PED-ONLY un atvērtā protokola pakotne" ("POI-CHIP-ONLY and Open Protocol Package") (4.0. vers.), ANSSI-CC-PP-2015/06;

   b) aparatūras drošības modulis:

      1) kriptogrāfisks modulis CSP parakstīšanas darbībām ar dublējumu – PP CMCSOB 14167-2 (0.35. vers.), ANSSI-CC-PP-2015/08;

      2) kriptogrāfisks modulis CSP atslēgu ģenerēšanas pakalpojumiem – PP CMCKG 14167-3 (0.20. vers.), ANSSI-CC-PP-2015/09;

      3) kriptogrāfisks modulis CSP parakstīšanas darbībām bez dublējuma – PP CMCSO 14167-4 (0.32. vers.), ANSSI-CC-PP-2015/10;

   c) tahogrāfs:

      1) digitālais tahogrāfs – kustības sensors (MS PP) (1.0. vers.), BSI-CC-PP-0093-2017;

      2) digitālais tahogrāfs – transportlīdzekļa bloks (VU PP) (1.15. vers.), BSI-CC-PP-0094-V2-2021;

      3) digitālais tahogrāfs – ārējā GNSS iekārta (EGF PP) (1.10. vers.), BSI-CC-PP-0092-V2-2021.

3. Cits: uzticamas izpildes vides aizsardzības profils – GPD_SPE_021 (1.3. vers.), ANSSI-CC-PP-2014/01-M02."

IV PIELIKUMS

Īstenošanas regulas (ES) 2024/482 IV pielikumu groza šādi:

1. pielikuma IV.2. iedaļas 4. punktu aizstāj ar šādu:

"4. Sertifikācijas struktūra pārskata atjaunināto izvērtēšanas tehnisko ziņojumu un sagatavo atkārtotās novērtēšanas ziņojumu. Pēc tam sākotnējā sertifikāta statusu maina saskaņā ar 13. vai 19. pantu. Ja atkārtotās novērtēšanas process ir sekmīgs, 13. panta 2. punkta a) vai c) apakšpunktu piemēro izstrādājuma sertifikācijas gadījumā un 19. panta 2. punkta a) vai c) apakšpunktu – aizsardzības profila sertifikācijas gadījumā. Ja atkārtotās novērtēšanas process nav sekmīgs, 13. panta 2. punkta b) vai d) apakšpunktu piemēro izstrādājuma sertifikācijas gadījumā un 19. panta 2. punkta b) vai d) apakšpunktu – aizsardzības profila sertifikācijas gadījumā.";

2. pielikuma IV.3. iedaļu groza šādi:

a) IV.3. iedaļas nosaukumu aizstāj ar šādu:

"IV.3. **Izmaiņas sertificētā IKT izstrādājumā – uzturēšana un atkārtota izvērtēšana**";

b) 4. un 5. punktu aizstāj ar šādiem:

"4. Pēc pārbaudes sertifikācijas struktūra nosaka, vai izmaiņu apmērs ir nebūtisks vai būtisks atbilstoši to ietekmei uz apliecinājumu, kas pausts *EUCC* sertifikātā.

5. Ja sertifikācijas struktūra ir apstiprinājusi, ka izmaiņas ir nebūtiskas, pārveidotajam IKT izstrādājumam neizdod jaunu sertifikātu saskaņā ar 13. panta 2. punkta a) apakšpunktu vai 19. panta 2. punkta a) apakšpunktu, un sagatavo sākotnējā sertifikācijas ziņojuma uzturēšanas ziņojumu.";

c) iekļauj šādu 5.a punktu:

"5.a Ja tiek veiktas jebkādas izmaiņas apliecinājuma pasākumos izstrādes vidē, tai skaitā tiek pievienotas apliecinājuma prasības no CC ALC_FLR saimes (trūkumu novēršana), sertifikācijas struktūra var pieprasīt *ITSEF* veikt skarto apliecinājuma pasākumu apakškopas novērtējumu. *ITSEF* izdod daļējas izvērtēšanas tehnisko ziņojumu, uz kura pamata sertifikācijas struktūra apstiprina, ka izmaiņas ir nebūtiskas vai būtiskas. Ja sertifikācijas struktūra ir apstiprinājusi, ka izmaiņas ir nebūtiskas, piemēro pielikuma IV.3. iedaļas 5. punktu. Ja sertifikācijas struktūra ir apstiprinājusi, ka izmaiņas ir būtiskas, piemēro pielikuma IV.3. iedaļas 7. punktu."

V PIELIKUMS

Īstenošanas regulas (ES) 2024/482 V pielikuma V.1. iedaļu aizstāj ar šādu:

"V.1. **Sertifikācijas ziņojums**

1. Pamatojoties uz *ITSEF* sniegtajiem izvērtēšanas tehniskajiem ziņojumiem, sertifikācijas struktūra sagatavo sertifikācijas ziņojumu, kas jāpublicē kopā ar attiecīgo *EUCC* sertifikātu un drošības mērķi.

2. Sertifikācijas ziņojums ir detalizētas un praktiskas informācijas avots par IKT izstrādājumu un par IKT izstrādājuma drošu izmantošanu. Tāpēc tajā iekļauj visu publiski pieejamo un kopīgojamo informāciju, kas ir būtiska lietotājiem un ieinteresētajām personām. Sertifikācijas ziņojumā var atsaukties uz publiski pieejamo un kopīgojamo informāciju.

3. Sertifikācijas ziņojumā ietver vismaz šādu informāciju:

   a) kopsavilkums;

   b) IKT izstrādājuma identifikācija;

   c) kontaktinformācija, kas saistīta ar IKT izstrādājuma izvērtēšanu;

   d) drošības politika;

   e) pieņēmumi un tvēruma precizēšana;

   f) arhitektūras informācija;

   g) attiecīgā gadījumā – papildinformācija par kiberdrošību;

   h) IKT izstrādājuma izvērtējuma kopsavilkums un izvērtētā konfigurācija;

   i) izvērtēšanas rezultāti un informācija par sertifikātu;

   j) attiecīgā gadījumā piezīmes un ieteikumi;

   k) attiecīgā gadījumā pielikumi;

   l) atsauce uz sertifikācijai iesniegtā IKT izstrādājuma drošības mērķi;

   m) ar shēmu saistītā zīme vai marķējums, ja tāds ir;

   n) glosārijs, ja tāds ir;

   o) bibliogrāfija.

4. Kopsavilkumā, kas minēts 3. punkta a) apakšpunktā, ir visa sertifikācijas ziņojuma īss kopsavilkums. Tajā sniedz skaidru un kodolīgu pārskatu par izvērtēšanas rezultātiem un ietver šādu informāciju:

   a) izvērtētā IKT izstrādājuma nosaukums;

   b) novērtējumu veikušā *ITSEF* nosaukums;

   c) izvērtēšanas pabeigšanas datums;

   d) sertifikāta izsniegšanas datums;

   e) attiecīgā gadījumā sākotnējā sertifikāta izsniegšanas datums;

   f) derīguma periods;

   g) sertifikāta unikālais identifikators, kā aprakstīts 11. pantā;

   h) īss sertifikācijas ziņojuma rezultātu apraksts, ieskaitot šādu informāciju:

      i) izvērtējumam piemēroto vienoto kritēriju redakcija un attiecīgā gadījumā laidiens;

      ii) vienoto kritēriju apliecinājuma pakete vai drošības apliecinājuma komponenti, AVA_VAN līmenis, kas piemērots izvērtēšanā, un tā attiecīgais apliecinājuma līmenis, kā noteikts Regulas (ES) 2019/881 52. pantā, uz kuru attiecas *EUCC* sertifikāts;

      iii) attiecīgā gadījumā aizsardzības profils(-i), kuram(-iem), kā norādīts, IKT izstrādājums atbilst;

      iv) atsauce uz izvērtētā IKT izstrādājuma drošības politiku;

      v) attiecīgā gadījumā atruna(-as).

5. 3. punkta b) apakšpunktā minētajā identifikācijā skaidri norāda izvērtēto IKT izstrādājumu, tai skaitā sniedz šādu informāciju:

   a) izvērtētā IKT izstrādājuma unikālā identifikācija;

   b) to IKT izstrādājuma komponentu uzskaitījums, ko aptver izvērtējums, norādot katra komponenta versijas numuru;

   c) atsauce uz papildu prasībām sertificētā IKT izstrādājuma darbības videi.

6. 3. punkta c) apakšpunktā minētajā kontaktinformācijā iekļauj vismaz šādu informāciju:

   a) izstrādātāja nosaukums;

   b) *EUCC* sertifikāta turētāja vārds, uzvārds / nosaukums un kontaktinformācija;

   c) sertifikātu izdevušās sertifikācijas struktūras nosaukums;

   d) atbildīgā valsts kiberdrošības sertifikācijas iestāde;

   e) tā *ITSEF* nosaukums, kas veicis izvērtēšanu, un attiecīgā gadījumā apakšuzņēmēju saraksts.

7. 3. punkta d) apakšpunktā minētajā drošības politikā iekļauj aprakstu par IKT izstrādājuma drošības politiku kā drošības pakalpojumu un politikas vai noteikumu, kas ar izvērtēto IKT izstrādājumu jāievieš vai jāievēro, kolekciju. Tajā iekļauj arī šādu informāciju:

   a) sertifikāta turētāja vārīgo vietu pārvaldības un vārīgo vietu atklāšanas procedūru apraksts, kurā iekļauj tikai informāciju, kuru var darīt publiski pieejamu;

   b) sertifikāta turētāja apliecinājuma pastāvīguma politika, tai skaitā attiecīgā gadījumā sertifikāta turētāja dzīves cikla pārvaldības vai ražošanas procesu apraksts saskaņā ar IV pielikuma IV.1. iedaļu;

   c) attiecīgā gadījumā ielāpu pārvaldības procedūras esību un tās novērtējuma rezultātus saskaņā ar IV pielikuma IV.4. iedaļu.

8. 3. punkta e) apakšpunktā minētie pieņēmumi un darbības jomas precizējums ietver informāciju par apstākļiem un mērķiem, kas saistīti ar izstrādājuma paredzēto lietojumu, kā minēts 7. panta 1. punkta c) apakšpunktā, un ietver šādu informāciju:

   a) pieņēmumus par IKT izstrādājuma izmantošanu un izvēršanu minimālo prasību veidā, piemēram, attiecībā uz pareizu uzstādīšanu un konfigurāciju un izpildāmām aparatūras prasībām;

   b) pieņēmumus par vidi IKT izstrādājuma atbilstīgai ekspluatācijai;

   c) aprakstu par jebkādiem IKT izstrādājuma apdraudējumiem, kurus nekompensē izstrādājuma novērtētās drošības funkcijas atbilstoši paredzētajam lietojumam, ja tos uzskata par būtisku potenciālam IKT izstrādājuma lietotājam.

   Pirmajā apakšpunktā uzskaitītajai informācijai jābūt maksimāli skaidrai un saprotamai, lai sertificētā IKT izstrādājuma iespējamie lietotāji varētu pieņemt pamatotus lēmumus par riskiem, kas saistīti ar tā lietošanu.

9. 3. punkta f) apakšpunktā minētajā arhitektūras informācijā ietver IKT izstrādājuma un tā galveno komponentu augsta līmeņa aprakstu, pamatojoties uz nodevumiem, kas noteikti vienoto kritēriju apliecinājumu saimē: izstrāde – *TOE* koncepcija (ADV_TDS).

10. 3. punkta g) apakšpunktā minētajā kiberdrošības papildinformācijā iekļauj saiti uz Regulas (ES) 2019/881 55. pantā minētā *EUCC* sertifikāta turētāja tīmekļa vietni.

11. Šā panta 3. punkta h) apakšpunktā minētajā IKT izstrādājuma izvērtēšanā un konfigurācijā apraksta gan izstrādātāja, gan vērtētāja testēšanas centienus, izklāstot testēšanas pieeju, konfigurāciju un dziļumu. Tajā ietver vismaz šādu informāciju:

    a) izmantoto apliecinājuma komponentu identifikāciju no 3. pantā minētajiem standartiem;

    b) aktuālā dokumenta redakciju un papildu drošības izvērtēšanas kritērijus, kas izmantoti izvērtēšanā;

    c) testēšanai un vārīgo vietu analīzei izmantotā *TOE* iestatījumus un konfigurāciju;

    d) izmantoto aizsardzības profilu, ietverot šādu informāciju: aizsardzības profila nosaukums, versija, datums un sertifikāts.

12. Izvērtēšanas rezultāti un informācija par 3. punkta i) apakšpunktā minēto sertifikātu ietver informāciju par panākto apliecinājuma līmeni, kā minēts šīs regulas 4. pantā un Regulas (ES) 2019/881 52. pantā.

13. Piezīmes un ieteikumus, kas minēti 3. punkta j) apakšpunktā, izmanto, lai sniegtu papildu informāciju par izvērtēšanas rezultātiem. Šie komentāri un ieteikumi var izpausties kā IKT izstrādājuma trūkumi, kas atklāti izvērtēšanas laikā, vai kā norādes uz funkcijām, kas ir īpaši noderīgas.

14. Šā panta 3. punkta k) apakšpunktā minētos pielikumus izmanto, lai izklāstītu jebkādu papildu informāciju, kas var būt noderīga ziņojuma auditorijai, bet kas loģiski neatbilst noteiktajām ziņojuma iedaļām, tai skaitā gadījumos, kad ir pilnīgs drošības politikas apraksts.

15. 3. punkta l) apakšpunktā minēto drošības mērķi ar atsauci sasaista ar izvērtēto drošības mērķi. Izvērtēto drošības mērķi norāda kopā ar sertifikācijas ziņojumu, lai to publicētu tīmekļa vietnē, kura norādīta Regulas (ES) 2019/881 50. panta 1. punktā. Ja pirms publicēšanas ir nepieciešama novērtētā drošības mērķa cenzēšana, to veic saskaņā ar šīs regulas V pielikuma V.2. punktu.

16. Ar *EUCC* shēmu, kas minēta 3. punkta m) apakšpunktā, saistīto zīmi vai marķējumu var iekļaut sertifikācijas ziņojumā saskaņā ar 11. pantā izklāstītajiem noteikumiem un procedūrām.

17. 3. punkta n) apakšpunktā minēto glosāriju izmanto, lai palielinātu ziņojuma lasāmību, sniedzot tādu akronīmu vai terminu definīcijas, kuru nozīme var nebūt uzreiz skaidra.

18. 3. punkta o) apakšpunktā minētajā bibliogrāfijā iekļauj atsauces uz visiem dokumentiem, kas izmantoti sertifikācijas ziņojuma izstrādē. Šajā informācijā iekļauj vismaz šādas ziņas:

    a) izmantotos drošības izvērtēšanas kritērijus, aktuālos dokumentus un attiecīgās papildu specifikācijas;

    b) izvērtēšanas tehnisko ziņojumu;

    c) attiecīgā gadījumā salikta izvērtējuma izvērtēšanas tehnisko ziņojumu;

    d) tehnisko atsauces dokumentāciju;

    e) izstrādātāja drošības norādījumus;

    f) izstrādātāja konfigurācijas sarakstu.

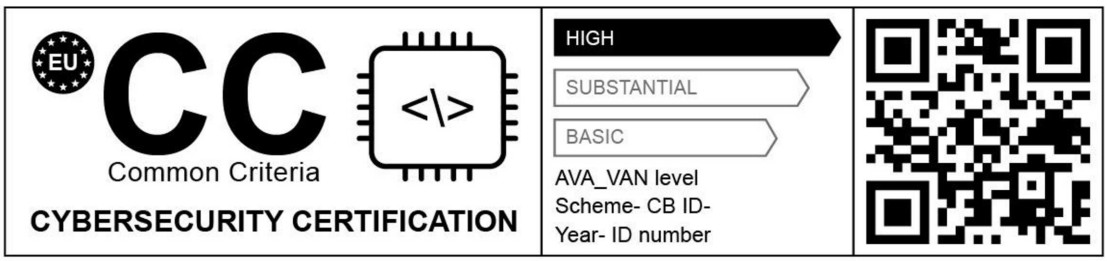
    Lai nodrošinātu izvērtējuma atkārtojamību, visa minētā dokumentācija ir unikāli jāidentificē, norādot pareizu izlaišanas datumu un pareizu redakcijas numuru.”

VI PIELIKUMS

"IX PIELIKUMS

Zīme un marķējums

1. Zīmes un marķējuma attēls:



2. Zīmi un marķējumu samazinot vai palielinot, ievēro 1. punktā dotās proporcijas.

3. Ja zīmi un marķējumu izmanto fiziski, tiem jābūt vismaz 5 mm augstiem."