►B

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2024/482

2024 m. sausio 31 d.

kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2019/881 taikymo taisyklės dėl bendraisiais kriterijais grindžiamos Europos kibernetinio saugumo sertifikavimo schemos (EKSSS) priėmimo

(Tekstas svarbus EEE)

(OL L 482, 2024 2 7, p. 1)

iš dalies keičiamas:

		Oficialusis leidinys		
		Nr.	puslapis	data
►M1	2024 m. gruodžio 18 d. Komisijos įgyvendinimo reglamentas (ES) 2024/3144	L 3144	1	2024 12 19

▼B

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2024/482

2024 m. sausio 31 d.

kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2019/881 taikymo taisyklės dėl bendraisiais kriterijais grindžiamos Europos kibernetinio saugumo sertifikavimo schemos (EKSSS) priėmimo

(Tekstas svarbus EEE)

I SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas ir taikymo sritis

Šiuo reglamentu nustatoma bendraisiais kriterijais grindžiama Europos kibernetinio saugumo sertifikavimo schema (EKSSS).

Šis reglamentas taikomas visiems informacinių ir ryšių technologijų (IRT) produktams, įskaitant jų dokumentus, kurie pateikiami sertifikuoti pagal EKSSS, ir visiems apsaugos profiliams, kurie pateikiami sertifikuoti vykdant IRT procesą, per kurį sertifikuojami IRT produktai.

2 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

▼M1

1) bendrieji kriterijai – standartuose ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 arba ISO/IEC 15408-5:2022 nustatyti bendrieji informacinių technologijų saugumo vertinimo kriterijai arba Susitarimo dėl bendrųjų kriterijų sertifikatų pripažinimo IT saugumo srityje dalyvių paskelbti (CC:2022 versija, 1–5 dalys) bendrieji informacinių technologijų saugumo vertinimo kriterijai;

2) bendra vertinimo metodika – standarte ISO/IEC 18045:2022 nustatyta bendra informacinių technologijų saugumo vertinimo metodika arba Susitarimo dėl bendrųjų kriterijų sertifikatų pripažinimo IT saugumo srityje dalyvių paskelbta (versija CEM:2022) bendra informacinių technologijų saugumo vertinimo metodika;

▼B

3) vertinimo objektas – IRT produktas ar jo dalis arba apsaugos profilis, kuris yra IRT proceso dalis, ir kuriam taikomas kibernetinio saugumo vertinimas siekiant gauti EKSSS sertifikatą;

4) saugumo uždavinys – pareiškimas dėl konkretaus IRT produkto saugumo reikalavimų, priklausomų nuo įgyvendinimo;

▼B

5) apsaugos profilis – IRT procesas, kuriuo nustatomi konkrečios kategorijos IRT produktų saugumo reikalavimai ir kuriuo tenkinami nuo įgyvendinimo nepriklausomi saugumo poreikiai bei kuris gali būti taikomas sertifikavimo tikslu vertinant tai konkrečiai kategorijai priskiriamus IRT produktus;

6) techninė vertinimo ataskaita – ITSVĮ parengtas dokumentas, kuriame pateikiamos išvados, sprendimai ir pagrindimai, gauti vertinant IRT produktą arba apsaugos profilį pagal šiame reglamente nustatytas taisykles ir pareigas;

7) ITSVĮ – informacinių technologijų saugumo vertinimo įstaiga, kuri yra Reglamento (EB) Nr. 765/2008 2 straipsnio 13 punkte apibrėžta atitikties vertinimo įstaiga, atliekanti vertinimo užduotis;

8) AVA_VAN lygis – saugumo užtikrinimo pažeidžiamumo analizės lygis, rodantis kibernetinio saugumo vertinimo veiklos, vykdomos siekiant nustatyti atsparumo galimam pasinaudojimui vertinimo objekto trūkumais ar silpnybėmis jo operacinėje aplinkoje, lygį, kaip nustatyta bendruosiuose kriterijuose;

9) EKSSS sertifikatas – kibernetinio saugumo sertifikatas, pagal EKSSS išduotas IRT produktams arba apsaugos profiliams, kurie gali būti naudojami tik IRT procese sertifikuojant IRT produktus;

10) sudėtinis produktas – IRT produktas, vertinamas kartu su kitu pagrindiniu IRT produktu, kuriam jau išduotas EKSSS sertifikatas ir nuo kurio saugumo funkcinių galimybių priklauso sudėtinis IRT produktas;

11) nacionalinė kibernetinio saugumo sertifikavimo institucija – valstybės narės pagal Reglamento (ES) 2019/881 58 straipsnio 1 dalį paskirta institucija;

12) sertifikavimo įstaiga – atitikties vertinimo įstaiga, kaip apibrėžta Reglamento (EB) Nr. 765/2008 2 straipsnio 13 punkte, kuri vykdo sertifikavimo veiklą;

13) techninė sritis – su konkrečia technologija susijusi suderinto sertifikavimo bendra techninė sistema su būdingais saugumo reikalavimais;

14) naujausias dokumentas – dokumentas, kuriame nurodomi vertinimo metodai, būdai ir priemonės, taikomi sertifikuojant IRT produktus, arba bendrosios IRT produktų kategorijos saugumo reikalavimai arba bet kokie kiti sertifikavimui būtini reikalavimai, siekiant suderinti vertinimą, visų pirma techninių sričių arba apsaugos profilių vertinimą;

15) rinkos priežiūros institucija – institucija, apibrėžta Reglamento (ES) 2019/1020 3 straipsnio 4 dalyje.

▼M1

3 straipsnis

Vertinimo standartai

1. Pagal EKSSS schemą atliekamiems vertinimams taikomi šie standartai:

a) bendrieji kriterijai;

b) bendra vertinimo metodika.

2. Iki 2027 m. gruodžio 31 d. sertifikatas gali būti išduodamas pagal EKSSS schemą, taikant vieną iš šių standartų:

a) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 arba ISO/IEC 15408-3:2008;

b) Susitarimo dėl bendrųjų kriterijų sertifikatų pripažinimo IT saugumo srityje dalyvių paskelbti bendrieji informacinių technologijų saugumo vertinimo kriterijai, 3.1 versija, 5 redakcija;

c) ISO/IEC 18045:2008;

d) Susitarimo dėl bendrųjų kriterijų sertifikatų pripažinimo IT saugumo srityje dalyvių paskelbta bendra informacinių technologijų saugumo vertinimo metodika, 5 versija, 3.1 redakcija.

3. Iki 2027 m. gruodžio 31 d. pagal EKSSS schemą gali būti išduodamas 1 dalyje nurodytais standartais grindžiamas sertifikatas, kuriuo pareiškiama atitiktis apsaugos profiliui, grindžiamam 2 dalyje išvardytais standartais.

4. Sertifikatas, grindžiamas 1 dalyje nurodytais standartais, taip pat gali būti išduodamas pagal EKSSS schemą ir juo pareiškiama atitiktis apsaugos profiliui, grindžiamam kuriuo nors iš toliau nurodytų standartų, jei naudoti tokį apsaugos profilį reikalaujama pagal Komisijos įgyvendinimo reglamentą (ES) 2016/799 ([1]), Europos Parlamento ir Tarybos reglamentą (ES) Nr. 910/2014 ([2]) arba Komisijos įgyvendinimo sprendimą (ES) 2016/650 ([3]):

([1]) 2016 m. kovo 18 d. Komisijos įgyvendinimo reglamentas (ES) 2016/799, kuriuo įgyvendinamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 165/2014 ir nustatomi tachografų ir jų komponentų konstrukcijos, bandymo, įrengimo, naudojimo ir remonto reikalavimai (OL L 139, 2016 5 26, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

([2]) 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (OL L 257, 2014 8 28, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) 2016 m. balandžio 25 d. Komisijos įgyvendinimo sprendimas (ES) 2016/650, kuriuo pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 30 straipsnio 3 dalį ir 39 straipsnio 2 dalį nustatomi kvalifikuotų parašo ir spaudo kūrimo įtaisų saugumo vertinimo standartai (OL L 109, 2016 4 26, p. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

▼M1

a) Susitarimo dėl bendrųjų kriterijų sertifikatų pripažinimo IT saugumo srityje dalyvių paskelbti bendrieji informacinių technologijų saugumo vertinimo kriterijai, 3.1 versija, 1–4 redakcijos;

b) Susitarimo dėl bendrųjų kriterijų sertifikatų pripažinimo IT saugumo srityje dalyvių paskelbta bendra informacinių technologijų saugumo vertinimo metodika, 3.1 versija, 1–4 redakcijos.

▼B

4 straipsnis

Saugumo užtikrinimo lygiai

1. Sertifikavimo įstaigos išduoda EKSSS sertifikatus, kuriuose nurodomas pakankamai aukštas arba aukštas saugumo užtikrinimo lygis.

2. EKSSS sertifikatai, kuriuose nurodomas pakankamai aukštas saugumo užtikrinimo lygis, atitinka sertifikatus, kuriuose nurodomas AVA_VAN 1 arba 2 lygis.

3. Aukšto saugumo užtikrinimo lygio EKSSS sertifikatai, kuriuose nurodomas aukštas saugumo užtikrinimo lygis, atitinka sertifikatus, kuriuose nurodomas AVA_VAN 3, 4 arba 5 lygis.

4. EKSSS sertifikate patvirtintas saugumo užtikrinimo lygis atskiriamas pagal reikalavimus atitinkantį ir padidintą užtikrinimo komponentų naudojimą, kaip nurodyta bendruosiuose kriterijuose pagal VIII priedą.

5. Atitikties vertinimo įstaigos taiko tuos užtikrinimo komponentus, nuo kurių priklauso pasirinktas AVA_VAN lygis, laikydamosi 3 straipsnyje nurodytų standartų.

5 straipsnis

IRT produktų sertifikavimo metodai

1. IRT produktas sertifikuojamas atsižvelgiant į su juo susijusį saugumo uždavinį:

a) kaip apibrėžė pareiškėjas, arba

▼M1

b) pareiškiant atitiktį sertifikuotam apsaugos profiliui vykdant IRT procesą, kai IRT produktas priskiriamas prie IRT produktų kategorijos, kuriai tas apsaugos profilis taikomas.

▼B

2. Apsaugos profiliai sertifikuojami tik siekiant sertifikuoti IRT produktus, priklausančius konkrečiai IRT produktų kategorijai, kuriai apsaugos profilis taikomas.

▼B

6 straipsnis

Savarankiškas atitikties vertinimas

Neleidžiama atlikti savarankiško atitikties vertinimo, kaip apibrėžta Reglamento (ES) 2019/881 53 straipsnyje.

II SKYRIUS

IRT PRODUKTŲ SERTIFIKAVIMAS

I SKIRSNIS

Specialieji vertinimo standartai ir reikalavimai

7 straipsnis

IRT produktų vertinimo kriterijai ir metodai

1. Sertifikavimui pateiktas IRT produktas vertinamas bent pagal:

a) taikytinus 3 straipsnyje nurodytų standartų elementus;

b) saugumo užtikrinimo reikalavimų klases, taikomas pažeidžiamumo vertinimo ir nepriklausomo funkcinio bandymo atvejais, kaip nustatyta 3 straipsnyje nurodytuose vertinimo standartuose;

c) rizikos, susijusios su numatyta atitinkamų IRT produktų paskirtimi pagal Reglamento (ES) 2019/881 52 straipsnį ir jų saugumo funkcijomis, kuriomis padedama siekti Reglamento (ES) 2019/881 51 straipsnyje nustatytų saugumo tikslų, lygį;

d) I priede išvardytus taikytinus naujausius dokumentus, ir

e) II priede išvardytus taikytinus sertifikuotus apsaugos profilius.

2. Išimtiniais ir tinkamai pagrįstais atvejais atitikties vertinimo įstaiga gali prašyti netaikyti atitinkamo naujausio dokumento. Tokiais atvejais atitikties vertinimo įstaiga informuoja nacionalinę kibernetinio saugumo sertifikavimo instituciją ir pateikia tinkamai pagrįstą savo prašymo pagrindimą. Nacionalinė kibernetinio saugumo sertifikavimo institucija įvertina išimties pagrindimą ir, jei ji pagrįsta, ją patvirtina. Atitikties vertinimo įstaiga sertifikatą išduoda tik po to, kai nacionalinė kibernetinio saugumo sertifikavimo institucija priima sprendimą. Nacionalinė kibernetinio saugumo sertifikavimo institucija nepagrįstai nedelsdama praneša apie patvirtintą išimtį Europos kibernetinio saugumo sertifikavimo grupei, kuri gali pateikti nuomonę. Nacionalinė kibernetinio saugumo sertifikavimo institucija kuo labiau atsižvelgia į Europos kibernetinio saugumo sertifikavimo grupės nuomonę.

▼B

3. IRT produktų sertifikavimas AVA_VAN 4 arba 5 lygiu galimas tik šiais atvejais:

a) jei IRT produktas priklauso kuriai nors I priede nurodytai techninei sričiai, jis vertinamas pagal taikytinus naujausius tų techninių sričių dokumentus,

b) jei IRT produktas priskiriamas prie IRT produktų, kuriems taikomas sertifikuotas apsaugos profilis, apimantis AVA_VAN 4 arba 5 lygius, ir kuris II priede nurodytas kaip naujausias apsaugos profilis, jis vertinamas pagal tam apsaugos profiliui taikomą vertinimo metodiką,

c) jei šios dalies a ir b punktai netaikomi ir jei techninės srities įtraukimas į I priedą arba sertifikuoto apsaugos profilio įtraukimas į II priedą artimiausioje ateityje mažai tikėtinas, ir tik išimtiniais ir tinkamai pagrįstais atvejais, laikantis 4 dalyje nustatytų sąlygų.

4. Jei atitikties vertinimo įstaiga mano, kad jai galioja 3 dalies c punkte nurodytas išimtinis ir tinkamai pagrįstas atvejis, ji apie numatomą sertifikavimą praneša nacionalinei kibernetinio saugumo sertifikavimo institucijai ir pateikia pagrindimą bei siūlomą vertinimo metodiką. Nacionalinė kibernetinio saugumo sertifikavimo institucija įvertina išimties pagrindimą ir pagrįstais atvejais patvirtina arba iš dalies pakeičia atitikties vertinimo įstaigos taikytiną vertinimo metodiką. Atitikties vertinimo įstaiga sertifikatą išduoda tik po to, kai nacionalinė kibernetinio saugumo sertifikavimo institucija priima sprendimą. Nacionalinė kibernetinio saugumo sertifikavimo institucija nepagrįstai nedelsdama praneša apie numatomą sertifikavimą Europos kibernetinio saugumo sertifikavimo grupei, kuri gali pateikti nuomonę. Nacionalinė kibernetinio saugumo sertifikavimo institucija kuo labiau atsižvelgia į Europos kibernetinio saugumo sertifikavimo grupės nuomonę.

5. Jei pagal atitinkamus naujausius dokumentus IRT produktas vertinamas kaip sudėtinis produktas, pagrindinio IRT produkto vertinimą atlikusi ITSVĮ dalijasi atitinkama informacija su sudėtinio IRT produkto vertinimą atliekančia ITSVĮ.

II SKIRSNIS

EKSSS sertifikatų išdavimas, atnaujinimas ir panaikinimas

8 straipsnis

▼M1

Sertifikavimo ir vertinimo reikmėms būtina informacija

1. Pareiškėjas, siekiantis gauti sertifikatą pagal EKSSS, pateikia sertifikavimo įstaigai ir ITSVĮ visą sertifikavimo ir vertinimo veiklai būtiną informaciją arba kitaip sudaro sąlygas su ja susipažinti.

▼B

2. 1 dalyje nurodyta informacija apima visus susijusius įrodymus pagal pasirinktam saugumo užtikrinimo lygiui ir susijusiems saugumo užtikrinimo reikalavimams taikomų bendrųjų kriterijų ir bendros vertinimo metodikos skirsnius „Kūrėjo veiksmų elementai“ tinkamu formatu, nustatytu skirsniuose „Įrodymo elemento turinys ir pateikimas“. Prireikus įrodymai apima išsamią informaciją apie IRT produktą ir jo pirminį kodą pagal šį reglamentą, taikant apsaugos nuo neteisėto atskleidimo priemones.

3. Pareiškėjai, siekiantys gauti sertifikatą, gali pateikti sertifikavimo įstaigai ir ITSVĮ atitinkamus vertinimo rezultatus, gautus atlikus ankstesnį sertifikavimą pagal:

a) šį reglamentą;

b) kitą Europos kibernetinio saugumo sertifikavimo schemą, priimtą pagal Reglamento (ES) 2019/881 49 straipsnį;

c) šio reglamento 49 straipsnyje nurodytą nacionalinę schemą.

4. Jei vertinimo rezultatai yra susiję su ITSVĮ užduotimis, ITSVĮ gali pakartotinai naudoti vertinimo rezultatus, jei tokie rezultatai atitinka taikomus reikalavimus ir yra patvirtintas jų autentiškumas.

5. Jei sertifikavimo įstaiga leidžia produktui taikyti sudėtinio produkto sertifikavimą, pareiškėjas, siekiantis gauti sertifikatą, pateikia sertifikavimo įstaigai ir ITSVĮ visą būtiną informaciją, kai taikoma, pagal naujausią dokumentą.

6. Pareiškėjai sertifikavimo įstaigai ir ITSVĮ taip pat pateikia šią informaciją:

a) nuorodą į savo interneto svetainę, kurioje pateikiama Reglamento (ES) 2019/881 55 straipsnyje nurodyta papildoma kibernetinio saugumo informacija;

b) pareiškėjo pažeidžiamumų valdymo ir atskleidimo procedūrų aprašymą.

7. Visus šiame straipsnyje nurodytus atitinkamus dokumentus sertifikavimo įstaiga, ITSVĮ ir pareiškėjas saugo penkerius metus nuo sertifikato galiojimo pabaigos.

▼B

9 straipsnis

EKSSS sertifikato išdavimo sąlygos

1. Sertifikavimo įstaigos išduoda EKSSS sertifikatą, jei tenkinamos visos šios sąlygos:

a) IRT produkto kategorija patenka į sertifikavimo įstaigos ir sertifikavimo procese dalyvaujančios ITSVĮ suteikiamos akreditacijos ir, kai taikytina, įgaliojimo taikymo sritį;

b) Pareiškėjas, siekiantis gauti sertifikatą, pasirašė pareiškimą, kuriuo prisiima visus 2 dalyje išvardytus įsipareigojimus;

c) ITSVĮ be prieštaravimų užbaigė vertinimą pagal 3 ir 7 straipsniuose nurodytus vertinimo standartus, kriterijus ir metodus;

d) sertifikavimo įstaiga be prieštaravimų užbaigė vertinimo rezultatų peržiūrą;

e) sertifikavimo įstaiga patikrino, ar ITSVĮ pateiktos techninės vertinimo ataskaitos atitinka pateiktus įrodymus ir ar buvo tinkamai taikomi 3 ir 7 straipsniuose nurodyti vertinimo standartai, kriterijai ir metodai.

2. Pareiškėjas, siekiantis gauti sertifikatą, prisiima šiuos įsipareigojimus:

a) pateikti sertifikavimo įstaigai ir ITSVĮ visą būtiną išsamią ir teisingą informaciją ir paprašius pateikti būtiną papildomą informaciją;

b) nereklamuoti IRT produkto kaip pagal EKSSS sertifikuojamo produkto, kol bus išduotas EKSSS sertifikatas;

c) reklamuoti IRT produktą kaip sertifikuotą tik EKSSS sertifikate nustatytos taikymo srities atžvilgiu;

d) nedelsiant nustoti reklamuoti IRT produktą kaip sertifikuotą tuo atveju, kai EKSSS sertifikato galiojimas laikinai sustabdomas, sertifikatas panaikinamas arba nustoja galioti;

e) užtikrinti, kad IRT produktai, parduodami nurodant EKSSS sertifikatą, būtų visiškai tapatūs IRT produktui, kuriam taikomas sertifikavimas;

f) laikytis EKSSS sertifikatui pagal 11 straipsnį nustatytų ženklo ir etiketės naudojimo taisyklių.

3. Jei pagal atitinkamus naujausius dokumentus IRT produktas sertifikuojamas kaip sudėtinis produktas, pagrindinio IRT produkto sertifikavimą atlikusi sertifikavimo įstaiga dalijasi atitinkama informacija su sudėtinio IRT produkto sertifikavimą atliekančia sertifikavimo įstaiga.

▼B

10 straipsnis

EKSSS sertifikato turinys ir formatas

1. EKSSS sertifikate pateikiama bent VII priede nurodyta informacija.

2. EKSSS sertifikate arba sertifikavimo ataskaitoje nedviprasmiškai apibrėžiama sertifikuoto IRT produkto taikymo sritis ir ribos, nurodant, ar sertifikuotas visas IRT produktas, ar tik jo dalys.

3. Sertifikavimo įstaiga pateikia pareiškėjui EKSSS sertifikatą bent elektronine forma.

4. Sertifikavimo įstaiga pagal V priedą parengia kiekvieno jos išduodamo EKSSS sertifikato sertifikavimo ataskaitą. Sertifikavimo ataskaita grindžiama ITSVĮ parengta technine vertinimo ataskaita. Techninėje vertinimo ataskaitoje ir sertifikavimo ataskaitoje nurodomi konkretūs 7 straipsnyje minimi vertinimo kriterijai ir metodai, taikyti atliekant vertinimą.

5. Sertifikavimo įstaiga nacionalinei kibernetinio saugumo sertifikavimo institucijai ir ENISA pateikia kiekvieną EKSSS sertifikatą ir kiekvieną sertifikavimo ataskaitą elektronine forma.

11 straipsnis

Ženklas ir etiketė

1. Sertifikato turėtojas gali paženklinti sertifikuotą IRT produktą ženklu ir etikete. Ženklu ir etikete įrodoma, kad IRT produktas yra sertifikuotas pagal šį reglamentą. Ženklas ir etiketė pritvirtinami pagal šį straipsnį ir IX priedą.

2. Ženklas ir etiketė pritvirtinami prie sertifikuoto IRT produkto arba jo duomenų plokštelės taip, kad jie būtų matomi, įskaitomi ir nenutrinami. Jeigu taip ženklinti produktą neįmanoma arba negalima dėl jo pobūdžio, ženklu ir etikete ženklinama pakuotė ir lydimieji dokumentai. Jei sertifikuotas IRT produktas pristatomas kaip programinė įranga, ženklas ir etiketė pateikiami lydimuosiuose dokumentuose taip, kad būtų matomi, įskaitomi ir nenutrinami, arba tie dokumentai naudotojams turi būti lengvai ir tiesiogiai prieinami interneto svetainėje.

3. Ženklas ir etiketė nustatomi taip, kaip nustatyta IX priede, ir juose nurodoma:

a) sertifikuoto IRT produkto saugumo užtikrinimo lygis ir AVA_VAN lygis;

b) unikalus sertifikato identifikavimo kodas, kurį sudaro:

   1) schemos pavadinimas;

   2) sertifikatą išdavusios sertifikavimo įstaigos akreditacijos registracijos numeris;

   3) išdavimo metai ir mėnuo;

   4) sertifikatą išdavusios sertifikavimo įstaigos priskirtas identifikacinis numeris.

▼B

4. Prie ženklo ir etiketės pridedamas QR kodas su nuoroda į interneto svetainę, kurioje pateikiama bent ši informacija:

a) informacija apie sertifikato galiojimą;

b) būtina sertifikavimo informacija, nurodyta V ir VII prieduose;

c) informacija, kurią sertifikato turėtojas turi viešai paskelbti pagal Reglamento (ES) 2019/881 55 straipsnį, ir

d) kai taikytina, istorinė informacija, susijusi su konkrečiu IRT produkto sertifikatu ar sertifikatais, kad būtų galima jį atsekti.

12 straipsnis

EKSSS sertifikato galiojimo laikotarpis

1. Sertifikavimo įstaiga nustato kiekvieno išduoto EKSSS sertifikato galiojimo laikotarpį, atsižvelgdama į sertifikuoto IRT produkto charakteristikas.

2. EKSSS sertifikatas galioja ne ilgiau kaip penkerius metus.

3. Nukrypstant nuo 2 dalies, tas laikotarpis gali būti ilgesnis kaip penkeri metai, jei tam iš anksto pritaria nacionalinė kibernetinio saugumo sertifikavimo institucija. Nacionalinė kibernetinio saugumo sertifikavimo institucija nepagrįstai nedelsdama praneša Europos kibernetinio saugumo sertifikavimo grupei apie suteiktą pritarimą.

13 straipsnis

EKSSS sertifikato peržiūra

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

2. Remdamasi peržiūros ir, kai taikytina, pakartotinio vertinimo rezultatais, sertifikavimo įstaiga:

a) patvirtina EKSSS sertifikatą;

b) panaikina EKSSS sertifikatą pagal 14 straipsnį;

c) panaikina EKSSS sertifikatą pagal 14 straipsnį ir išduoda naują vienodos taikymo srities ir pratęsto galiojimo laikotarpio EKSSS sertifikatą, ir

d) panaikina EKSSS sertifikatą pagal 14 straipsnį ir išduoti naują kitokios taikymo srities EKSSS sertifikatą.

3. Sertifikavimo įstaiga gali nuspręsti nepagrįstai nedelsdama sustabdyti EKSSS sertifikato galiojimą pagal 30 straipsnį, kol EKSSS sertifikato turėtojas imsis taisomųjų veiksmų.

▼B

14 straipsnis

EKSSS sertifikato panaikinimas

1. Nepažeidžiant Reglamento (ES) 2019/881 58 straipsnio 8 dalies e punkto, EKSSS sertifikatą panaikina tą sertifikatą išdavusi sertifikavimo įstaiga.

2. 1 dalyje nurodyta sertifikavimo įstaiga praneša nacionalinei kibernetinio saugumo sertifikavimo institucijai apie sertifikato panaikinimą. Ji taip pat praneša ENISA apie tokį panaikinimą, kad palengvintų jos užduoties pagal Reglamento (ES) 2019/881 50 straipsnį vykdymą. Nacionalinė kibernetinio saugumo sertifikavimo institucija apie tai praneša kitoms atitinkamoms rinkos priežiūros institucijoms.

3. EKSSS sertifikato turėtojas gali prašyti panaikinti sertifikatą.

III SKYRIUS

APSAUGOS PROFILIŲ SERTIFIKAVIMAS

I SKIRSNIS

Specialieji Vertinimo Standartai Ir Reikalavimai

15 straipsnis

Vertinimo kriterijai ir metodai

1. Apsaugos profilis vertinamas bent pagal šiuos kriterijus:

a) taikytinus 3 straipsnyje nurodytų standartų elementus;

b) rizikos, susijusios su numatyta atitinkamų IRT produktų paskirtimi pagal Reglamento (ES) 2019/881 52 straipsnį ir jų saugumo funkcijomis, kuriomis padedama siekti to reglamento 51 straipsnyje nustatytų saugumo tikslų, lygį, ir

c) I priede išvardytus taikytinus naujausius dokumentus. Į techninę sritį įtrauktas apsaugos profilis sertifikuojamas pagal toje techninėje srityje nustatytus reikalavimus.

2. Išimtiniais ir tinkamai pagrįstais atvejais atitikties vertinimo įstaiga gali sertifikuoti apsaugos profilį netaikydama atitinkamų naujausių dokumentų. Tokiais atvejais ji informuoja kompetentingą nacionalinę kibernetinio saugumo sertifikavimo instituciją ir pateikia numatomo sertifikavimo netaikant atitinkamų naujausios dokumentų ir siūlomos vertinimo metodikos pagrindimą. Nacionalinė kibernetinio saugumo sertifikavimo institucija įvertina pagrindimą ir, kai pagrįsta, patvirtina, kad atitinkami naujausi dokumentai netaikomi, ir prireikus patvirtina arba iš dalies pakeičia vertinimo metodiką, kurią turi taikyti atitikties vertinimo įstaiga. Atitikties vertinimo įstaiga apsaugos

▼B

profilio sertifikatą išduoda tik po to, kai nacionalinė kibernetinio saugumo sertifikavimo institucija priima sprendimą. Nacionalinė kibernetinio saugumo sertifikavimo institucija nepagrįstai nedelsdama praneša apie leidimą netaikyti atitinkamų naujausių dokumentų Europos kibernetinio saugumo sertifikavimo grupei, kuri gali pateikti nuomonę. Nacionalinė kibernetinio saugumo sertifikavimo institucija kuo labiau atsižvelgia į Europos kibernetinio saugumo sertifikavimo grupės nuomonę.

II SKIRSNIS

Apsaugos profilių eksss sertifikatų išdavimas, atnaujinimas ir panaikinimas

▼M1

16 straipsnis

Apsaugos profiliams sertifikuoti ir vertinti būtina informacija

Pareiškėjas, siekiantis gauti apsaugos profilio sertifikatą, pateikia sertifikavimo įstaigai ir ITSVĮ visą teisingą sertifikavimo ir vertinimo veiklai būtiną informaciją arba kitaip sudaro sąlygas su ja susipažinti. *Mutatis mutandis* taikomos 8 straipsnio 2, 3, 4 ir 7 dalys.

▼B

17 straipsnis

Apsaugos profilių EKSSS sertifikatų išdavimas

▼M1

_____

▼B

2. *Mutatis mutandis* taikomi 9 ir 10 straipsniai.

3. ITSVĮ įvertina, ar apsaugos profilis yra išsamus, nuoseklus, techniškai patikimas ir veiksmingas IRT produkto kategorijos, kuriai taikomas tas apsaugos profilis, numatytos paskirties ir saugumo tikslų atžvilgiu.

4. Apsaugos profilį sertifikuoja tik:

a) nacionalinė kibernetinio saugumo sertifikavimo institucija arba kita kaip sertifikavimo įstaiga akredituota viešoji įstaiga, arba

b) sertifikavimo įstaiga, kiekvieno atskiro apsaugos profilio atveju gavusi išankstinį nacionalinės kibernetinio saugumo sertifikavimo institucijos patvirtinimą.

18 straipsnis

Apsaugos profilio EKSSS sertifikato galiojimo laikotarpis

1. Sertifikavimo įstaiga nustato kiekvieno EKSSS sertifikato galiojimo laikotarpį.

2. Galiojimo laikotarpis gali trukti iki atitinkamo apsaugos profilio naudojimo trukmės pabaigos.

▼B

19 straipsnis

Apsaugos profilio EKSSS sertifikato peržiūra

1. Sertifikato turėtojo prašymu arba dėl kitų pagrįstų priežasčių sertifikavimo įstaiga gali nuspręsti peržiūrėti apsaugos profilio EKSSS sertifikatą. Peržiūra atliekama taikant 15 straipsnyje nustatytas sąlygas. Peržiūros apimtį nustato sertifikavimo įstaiga. Jei tai būtina peržiūrai atlikti, sertifikavimo įstaiga paprašo ITSVĮ atlikti pakartotinį sertifikuoto apsaugos profilio vertinimą.

2. Remdamasi peržiūros ir, kai taikytina, pakartotinio vertinimo rezultatais, sertifikavimo įstaiga:

a) patvirtina EKSSS sertifikatą;

b) panaikina EKSSS sertifikatą pagal 20 straipsnį;

c) panaikina EKSSS sertifikatą pagal 20 straipsnį ir išduoda naują vienodos taikymo srities ir pratęsto galiojimo laikotarpio EKSSS sertifikatą

d) panaikina EKSSS sertifikatą pagal 20 straipsnį ir išduoda naują kitokios taikymo srities EKSSS sertifikatą.

20 straipsnis

Apsaugos profilio EKSSS sertifikato panaikinimas

1. Nepažeidžiant Reglamento (ES) 2019/881 58 straipsnio 8 dalies e punkto, apsaugos profilio EKSSS sertifikatą panaikina sertifikavimo įstaiga, išdavusi tą sertifikatą. 14 straipsnis taikomas *mutatis mutandis*.

2. Pagal 17 straipsnio 4 dalies b punktą išduotą apsaugos profilio sertifikatą panaikina tą sertifikatą patvirtinusi nacionalinė kibernetinio saugumo sertifikavimo institucija.

IV SKYRIUS

ATITIKTIES VERTINIMO ĮSTAIGOS

▼M1

20a straipsnis

Atitikties vertinimo įstaigų akreditavimo reikalavimų specifikacija

Akredituojant atitikties vertinimo įstaigas atsižvelgiama į sertifikavimo įstaigų ir ITSVĮ akreditavimo reikalavimų specifikaciją, nustatytą taikytinuose naujausiuose dokumentuose, išvardytuose I priedo 2 punkte.

▼B

21 straipsnis

Sertifikavimo įstaigai taikomi papildomi arba specialūs reikalavimai

1. Nacionalinė kibernetinio saugumo sertifikavimo institucija įgalioja sertifikavimo įstaigą išduoti EKSSS sertifikatus, kuriuose nurodomas aukštas saugumo užtikrinimo lygis, jei ta įstaiga ne tik atitinka Reglamento (ES) 2019/881 60 straipsnio 1 dalyje ir priede nustatytus reikalavimus, susijusius su atitikties vertinimo įstaigų akreditavimu, bet ir įrodo, kad ji:

a) turi ekspertinių žinių ir kompetencijos, kurių reikia priimant sprendimą dėl sertifikavimo, kuriame nurodomas aukštas saugumo užtikrinimo lygis;

b) vykdo sertifikavimo veiklą bendradarbiaudama ITSVĮ, įgaliota pagal 22 straipsnį, ir

c) ne tik atitinka 43 straipsnyje nustatytus reikalavimus, bet ir turi reikiamą kompetenciją bei taiko tinkamas technines ir operatyvines priemones, kad galėtų veiksmingai apsaugoti konfidencialią ir neskelbtiną informaciją, taip užtikrinant aukštą saugumo užtikrinimo lygį.

2. Nacionalinė kibernetinio saugumo sertifikavimo institucija įvertina, ar sertifikavimo įstaiga atitinka visus 1 dalyje nustatytus reikalavimus. Tas vertinimas apima bent struktūruotus pokalbius ir bent vieno bandomojo sertifikavimo įstaigos pagal šį reglamentą atliekamo sertifikavimo atvejo peržiūrą.

Atlikdama vertinimą nacionalinė kibernetinio saugumo sertifikavimo institucija gali pakartotinai naudoti visus tinkamus įrodymus, gautus pagal ankstesnį įgaliojimą arba vykdant panašią veiklą pagal:

a) šį reglamentą;

b) kitą Europos kibernetinio saugumo sertifikavimo schemą, priimtą pagal Reglamento (ES) 2019/881 49 straipsnį;

c) šio reglamento 49 straipsnyje nurodytą nacionalinę schemą.

3. Nacionalinė kibernetinio saugumo sertifikavimo institucija parengia įgaliojimo ataskaitą, kuriai taikoma pagal Reglamento (ES) 2019/881 59 straipsnio 3 dalies d punktą atliekama tarpusavio peržiūra.

4. Nacionalinė kibernetinio saugumo sertifikavimo institucija nurodo IRT produktų kategorijas ir apsaugos profilius, kuriems taikomas įgaliojimas. Įgaliojimas galioja ne ilgiau nei akreditacija. Pateikus prašymą, jis gali būti pratęstas, jei sertifikavimo įstaiga vis dar atitinka šiame straipsnyje nustatytus reikalavimus. Norint atnaujinti įgaliojimą, bandomųjų vertinimų atlikti nereikia.

5. Nacionalinė kibernetinio saugumo sertifikavimo institucija panaikina sertifikavimo įstaigos įgaliojimą, jei ji nebeatitinka šiame straipsnyje nustatytų sąlygų. Panaikinus įgaliojimą, sertifikavimo įstaiga nedelsdama nustoja viešinti save kaip įgaliotąją sertifikavimo įstaigą.

▼B

22 straipsnis

ITSVĮ taikomi papildomi arba specialūs reikalavimai

1. Nacionalinė kibernetinio saugumo sertifikavimo institucija įgalioja ITSVĮ atlikti IRT produktų, kurie sertifikuojami nurodant aukštą saugumo užtikrinimo lygį, vertinimą, jei ITSVĮ ne tik atitinka Reglamento (ES) 2019/881 60 straipsnio 1 dalyje ir priede nustatytus reikalavimus, susijusius su atitikties vertinimo įstaigų akreditavimu, bet ir įrodo, kad ji atitinka visas toliau nurodytas sąlygas:

a) ji turi reikiamų ekspertinių žinių vertinimo veiklai atlikti, kad būtų galima nustatyti atsparumą naujausiomis technologijomis pagrįstiems kibernetiniams išpuoliams, kuriuos vykdo aukšto lygio įgūdžių ir daug išteklių turintys subjektai;

b) techninių sričių ir apsaugos profilių, kurie yra tų IRT produktų IRT proceso dalis, atveju ji turi:

   1) ekspertinių žinių, reikalingų siekiant atlikti konkrečią vertinimo veiklą, būtiną tam, kad būtų galima metodiškai nustatyti vertinimo objekto atsparumą aukšto lygio įgūdžių turinčių subjektų išpuoliams jo operacinėje aplinkoje, darant prielaidą, kad išpuolio potencialas yra vidutinis arba didelis, kaip nustatyta 3 straipsnyje nurodytuose standartuose;

   2) techninius gebėjimus, nurodytus I priede išvardytuose naujausiuose dokumentuose;

c) ne tik atitinka 43 straipsnyje nustatytus reikalavimus, bet ir turi reikiamą kompetenciją bei taiko tinkamas technines ir operatyvines priemones, kad galėtų veiksmingai apsaugoti konfidencialią ir neskelbtiną informaciją, taip užtikrinant aukštą saugumo užtikrinimo lygį.

2. Nacionalinė kibernetinio saugumo sertifikavimo institucija įvertina, ar ITSVĮ atitinka visus 1 dalyje nustatytus reikalavimus. Tas vertinimas apima bent struktūruotus pokalbius ir bent vieno bandomojo pagal šį reglamentą ITSVĮ atliekamo vertinimo atvejo peržiūrą.

3. Atlikdama vertinimą nacionalinė kibernetinio saugumo sertifikavimo institucija gali pakartotinai naudoti visus tinkamus įrodymus, gautus pagal ankstesnį įgaliojimą arba vykdant panašią veiklą pagal:

a) šį reglamentą;

b) kitą Europos kibernetinio saugumo sertifikavimo schemą, priimtą pagal Reglamento (ES) 2019/881 49 straipsnį;

c) šio reglamento 49 straipsnyje nurodytą nacionalinę schemą.

4. Nacionalinė kibernetinio saugumo sertifikavimo institucija parengia įgaliojimo ataskaitą, kuriai taikoma pagal Reglamento (ES) 2019/881 59 straipsnio 3 dalies d punktą atliekama tarpusavio peržiūra.

▼B

5. Nacionalinė kibernetinio saugumo sertifikavimo institucija nurodo IRT produktų kategorijas ir apsaugos profilius, kuriems taikomas įgaliojimas. Įgaliojimas galioja ne ilgiau nei akreditacija. Pateikus prašymą, jis gali būti pratęstas, jei ITSVĮ vis dar atitinka šiame straipsnyje nustatytus reikalavimus. Norint atnaujinti įgaliojimą neturėtų būti reikalaujama atlikti jokių bandomųjų vertinimų.

6. Nacionalinė kibernetinio saugumo sertifikavimo institucija panaikina ITSVĮ įgaliojimą, jei ITSVĮ nebeatitinka šiame straipsnyje nustatytų sąlygų. Panaikinus įgaliojimą ITSVĮ nustoja save viešinti kaip įgaliotąją ITSVĮ.

▼M1

———————

▼B

V SKYRIUS

STEBĖSENA, REIKALAVIMŲ NESILAIKYMAS IR NEATITIKTIS

I SKIRSNIS

Atitikties stebėsena

25 straipsnis

Nacionalinės kibernetinio saugumo sertifikavimo institucijos vykdoma stebėsenos veikla

1. Nepažeidžiant Reglamento (ES) 2019/881 58 straipsnio 7 dalies, nacionalinė kibernetinio saugumo sertifikavimo institucija stebi:

a) ar sertifikavimo įstaiga ir ITSVĮ laikosi savo pareigų pagal šį reglamentą ir Reglamentą (ES) 2019/881;

b) ar EKSSS sertifikato turėtojai laikosi savo pareigų pagal šį reglamentą ir Reglamentą (ES) 2019/881;

c) sertifikuotų IRT produktų atitiktį EKSSS nustatytiems reikalavimams;

d) EKSSS sertifikate pateikto saugumo užtikrinimo atitiktį sprendžiant kintančios grėsmių padėties klausimą.

2. Nacionalinė kibernetinio saugumo sertifikavimo institucija savo stebėsenos veiklą vykdo visų pirma remdamasi:

a) iš sertifikavimo įstaigų, nacionalinių akreditacijos įstaigų ir atitinkamų rinkos priežiūros institucijų gauta informacija;

b) informacija, gauta jai pačiai ar kitai institucijai atlikus auditą ir tyrimus;

c) atrankiniu tyrimu, atliekamu pagal 3 dalį;

d) gautais skundais.

▼B

3. Nacionalinė kibernetinio saugumo sertifikavimo institucija, bendradarbiaudama su kitomis rinkos priežiūros institucijomis, kasmet atlieka atrankinį tyrimą, kuriam atrenka bent 4 proc. EKSSS sertifikatų, kaip nustatyta rizikos vertinime. Kompetentingos nacionalinės kibernetinio saugumo sertifikavimo institucijos prašymu ir veikdamos jos vardu sertifikavimo įstaigos ir, jei reikia, ITSVĮ padeda tai institucijai stebėti atitiktį.

4. Nacionalinė kibernetinio saugumo sertifikavimo institucija atrenka sertifikuotus IRT produktus, kurie turi būti patikrinti pagal objektyvius kriterijus, įskaitant:

a) produkto kategoriją;

b) produktų saugumo užtikrinimo lygius;

c) sertifikato turėtoją;

d) sertifikavimo įstaigą ir, kai taikoma, ITSVĮ, kuri yra jos subrangovė;

e) visą kitą institucijai pateiktą informaciją.

5. Nacionalinė kibernetinio saugumo sertifikavimo institucija informuoja EKSSS sertifikato turėtojus apie atrinktus IRT produktus ir atrankos kriterijus.

6. Nacionalinei kibernetinio saugumo sertifikavimo institucijai paprašius, sertifikavimo įstaiga, kuri sertifikavo atrinktą IRT produktą, padedant atitinkamai ITSVĮ, atlieka papildomą peržiūrą pagal IV priedo IV.2 skirsnyje nustatytą procedūrą ir informuoja nacionalinę kibernetinio saugumo sertifikavimo instituciją apie jos rezultatus.

7. Jeigu nacionalinė kibernetinio saugumo sertifikavimo institucija turi pakankamą pagrindą manyti, kad sertifikuotas IRT produktas nebeatitinka šio reglamento arba Reglamento (ES) 2019/881, ji gali atlikti tyrimus arba pasinaudoti kitais stebėsenos įgaliojimais, nustatytais Reglamento (ES) 2019/881 58 straipsnio 8 dalyje.

8. Nacionalinė kibernetinio saugumo sertifikavimo institucija informuoja sertifikavimo įstaigą ir atitinkamą ITSVĮ apie vykdomus tyrimus, susijusius su atrinktais IRT produktais.

9. Jei nacionalinė kibernetinio saugumo sertifikavimo institucija nustato, kad vykdomas tyrimas susijęs su IRT produktais, kuriuos sertifikavo kitose valstybėse narėse įsisteigusios sertifikavimo įstaigos, ji apie tai informuoja atitinkamų valstybių narių nacionalines kibernetinio saugumo sertifikavimo institucijas, kad prireikus galėtų bendradarbiauti atliekant tyrimus. Tokia nacionalinė kibernetinio saugumo sertifikavimo institucija taip pat praneša Europos kibernetinio saugumo sertifikavimo grupei apie tarpvalstybinius tyrimus ir vėlesnius jų rezultatus.

▼B

26 straipsnis

Sertifikavimo įstaigos vykdoma stebėsena

1. Sertifikavimo įstaiga stebi:

a) ar sertifikato turėtojai laikosi savo pareigų pagal šį reglamentą ir Reglamentą (ES) 2019/881 dėl EKSSS sertifikato, kurį išdavė ta sertifikavimo įstaiga;

b) jos sertifikuotų IRT produktų atitiktį jų atitinkamiems saugumo reikalavimams;

c) sertifikuotuose apsaugos profiliuose pateiktą saugumo užtikrinimą.

2. Sertifikavimo įstaiga vykdo stebėsenos veiklą remdamasi:

a) informacija, pateikta remiantis 9 straipsnio 2 dalyje nurodytais sertifikatą siekiančio gauti pareiškėjo įsipareigojimais;

b) informacija, gauta iš kitų atitinkamų rinkos priežiūros institucijų veiklos;

c) gautais skundais;

d) informacija apie pažeidžiamumą, kuri galėtų daryti poveikį jos sertifikuotiems IRT produktams.

3. Nacionalinė kibernetinio saugumo sertifikavimo institucija, nedarydama poveikio veiklai, susijusiai su kitomis atitinkamomis rinkos priežiūros institucijomis, gali parengti taisykles, pagal kurias būtų periodiškai vykdomas sertifikavimo įstaigų ir EKSSS sertifikatų turėtojų dialogas, kuriuo siekiama patikrinti, kaip laikomasi pagal 9 straipsnio 2 dalį prisiimtų įsipareigojimų, ir apie tai pranešti.

27 straipsnis

Sertifikato turėtojo vykdoma stebėsena

1. EKSSS sertifikato turėtojas, siekdamas stebėti sertifikuoto IRT produkto atitiktį jo saugumo reikalavimams, atlieka šias užduotis:

a) stebėti su sertifikuotu IRT produktu susijusią informaciją apie pažeidžiamumą, įskaitant žinomus priklausomumo atvejus, savo priemonėmis, taip pat atsižvelgiant į:

   1) Reglamento (ES) 2019/881 55 straipsnio 1 dalies c punkte nurodytą naudotojo arba saugumo srities tyrėjo paskelbtą arba pateiktą informaciją apie pažeidžiamumą;

   2) bet kurio kito šaltinio pateikta informaciją;

b) stebėti EKSSS sertifikate nurodytą saugumo užtikrinimą.

▼B

2. EKSSS sertifikato turėtojas bendradarbiauja su sertifikavimo įstaiga, ITSVĮ ir, kai taikytina, nacionaline kibernetinio saugumo sertifikavimo institucija, kad padėtų joms vykdyti stebėsenos veiklą.

II SKIRSNIS

REIKALAVIMŲ LAIKYMASIS IR ATITIKTIS

28 straipsnis

Sertifikuoto IRT produkto arba apsaugos profilio neatitikties reikalavimams padariniai

1. Jei sertifikuotas IRT produktas arba apsaugos profilis neatitinka šiame reglamente ir Reglamente (ES) 2019/881 nustatytų reikalavimų, sertifikavimo įstaiga informuoja EKSSS sertifikato turėtoją apie nustatytą neatitiktį ir paprašo imtis taisomųjų veiksmų.

2. Jei neatitikties šio reglamento nuostatoms atvejis gali turėti įtakos atitikčiai kitiems atitinkamiems Sąjungos teisės aktams, kuriuose numatyta galimybė pagrįsti atitikties to teisės akto reikalavimams prielaidą naudojant EKSSS sertifikatą, sertifikavimo įstaiga nedelsdama apie tai informuoja nacionalinę kibernetinio saugumo sertifikavimo instituciją. Nacionalinė kibernetinio saugumo sertifikavimo institucija nedelsdama praneša rinkos priežiūros institucijai, atsakingai už tokius kitus atitinkamus Sąjungos teisės aktus, apie nustatytą neatitikties atvejį.

3. Gavęs 1 dalyje nurodytą informaciją, EKSSS sertifikato turėtojas per sertifikavimo įstaigos nustatytą laikotarpį, kuris yra ne ilgesnis kaip 30 dienų, pasiūlo sertifikavimo įstaigai taisomuosius veiksmus, būtinus neatitikčiai pašalinti.

4. Sertifikavimo įstaiga pagal 30 straipsnį gali nepagrįstai nedelsdama sustabdyti EKSSS sertifikato galiojimą ekstremaliosios situacijos atveju arba kai EKSSS sertifikato turėtojas tinkamai nebendradarbiauja su sertifikavimo įstaiga.

5. Sertifikavimo įstaiga atlieka peržiūrą pagal 13 ir 19 straipsnius ir įvertina, ar taisomaisiais veiksmais neatitiktis pašalinama.

6. Jei EKSSS sertifikato turėtojas nepasiūlo tinkamų taisomųjų veiksmų per 3 dalyje nurodytą laikotarpį, sertifikato galiojimas sustabdomas pagal 30 straipsnį arba panaikinamas pagal 14 arba 20 straipsnį.

7. Šis straipsnis netaikomas pažeidžiamumų, darančių poveikį sertifikuotam IRT produktui, atvejams; jie turi būti sprendžiami taip, kaip nustatyta VI skyriuje.

29 straipsnis

Sertifikato turėtojo reikalavimų nesilaikymo padariniai

1. Kai sertifikavimo įstaiga nustato, kad:

a) EKSSS sertifikato turėtojas arba pareiškėjas, siekiantis gauti sertifikatą, nesilaiko savo įsipareigojimų ir pareigų, nustatytų 9 straipsnio 2 dalyje, 17 straipsnio 2 dalyje ir 27 bei 41 straipsniuose, arba

▼B

b) EKSSS sertifikato turėtojas nesilaiko Reglamento (ES) 2019/881 56 straipsnio 8 dalies arba šio reglamento VI skyriaus nuostatų,

ji nustato ne ilgesnį kaip 30 dienų laikotarpį, per kurį EKSSS sertifikato turėtojas turi imtis taisomųjų veiksmų.

▼M1

2. Jei EKSSS sertifikato turėtojas nepasiūlo tinkamų taisomųjų veiksmų per 1 dalyje nurodytą laikotarpį, sertifikato galiojimas sustabdomas pagal 30 straipsnį arba panaikinamas pagal 14 straipsnį ar 20 straipsnį.

▼B

3. Tolesnio ar pasikartojančio EKSSS sertifikato turėtojo daromo 1 dalyje nurodytų pareigų pažeidimo atveju EKSSS sertifikatas panaikinamas pagal 14 arba 20 straipsnį.

4. Sertifikavimo įstaiga informuoja nacionalinę kibernetinio saugumo sertifikavimo instituciją apie 1 dalyje nurodytus pažeidimus. Jei reikalavimų nesilaikymo atvejis turi įtakos atitikčiai kitiems atitinkamiems Sąjungos teisės aktams, nacionalinė kibernetinio saugumo sertifikavimo institucija nedelsdama praneša apie nustatytą reikalavimų nesilaikymo atvejį už tokius kitus atitinkamus Sąjungos teisės aktus atsakingai rinkos priežiūros institucijai.

30 straipsnis

EKSSS sertifikato galiojimo sustabdymas

1. Tais atvejais, kai šiame reglamente nurodomas EKSSS sertifikato galiojimo sustabdymas, sertifikavimo įstaiga sustabdo atitinkamo EKSSS sertifikato galiojimą laikotarpiui, kuris yra ne ilgesnis nei 42 dienos, atsižvelgiant į aplinkybes, dėl kurių sertifikato galiojimas sustabdomas. Sertifikato galiojimo sustabdymo laikotarpis prasideda kitą dieną po sertifikavimo įstaigos sprendimo priėmimo dienos. Sertifikato galiojimo sustabdymas neturi įtakos sertifikato galiojimui.

2. Sertifikavimo įstaiga nepagrįstai nedelsdama praneša sertifikato turėtojui ir nacionalinei kibernetinio saugumo sertifikavimo institucijai apie sertifikato galiojimo sustabdymą ir nurodo jo sustabdymo priežastis, veiksmus, kurių prašoma imtis, ir sertifikato galiojimo sustabdymo laikotarpį.

3. Sertifikato turėtojai praneša atitinkamų IRT produktų pirkėjams apie sertifikato galiojimo sustabdymą ir sertifikavimo įstaigos nurodytas sustabdymo priežastis, išskyrus tas priežasčių dalis, kuriomis dalijantis kiltų saugumo rizika arba kuriose yra neskelbtinos informacijos. Šią informaciją sertifikato turėtojas taip pat viešai paskelbia.

4. Jeigu kituose atitinkamuose Sąjungos teisės aktuose numatyta atitikties prielaida, pagrįsta pagal šio reglamento nuostatas išduotais sertifikatais, nacionalinė kibernetinio saugumo sertifikavimo institucija apie sertifikato galiojimo sustabdymą informuoja rinkos priežiūros instituciją, atsakingą už tokius kitus atitinkamus Sąjungos teisės aktus.

5. Apie sertifikato galiojimo sustabdymą pranešama ENISA pagal 42 straipsnio 3 dalį.

6. Tinkamai pagrįstais atvejais nacionalinė kibernetinio saugumo sertifikavimo institucija gali leisti pratęsti EKSSS sertifikato galiojimo sustabdymo laikotarpį. Bendras sustabdymo laikotarpis negali būti ilgesnis nei vieni metai.

▼B

31 straipsnis

Atitikties vertinimo įstaigos reikalavimų nesilaikymo padariniai

1. Jei sertifikavimo įstaiga nesilaiko savo pareigų arba atitinkama sertifikavimo įstaiga nustato, kad ITSVĮ nesilaiko reikalavimų, nacionalinė kibernetinio saugumo sertifikavimo institucija nepagrįstai nedelsdama:

a) nustato EKSSS sertifikatus, kuriems gali būti daromas poveikis, padedant atitinkamai ITSVĮ;

b) prireikus paprašo, kad vertinimą atlikusi ITSVĮ arba bet kuri kita akredituota ir, kai taikytina, įgaliotoji ITSVĮ, kuri gali turėti geresnes technines galimybes padėti nustatyti tuos sertifikatus, atliktų vieno ar daugiau IRT produktų ar apsaugos profilių vertinimo veiklą;

c) išnagrinėja reikalavimų nesilaikymo padarinius;

d) apie tai praneša EKSSS sertifikato, kuriam reikalavimų nesilaikymo atvejis daro poveikį, turėtojui.

2. Remdamasi 1 dalyje nurodytomis priemonėmis, sertifikavimo įstaiga dėl kiekvieno paveikto EKSSS sertifikato priima vieną iš šių sprendimų:

a) EKSSS sertifikatą palikti nepakeistą;

b) panaikinti EKSSS sertifikatą pagal 14 arba 20 straipsnį ir, kai tinkama, išduoti naują EKSSS sertifikatą.

3. Remdamasi 1 dalyje nurodytomis priemonėmis, nacionalinė kibernetinio saugumo sertifikavimo institucija:

a) prireikus praneša nacionalinei akreditacijos įstaigai apie tai, kad sertifikavimo įstaiga arba susijusi ITSVĮ nesilaiko reikalavimų;

b) kai taikytina, įvertina galimą poveikį įgaliojimui.

VI SKYRIUS

PAŽEIDŽIAMUMŲ VALDYMAS IR ATSKLEIDIMAS

32 straipsnis

Pažeidžiamumų valdymo apimtis

Šis skyrius taikomas IRT produktams, kuriems išduotas EKSSS sertifikatas.

I SKIRSNIS

Pažeidžiamumų valdymas

33 straipsnis

Pažeidžiamumų valdymo procedūros

1. EKSSS sertifikato turėtojas nustato ir taiko visas būtinas pažeidžiamumų valdymo procedūras pagal šiame skirsnyje nustatytas taisykles ir prireikus papildomas standarte EN ISO/IEC 30111 nustatytas procedūras.

▼B

2. EKSSS sertifikato turėtojas taiko ir paskelbia tinkamus metodus, kaip iš išorės šaltinių, įskaitant naudotojus, sertifikavimo įstaigas ir saugumo srities tyrėjus, gauti informaciją apie pažeidžiamumą, susijusį su jo produktais.

3. Jei EKSSS sertifikato turėtojas aptinka arba gauna informaciją apie galimą pažeidžiamumą, darantį poveikį sertifikuotam IRT produktui, jis jį užregistruoja ir atlieka pažeidžiamumo poveikio analizę.

4. Kai galimas pažeidžiamumas daro poveikį sudėtiniam produktui, EKSSS sertifikato turėtojas informuoja priklausomų EKSSS sertifikatų turėtoją apie galimą pažeidžiamumą.

5. Gavęs pagrįstą sertifikatą išdavusios sertifikavimo įstaigos prašymą EKSSS sertifikato turėtojas perduoda tai sertifikavimo įstaigai visą svarbią informaciją apie galimą pažeidžiamumą.

34 straipsnis

Pažeidžiamumo poveikio analizė

1. Pažeidžiamumo poveikio analizėje nurodomas vertinimo tikslas ir sertifikate pateikti saugumo užtikrinimo pareiškimai. Pažeidžiamumo poveikio analizė atliekama per tokį laiką, kuris atitinka galimybes pasinaudoti sertifikuoto IRT produkto galimu pažeidžiamumu ir jo kritiškumo lygį.

2. Kai taikytina, pagal atitinkamą metodiką, įtrauktą į 3 straipsnyje nurodytus standartus, ir atitinkamus naujausius dokumentus, išvardytus I priede, atliekamas išpuolio potencialo skaičiavimas, siekiant nustatyti galimybes pasinaudoti pažeidžiamumu. Atsižvelgiama į EKSSS sertifikato AVA_VAN lygį.

35 straipsnis

Pažeidžiamumo poveikio analizės ataskaita

1. Sertifikato turėtojas parengia pažeidžiamumo poveikio analizės ataskaitą, jei iš poveikio analizės matyti, kad tikėtina, jog pažeidžiamumas gali paveikti IRT produkto atitiktį jo sertifikatui.

2. Pažeidžiamumo poveikio analizės ataskaitoje įvertinami šie elementai:

a) pažeidžiamumo poveikis sertifikuotam IRT produktui;

b) galima rizika, susijusi su išpuolio tikėtinumu ar galimybe jį įvykdyti;

c) ar pažeidžiamumas gali būti ištaisytas;

d) jei pažeidžiamumas gali būti ištaisytas, galimus pažeidžiamumo ištaisymo sprendimus.

3. Atitinkamais atvejais pažeidžiamumo poveikio analizės ataskaitoje pateikiama išsami informacija apie galimus pasinaudojimo pažeidžiamumu būdus. Informacija apie galimus pasinaudojimo pažeidžiamumu būdus tvarkoma laikantis tinkamų saugumo priemonių, kad būtų apsaugotas jos konfidencialumas ir prireikus užtikrintas ribotas jos platinimas.

▼B

4. EKSSS sertifikato turėtojas pagal Reglamento (ES) 2019/881 56 straipsnio 8 dalį nepagrįstai nedelsdamas perduoda pažeidžiamumo poveikio analizės ataskaitą sertifikavimo įstaigai arba nacionalinei kibernetinio saugumo sertifikavimo institucijai.

5. Jei pažeidžiamumo poveikio analizės ataskaitoje nustatoma, kad pažeidžiamumas nėra liekamasis, kaip apibrėžta 3 straipsnyje nurodytuose standartuose, ir kad jį galima ištaisyti, taikomas 36 straipsnis.

6. Jei pažeidžiamumo poveikio analizės ataskaitoje nustatoma, kad pažeidžiamumas nėra liekamasis ir kad jo ištaisyti neįmanoma, EKSSS sertifikatas panaikinamas pagal 14 straipsnį.

7. EKSSS sertifikato turėtojas stebi visus liekamuosius pažeidžiamumus, siekdamas užtikrinti, kad pasikeitus operacinei aplinkai jais nebūtų galima pasinaudoti.

36 straipsnis

Pažeidžiamumo ištaisymas

EKSSS sertifikato turėtojas sertifikavimo įstaigai pateikia pasiūlymą dėl tinkamų taisomųjų veiksmų. Sertifikavimo įstaiga peržiūri sertifikatą pagal 13 straipsnį. Peržiūros apimtis nustatoma pagal siūlomą pažeidžiamumo ištaisymą.

II SKIRSNIS

Pažeidžiamumo atskleidimas

37 straipsnis

Informacija, kuria dalijamasi su nacionaline kibernetinio saugumo sertifikavimo institucija

1. Sertifikavimo įstaigos nacionalinei kibernetinio saugumo sertifikavimo institucijai teikiama informacija apima visus elementus, kurių reikia, kad nacionalinė kibernetinio saugumo sertifikavimo institucija suprastų pažeidžiamumo poveikį, atliktinus IRT produkto pakeitimus ir, kai prieinama, visą sertifikavimo įstaigos pateiktą informaciją apie platesnio masto pažeidžiamumo poveikį kitiems sertifikuotiems IRT produktams.

2. Pagal 1 dalį pateiktoje informacijoje neturi būti išsamios informacijos apie pasinaudojimo pažeidžiamumu būdus. Šia nuostata nedaromas poveikis nacionalinės kibernetinio saugumo sertifikavimo institucijos tyrimo įgaliojimams.

38 straipsnis

Bendradarbiavimas su kitomis nacionalinėmis kibernetinio saugumo sertifikavimo institucijomis

1. Nacionalinė kibernetinio saugumo sertifikavimo institucija dalijasi pagal 37 straipsnį gauta atitinkama informacija su kitomis nacionalinėmis kibernetinio saugumo sertifikavimo institucijomis ir ENISA.

▼B

2. Kitos nacionalinės kibernetinio saugumo sertifikavimo institucijos gali nuspręsti toliau analizuoti pažeidžiamumą arba, informavusios EKSSS sertifikato turėtoją, paprašyti atitinkamų sertifikavimo įstaigų įvertinti, ar pažeidžiamumas gali daryti poveikį kitiems sertifikuotiems IRT produktams.

39 straipsnis

Pranešimas apie pažeidžiamumą

Panaikinus sertifikatą, EKSSS sertifikato turėtojas atskleidžia ir užregistruoja visus viešai žinomus ir ištaisytus IRT produkto pažeidžiamumus Europos pažeidžiamumų duomenų bazėje, sukurtoje pagal Europos Parlamento ir Tarybos direktyvos (ES) 2022/2555 ([1]) 12 straipsnį, arba kitose Reglamento (ES) 2019/881 55 straipsnio 1 dalies d punkte nurodytose internetinėse duomenų saugyklose.

VII SKYRIUS

INFORMACIJOS SAUGOJIMAS, ATSKLEIDIMAS IR APSAUGA

40 straipsnis

Sertifikavimo įstaigų ir ITSVĮ įrašų saugojimas

1. ITSVĮ ir sertifikavimo įstaigos tvarko įrašų sistemą, kurioje saugomi visi su kiekvienu jų atliekamu vertinimu ir sertifikavimu susiję dokumentai.

2. Sertifikavimo įstaigos ir ITSVĮ įrašus saugo saugiai ir tiek ilgai, kiek reikia šio reglamento tikslams įgyvendinti, bet ne trumpiau kaip penkerius metus po atitinkamo EKSSS sertifikato panaikinimo. Sertifikavimo įstaigai pagal 13 straipsnio 2 dalies c punktą išdavus naują EKSSS sertifikatą, ji saugo panaikinto EKSSS sertifikato dokumentus kartu su naujuoju EKSSS sertifikatu tiek pat laiko, kiek ir naująjį EKSSS sertifikatą.

41 straipsnis

Sertifikato turėtojo pateikiama informacija

1. Reglamento (ES) 2019/881 55 straipsnyje nurodyta informacija pateikiama naudotojams lengvai prieinama kalba.

2. Šio reglamento tikslais būtiną laikotarpį, bet ne trumpiau kaip penkerius metus po atitinkamo EKSSS sertifikato panaikinimo EKSSS sertifikato turėtojas saugiai saugo:

a) sertifikavimo įstaigai ir ITSVĮ per sertifikavimo procesą pateiktos informacijos įrašus

b) sertifikuoto IRT produkto pavyzdį.

([1]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva) (OL L 333, 2022 12 27, p. 80).

▼B

3. Sertifikavimo įstaigai pagal 13 straipsnio 2 dalies c punktą išdavus naują EKSSS sertifikatą, jo turėtojas saugo panaikinto EKSSS sertifikato dokumentus kartu su naujuoju EKSSS sertifikatu tiek pat laiko, kiek ir naująjį EKSSS sertifikatą.

4. Sertifikavimo įstaigos arba nacionalinės kibernetinio saugumo sertifikavimo institucijos prašymu EKSSS sertifikato turėtojas pateikia 2 dalyje nurodytus įrašus ir kopijas.

42 straipsnis

ENISA teiktina informacija

1. ENISA Reglamento (ES) 2019/881 50 straipsnio 1 dalyje nurodytoje interneto svetainėje skelbia šią informaciją:

a) visus EKSSS sertifikatus;

b) informaciją apie EKSSS sertifikato statusą, visų pirma tai, ar jis galioja, ar jo galiojimas sustabdytas, ar sertifikatas yra panaikintas, ar jo galiojimas yra pasibaigęs;

c) sertifikavimo ataskaitas, atitinkančias kiekvieną EKSSS sertifikatą;

d) akredituotų atitikties vertinimo įstaigų sąrašą;

e) įgaliotų atitikties vertinimo įstaigų sąrašą;

f) I priede išvardytus naujausius dokumentus;

g) Reglamento (ES) 2019/881 62 straipsnio 4 dalies c punkte nurodytas Europos kibernetinio saugumo sertifikavimo grupės nuomones;

h) tarpusavio vertinimo ataskaitas, pateiktas pagal 47 straipsnį.

2. 1 dalyje nurodyta informacija pateikiama bent anglų kalba.

3. Sertifikavimo įstaigos ir, kai taikytina, nacionalinės kibernetinio saugumo sertifikavimo institucijos nedelsdamos informuoja ENISA apie savo sprendimus, kurie daro poveikį 1 dalies b punkte nurodyto EKSSS sertifikato turiniui ar būsenai.

4. ENISA užtikrina, kad pagal 1 dalies a, b ir c punktus paskelbtoje informacijoje būtų aiškiai nurodytos sertifikuoto IRT produkto versijos, kurioms taikomas EKSSS sertifikatas.

43 straipsnis

Informacijos apsauga

Atitikties vertinimo įstaigos, nacionalinės kibernetinio saugumo sertifikavimo institucijos, EKSSG, ENISA, Komisija ir visos kitos šalys užtikrina verslo paslapčių ir kitos konfidencialios informacijos, įskaitant komercines paslaptis, saugumą ir apsaugą, taip pat intelektinės nuosavybės teisių išsaugojimą ir imasi būtinų bei tinkamų techninių ir organizacinių priemonių.

▼B

VIII SKYRIUS

TARPUSAVIO PRIPAŽINIMO SUSITARIMAI SU TREČIOSIOMIS ŠALIMIS

44 straipsnis

Sąlygos

1. Trečiosios šalys, pageidaujančios sertifikuoti savo produktus pagal šį reglamentą ir norinčios, kad toks sertifikavimas būtų pripažintas Sąjungoje, su Sąjunga sudaro tarpusavio pripažinimo susitarimą.

2. Tarpusavio pripažinimo susitarimas apima IRT produktams ir, kai taikoma, apsaugos profiliams taikytinus saugumo užtikrinimo lygius.

3. 1 dalyje nurodyti tarpusavio pripažinimo susitarimai gali būti sudaromi tik su trečiosiomis šalimis, kurios atitinka šias sąlygas:

a) turi instituciją, kuri:

   1) yra viešoji įstaiga, organizacinės ir teisinės struktūros, finansavimo ir sprendimų priėmimo proceso požiūriu nepriklausoma nuo subjektų, kurių veiklą ji prižiūri ir stebi;

   2) turi tinkamus stebėsenos ir priežiūros įgaliojimus, kad galėtų atlikti tyrimus, taip pat yra įgaliota imtis tinkamų taisomųjų priemonių reikalavimų laikymuisi užtikrinti;

   3) turi veiksmingų, proporcingų ir atgrasomų sankcijų sistemą reikalavimų laikymuisi užtikrinti;

   4) sutinka bendradarbiauti su Europos kibernetinio saugumo sertifikavimo grupe ir ENISA, kad būtų keičiamasi geriausios praktikos pavyzdžiais ir atitinkamomis naujovėmis kibernetinio saugumo sertifikavimo srityje, ir siekti vienodai aiškinti šiuo metu taikomus vertinimo kriterijus ir metodus, be kita ko, taikant suderintus dokumentus, lygiaverčius I priede išvardytiems naujausiems dokumentams;

b) turi nepriklausomą akreditacijos įstaigą, atliekančią akreditavimą pagal standartus, lygiaverčius nurodytiems Reglamente (EB) Nr. 765/2008;

c) įsipareigoja užtikrinti, kad vertinimo ir sertifikavimo procesai ir procedūros būtų vykdomi tinkamai ir profesionaliai, atsižvelgiant į atitiktį šiame reglamente, visų pirma 3 straipsnyje, nurodytiems tarptautiniams standartams;

d) yra pajėgios pranešti apie anksčiau neaptiktus pažeidžiamumus ir turi nustatytą tinkamą pažeidžiamumų valdymo ir atskleidimo procedūrą;

e) yra nustačiusios procedūras, pagal kurias galima veiksmingai teikti ir nagrinėti skundus ir suteikti skundo pateikėjui veiksmingas teisių gynimo priemones;

▼B

f) kuria mechanizmą, taikytiną bendradarbiavimui su kitomis Sąjungos ir valstybių narių įstaigomis, susijusiomis su kibernetinio saugumo sertifikavimu pagal šį reglamentą, įskaitant dalijimąsi informacija apie galimą sertifikatų neatitiktį, atitinkamų pokyčių sertifikavimo srityje stebėseną ir bendro požiūrio į sertifikavimo priežiūrą ir peržiūrą užtikrinimą.

4. Be 3 dalyje nustatytų sąlygų, 1 dalyje nurodytas tarpusavio pripažinimo susitarimas, apimantis aukštą saugumo užtikrinimo lygį, gali būti sudarytas su trečiosiomis šalimis tik tuo atveju, jei tenkinamos šios sąlygos:

a) trečioji šalis turi nepriklausomą ir viešą kibernetinio saugumo sertifikavimo instituciją, kuri vykdo arba deleguoja vertinimo veiklą, būtiną tam, kad būtų galima vykdyti sertifikavimą patvirtinant aukštą saugumo užtikrinimo lygį, kuri yra lygiavertė šiame reglamente ir Reglamente (ES) 2019/881 nacionalinėms kibernetinio saugumo institucijoms nustatytiems reikalavimams ir procedūroms;

b) tarpusavio pripažinimo susitarimu nustatomas bendras mechanizmas, lygiavertis EKSSS sertifikavimo tarpusavio vertinimui, kuriuo siekiama pagerinti keitimąsi patirtimi ir bendrai spręsti vertinimo ir sertifikavimo srities klausimus.

IX SKYRIUS

SERTIFIKAVIMO ĮSTAIGŲ TARPUSAVIO VERTINIMAS

45 straipsnis

Tarpusavio vertinimo procedūra

1. Sertifikavimo įstaigos, išduodančios EKSSS sertifikatus, kuriuose nurodomas aukštas saugumo užtikrinimo lygis, tarpusavio vertinimas atliekamas reguliariai ir ne rečiau kaip kas penkerius metus. VI priede išvardytos įvairios tarpusavio vertinimo rūšys.

2. Europos kibernetinio saugumo sertifikavimo grupė parengia ir tvarko tarpusavio vertinimų tvarkaraštį, kuriuo užtikrinama, kad būtų laikomasi tokio periodiškumo. Išskyrus tinkamai pagrįstus atvejus, tarpusavio vertinimai atliekami vietoje.

3. Tarpusavio vertinimas gali būti grindžiamas įrodymais, surinktais per ankstesnius tarpusavio vertinimus arba lygiavertes procedūras, kurias atliko tarpusavyje įvertinta sertifikavimo įstaiga arba nacionalinė kibernetinio saugumo sertifikavimo institucija, jeigu:

a) rezultatai yra ne senesni kaip penkerių metų;

b) prie rezultatų pridedamas tai schemai nustatytų tarpusavio vertinimo procedūrų aprašymas, jei jie susiję su tarpusavio vertinimu, atliekamu pagal kitą sertifikavimo schemą;

c) 47 straipsnyje minimoje tarpusavio vertinimo ataskaitoje nurodoma, kurie rezultatai buvo pakartotinai panaudoti atliekant tolesnį vertinimą arba jo neatliekant.

▼B

4. Jei tarpusavio vertinimas apima techninę sritį, taip pat įvertinama atitinkama ITSVĮ.

5. Tarpusavio vertinimą atlikusi sertifikavimo įstaiga ir, kai būtina, nacionalinė kibernetinio saugumo sertifikavimo institucija užtikrina, kad tarpusavio vertinimo grupei būtų pateikta visa svarbi informacija.

6. Tarpusavio vertinimą atlieka pagal VI priedą sudaryta tarpusavio vertinimo grupė.

46 straipsnis

Tarpusavio vertinimo etapai

1. Parengiamuoju etapu tarpusavio vertinimo grupės nariai peržiūri sertifikavimo įstaigos dokumentus, apimančius jos politiką ir procedūras, įskaitant naujausių dokumentų naudojimą.

2. Apsilankymo vietoje etapu tarpusavio vertinimo grupė įvertina įstaigos techninę kompetenciją ir, kai taikoma, ITSVĮ, atlikusios bent vieną IRT produkto vertinimą, kuriam taikomas tarpusavio vertinimas, kompetenciją.

3. Apsilankymo vietoje etapo trukmė gali būti pratęsta arba sutrumpinta atsižvelgiant į tokius veiksnius, kaip galimybė pakartotinai panaudoti turimus tarpusavio vertinimo įrodymus ir rezultatus, arba į ITSVĮ ir techninių sričių, kurioms skirtus sertifikatus sertifikavimo įstaiga išduoda, skaičių.

4. Jei taikoma, tarpusavio vertinimo grupė nustato kiekvienos ITSVĮ techninę kompetenciją, apsilankydama jos techninėje laboratorijoje ar laboratorijose ir apklausdama jos vertintojus apie techninę sritį ir susijusius konkrečius išpuolių vykdymo metodus.

5. Ataskaitos teikimo etapu vertinimo grupė savo išvadas dokumentais pagrindžia tarpusavio vertinimo ataskaitoje, apimančioje nuosprendį ir, kai taikoma, pastebėtų neatitikčių sąrašą, suskirstytą pagal kritiškumo lygį.

6. Tarpusavio vertinimo ataskaita pirmiausia turi būti aptarta su tarpusavyje įvertinta sertifikavimo įstaiga. Po šių diskusijų tarpusavyje įvertinta sertifikavimo įstaiga nustato priemonių, kurių reikia imtis, kad būtų atsižvelgta į išvadas, įgyvendinimo tvarkaraštį.

47 straipsnis

Tarpusavio vertinimo ataskaita

1. Tarpusavio vertinimo grupė pateikia tarpusavyje įvertintai sertifikavimo įstaigai tarpusavio vertinimo ataskaitos projektą.

2. Tarpusavyje įvertinta sertifikavimo įstaiga tarpusavio vertinimo grupei pateikia pastabas dėl išvadų ir įsipareigojimų pašalinti tarpusavio vertinimo ataskaitos projekte nustatytus trūkumus sąrašą.

▼B

3. Tarpusavio vertinimo grupė pateikia Europos kibernetinio saugumo sertifikavimo grupei galutinę tarpusavio vertinimo ataskaitą, į kurią taip pat įtraukiamos tarpusavyje įvertintos sertifikavimo įstaigos pateiktos pastabos ir prisiimti įsipareigojimai. Tarpusavio vertinimo grupė taip pat pateikia savo poziciją dėl pastabų ir dėl to, ar tų įsipareigojimų pakanka nustatytiems trūkumams pašalinti.

4. Jei tarpusavio vertinimo ataskaitoje nustatoma neatitikimų, Europos kibernetinio saugumo sertifikavimo grupė gali nustatyti tinkamą terminą, iki kurio tarpusavyje įvertinta sertifikavimo įstaiga turi pašalinti neatitikimus.

5. Europos kibernetinio saugumo sertifikavimo grupė priima nuomonę dėl tarpusavio vertinimo ataskaitos:

a) jei tarpusavio vertinimo ataskaitoje neatitikčių nenustatyta arba jei tarpusavyje įvertinta sertifikavimo įstaiga tinkamai pašalino neatitikimus, Europos kibernetinio saugumo sertifikavimo grupė gali pateikti teigiamą nuomonę, o visi susiję dokumentai skelbiami ENISA sertifikavimo svetainėje;

b) jei tarpusavyje įvertinta sertifikavimo įstaiga iki nustatyto termino tinkamai nepašalina neatitikimų, Europos kibernetinio saugumo sertifikavimo grupė gali pateikti neigiamą nuomonę, kuri skelbiama ENISA sertifikavimo svetainėje, įskaitant tarpusavio vertinimo ataskaitą ir visus susijusius dokumentus.

6. Prieš paskelbiant nuomonę visa neskelbtina, asmeninė arba nuosavybės teise priklausanti informacija pašalinama iš skelbiamų dokumentų.

X SKYRIUS

SCHEMOS PRIEŽIŪRA

48 straipsnis

EKSSS priežiūra

1. Komisija gali paprašyti Europos kibernetinio saugumo sertifikavimo grupės priimti nuomonę EKSSS priežiūros tikslais ir imtis būtinų parengiamųjų darbų.

2. Europos kibernetinio saugumo sertifikavimo grupė gali priimti nuomonę, kad patvirtintų naujausius dokumentus.

3. Europos kibernetinio saugumo sertifikavimo grupės patvirtintus naujausius dokumentus skelbia ENISA.

▼M1

4. Jei I arba II priede nenurodyta kitaip, naujausi dokumentai taikomi nuo dalinio pakeitimo akto, kuriuo jie buvo įtraukti į I arba II priedą, taikymo pradžios dienos.

▼B

XI SKYRIUS

BAIGIAMOSIOS NUOSTATOS

49 straipsnis

Nacionalinės schemos, kurioms taikoma EKSSS

1. Pagal Reglamento (ES) 2019/881 57 straipsnio 1 dalį ir nepažeidžiant to reglamento 57 straipsnio 3 dalies, visos nacionalinės kibernetinio saugumo sertifikavimo schemos ir susijusios procedūros, taikomos IRT produktams ir procesams, kuriems taikoma EKSSS, netenka galios praėjus 12 mėnesių nuo šio reglamento įsigaliojimo.

2. Nukrypstant nuo 50 straipsnio, sertifikavimo procesas pagal nacionalinę kibernetinio saugumo sertifikavimo schemą gali būti pradėtas per 12 mėnesių nuo šio reglamento įsigaliojimo dienos, su sąlyga, kad sertifikavimo procesas bus baigtas ne vėliau kaip per 24 mėnesius nuo šio reglamento įsigaliojimo dienos.

3. Pagal nacionalines kibernetinio saugumo sertifikavimo schemas išduoti sertifikatai gali būti peržiūrėti. Nauji sertifikatai, pakeičiantys peržiūrėtus sertifikatus, išduodami pagal šį reglamentą.

▼M1

4. Atliekant 3 dalyje nurodytą peržiūrą per dvejus metus nuo pirminio sertifikato išdavimo ir kai atlikus tokią peržiūrą pagal šį reglamentą išduodamas naujas sertifikatas, gali būti taikomi 3 straipsnio 2 dalyje išvardyti standartai. Pirminio sertifikato išdavimo data suprantama kaip IRT produkto arba apsaugos profilio, kuriuo grindžiamas galiojantis sertifikatas, paskutinio sertifikato išdavimo data.

▼B

50 straipsnis

Įsigaliojimas

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

Jis taikomas nuo 2025 m. vasario 27 d.

IV skyrius ir V priedas taikomi nuo šio reglamento įsigaliojimo dienos.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

▼M1

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“ (liet. „ITSVĮ taikomi būtiniausi lustinių kortelių ir panašių priemonių saugumo vertinimo reikalavimai“, 1.1 versija;

      2) „Minimum Site Security Requirements“ (liet. „Būtiniausi objekto saugumo reikalavimai“), 1.1 versija;

      3) „Application of Common Criteria to integrated circuits“ (liet. „Bendrųjų kriterijų taikymas integriniams grandynams“), 1.1 versija;

      4) „Security Architecture requirements (ADV_ARC) for smart cards and similar devices“ (liet. „Lustinėms kortelėms ir panašioms priemonėms taikomi saugumo architektūros reikalavimai (ADV_ARC)“), 1.1 versija;

      5) „Certification of „open“ smart card products“ (liet. „Atviruųjų lustinių kortelių produktų sertifikavimas“), 1.1 versija;

      6) „Composite product evaluation for smart cards and similar devices“ (liet. „Sudėtinių produktų vertinimas, taikomas lustinėms kortelėms ir panašioms priemonėms“), 1.1 versija;

      7) „Application of Attack Potential to Smartcards“ (liet. „Išpuolio potencialo taikymas lustinėms kortelėms“), 1.2 versija;

   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“ (liet. „ITSVĮ taikomi būtiniausi aparatinės įrangos įtaisų su apsauginėmis dėžėmis saugumo vertinimo reikalavimai“), 1.1 versija;

      2) „Minimum Site Security Requirements“ (liet. „Būtiniausi objekto saugumo reikalavimai“), 1.1 versija;

      3) „Application of Attack Potential to hardware devices with security boxes“ (liet. „Išpuolio potencialo taikymas aparatinės įrangos įtaisams su apsauginėmis dėžėmis“), 1.2 versija.

2. Naujausi dokumentai, susiję su suderintu atitikties vertinimo įstaigų akreditavimu:

   a) „Accreditation of ITSEFs for the EUCC“ (liet. „ITSVĮ akreditavimas taikyti EKSSS“), 1.1 versija, jei akreditacija suteikta iki 2025 m. liepos 8 d.;

   b) „Accreditation of ITSEFs for the EUCC“ (liet. „ITSVĮ akreditavimas taikyti EKSSS“), 1.6c versija, jei akreditacija naujai suteikta arba peržiūrėta po 2025 m. liepos 8 d.;

   c) „Accreditation of CBs for the EUCC“ (liet. „Sertifikavimo įstaigų akreditavimas taikyti EKSSS“), 1.6b versija.

▼B

II PRIEDAS

AVA_VAN 4 arba 5 lygiu sertifikuoti apsaugos profiliai

1. Nuotolinio kvalifikuoto parašo ir spaudo kūrimo įtaisų kategorijos atveju:

   1) EN 419241-2:2019. Patikimos pasirašymo elektroniniu parašu sistemos. 2 dalis. Patvirtintų elektroninio parašo kūrimo įtaisų apsaugos profilis, skirtas pasirašymui elektroniniu parašu;

   2) EN 419221-5:2018. Patikimumo užtikrinimo paslaugų teikėjo kriptografinių modulių apsaugos profiliai. 5 dalis. Patikimumo užtikrinimo paslaugų kriptografinis modulis

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

   [TUŠČIA]

▼B

III PRIEDAS

Rekomenduojami apsaugos profiliai (rodantys technines sritis iš I priedo)

Apsaugos profiliai, naudojami sertifikuojant toliau nurodytus IRT produktus, priskiriamus toliau nurodytai IRT produktų kategorijai:

a) mašininio nuskaitymo kelionės dokumentų kategorijos atveju:

1) *PP Machine Readable Travel Document using Standard Inspection Procedure with PACE* (liet. AP „Mašininio nuskaitymo kelionės dokumentas, kuriam taikoma standartinė patikrinimo procedūra su PACE“), BSI-CC-PP-0068-V2-2011-MA-01;

2) *PP Machine Readable Travel Document using Standard Inspection Procedure with PACE* (liet. AP „Mašininio nuskaitymo kelionės dokumento su „ICAO taikomosios programos“ išplėstine prieigos kontrole“), BSI-CC-PP-0056-2009;

3) *PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE* (liet. AP „Mašininio nuskaitymo kelionės dokumento su „ICAO taikomosios programos“ išplėstine prieigos kontrole su PACE“), BSI-CC-PP-0056-V2-2012-MA-02;

4) *PP for a Machine Readable Travel Document with "ICAO Application" Basic Access Control* (liet. AP „Mašininio nuskaitymo kelionės dokumento su „ICAO taikomosios programos“ bazine prieigos kontrole“), BSI-CC-PP-0055-2009;

b) saugių elektroninio parašo kūrimo įtaisų kategorijos atveju:

1) EN 419211-1:2014. Saugiojo elektroninio parašo kūrimo įtaiso apsaugos profiliai. 1 dalis. Apžvalga;

2) EN 419211-2:2013. Saugiojo elektroninio parašo kūrimo įtaiso apsaugos profiliai. 2 dalis. Įtaisas su rakto generatoriumi;

3) EN 419211-3:2013. Saugiojo elektroninio parašo kūrimo įtaiso apsaugos profiliai. 3 dalis. Įtaisas, atliekantis rakto importą;

4) EN 419211-4:2013. Saugiojo elektroninio parašo kūrimo įtaiso apsaugos profiliai. 4 dalis. Plėtinys, taikomas įtaisui, generuojančiam raktą ir užtikrinančiam patikimą ryšį su sertifikato kūrimo taikomąja programa;

5) EN 419211-5:2013. Saugiojo elektroninio parašo kūrimo įtaiso apsaugos profiliai. 5 dalis. Plėtinys, taikomas įtaisui, generuojančiam raktą ir užtikrinančiam patikimą ryšį su elektroninio parašo kūrimo taikomąja programa;

6) EN 419211-6:2014. Saugiojo elektroninio parašo kūrimo įtaiso apsaugos profiliai. 6 dalis. Plėtinys, taikomas įtaisui, atliekančiam rakto importą ir užtikrinančiam patikimą ryšį su parašo kūrimo taikomąja programa;

c) skaitmeninių tachografų kategorijos atveju:

1) Skaitmeninis tachografas. Tachografo kortelė, kaip nurodyta 2016 m. kovo 18 d. Komisijos įgyvendinimo reglamente (ES) 2016/799, kuriuo įgyvendinamas Reglamentas (ES) 165/2014 (1C priedas);

2) Skaitmeninis tachografas. Komisijos reglamento (EB) Nr. 1360/2002 IB priede nurodytas transporto priemonės blokas, skirtas įrengti kelių transporto priemonėse;

▼B

3) Skaitmeninis tachografas. Išorinis GNSS įrenginys (IGĮ AP), kaip nurodyta 2016 m. kovo 18 d. Komisijos įgyvendinimo reglamento (ES) 2016/799, kuriuo įgyvendinamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 165/2014, 1C priede;

4) Skaitmeninis tachografas. Judesio jutiklis (JJ AP), kaip nurodyta 2016 m. kovo 18 d. Komisijos įgyvendinimo reglamento (ES) 2016/799, kuriuo įgyvendinamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 165/2014, 1C priede;

d) saugiųjų integrinių grandynų, lustinių kortelių ir susijusių prietaisų kategorijos atveju:

1) *Security IC Platform PP* (liet. AP „Saugumo IG platforma“, BSI-CC-PP-0084-2014;

2) *Java Card System - Open Configuration* (liet. „„Java“ kortelių sistema. Atvira konfigūracija“), V3.0.5 BSI-CC-PP-0099-2017;

3) *Java Card System - Closed Configuration* (liet. „„Java“ kortelių sistema. Uždara konfigūracija“, BSI-CC-PP-0101-2017;

4) *PP for a PC Client Specific Trusted Platform Module Family 2.0 Level 0 Revision 1.16*, (liet. AP „AK konkrečiam klientui skirtų patikimų platformos modulių grupė 2.0, 0 lygis, 1.16 redakcija“), ANSSI-CC-PP-2015/07;

5) *Universal SIM card* (liet. „Universalioji SIM kortelė“), PU-2009-RT-79, ANSSI-CC-PP-2010/04;

6) *Embedded UICC (eUICC) for Machine-to-Machine Devices* (liet. „Įtaisytoji universalioji lustinė kortelė, skirta įrenginių tarpusavio sąveikos įtaisams“), BSI-CC-PP-0089-2015;

e) (mokėjimo) sąveikos taškų ir mokėjimo terminalų kategorijos atveju:

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

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

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

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

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

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

▼B

f) aparatinės įrangos įtaisų su apsauginėmis dėžėmis kategorijos atveju:

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

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

3) *Cryptographic Module for CSP Signing Operations without Backup* (liet. „Sertifikavimo paslaugų teikėjų pasirašymo operacijų kriptografinis modulis be atkūrimo galimybės“) – AP CMCSO, AP HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10.

▼B

IV PRIEDAS

Užtikrinimo tęstinumas ir sertifikatų peržiūra

IV.1. **Užtikrinimo tęstinumas: taikymo sritis**

1. Šie užtikrinimo tęstinumo reikalavimai taikomi priežiūros veiklai, susijusiai su:

   a) pakartotiniu vertinimu, jei nepakitęs sertifikuotas IRT produktas vis dar atitinka jam taikomus saugumo reikalavimus;

   b) sertifikuoto IRT produkto pakeitimų poveikio jo sertifikavimui vertinimu;

   c) pataisų taikymu pagal įvertintą pataisų valdymo procesą, jei pataisų taikymas yra įtrauktas į sertifikavimą;

   d) jei įtraukta, sertifikato turėtojo gyvavimo ciklo valdymo arba gamybos procesų peržiūra.

2. EKSSS sertifikato turėtojas gali prašyti peržiūrėti sertifikatą šiais atvejais:

   a) EKSSS sertifikato galiojimas baigiasi per devynis mėnesius;

   b) buvo pakeistas sertifikuotas IRT produktas arba kitas veiksnys, galintis turėti įtakos jo saugumo funkcinėms galimybėms;

   c) sertifikato turėtojas reikalauja, kad pažeidžiamumo vertinimas būtų dar kartą atliktas, siekiant dar kartą patvirtinti EKSSS sertifikate pateiktą užtikrinimą, susijusį su IRT produkto atsparumu dabartiniams kibernetiniams išpuoliams.

IV.2. **Pakartotinis vertinimas**

1. Jei reikia įvertinti nepakitusio sertifikuoto IRT produkto grėsmės aplinkos pokyčių poveikį, sertifikavimo įstaigai pateikiamas prašymas atlikti pakartotinį vertinimą.

2. Pakartotinį vertinimą atlieka ta pati ITSVĮ, kuri dalyvavo atliekant ankstesnį vertinimą, kuris buvo įtrauktas į ankstesnį vertinimą, pakartotinai panaudodama visus tebetaikomus jo rezultatus. Atliekant vertinimą daugiausia dėmesio skiriama saugumo užtikrinimo veiklai, kurią gali paveikti pakeista sertifikuoto IRT produkto grėsmės aplinka, visų pirma atitinkamai AVA_VAN grupei ir, be to, užtikrinimo gyvavimo ciklo grupei, kurioje vėl surenkama pakankamai įrodymų apie kūrimo aplinkos priežiūrą.

3. ITSVĮ aprašo pakeitimus ir išsamiai išdėsto pakartotinio vertinimo rezultatus bei atnaujina techninę ankstesnio vertinimo ataskaitą.

4. Sertifikavimo įstaiga peržiūri atnaujintą techninę vertinimo ataskaitą ir parengia pakartotinio vertinimo ataskaitą. Tuomet pirminio sertifikato būsena pakeičiama pagal 13 straipsnį.

5. Pakartotinio vertinimo ataskaita ir atnaujintas sertifikatas pateikiami nacionalinei kibernetinio saugumo sertifikavimo institucijai ir ENISA, kad ši agentūra paskelbtų juos savo kibernetinio saugumo sertifikavimo svetainėje.

▼B

IV.3. **Sertifikuoto IRT produkto pakeitimai**

1. Jei sertifikuotas IRT produktas buvo pakeistas, sertifikato turėtojas, norintis išlaikyti sertifikatą, pateikia sertifikavimo įstaigai poveikio analizės ataskaitą.

2. Poveikio analizės ataskaitoje pateikiama ši informacija:

   a) įvadas, kuriame pateikiama informacija, būtina tam, kad būtų galima nustatyti poveikio analizės ataskaitą ir pakeistą vertinimo objektą;

   b) produkto pakeitimų aprašymas;

   c) informacija apie susijusio kūrėjo įrodymus;

   d) kūrėjo įrodymų pakeitimų aprašymas;

   e) nustatyti faktai ir išvados dėl kiekvieno pakeitimo poveikio saugumo užtikrinimui.

3. Sertifikavimo įstaiga išnagrinėja poveikio analizės ataskaitoje aprašytus pakeitimus, kad patvirtintų jų poveikį sertifikuoto vertinimo objekto saugumo užtikrinimui, kaip siūloma poveikio analizės ataskaitos išvadose.

4. Atlikusi patikrinimą, sertifikavimo įstaiga nustato, ar pakeitimas yra nereikšmingo, ar reikšmingo masto, atsižvelgiant į jo poveikį.

▼M1

5. Jei sertifikavimo įstaiga patvirtina, kad pakeitimai yra nereikšmingi, pakeistam IRT produktui naujas sertifikatas neišduodamas ir parengiama prie pradinės sertifikavimo ataskaitos pridedama priežiūros ataskaita.

   Priežiūros ataskaita įtraukiama į poveikio analizės ataskaitą kaip jos atskira dalis ir ją sudaro šie skirsniai:

   a) įvadas;

   b) pakeitimų aprašymas;

   c) susijusio kūrėjo įrodymai.

6. 5 punkte nurodyta priežiūros ataskaita pateikiama ENISA, kad ši agentūra paskelbtų ją savo kibernetinio saugumo sertifikavimo svetainėje.

▼B

7. Patvirtinus, kad pakeitimai yra reikšmingi, atliekamas pakartotinis vertinimas, atsižvelgiant į ankstesnį vertinimą ir pakartotinai panaudojant visus vis dar taikomus ankstesnio vertinimo rezultatus.

8. Užbaigus pasikeitusio vertinimo objekto vertinimą, ITSVĮ parengia naują techninę vertinimo ataskaitą. Sertifikavimo įstaiga peržiūri atnaujintą techninę vertinimo ataskaitą ir, kai taikoma, parengia naują sertifikatą su nauja sertifikavimo ataskaita.

9. Naujas sertifikatas ir sertifikavimo ataskaita pateikiami ENISA, kad ši agentūra juos paskelbtų.

▼B

IV.4. **Pataisų valdymas**

1. Pataisų valdymo procedūroje numatytas struktūrizuotas sertifikuoto IRT produkto atnaujinimo procesas. Pataisų valdymo procedūra, įskaitant mechanizmą, kurį IRT produkte įdiegė sertifikavimo prašantis pareiškėjas, gali būti taikoma po IRT produkto sertifikavimo, už kurį atsako atitikties vertinimo įstaiga.

2. Sertifikavimo prašantis pareiškėjas gali įtraukti į IRT produkto sertifikavimą pataisų mechanizmą, kuris yra dalis sertifikuotos valdymo procedūros, įdiegtos į IRT produktą, esant vienai iš šių sąlygų:

   a) funkcinės galimybės, kurioms įtakos turi pataisa, nėra susijusios su sertifikuoto IRT produkto vertinimo objektu;

   b) pataisa susijusi su iš anksto nustatytu nedideliu sertifikuoto IRT produkto pakeitimu;

   c) pataisa susijusi su patvirtintu pažeidžiamumu, turinčiu itin didelį poveikį sertifikuoto IRT produkto saugumui.

3. Jei pataisa susijusi su svarbiu sertifikuoto IRT produkto vertinimo objekto pakeitimu, susijusiu su anksčiau nenustatytu pažeidžiamumu, neturinčiu itin didelio poveikio IRT produkto saugumui, taikomos 13 straipsnio nuostatos.

4. IRT produkto pataisų valdymo procedūrą sudarys šie elementai:

   a) IRT produkto pataisos kūrimo ir išleidimo procesas;

   b) techninis mechanizmas ir funkcijos, skirti tam, kad pataisa būtų įtraukta į IRT produktą;

   c) su techninio mechanizmo efektyvumu ir veiksmingumu susijusios veiklos rūšių rinkinys.

5. Sertifikuojant IRT produktą:

   a) pareiškėjas, prašantis sertifikuoti IRT produktą, pateikia pataisų valdymo procedūros aprašymą;

   b) ITSVĮ patikrina šiuos elementus:

      1) ar kūrėjas IRT produkte įdiegė pataisų mechanizmus pagal sertifikavimui pateiktą pataisų valdymo procedūrą;

      2) ar vertinimo objekto ribos yra atskirtos taip, kad atskirtų procesų pakeitimai nedarytų poveikio vertinimo objekto saugumui;

      3) ar techninių pataisų mechanizmas veikia pagal šio skirsnio nuostatas ir pareiškėjo teiginius;

   c) sertifikavimo įstaiga į sertifikavimo ataskaitą įtraukia įvertintos pataisų valdymo procedūros rezultatus.

6. Sertifikato turėtojas atitinkamam sertifikuotam IRT produktui gali pradėti taikyti pagal sertifikuotą pataisų valdymo procedūrą atliktą pataisą ir per penkias darbo dienas atlieka šiuos veiksmus šiais atvejais:

▼B

a) 2 punkto a papunktyje nurodytu atveju praneša apie atitinkamą pataisą sertifikavimo įstaigai, kuri negali pakeisti atitinkamo EKSSS sertifikato;

b) 2 punkto b papunktyje nurodytu atveju pateikia atitinkamą pataisą peržiūrėti ITSVĮ. Gavusi pataisą, ITSVĮ informuoja sertifikavimo įstaigą, kuri imasi tinkamų veiksmų, susijusių su naujos atitinkamo EKSSS sertifikato versijos išdavimu ir sertifikavimo ataskaitos atnaujinimu;

c) 2 punkto c papunktyje nurodytu atveju pateikia atitinkamą pataisą ITSVĮ, kad būtų atliktas būtinas pakartotinis vertinimas, tačiau tuo pat metu gali diegti pataisą. ITSVĮ informuoja sertifikavimo įstaigą, kuri po to pradeda susijusią sertifikavimo veiklą.

▼B

V PRIEDAS

Sertifikavimo ataskaitos turinys

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.

2. Sertifikavimo ataskaita yra išsamios ir praktinės informacijos apie IRT produktą arba IRT produktų kategoriją ir saugų IRT produkto diegimą šaltinis, todėl joje pateikiama visa naudotojams ir suinteresuotosioms šalims aktuali viešai prieinama ir bendrai naudojama informacija. Viešai prieinama ir bendrai naudojama informacija gali būti nurodyta sertifikavimo ataskaitoje.

3. Sertifikavimo ataskaitą sudaro bent šie skirsniai:

   a) santrauka;

   b) informacija apie IRT produktą arba IRT produktų kategoriją, kuriam arba kuriai taikomi apsaugos profiliai;

   c) apsaugos paslaugos;

   d) prielaidos ir taikymo srities paaiškinimas;

   e) architektūrinė informacija;

   f) papildoma kibernetinio saugumo informacija, jei taikoma;

   g) IRT produkto bandymai, jei jie buvo atlikti;

   h) kai taikoma, sertifikato turėtojo gyvavimo ciklo valdymo procesų ir gamybos įrenginių identifikavimo duomenys;

   i) vertinimo rezultatai ir informacija apie sertifikatą;

   j) sertifikuoti pateikto IRT produkto saugumo uždavinio santrauka;

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

   l) bibliografija.

4. Santrauka yra trumpa visos sertifikavimo ataskaitos santrauka. Santraukoje aiškiai ir glaustai apžvelgiami vertinimo rezultatai ir pateikiama ši informacija:

   a) vertinamo IRT produkto pavadinimas, produkto komponentų, kurie yra vertinimo dalis, sąrašas ir IRT produkto versija;

   b) vertinimą atlikusios ITSVĮ pavadinimas ir, kai taikoma, subrangovų sąrašas;

   c) vertinimo užbaigimo data;

   d) nuoroda į ITSVĮ parengtą techninę vertinimo ataskaitą;

   e) trumpas sertifikavimo ataskaitos rezultatų aprašymas, įskaitant:

      1) vertinimui taikomų bendrųjų kriterijų versiją ir, jei taikoma, laidą;

      2) bendrųjų kriterijų saugumo užtikrinimo dokumentų rinkinį ir saugumo užtikrinimo komponentus, įskaitant AVA_VAN lygį, taikytą atliekant vertinimą, ir atitinkamą saugumo užtikrinimo lygį, kaip nustatyta Reglamento (ES) 2019/881 52 straipsnyje, su kuriuo susijęs EKSSS sertifikatas;

▼B

3) vertinamo IRT produkto saugumo funkcinės galimybės;

4) grėsmių ir organizacijos saugumo politikos, su kuriomis susiję klausimai sprendžiami naudojant įvertintą IRT produktą, santrauka;

5) specialūs konfigūracijos reikalavimai;

6) prielaidos dėl operacinės aplinkos;

7) jei taikoma, ar yra patvirtinta pataisų valdymo procedūra pagal IV priedo IV.4 skirsnį;

8) atsakomybės ribojimo pareiškimas (-ai).

5. Įvertintas IRT produktas aiškiai nurodomas, be kita ko, pateikiant šią informaciją:

a) įvertinto IRT produkto pavadinimą;

b) IRT produkto komponentų, kurie yra vertinimo dalis, sąrašą;

c) IRT produkto komponentų versijos numerį;

d) papildomus reikalavimus, taikomus sertifikuoto IRT produkto operacinei aplinkai;

e) EKSSS sertifikato turėtojo vardą, pavardę (pavadinimą) ir kontaktinius duomenis;

f) kai taikoma, informaciją apie pataisų valdymo procedūrą, įtrauktą į sertifikatą;

g) nuorodą į EKSSS sertifikato turėtojo interneto svetainę, kurioje pateikiama papildoma kibernetinio saugumo informacija apie sertifikuotą IRT produktą pagal Reglamento (ES) 2019/881 55 straipsnį.

6. Į šį skirsnį įtraukta informacija turi būti kuo tikslesnė, kad būtų užtikrintas išsamus ir tikslus IRT produkto aprašymas, kurį galima pakartotinai naudoti atliekant būsimus vertinimus.

7. Saugumo politikos skirsnyje aprašoma IRT produkto saugumo politika ir politika ar taisyklės, kurių vykdymą įvertintas IRT produktas turi padėti užtikrinti arba kurių reikalavimus tas produktas turi atitikti. Jame taip pat nurodoma ir aprašoma ši politika:

a) sertifikato turėtojo pažeidžiamumų valdymo politika;

b) sertifikato turėtojo saugumo tęstinumo politika.

8. Kai taikytina, į politiką gali būti įtrauktos sąlygos, susijusios su pataisų valdymo procedūros taikymu sertifikato galiojimo laikotarpiu.

9. Prielaidų ir taikymo srities paaiškinimo skirsnyje pateikiama išsami informacija apie aplinkybes ir tikslus, susijusius su numatoma produkto paskirtimi, kaip nurodyta 7 straipsnio 1 dalies c punkte. Informaciją sudaro:

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;

▼B

10. 9 punkte nurodyta informacija turi būti kuo suprantamesnė, kad sertifikuoto IRT produkto naudotojai galėtų priimti informacija pagrįstus sprendimus dėl rizikos, susijusios su jo naudojimu.

11. Architektūrinės informacijos skirsnyje pateikiamas platus IRT produkto ir jo pagrindinių komponentų aprašymas pagal bendrųjų kriterijų ADV_TDS posistemių projektą.

12. Išsamus papildomos IRT produkto kibernetinio saugumo informacijos sąrašas pateikiamas pagal Reglamento (ES) 2019/881 55 straipsnį. Visi susiję dokumentai žymimi versijos numeriais.

13. IRT produktų bandymų skirsnyje pateikiama ši informacija:

    a) sertifikatą išdavusios institucijos arba įstaigos, įskaitant atsakingą nacionalinę kibernetinio saugumo sertifikavimo instituciją, pavadinimas ir kontaktinis punktas;

    b) vertinimą atlikusios ITSVĮ pavadinimas, jei ITSVĮ skiriasi nuo sertifikavimo įstaigos;

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

    d) naujausio dokumento versija ir atliekant vertinimą taikyti papildomi saugumo vertinimo kriterijai;

    e) išsamūs ir tikslūs IRT produkto nuostačiai ir konfigūracija vertinimo laikotarpiu, įskaitant su naudojimu susijusias ir kitas pastabas, jei tokių yra;

    f) bet koks naudotas apsaugos profilis, be kita ko, nurodant šią informaciją:

        1) apsaugos profilio autorių;

        2) apsaugos profilio pavadinimą ir identifikatorių;

        3) apsaugos profilio sertifikato identifikatorių;

        4) sertifikavimo įstaigos ir vertinant apsaugos profilį dalyvavusios ITSVĮ pavadinimus ir kontaktinius duomenis;

        5) informaciją apie saugumo užtikrinimo paketą (-us), reikalaujamą (-us) apsaugos profilį atitinkančiam produktui.

14. Vertinimo rezultatai ir informacija apie sertifikato skirsnį apima šią informaciją:

    a) patvirtinimą, kad pasiektas saugumo užtikrinimo lygis, nurodytas šio reglamento 4 straipsnyje ir Reglamento (ES) 2019/881 52 straipsnyje;

    b) informaciją apie 3 straipsnyje nurodytuose standartuose nustatytus užtikrinimo reikalavimus, kuriuos IRT produktas arba apsaugos profilis faktiškai atitinka, įskaitant AVA_VAN lygį;

    c) išsamų saugumo užtikrinimo reikalavimų aprašymą, taip pat išsamią informaciją apie tai, kaip produktas atitinka kiekvieną iš jų;

    d) sertifikato išdavimo datą ir galiojimo laikotarpį;

    e) unikalų sertifikato identifikatorių.

▼B

15. Saugumo uždavinys įtraukiamas į sertifikavimo ataskaitą arba joje nurodomas ir apibendrinamas ir pateikiamas kartu su sertifikavimo ataskaita, kad būtų paskelbtas.

16. Saugumo uždavinys gali būti išvalomas pagal VI.2 skirsnį.

17. Pagal 11 straipsnyje nustatytas taisykles ir procedūras į sertifikavimo ataskaitą gali būti įtrauktas su EKSSS susijęs ženklas arba etiketė.

18. Bibliografijos skirsnyje pateikiamos nuorodos į visus dokumentus, naudotus rengiant sertifikavimo ataskaitą. Ta informacija apima bent:

    a) saugumo vertinimo kriterijus, naujausius dokumentus ir kitas naudotas atitinkamas specifikacijas bei jų versijas;

    b) techninę vertinimo ataskaitą;

    c) jei taikoma, sudėtinio vertinimo atveju rengiamą techninę vertinimo ataskaitą;

    d) techninius informacinius dokumentus;

    e) kūrėjo dokumentaciją, naudotą atliekant vertinimą.

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

V.2. **Skelbtino saugumo uždavinio išvalymas**

1. Saugumo uždavinys, kuris turi būti įtrauktas į sertifikavimo ataskaitą arba nurodytas joje pagal VI.1 skirsnio 1 punktą, gali būti išvalomas pašalinant arba perfrazuojant nuosavybinę techninę informaciją.

2. Gautas išvalytas saugumo uždavinys turi būti tikrasis išsamios originalios versijos aprašymas. Tai reiškia, kad į išvalytą saugumo uždavinį negali būti neįtraukta informacija, kuri yra būtina norint suprasti vertinimo objekto saugumo savybes ir vertinimo apimtį.

3. Išvalyto saugumo uždavinio turinys turi atitikti šiuos būtiniausius reikalavimus:

    a) jis pristatomas neišvalytas, nes jame apskritai nėra jokios nuosavybinės informacijos;

    b) išvalytas saugumo uždavinys turi turėti unikalų identifikatorių, kuris skirtųsi nuo išsamios originalios versijos identifikatoriaus;

    c) vertinimo objekto aprašymas gali būti sutrumpintas, nes jis gali apimti nuosavybinę ir išsamią informaciją apie vertinimo objekto projektą, kuris neturėtų būti skelbiamas;

    d) vertinimo objekto saugumo aplinkos aprašymas (prielaidos, grėsmės, organizacijos saugumo politika) nesutrumpinamas, jei ta informacija yra būtina vertinimo apimčiai suprasti;

    e) saugumo tikslai nesumažinami, nes visa informacija turi būti skelbiama viešai, kad būtų galima suprasti saugumo uždavinio tikslą ir vertinimo objektą;

▼B

f) visi saugumo reikalavimai skelbiami viešai. Paraiškos pastabose gali būti pateikta informacija apie tai, kaip 3 straipsnyje nurodytų bendrųjų kriterijų funkciniai reikalavimai buvo naudojami saugumo uždaviniui suprasti;

g) vertinimo objekto specifikacijos santrauka apima visas vertinimo objekto saugumo funkcijas, tačiau papildoma nuosavybinė informacija gali būti išvalyta;

h) įtraukiamos nuorodos į apsaugos profilius, taikomus vertinimo objektui;

i) loginis pagrindimas gali būti išvalytas, siekiant pašalinti nuosavybinę informaciją.

4. Net jei išvalytas saugumo uždavinys nėra oficialiai įvertintas pagal 3 straipsnyje nurodytus vertinimo standartus, sertifikavimo įstaiga užtikrina, kad jis atitiktų išsamų ir įvertintą saugumo uždavinį, o sertifikavimo ataskaitoje nurodo tiek išsamų, tiek išvalytą saugumo uždavinį.

▼B

VI PRIEDAS

Tarpusavio vertinimų apimtis ir grupės sudėtis

VI.1. **Tarpusavio vertinimo apimtis**

1. Taikomi šių rūšių tarpusavio vertinimai:

   a) 1 rūšis: kai sertifikavimo įstaiga vykdo AVA_VAN.3 lygio sertifikavimo veiklą;

   b) 2 rūšis: kai sertifikavimo įstaiga vykdo sertifikavimo veiklą, susijusią su technine sritimi, kuri I priede nurodyta kaip naujausi dokumentai;

   c) 3 rūšis: kai sertifikavimo įstaiga vykdo aukštesnio nei AVA_VAN.3 lygio sertifikavimo veiklą, naudodamasi apsaugos profiliu, II arba III priede nurodytu kaip naujausi dokumentai.

2. Tarpusavyje vertinama sertifikavimo įstaiga pateikia sertifikuotų IRT produktų, kuriuos tarpusavio vertinimo grupė gali peržiūrėti, sąrašą, laikydamasi šių taisyklių:

   a) produktai, kurie gali būti peržiūrėti, apima sertifikavimo įstaigos įgaliojimo techninę taikymo sritį; atliekant tarpusavio vertinimą bus analizuojami bent du skirtingi produktų vertinimai, susiję su aukštu saugumo užtikrinimo lygiu, ir vienas apsaugos profilis, jei sertifikavimo įstaiga išdavė sertifikatą, kuriame nurodomas aukštas saugumo užtikrinimo lygis;

   b) atliekant 2 rūšies tarpusavio vertinimą, sertifikavimo įstaiga pateikia bent po vieną produktą pagal techninę sritį ir pagal susijusią ITSVĮ;

   c) atliekant 3 rūšies tarpusavio vertinimą, bent vienas produktas, kuris gali būti peržiūrėtas, vertinamas pagal taikomus atitinkamus apsaugos profilius.

VI.2. **Tarpusavio vertinimo grupė**

1. Vertinimo grupę sudaro bent du ekspertai, atrinkti iš skirtingų valstybių narių skirtingų sertifikavimo įstaigų, išduodančių sertifikatus, kuriuose nurodomas aukštas saugumo užtikrinimo lygis. Ekspertai turėtų įrodyti, kad turi atitinkamų ekspertinių žinių, susijusių su 3 straipsnyje nurodytais standartais ir naujausiais dokumentais, kuriems taikomas tarpusavio vertinimas.

2. Reglamento (ES) 2019/881 56 straipsnio 6 dalyje nurodyto įgaliojimų išduoti sertifikatus delegavimo arba išankstinio sertifikatų patvirtinimo atveju nacionalinės kibernetinio saugumo sertifikavimo institucijos ekspertas, susijęs su atitinkama sertifikavimo įstaiga, taip pat dalyvauja pagal šio skirsnio 1 dalį atrinktų ekspertų grupės veikloje.

3. Atliekant 2 rūšies tarpusavio vertinimą, grupės nariai atrenkami iš sertifikavimo įstaigų, įgaliotų dirbti atitinkamoje techninėje srityje.

4. Kiekvienas vertinimo grupės narys turi turėti bent dvejų metų sertifikavimo veiklos sertifikavimo įstaigoje patirtį.

5. Atliekant 2 arba 3 rūšies tarpusavio vertinimą, kiekvienas vertinimo grupės narys turi turėti bent dvejų metų sertifikavimo veiklos toje atitinkamoje techninėje srityje arba apsaugos profilio sertifikavimo patirtį ir įrodytą kompetenciją, taip pat dalyvavimo suteikiant ITSVĮ įgaliojimus patirtį.

▼B

6. Tarpusavio vertinime stebėtojo teisėmis dalyvauja nacionalinė kibernetinio saugumo sertifikavimo institucija, stebinti ir prižiūrinti tarpusavio vertinimą, ir bent viena nacionalinė kibernetinio saugumo sertifikavimo institucija, kurios sertifikavimo įstaigai tarpusavio vertinimas netaikomas. ENISA taip pat gali dalyvauti tarpusavio vertinime kaip stebėtoja.

7. Tarpusavyje vertinama sertifikavimo įstaiga supažindinama su tarpusavio vertinimo grupės sudėtimi. Pagrįstais atvejais ji gali ginčyti tarpusavio vertinimo grupės sudėtį ir prašyti ją peržiūrėti.

▼B

VII PRIEDAS

EKSSS sertifikato turinys

EKSSS sertifikate pateikiama bent ši informacija:

a) sertifikatą išduodančios sertifikavimo įstaigos nustatytas unikalus identifikatorius;

b) informacija, susijusi su sertifikuotu IRT produktu arba apsaugos profiliu ir sertifikato turėtoju, įskaitant:

   1) IRT produkto arba apsaugos profilio pavadinimą ir, kai taikytina, vertinimo objektą;

   2) IRT produkto arba apsaugos profilio rūšį ir, kai taikytina, vertinimo objektą;

   3) IRT produkto arba apsaugos profilio versiją;

   4) EKSSS sertifikato turėtojo vardą, pavardę (pavadinimą), adresą ir kontaktinius duomenis;

   5) nuorodą į sertifikato turėtojo interneto svetainę, kurioje pateikiama Reglamento (ES) 2019/881 55 straipsnyje nurodyta papildoma kibernetinio saugumo informacija;

c) informacija, susijusi su IRT produkto arba apsaugos profilio vertinimu ir sertifikavimu, įskaitant:

   1) EKSSS sertifikato turėtojo vardą, pavardę (pavadinimą), adresą ir kontaktinius duomenis;

   2) vertinimą atlikusios ITSVĮ pavadinimą, jei ITSVĮ skiriasi nuo sertifikavimo įstaigos,

   3) atsakingos nacionalinės kibernetinio saugumo sertifikavimo institucijos pavadinimą;

   4) nuorodą į šį reglamentą;

   5) nuorodą į sertifikavimo ataskaitą, susijusią su V priede nurodytu sertifikatu;

   6) taikytiną saugumo užtikrinimo lygį pagal 4 straipsnį;

   7) nuorodą į 3 straipsnyje nurodytų standartų, taikomų atliekant vertinimą, versiją;

   8) informaciją apie saugumo užtikrinimo lygį arba paketą, nurodytą 3 straipsnyje minimuose standartuose ir atitinkantį VIII priedo reikalavimus, įskaitant naudojamus saugumo užtikrinimo komponentus ir AVA_VAN lygį;

   9) kai taikytina, nuorodą į vieną ar daugiau apsaugos profilių, kuriuos IRT produktas arba apsaugos profilis atitinka;

   10) išdavimo datą;

   11) sertifikato galiojimo laikotarpį;

d) ženklas ir etiketė, susiję su sertifikatu pagal 11 straipsnį.

▼B

VIII PRIEDAS

Saugumo užtikrinimo paketo paskelbimas

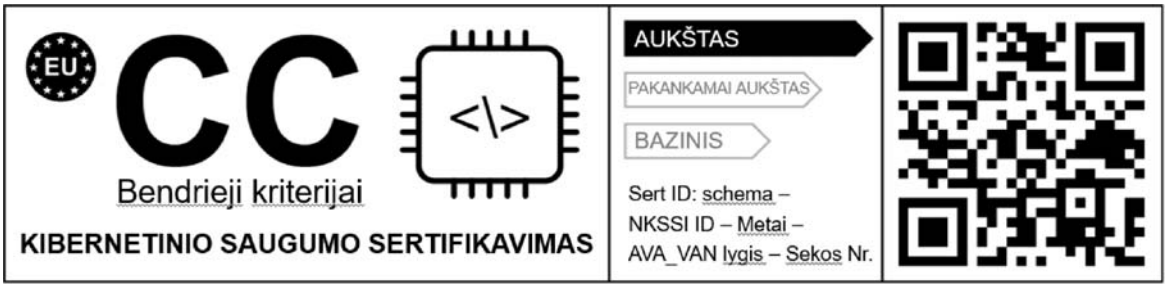
1. Priešingai nei nustatyta bendruosiuose kriterijuose, papildymas:
   a) neturi būti žymimas santrumpa „+“;
   b) nurodomas pateikiant visų susijusių komponentų sąrašą;
   c) išsamiai aprašomas sertifikavimo ataskaitoje.
2. EKSSS sertifikate patvirtintas saugumo užtikrinimo lygis gali būti papildytas vertinimo užtikrinimo lygiu, kaip nurodyta šio reglamento 3 straipsnyje.
3. Jei EKSSS sertifikate patvirtintas saugumo užtikrinimo lygis nėra susijęs su papildymu, EKSSS sertifikate nurodomas vienas iš šių paketų:
   a) „konkretus užtikrinimo paketas“;
   b) „apsaugos profilį atitinkantis užtikrinimo paketas“, jei nurodomas apsaugos profilis be vertinimo užtikrinimo lygio.

▼B

IX PRIEDAS

Ženklas ir etiketė

1. Ženklo ir etiketės forma:



2. Jei ženklas ir etiketė sumažinami arba padidinami, turi būti laikomasi pirmiau pateiktame piešinyje nurodytų proporcijų.
3. Kai ženklas ir etiketė naudojami fiziniu pavidalu, jie turi būti bent 5 mm aukščio.