Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/2462

2025 12 9

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2025/2462

2025 m. gruodžio 8 d.

kuriuo dėl apibrėžčių, IRT produktų serijos sertifikavimo, saugumo užtikrinimo tęstinumo ir naujausių dokumentų iš dalies keičiamas Įgyvendinimo reglamentas (ES) 2024/482

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentą (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013, (Kibernetinio saugumo aktą) ([1]), ypač į jo 49 straipsnio 7 dalį,

kadangi:

(1) Komisijos įgyvendinimo reglamentu (ES) 2024/482 ([2]) nustatomos su bendraisiais kriterijais grindžiama Europos kibernetinio saugumo sertifikavimo schema (EKSSS) susijusios funkcijos, taisyklės ir pareigos, taip pat tos schemos struktūra, atitinkanti Reglamente (ES) 2019/881 nustatytą Europos kibernetinio saugumo sertifikavimo sistemą;

(2) su bendraisiais kriterijais taikoma bendra vertinimo metodika – tarptautinis informacijos saugumo vertinimo standartas – leidžia sertifikavimo tikslais įvertinti IRT produktų saugumą. Atsižvelgiant į tai, kai kurie IRT produktai gali būti kuriami tuo pačiu funkciniu pagrindu, kad būtų galima siūlyti panašias saugumo funkcijas įvairiose platformose ar prietaisuose, tai vadinama produktų serijomis. Tačiau IRT produktų dizainas, aparatinė įranga, aparatinė programinė įranga ar programinė įranga gali skirtis. Sertifikavimo įstaiga kiekvienu konkrečiu atveju turi nuspręsti, ar galima sertifikuoti produktų seriją. Produktų serijos sertifikavimo sąlygos galėtų būti išsamiau paaiškintos pagalbinėse EKSSS gairėse;

(3) siekiant išlaikyti sertifikuotų produktų patikimumą, būtina apibrėžti, kas yra svarbus vertinimo objekto ar jo aplinkos, įskaitant jo naudojimo ar programavimo aplinką, pakeitimas ir kas yra nedidelis pakeitimas. Todėl šias sąvokas būtina patikslinti atsižvelgiant į esamas ir plačiai naudojamas vyresniųjų pareigūnų grupės informacinių sistemų saugumo klausimams ir susitarimų dėl bendrųjų kriterijų sertifikatų pripažinimo IT saugumo srityje dalyvių parengtas technines specifikacijas;

(4) nedideliems pakeitimams dažnai būdingas ribotas poveikis išduotame EKSSS sertifikate pateiktam gaminio saugumo užtikrinimo pareiškimui. Todėl nedideli pakeitimai turėtų būti valdomi pagal techninės priežiūros procedūras ir iš naujo vertinti produkto saugumo funkcijų dėl jų nereikia. Nedidelių pakeitimų, kurie turėtų būti sprendžiami atliekant techninę priežiūrą, pavyzdžiai, be kita ko, yra redakciniai pakeitimai, tikslinės vertinimo aplinkos pakeitimai, kuriais sertifikuotas vertinimo objektas nekeičiamas, ir sertifikuoto vertinimo objekto pakeitimai, kurie saugumo užtikrinimo įrodymams poveikio neturi. Programavimo aplinkos pakeitimai taip pat gali būti laikomi nedideliais, jei jie neturi tolesnio poveikio esamoms saugumo užtikrinimo priemonėms. Tačiau tam tikrais atvejais gali reikėti atlikti dalinį atitinkamų priemonių vertinimą;

([1]) OL L 151, 2019 6 7, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.
([2]) 2024 m. sausio 31 d. Komisijos įgyvendinimo reglamentas (ES) 2024/482, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2019/881 taikymo taisyklės dėl bendraisiais kriterijais grindžiamos Europos kibernetinio saugumo sertifikavimo schemos (EKSSS) priėmimo, (OL L, 2024/482, 2024 2 7, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) svarbus pakeitimas yra bet koks sertifikuoto vertinimo objekto arba jo aplinkos pakeitimas, kuris gali neigiamai paveikti EKSSS sertifikate nurodytą saugumo užtikrinimą, todėl jį reikėtų iš naujo įvertinti. Svarbių pakeitimų pavyzdžiai, be kita ko, apima deklaruojamų saugumo užtikrinimo reikalavimų rinkinio pakeitimus, išskyrus bendrųjų kriterijų ALC_FLR grupės saugumo užtikrinimo reikalavimus (trūkumų šalinimas); programavimo aplinkos konfidencialumo arba vientisumo kontrolės pakeitimus, kai tokie pakeitimai galėtų turėti įtakos saugiam vertinimo objekto programavimui ar gamybai, arba vertinimo objekto pakeitimus siekiant pašalinti išnaudojamą pažeidžiamumą. Be to, nedidelių pakeitimų, kurie kartu daro didelį poveikį saugumui, rinkinys taip pat gali būti laikomas svarbiu pakeitimu. Taip pat svarbu pripažinti, kad nors klaidų ištaisymas gali turėti įtakos tik tam tikram vertinimo objekto aspektui, jo nenuspėjamumas ir galimas poveikis saugumo užtikrinimui gali lemti tai, kad jis bus laikomas svarbiu pakeitimu, jei dėl jo pablogėja sertifikavimu užtikrintos saugumo garantijos;

(6) pasikeitus sertifikuoto IRT produkto grėsmės aplinkai gali reikėti atlikti pakartotinį vertinimą, nors pats IRT produktas nepakito. Turėtų būti aiškiai nustatyti galimi tokio pakartotinio vertinimo proceso rezultatai, visų pirma jo poveikis EKSSS sertifikatui. Jei pakartotinis vertinimas užbaigtas sėkmingai, sertifikavimo įstaiga turėtų patvirtinti sertifikatą arba išduoti naują sertifikatą, kurio galiojimo pabaigos terminas pratęstas. Jei pakartotinio vertinimo proceso rezultatas neigiamas, sertifikavimo įstaiga turėtų panaikinti sertifikatą ir galbūt išduoti naują kitokios taikymo srities sertifikatą. Tokios nuostatos turėtų būti taikomos *mutatis mutandis* pakartotiniam apsaugos profilių vertinimui;

(7) Įgyvendinimo reglamento (ES) 2024/482 I priede išvardyti taikytini naujausi IRT produktų ir apsaugos profilių vertinimo dokumentai. Tie naujausi dokumentai turėtų būti atnaujinti, kad būtų atsižvelgta į naujausius pokyčius, pavyzdžiui, susijusius su technologine plėtra, kibernetinių grėsmių aplinka, sektoriaus praktika ar tarptautiniais standartais. Toks atnaujinimas reikalingas naujausiems dokumentams, susijusiems su būtiniausiais objekto saugumo reikalavimais, išpuolio potencialo taikymu lustinėms kortelėms, išpuolio potencialo taikymu aparatinės įrangos įtaisams su apsauginėmis dėžėmis, bendrųjų kriterijų taikymu integriniams grandynams ir sudėtinio produkto vertinimu, taikomu lustinėms kortelėms ir panašiems prietaisams. Be to, neįtraukti naujausi dokumentai, susiję su sudėtinių produktų vertinimu ir sertifikavimu pagal naujausią bendrųjų kriterijų standartų versiją, pakartotiniu objekto audito rezultatų naudojimu ir paaiškinimais dėl apsaugos profilių, susijusių su kvalifikuotais elektroninio parašo kūrimo įtaisais, tachografais ir aparatinės įrangos saugumo moduliais, aiškinimo. Siekiant užtikrinti vienodą IRT produktų vertinimą pagal EKSSS, I priedas turėtų būti iš dalies pakeistas, kad į jį būtų įtraukti tie atnaujinti ir nauji naujausi dokumentai, kai juos patvirtins Europos kibernetinio saugumo sertifikavimo grupė (EKSSG);

(8) be to, į schemą turėtų būti įtrauktas naujausias dokumentas „ADV_SPM.1 interpretation for CC:2022 transition“ („ADV_SPM.1 aiškinimas CC:2022 pereinamuoju laikotarpiu“), siekiant užtikrinti, kad sertifikavimo procesai, grindžiami konkrečiais apsaugos profiliais, galėtų būti tęsiami naudojant oficialų modeliavimą (ADV_SPM.1), kol bus atnaujinti atitinkami apsaugos profiliai, pavyzdžiui, įtraukiant CC:2022 atitinkančią keleriopo saugumo užtikrinimo profilio konfigūraciją, kuri palaiko ADV_SPM.1. Siekiant suteikti pakankamai laiko rinkai pereiti prie atnaujintų bendrųjų kriterijų standartų, reikia numatyti specialias pereinamojo laikotarpio taisykles apsaugos profiliams „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, arba „Java Card System – Open Configuration“ (v3.1), BSI-CC-PP-0099-V2–2020. Kad būtų išvengta rinkos sutrikdymo, tikslinga nustatyti, kad naujausias dokumentas dėl ADV_SPM.1 aiškinimo CC:2022 pereinamuoju laikotarpiu būtų taikomas sertifikavimo procesams, kurie buvo pradėti prieš priimant šį reglamentą. Tačiau šis dokumentas turėtų būti taikomas griežtai tik tiek, kiek būtina, atsižvelgiant į laiką, kurio reikia atitinkamų apsaugos profilių atnaujinimui užbaigti. Tiksliau, kalbant apie sertifikavimo procesus, kuriuose naudojami apsaugos profiliai „Security IC Platform PP with Augmentation Packages“ (v1.0), BSI-CC-PP-0084-2014, arba „Java Card System – Closed Configuration“ (v3.1), BSI-CC-PP-0101-V2-2020, naujausias dokumentas turėtų būti taikomas procesams, kurie buvo pradėti iki 2026 m. spalio 1 d. Sertifikavimo procesams, kuriuose naudojamas apsaugos profilis „Java Card System – Open Configuration“ (v3.1), BSI-CC-PP-0099-V2-2020, naujausias dokumentas turėtų būti taikomas tik tiems procesams, kurie buvo pradėti iki šio reglamento įsigaliojimo dienos, atsižvelgiant į tai, kad jau yra nauja apsaugos profilio „Java Card System – Open Configuration“ versija;

(9) pakeitus naujausius dokumentus sertifikavimo proceso metu, gali būti sutrikdytas produkto vertinimas ir uždelstas sertifikato išdavimas. Todėl naujiems arba atnaujintiems naujausiems dokumentams reikia tinkamų pereinamojo laikotarpio taisyklių, kad pardavėjai, ITSVĮ, sertifikavimo įstaigos ir kiti suinteresuotieji subjektai galėtų atlikti reikiamus pakeitimus. Taikytini atnaujinti ir nauji naujausi dokumentai turėtų būti susiję su sertifikavimo paraiškomis, įskaitant pakartotinio vertinimo paraiškas, o jau vykstantiems sertifikavimo procesams turėtų būti galima toliau naudoti ankstesnes naujausių dokumentų versijas;

(10) Įgyvendinimo reglamento (ES) 2024/482 II ir III prieduose išvardyti atitinkamai apsaugos profiliai, sertifikuoti AVA_VAN 4 arba 5 lygiu, ir rekomenduojami apsaugos profiliai. Kelios nuorodos yra neišsamios arba dėl apsaugos profilių atnaujinimo yra pasenusios. Tos nuorodos turėtų būti atnaujintos, be to, turėtų būti įtrauktos naujos nuorodos, kad būtų užtikrinta geresnė saugių integrinių grandynų, lustinių kortelių ir susijusių prietaisų bei patikimumo kompiuterijos aprėptis;

(11) būtina iš dalies pakeisti Įgyvendinimo reglamento (ES) 2024/482 19 straipsnį, siekiant paaiškinti, kad IV priedas su būtinais pakeitimais taikomas atliekant apsaugos profilių EKSSS sertifikatų peržiūrą;

(12) atsižvelgiant į tai, kad saugumo uždavinys yra pagrindinis elementas, leidžiantis suprasti sertifikavimo proceso apimtį, taip pat būtina, kad ENISA savo interneto svetainėje paskelbtų kiekvieną EKSSS sertifikatą atitinkantį saugumo uždavinį;

(13) be to, sertifikavimo įstaigos turėtų ENISA pateikti saugumo uždavinio aprašą ir sertifikavimo ataskaitą anglų kalba, kad agentūra galėtų tą informaciją anglų kalba pateikti atitinkamoje interneto svetainėje pagal Įgyvendinimo reglamento (ES) 2024/482 42 straipsnio 2 dalį. Dėl šios priežasties pareiškėjai, prašantys išduoti sertifikatą, turėtų sertifikavimo įstaigoms pateikti saugumo uždavinio aprašą anglų kalba, kai to prašoma;

(14) nebūtina sertifikavimo įstaigos pavadinimo nuorodos pateikti unikaliame sertifikato identifikatoriuje, nes sertifikavimo įstaigos identifikacinio numerio pakanka šiai įstaigai vienareikšmiškai identifikuoti. Išdavimo mėnesio taip pat nereikia nurodyti, nes sertifikatai skaičiuojami metų intervalais. Todėl supaprastinimo tikslais tas reikalavimas turėtų būti išbrauktas. Kadangi sertifikato išdavimo metai yra pirmojo sertifikato išdavimo metai, ta pati data turėtų būti nurodyta po peržiūros išduotuose sertifikatuose, kad būtų užtikrintas atsekamumas;

(15) todėl Įgyvendinimo reglamentas (ES) 2024/482 turėtų būti atitinkamai iš dalies pakeistas;

(16) šiame reglamente nustatytos priemonės atitinka pagal Reglamento (ES) 2019/881 66 straipsnį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Įgyvendinimo reglamentas (ES) 2024/482 iš dalies keičiamas taip:

1) 2 straipsnis papildomas 16, 17 ir 18 punktais:

„16) produktų serija – pareiškėjo IRT produktų rinkinys, kuris grindžiamas tuo pačiu funkciniu pagrindu siekiant patenkinti tuos pačius saugumo poreikius ir kuriam priklausančių IRT produktų dizainas, aparatinė įranga, aparatinė programinė įranga ar programinė įranga gali skirtis;

17) nedidelis pakeitimas – sertifikuoto vertinimo objekto arba jo aplinkos pakeitimas, kuris nedaro neigiamo poveikio EKSSS sertifikate nurodytam saugumo užtikrinimui;

18) svarbus pakeitimas – sertifikuoto vertinimo objekto arba jo aplinkos pakeitimas, kuris gali neigiamai paveikti EKSSS sertifikate nurodytą saugumo užtikrinimą.“;

2) 5 straipsnis papildomas 3 dalimi:

„3. Sertifikavimo įstaiga gali leisti sertifikuoti produktų seriją.“;

3) 9 straipsnio 2 dalies a punktas pakeičiamas taip:

„a) pateikti sertifikavimo įstaigai ir ITSVĮ visą būtiną išsamią ir teisingą informaciją ir paprašius pateikti būtiną papildomą informaciją, įskaitant saugumo uždavinio aprašą anglų kalba;“;

4) 11 straipsnio 3 dalies b punktas pakeičiamas taip:

„b) unikalus sertifikato identifikavimo kodas, kurį sudaro:

1) schemos pavadinimas;

2) sertifikatą išdavusios sertifikavimo įstaigos identifikacinis numeris pagal Įgyvendinimo reglamento (ES) 2024/3143 3 straipsnį;

3) pradinio sertifikato išdavimo metai;

4) sertifikatą išdavusios sertifikavimo įstaigos priskirtas identifikacinis numeris.“;

5) 19 straipsnio 1 dalis pakeičiama taip:

„1. Sertifikato turėtojo prašymu arba dėl kitų pagrįstų priežasčių sertifikavimo įstaiga gali nuspręsti peržiūrėti apsaugos profilio EKSSS sertifikatą. Peržiūra atliekama pagal IV priedą. Peržiūros apimtį nustato sertifikavimo įstaiga. Jei tai būtina peržiūrai atlikti, sertifikavimo įstaiga paprašo ITSVĮ atlikti pakartotinį sertifikuoto apsaugos profilio vertinimą.“;

6) 42 straipsnis iš dalies keičiamas taip:

a) 1 dalis papildoma i punktu:

„i) saugumo uždavinį, atitinkantį kiekvieną EKSSS sertifikatą.“;

b) 2 dalis pakeičiama taip:

„2. 1 dalyje nurodyta informacija pateikiama bent anglų kalba. Tuo tikslu sertifikavimo įstaigos pateikia ENISA sertifikavimo ataskaitas ir saugumo uždavinių aprašus originalo kalba ir, be to, nepagrįstai nedelsdamos pateikia tokius dokumentus anglų kalba.“;

7) 48 straipsnio 4 dalis pakeičiama taip:

„4. Jei I arba II priede nenurodyta kitaip, naujausi dokumentai taikomi sertifikavimo procesams, įskaitant pakartotinio vertinimo procesus, pradėtiems nuo pakeitimų akto, kuriuo tie naujausi dokumentai buvo įtraukti į I arba II priedą, taikymo pradžios dienos.“;

8) I priedas pakeičiamas šio reglamento I priedo tekstu;

9) II priedas pakeičiamas šio reglamento II priedo tekstu;

10) III priedas pakeičiamas šio reglamento III priedo tekstu;

11) IV priedas iš dalies keičiamas pagal šio reglamento IV priedą;

12) V priedas iš dalies keičiamas pagal šio reglamento V priedą;

13) IX priedas pakeičiamas šio reglamento VI priedo tekstu.

2 straipsnis

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2025 m. gruodžio 8 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN

I PRIEDAS

„I PRIEDAS

Techninėms sritims svarbūs naujausi dokumentai ir kiti naujausi dokumentai

1. AVA_VAN 4 arba 5 lygio techninėms sritims svarbūs naujausi dokumentai:
   a) šie dokumentai, susiję su techninės srities „Lustinės kortelės ir panašios priemonės“ suderintu vertinimu:
      1) „Minimum ITSEF requirements for security evaluations of smart cards and similar devices“ („ITSVĮ taikomi būtiniausi lustinių kortelių ir panašių priemonių saugumo vertinimo reikalavimai“), 1.1 versija;
      2) „Minimum Site Security Requirements“ („Būtiniausi objekto saugumo reikalavimai“), 2 versija;
      3) „Reusing evaluation results of site audits (STAR)“ („Pakartotinis objekto audito rezultatų panaudojimas (STAR)“), 1 versija;
      4) „Application of Common Criteria to integrated circuits“ („Bendrųjų kriterijų taikymas integriniams grandynams“), 2 versija;
      5) „Security Architecture requirements (ADV_ARC) for smart cards and similar devices“ („Lustinėms kortelėms ir panašioms priemonėms taikomi saugumo architektūros reikalavimai (ADV_ARC)“), 1.1 versija;
      6) „Certification of „open“ smart card products“ („Atviruųjų lustinių kortelių produktų sertifikavimas“), 1.1 versija;
      7) „Composite product evaluation for smart cards and similar devices CC3.1“ („Sudėtinių produktų vertinimas, taikomas lustinėms kortelėms ir panašioms priemonėms“), 2 versija;
      8) „Composite product evaluation and certification for CC:2022“ („Sudėtinių produktų vertinimas ir sertifikavimas pagal CC:2022“), 1 versija;
      9) „Application of Attack Potential to Smartcards and Similar Devices“ („Išpuolio potencialo taikymas lustinėms kortelėms ir panašioms priemonėms“), 2 versija;
      10) „Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices“ („Kvalifikuotų elektroninio parašo ir spaudo kūrimo įtaisų saugumo vertinimas ir sertifikavimas“), 1 versija;
      11) „ADV_SPM.1 interpretation for CC:2022 transition“ („ADV_SPM.1 aiškinimas CC:2022 pereinamuoju laikotarpiu“), 1.1 versija, taikytinas sertifikavimo procesams, kuriuose naudojami šie apsaugos profiliai:
         a) „Security IC Platform PP with Augmentation Packages“ (v1.0), BSI-CC-PP-0084-2014, arba „Java Card System – Closed Configuration“ (v3.1), BSI-CC-PP-0101-V2-2020 – procesams, pradėtiems iki 2026 m. spalio 1 d.;
         b) „Java Card System – Open Configuration“ (v3.1), BSI-CC-PP-0099-V2-2020 – procesams, pradėtiems iki 2025 m. gruodžio 29 d.;
   b) šie dokumentai, susiję su techninės srities „Aparatinės įrangos įtaisai su apsauginėmis dėžėmis“ suderintu vertinimu:
      1) „Minimum ITSEF requirements for security evaluations of hardware devices with security boxes“ („ITSVĮ taikomi būtiniausi aparatinės įrangos įtaisų su apsauginėmis dėžėmis saugumo vertinimo reikalavimai“), 1.1 versija;
      2) „Minimum Site Security Requirements“ („Būtiniausi objekto saugumo reikalavimai“), 2 versija;
      3) „Reusing evaluation results of site audits (STAR)“ („Pakartotinis objekto audito rezultatų panaudojimas (STAR)“), 1 versija;
      4) „Application of Attack Potential to hardware devices with security boxes“ („Išpuolio potencialo taikymas aparatinės įrangos įtaisams su apsauginėmis dėžėmis“), 2 versija;
      5) „Hardware assessment in EN 419221-5 (HSM PP)“ („Aparatinės įrangos vertinimas pagal EN 419221-5 (HSM PP)“, 1 versija;
      6) „JIL Tachograph MS PP Clarification“ („JIL tachografo MS PP paaiškinimas“), 1 versija.
2. Naujausi dokumentai, susiję su suderintu atitikties vertinimo įstaigų akreditavimu:
   a) „Accreditation of ITSEFs for the EUCC“ („ITSVĮ akreditavimas taikyti EKSSS“), 1.1 versija, jei akreditacija suteikta iki 2025 m. liepos 8 d.;
   b) „Accreditation of ITSEFs for the EUCC“ („ITSVĮ akreditavimas taikyti EKSSS“), 1.6c versija, jei suteikta nauja akreditacija arba akreditacija peržiūrėta po 2025 m. liepos 8 d.;
   c) „Accreditation of CBs for the EUCC“ („Sertifikavimo įstaigų akreditavimas taikyti EKSSS“), 1.6b versija.“

II PRIEDAS

„II PRIEDAS

AVA_VAN 4 arba 5 lygiu sertifikuoti apsaugos profiliai

1. Nuotoliniams kvalifikuoto parašo ir spaudo kūrimo įtaisams:

   a) EN 419241-2:2019. Patikimos pasirašymo elektroniniu parašu sistemos. 2 dalis. Patvirtintų elektroninio parašo kūrimo įtaisų apsaugos profilis, skirtas pasirašymui elektroniniu parašu (v0.16), ANSSI-CC-PP-2018/02-M01;

   b) EN 419221-5:2018. Patikimumo užtikrinimo paslaugų teikėjų kriptografinių modulių apsaugos profiliai. 5 dalis. Patikimumo užtikrinimo paslaugoms skirtas kriptografinis modulis (v0.15), ANSSI-CC-PP-2016/05-M01.

2. Apsaugos profiliai, kurie buvo patvirtinti kaip naujausi dokumentai:

   [TUŠČIA].“

III PRIEDAS

„III PRIEDAS

Rekomenduojami apsaugos profiliai

Apsaugos profiliai, naudojami sertifikuojant IRT produktus, įskaitant techninių sričių produktus:

1. Lustinės kortelės ir panašios priemonės:
   a) pasas:
      1) „PP Machine Readable Travel Document with „ICAO Application" Basic Access Control" („Mašininio nuskaitymo kelionės dokumento su „ICAO taikomosios programos" bazine prieigos kontrole apsaugos profilis") (v1.10), BSI-CC-PP-0055-2009;
      2) „PP Machine Readable Travel Document using Standard Inspection Procedure with PACE" („Mašininio nuskaitymo kelionės dokumentas, kuriam taikoma standartinė patikrinimo procedūra su PACE apsaugos profilis") (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" („Mašininio nuskaitymo kelionės dokumento su „ICAO taikomosios programos" išplėstine prieigos kontrole su PACE apsaugos profilis") (v1.3), BSI-CC-PP-0056-V2-2012-MA-02;
   b) saugūs elektroninio parašo kūrimo įtaisai (SSCD):
      1) EN 419211-2:2013. Saugiojo elektroninio parašo kūrimo įtaiso apsaugos profiliai. 2 dalis. Įtaisas su rakto generatoriumi (v1.03), BSI-CC-PP-0059-2009-MA-02;
      2) EN 419211-3:2013. Saugiojo elektroninio parašo kūrimo įtaiso apsaugos profiliai. 3 dalis. Įtaisas su rakto importu (v1.0.2), BSI-CC-PP-0075-2012-MA-01;
      3) EN 419211-4:2013. Saugiojo elektroninio parašo kūrimo įtaiso apsaugos profiliai. 4 dalis. Įtaiso, generuojančio raktą ir užtikrinančio patikimą ryšį su liudijimo generavimo taikmeniu, plėtinys (V1.0.1), BSI-CC-PP-0071-2012-MA-01;
      4) EN 419211-5:2013. Saugiojo elektroninio parašo kūrimo įtaiso apsaugos profiliai. 5 dalis. Įtaiso, generuojančio raktą ir užtikrinančio patikimą ryšį su elektroninio parašo kūrimo taikmeniu, plėtinys (V1.0.1), BSI-CC-PP-0072-2012-MA-01;
      5) EN 419211-6:2014. Saugiojo elektroninio parašo kūrimo įtaiso apsaugos profiliai. 6 dalis. Įtaiso, atliekančio rakto importą ir užtikrinančio patikimą ryšį su elektroninio parašo kūrimo taikmeniu, plėtinys (V1.0.4), BSI-CC-PP-0076-2013-MA-01;
   c) tachografas: „Digital Tachograph – Tachograph Card" („Skaitmeninis tachografas. Tachografo kortelė") (TC PP) (v1.0), BSI-CC-PP-0091-2017;
   d) saugūs integriniai grandynai, „Java Card" platforma ir įtaisytoji universalioji lustinė kortelė:
      1) „Universal SIM Java Card Platform Protection Profile Basic and SCWS Configurations" („Universaliosios SIM „Java Card" platformos bazinis ir SCWS konfigūracijų apsaugos profilis") (v2.0.2), ANSSI-CC-PP-2010/04 (bazinis), ANSSI-CC-PP-2010/05 (bazinis ir SCWS);
      2) „Security IC Platform PP with Augmentation Packages" („Saugių integrinių grandynų platformos apsaugos profilis su papildomais paketais") (v1.0), BSI-CC-PP-0084-2014;
      3) „Embedded UICC (eUICC) for Machine-to-Machine Devices" („Įtaisytoji universalioji lustinė kortelė, skirta įrenginių tarpusavio sąveikos įtaisams") (v1.1), BSI-CC-PP-0089-2015;
      4) „Cryptographic Service Provider" („Šifravimo paslaugų teikėjas") (CSP) (v0.9.8), BSI-CC-PP-0104-2019;
      5) „Cryptographic Service Provider – Time Stamp Service and Audit" („Šifravimo paslaugų teikėjas. Laiko žymos paslauga ir auditas") (PPC-CSP-TS-Au), 0.9.5 versija, BSI-CC-PP-0107-2019;
      6) „Cryptographic Service Provider – Time Stamp Service, Audit and Clustering" („Šifravimo paslaugų teikėjas. Laiko žymos paslauga, auditas ir grupavimas" (PPC-CSP-TS-Au-Cl), 0.9.4 versija, BSI-CC-PP-0108-2019;
      7) „Java Card System – Closed Configuration" („Java" kortelių sistema. Uždara konfigūracija") (v3.1), BSI-CC-PP-0101-V2-2020;
      8) „Secure Element Protection Profile – GPC_SPE_174" („Saugaus elemento apsaugos profilis GPC_SPE_174") (v1.0), CCN-CC-PP-5-2021;
      9) „Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile" („Vienalustės sistemos saugaus posistemio (SoC 3S) apsaugos profilis") (v1.8), BSI-CC-PP-0117-V2-2023;
      10) „Java Card System – Open Configuration" („Java" kortelių sistema. Atvira konfigūracija") (v3.2), BSI-CC-PP-0099-V3-2024;
      11) „Embedded UICC for Consumer Devices Protection Profile" („Įtaisytosios universaliosios lustinės kortelės vartotojų įrenginiams apsaugos profilis") (v2.1), BSI-CC-PP-0100-V2-2025;
   e) patikimas platformos modulis: „Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0; Level 0; Revision 1.59" („Specialaus kliento kompiuterio patikimo platformos modulio apsaugos profilio specifikacijų grupė 2.0; 0 lygmuo; 1.59 redakcija") (v1.3), ANSSI-CC-PP-2021/02.

2. Aparatinės įrangos įtaisai su apsauginėmis dėžėmis:

   a) sąveikos (mokėjimo) punktai ir mokėjimo terminalai (POI):

      1) „Point of Interaction „POI-CHIP-ONLY““ („Sąveikos punktas „POI-CHIP-ONLY““) (v4.0), ANSSI-CC-PP-2015/01;

      2) „Point of Interaction POI-CHIP-ONLY and Open Protocol Package“ („Sąveikos punktas „POI-CHIP-ONLY ir atviro protokolo paketas“) (v4.0), ANSSI-CC-PP-2015/02;

      3) „Point of Interaction POI-COMPREHENSIVE“ („Sąveikos punktas POI-COMPREHENSIVE“) (v4.0), ANSSI-CC-PP-2015/03;

      4) „Point of Interaction POI-COMPREHENSIVE and Open Protocol Package“ („Sąveikos punktas POI-COMPREHENSIVE ir atviro protokolo paketas“) (v4.0), ANSSI-CC-PP-2015/04;

      5) „Point of Interaction „POI-PED-ONLY““ („Sąveikos punktas „POI-PED-ONLY““) (v4.0), ANSSI-CC-PP-2015/05;

      6) „Point of Interaction „POI-PED-ONLY and Open Protocol Package““ („Sąveikos punktas „POI-PED-ONLY ir atviro protokolo paketas““) (v4.0), ANSSI-CC-PP-2015/06;

   b) aparatinis saugumo modulis:

      1) „Cryptographic Module for CSP Signing Operations with Backup“ („Sertifikavimo paslaugų teikėjų pasirašymo operacijų kriptografinis modulis su atkūrimo galimybe“), PP CMCSOB 14167-2 (v0.35), ANSSI-CC-PP-2015/08;

      2) „Cryptographic Module for CSP key generation services“ („Sertifikavimo paslaugų teikėjų raktų generavimo paslaugų kriptografinis modulis“), PP CMCKG 14167-3 (v0.20), ANSSI-CC-PP-2015/09;

      3) „Cryptographic Module for CSP Signing Operations without Backup“ („Sertifikavimo paslaugų teikėjų pasirašymo operacijų kriptografinis modulis be atkūrimo galimybės“), PP CMCSO 14167-4 (v0.32), ANSSI-CC-PP-2015/10;

   c) tachografas:

      1) „Digital Tachograph – Motion Sensor“ („Skaitmeninis tachografas. Judėjimo jutiklis“) (MS PP) (v1.0), BSI-CC-PP-0093-2017;

      2) „Digital Tachograph – Vehicle Unit“ („Skaitmeninis tachografas. Transporto priemonės blokas“) (VU PP) (v1.15), BSI-CC-PP-0094-V2-2021;

      3) „Digital Tachograph – External GNSS Facility“ („Skaitmeninis tachografas. Išorinis GNSS įrenginys“) (EGF PP) (v1.10), BSI-CC-PP-0092-V2-2021.

3. Kita: „Trusted Execution Environment Protection Profile – GPD_SPE_021“ („Patikimos vykdymo aplinkos apsaugos profilis GPD_SPE_021“) (v1.3), ANSSI-CC-PP-2014/01-M02.“

IV PRIEDAS

Įgyvendinimo reglamento (ES) 2024/482 IV priedas iš dalies keičiamas taip:

1. IV.2 punkto 4 papunktis pakeičiamas taip:

„4. Sertifikavimo įstaiga peržiūri atnaujintą techninę vertinimo ataskaitą ir parengia pakartotinio vertinimo ataskaitą. Tuomet pirminio sertifikato būsena pakeičiama pagal 13 arba 19 straipsnį. Jei pakartotinio vertinimo rezultatas teigiamas, produkto sertifikavimo atveju taikomas 13 straipsnio 2 dalies a arba c punktas, o apsaugos profilio sertifikavimo atveju – 19 straipsnio 2 dalies a arba c punktas. Jei pakartotinio vertinimo rezultatas neigiamas, produkto sertifikavimo atveju taikomas 13 straipsnio 2 dalies b arba d punktas, o apsaugos profilio sertifikavimo atveju – 19 straipsnio 2 dalies b arba d punktas.“;

2. IV.3 punktas iš dalies keičiamas taip:

a) IV.3 punkto antraštė pakeičiama taip:

„IV.3. **Sertifikuoto IRT produkto pakeitimai. Techninė priežiūra ir pakartotinis vertinimas**“;

b) 4 ir 5 papunkčiai pakeičiami taip:

„4. Atlikusi patikrinimą, sertifikavimo įstaiga nustato, ar pakeitimas yra svarbus, ar jis yra nedidelis, atsižvelgiant į jo poveikį saugumo užtikrinimui, nurodytam EKSSS sertifikate.

5. Jei sertifikavimo įstaiga patvirtina, kad pakeitimai yra nedideli, pakeistam IRT produktui pagal 13 straipsnio 2 dalies a punktą arba 19 straipsnio 2 dalies a punktą naujas sertifikatas neišduodamas ir parengiama prie pradinės sertifikavimo ataskaitos pridedama techninės priežiūros ataskaita.“;

c) įterpiamas 5a papunktis:

„5a. Jei padaroma programavimo aplinkos saugumo užtikrinimo priemonių pakeitimų, įskaitant bendrųjų kriterijų ALC_FLR grupės saugumo užtikrinimo reikalavimų (trūkumų šalinimas) įtraukimą, sertifikavimo įstaiga gali prašyti ITSVĮ atlikti paveiktų saugumo užtikrinimo priemonių poaibio vertinimą. ITSVĮ parengia techninę dalinio vertinimo ataskaitą, o sertifikavimo įstaiga, remdamasi ta ataskaita, patvirtina, ar pakeitimai yra nedideli, ar svarbūs. Jei sertifikavimo įstaiga patvirtina, kad pakeitimai nedideli, taikomas IV.3 punkto 5 papunktis. Jei sertifikavimo įstaiga patvirtina, kad pakeitimai svarbūs, taikomas IV.3 punkto 7 papunktis.“

V PRIEDAS

Įgyvendinimo reglamento (ES) 2024/482 V priedo V.1 punktas pakeičiamas taip:

„V.1. **Sertifikavimo ataskaita**

1. Remdamasi ITSVĮ pateiktomis techninėmis vertinimo ataskaitomis, sertifikavimo įstaiga parengia sertifikavimo ataskaitą, kuri turi būti skelbiama kartu su atitinkamu EKSSS sertifikatu ir saugumo uždaviniu.

2. Sertifikavimo ataskaitoje pateikiama išsami ir praktinė informacija apie IRT produktą ir jo saugų diegimą. Todėl į ją įtraukiama visa viešai prieinama ir tinkama dalytis informacija, aktuali naudotojams ir suinteresuotosioms šalims. Viešai prieinama ir tinkama dalytis informacija sertifikavimo ataskaitoje gali būti pateikiama kaip nuoroda.

3. Sertifikavimo ataskaitoje pateikiama bent ši informacija:

   a) santrauka;

   b) IRT produkto identifikavimas;

   c) su IRT produkto vertinimu susijusi kontaktinė informacija;

   d) saugumo politika;

   e) prielaidos ir taikymo srities paaiškinimas;

   f) architektūros informacija;

   g) papildoma kibernetinio saugumo informacija, jei taikytina;

   h) IRT produkto vertinimo santrauka ir įvertinta konfigūracija;

   i) vertinimo rezultatai ir informacija apie sertifikatą;

   j) pastabos ir rekomendacijos, jei taikytina;

   k) priedai, jei taikytina;

   l) nuoroda į sertifikuoti pateikto IRT produkto saugumo uždavinį;

   m) jei yra, su schema susijęs ženklas arba etiketė;

   n) glosarijus, jei taikytina;

   o) bibliografija.

4. 3 dalies a punkte nurodyta santrauka yra trumpa visos sertifikavimo ataskaitos santrauka. Joje aiškiai ir glaustai apžvelgiami vertinimo rezultatai ir pateikiama ši informacija:

   a) įvertinto IRT produkto pavadinimas;

   b) vertinimą atlikusios ITSVĮ pavadinimas;

   c) vertinimo užbaigimo data;

   d) sertifikato išdavimo data;

   e) kai taikytina – pradinio sertifikato išdavimo data;

   f) galiojimo laikotarpis;

   g) unikalus sertifikato identifikatorius, aprašytas 11 straipsnyje;

   h) trumpas sertifikavimo ataskaitos rezultatų aprašymas, įskaitant:

      i) vertinimui taikytų bendrųjų kriterijų versiją ir, jei taikytina, laidą;

      ii) bendrųjų kriterijų saugumo užtikrinimo paketą arba saugumo užtikrinimo komponentų sąrašą, atliekant vertinimą taikytą AVA_VAN lygį ir atitinkamą saugumo užtikrinimo lygį, nurodytą EKSSS sertifikate, kaip nustatyta Reglamento (ES) 2019/881 52 straipsnyje;

      iii) kai taikytina, apsaugos profilį, kurį, kaip teigiama, atitinka IRT produktas;

      iv) nuorodą į vertinamo IRT produkto saugumo politiką;

      v) atsakomybės ribojimo pareiškimą, jei taikytina.

5. 3 dalies b punkte nurodytas identifikavimas turi aiškiai nurodyti įvertintą IRT produktą ir apimti šią informaciją:

a) unikalų įvertinto IRT produkto identifikatorių;

b) IRT produkto komponentų, kurie yra vertinimo dalis, sąrašą su kiekvieno komponento versijos numeriu;

c) nuorodą į papildomus reikalavimus, taikomus sertifikuoto IRT produkto veikimo (operacinei) aplinkai.

6. 3 dalies c punkte nurodytą kontaktinę informaciją sudaro bent ši informacija:

a) kūrėjo vardas ir pavardė (pavadinimas);

b) EKSSS sertifikato turėtojo vardas ir pavardė (pavadinimas) ir kontaktiniai duomenys;

c) EKSSS sertifikatą išdavusios sertifikavimo įstaigos pavadinimas;

d) atsakinga nacionalinė kibernetinio saugumo sertifikavimo institucija;

e) vertinimą atlikusios ITSVĮ pavadinimas ir, kai taikytina, subrangovų sąrašas.

7. 3 dalies d punkte nurodytos saugumo politikos apraše pateikiamas IRT produkto saugumo politikos aprašas, kaip saugumo užtikrinimo paslaugų ir politikos, kurios vykdymą įvertintas IRT produktas užtikrina, arba taisyklių, kurias tas produktas atitinka, rinkinys. Be to, į jį įtraukiama ši informacija:

a) sertifikato turėtojo pažeidžiamumo valdymo ir pažeidžiamumo atskleidimo procedūrų aprašas, kuriame pateikiama tik tokia informacija, kurią galima skelbti viešai;

b) sertifikato turėtojo saugumo užtikrinimo tęstinumo politika, įskaitant, kai taikytina, sertifikato turėtojo gyvavimo ciklo valdymo arba gamybos procesus pagal IV priedo IV.1 punktą;

c) kai taikytina, informacija apie tai, ar yra nustatyta pataisų valdymo procedūra ir jos vertinimo rezultatas pagal IV priedo IV.4 punktą.

8. 3 dalies e punkte nurodytų prielaidų ir taikymo srities paaiškinimo skirsnyje pateikiama informacija apie aplinkybes ir tikslus, susijusius su produkto numatyta paskirtimi, kaip nurodyta 7 straipsnio 1 dalies c punkte, ir į jį įtraukiama:

a) prielaidos dėl IRT produkto naudojimo ir diegimo, pateiktos kaip būtinieji reikalavimai, pvz., tinkamo įrengimo ir konfigūracijos bei aparatinės įrangos reikalavimai, kuriuos IRT produktas atitinka;

b) prielaidos dėl reikalavimus atitinkančio IRT produkto veikimo (operacinės) aplinkos;

c) grėsmių IRT produktui, kurių neužkardo įvertintos produkto saugumo funkcijos naudojant jį pagal numatytą paskirtį, aprašas, jei manoma, kad tai aktualu potencialiam IRT produkto naudotojui.

Pirmoje pastraipoje nurodyta informacija turi būti kuo aiškesnė ir suprantamesnė, kad potencialūs sertifikuoto IRT produkto naudotojai galėtų priimti informacija pagrįstus sprendimus dėl rizikos, susijusios su jo naudojimu.

9. 3 dalies f punkte nurodyta architektūros informacija apima IRT produkto ir pagrindinių jo komponentų apibendrinamąjį apibūdinimą remiantis siektinais rezultatais, apibrėžtais bendrųjų kriterijų saugumo užtikrinimo grupėje: „Development – TOE Design“ (ADV_TDS).

10. 3 dalies g punkte nurodytoje papildomoje kibernetinio saugumo informacijoje pagal Reglamento (ES) 2019/881 55 straipsnį pateikiama nuoroda į EKSSS sertifikato turėtojo interneto svetainę.

11. 3 dalies h punkte nurodytos IRT produkto vertinimo ir konfigūracijos skirsnyje aprašomos ir kūrėjo, ir vertintojo bandymų pastangos, bandymo metodas, konfigūracija ir išsamumas. Jame pateikiama bent ši informacija:

    a) informacija apie naudotus saugumo užtikrinimo komponentus, nurodytus 3 straipsnyje minimuose standartuose;

    b) naujausių dokumentų versija ir atliekant vertinimą taikyti papildomi saugumo vertinimo kriterijai;

    c) bandymams ir pažeidžiamumo analizei naudoti TOE nuostačiai ir konfigūracija;

    d) naudotas (jei naudotas) apsaugos profilis, be kita ko, nurodant šią informaciją: apsaugos profilio pavadinimą, versiją, datą ir sertifikatą.

12. 3 dalies i punkte nurodyti vertinimo rezultatai ir informacija apie sertifikatą apima informaciją apie pasiektą saugumo užtikrinimo lygį, kaip nurodyta šio reglamento 4 straipsnyje ir Reglamento (ES) 2019/881 52 straipsnyje.

13. 3 dalies j punkte nurodytų pastabų ir rekomendacijų skirsnyje gali būti pateikiama papildoma informacija apie vertinimo rezultatus. Tomis pastabomis ir rekomendacijomis gali būti apibūdinami vertinimo metu nustatyti IRT produkto trūkumai arba nurodomos itin naudingos savybės.

14. 3 dalies k punkte nurodytuose prieduose pateikiama papildoma informacija, kuri gali būti naudinga ataskaitos adresatams, bet logiškai netinkama pateikti kituose nurodytuose ataskaitos skirsniuose, įskaitant atvejus, kai išsamiai aprašoma saugumo politika.

15. 3 dalies l punkte nurodyto saugumo uždavinio skirsnyje nurodomas vertintas saugumo uždavinys. Vertintas saugumo uždavinys kartu su sertifikavimo ataskaita pateikiamas tam, kad jį būtų galima paskelbti Reglamento (ES) 2019/881 50 straipsnio 1 dalyje nurodytoje interneto svetainėje. Jeigu prieš paskelbiant reikia pašalinti neskelbtinus vertinto saugumo uždavinio duomenis, tai daroma pagal šio reglamento V priedo V.2 punktą.

16. 3 dalies m punkte nurodyti su EKSSS schema susiję ženklai ar etiketės į sertifikavimo ataskaitą įterpiami laikantis 11 straipsnyje nustatytų taisyklių ir procedūrų.

17. 3 dalies n punkte nurodytas glosarijus skirtas ataskaitos skaitomumui palengvinti – jame apibrėžiami akronimai ar terminai, kurių reikšmė gali nebūti akivaizdi.

18. 3 dalies o punkte nurodytos bibliografijos skirsnyje pateikiamos nuorodos į visus dokumentus, naudotus rengiant sertifikavimo ataskaitą. Ta informacija apima bent:

    a) saugumo vertinimo kriterijus, naujausius dokumentus ir kitas aktualias naudotas specifikacijas;

    b) techninę vertinimo ataskaitą;

    c) kai taikytina, techninę sudėtinio produkto vertinimo ataskaitą;

    d) techninius informacinius dokumentus;

    e) saugumo gaires kūrėjui;

    f) konfigūravimo sąrašą kūrėjui.

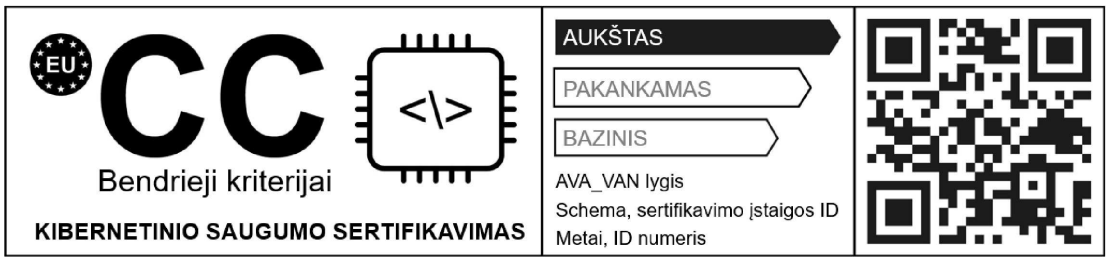
    Siekiant užtikrinti vertinimo atkuriamumą, visi nurodyti dokumentai turi būti vienareikšmiškai identifikuojami pagal jų tikrąją išleidimo datą ir tikrąjį versijos numerį.“

VI PRIEDAS

„IX PRIEDAS

Ženklas ir etiketė

1. Ženklo ir etiketės forma:



2. Jei ženklas ir etiketė sumažinami arba padidinami, turi būti išlaikomos 1 punkte nurodytos proporcijos.

3. Kai ženklas ir etiketė naudojami fiziniu pavidalu, jie turi būti bent 5 mm aukščio.“