Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2024/482

7.2.2024.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2024/482

(2024. gada 31. janvāris)

par to, kā vienotos kritērijos balstītas Eiropas kiberdrošības sertifikācijas shēmas (*EUCC*) pieņemšanas sakarā piemērojama Eiropas Parlamenta un Padomes Regula (ES) 2019/881

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

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

tā kā:

(1) Šī regula nosaka vienotos kritērijos balstītas Eiropas kiberdrošības sertifikācijas shēmas (*EUCC*) uzdevumus, noteikumus un pienākumus, kā arī struktūru saskaņā ar Regulā (ES) 2019/881 noteikto Eiropas kiberdrošības sertifikācijas satvaru. *EUCC* ir balstīta uz Informācijas sistēmu drošības augstāko amatpersonu grupas (*SOG-IS*) Savstarpējās atzīšanas nolīgumu (*MRA*) par informācijas tehnoloģiju drošības sertifikātiem ([2]), izmantojot vienotos kritērijus, ieskaitot grupas procedūras un dokumentus.

(2) Shēmas pamatā būtu jābūt atzītiem starptautiskiem standartiem. Vienotie kritēriji ("Common Criteria") ir starptautisks informācijas drošības izvērtēšanas standarts, kas publicēts, piemēram, kā standarts ISO/IEC 15408 "Information security, cybersecurity and privacy protection – Evaluation criteria for IT security". Tas balstās uz izvērtēšanu, ko izdara trešās personas, un paredz septiņus izvērtējuma apliecinājuma līmeņus (*EAL*). Vienotos kritērijus papildina vienotā izvērtēšanas metodika, kas publicēta, piemēram, kā standarts ISO/IEC 18045 "Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Methodology for IT security evaluation". Specifikācijas un dokumenti, ar kuriem piemēro šīs regulas noteikumus, var attiekties uz publiski pieejamu standartu, kas atspoguļo saskaņā ar šo regulu veiktā sertifikācijā izmantoto standartu, piemēram, vienotos informācijas tehnoloģiju drošības izvērtēšanas kritērijus un vienoto informācijas tehnoloģiju drošības izvērtēšanas metodiku.

(3) *EUCC* izmanto vienoto kritēriju vārīgo vietu novērtējuma saimi (AVA_VAN), 1.–5. komponentu. Šie pieci komponenti sniedz visus IKT izstrādājumu vārīgo vietu analīzei nepieciešamos galvenos faktorus un atkarības. Tā kā komponenti atbilst šajā regulā noteiktajiem apliecinājuma līmeņiem, tie palīdz izdarīt pietiekamā informācijā balstītu apliecinājuma izvēli, pamatojoties uz drošības prasību un ar IKT izstrādājuma paredzēto lietojumu saistītā riska izvērtējumiem. *EUCC* sertifikāta pieteikuma iesniedzējam būtu jāiesniedz dokumentācija, kas saistīta ar IKT izstrādājuma paredzēto lietojumu un ar šādu lietojumu saistīto risku līmeņu analīzi, lai atbilstības novērtēšanas struktūra varētu izvērtēt izvēlētā apliecinājuma līmeņa piemērotību. Ja izvērtēšanas un sertifikācijas darbības veic viena un tā pati atbilstības novērtēšanas struktūra, pieteikuma iesniedzējam pieprasītā informācija jāiesniedz tikai vienu reizi.

(4) Tehniskā joma ir pamatprincipu kopums, kas aptver tādu IKT izstrādājumu grupu, kuriem ir īpaša un līdzīga drošības funkcionalitāte, kas mazina uzbrukumus, ja raksturlielumi ir kopīgi attiecīgajam apliecinājuma līmenim. Tehniskā joma aktuālajos dokumentos norāda īpašās drošības prasības, kā arī papildu izvērtēšanas metodes, paņēmienus un rīkus, kas attiecas uz to IKT izstrādājumu sertifikāciju, uz kuriem attiecas šī tehniskā joma. Tāpēc tehniskā joma veicina arī aptverto IKT izstrādājumu izvērtēšanas saskaņošanu. Pašlaik sertifikācijai AVA_VAN 4. un 5. līmenī tiek plaši izmantotas divas tehniskās jomas. Pirmā tehniskā joma ir "viedkartes un tamlīdzīgas ierīces",

([1]) OV L 151, 7.6.2019., 15. lpp.

([2]) Savstarpējās atzīšanas nolīgums par informācijas tehnoloģiju drošības izvērtējuma sertifikātiem, 2010. gada janvāra redakcija 3.0, pieejama vietnē sogis.eu, ko apstiprinājusi Eiropas Komisijas Informācijas sistēmu drošības augstāko amatpersonu grupa (*SOG-IS*), atbildot uz 3. punktu Padomes 1995. gada 7. aprīļa Ieteikumā 95/144/EK par kopējiem informācijas tehnoloģiju drošības izvērtēšanas kritērijiem (OV L 93, 26.4.1995., 27. lpp.).

kas ir tehniskā joma, kurā būtiska nepieciešamās drošības funkcionalitātes daļa ir atkarīga no konkrētiem, pielāgotiem un bieži atdalāmiem aparatūras elementiem (piemēram, viedkaršu aparatūra, integrālās shēmas, viedkaršu kombinētie izstrādājumi, uzticamo platformu moduļi, ko izmanto uzticamā datošanā, vai digitālā tahogrāfa kartes). Otrā tehniskā joma ir "aparatūras ierīces ar drošības kastēm", kurā būtiska nepieciešamās drošības funkcionalitātes daļa ir atkarīga no aparatūras fiziskā apvalka (saukts par "drošības kasti"), kas projektēts, lai pretotos tiešiem uzbrukumiem (piemēram, maksājumu termināli, transportlīdzekļu tahogrāfa ierīces, viedie skaitītāji, piekļuves vadības termināļi un aparatūras drošības moduļi).

(5) Piesakoties uz sertifikāciju, pieteikuma iesniedzējam savs pamatojums apliecinājuma līmeņa izvēlei būtu jāsaista ar Regulas (ES) 2019/881 51. pantā noteiktajiem mērķiem un komponentu atlasi no drošības funkcionālo prasību un drošības apliecinājuma prasību kataloga, kas ietverts vienotajos kritērijos. Sertifikācijas struktūrām jānovērtē izvēlētā apliecinājuma līmeņa atbilstība un jānodrošina, ka izvēlētais līmenis ir samērīgs ar riska līmeni, kas saistīts ar IKT izstrādājumam paredzēto lietojumu.

(6) Saskaņā ar kopējiem kritērijiem sertifikāciju veic, ņemot vērā drošības mērķi, kas ietver IKT izstrādājuma drošības problēmas definīciju, kā arī drošības mērķus, kas risina drošības problēmu. Drošības problēma sniedz sīkāku informāciju par IKT izstrādājumam paredzēto lietojumu un ar to saistītajiem riskiem. Izvēlētais drošības prasību kopums atbilst gan IKT izstrādājuma drošības problēmai, gan tā drošības mērķiem.

(7) Aizsardzības profili ir efektīvs līdzeklis, ar kuru iepriekš noteikt kopējos kritērijus, kas piemērojami konkrētai IKT izstrādājumu kategorijai, un tādēļ tie ir arī būtisks elements to IKT izstrādājumu sertifikācijas procesā, uz kuriem attiecas aizsardzības profils. Aizsardzības profilu izmanto, lai novērtētu turpmākos drošības mērķus, kas ietilpst konkrētajā IKT izstrādājumu kategorijā, uz kuru attiecas minētais aizsardzības profils. Tie arī racionalizē un uzlabo IKT izstrādājumu sertifikācijas procesa efektivitāti un palīdz lietotājiem pareizi un efektīvi noteikt IKT izstrādājuma funkcionalitāti. Tāpēc aizsardzības profili būtu jāuzskata par neatņemamu sastāvdaļu IKT procesā, kurā sertificē IKT izstrādājumus.

(8) Lai nodrošinātu aizsardzības profilu nozīmi IKT procesā, kas atbalsta sertificēta IKT izstrādājuma izstrādi un piegādi, pašiem aizsardzības profiliem jābūt iespējai, ka tos var sertificēt neatkarīgi no tāda konkrētā IKT izstrādājuma sertifikācijas, uz kuru attiecas attiecīgais aizsardzības profils. Tāpēc ir svarīgi aizsardzības profiliem piemērot vismaz tādu pašu pārbaudes līmeni kā drošības mērķiem, lai nodrošinātu augstu kiberdrošības līmeni. Aizsardzības profili jāizvērtē un jāsertificē atsevišķi no saistītā IKT izstrādājuma un tikai piemērojot vienoto kritēriju un vienotās izvērtēšanas metodikas apliecinājuma klasi aizsardzības profiliem (*APE*) un attiecīgā gadījumā aizsardzības profilu konfigurācijām (*ACE*). Ņemot vērā to svarīgo un sensitīvo lomu kā IKT izstrādājumu sertifikācijas etalonam, tie jāsertificē tikai publiskām struktūrām vai sertifikācijas struktūrai, kas saņēmusi valsts kiberdrošības sertifikācijas iestādes iepriekšēju apstiprinājumu saistībā ar konkrēto aizsardzības profilu. Ņemot vērā to būtisko nozīmi apliecinājuma līmeņa "augsts" sertifikācijā, sevišķi ārpus tehniskām jomām, aizsardzības profili jāizstrādā kā aktuālie dokumenti, kas jāapstiprina Eiropas Kiberdrošības sertifikācijas grupai.

(9) Sertificēti aizsardzības profili būtu jāiekļauj *EUCC* izpildes un atbilstības pārraudzībā, ko veic valsts kiberdrošības sertifikācijas iestādes. Ja metodika, instrumenti un prasmes, ko piemēro IKT izstrādājumu izvērtēšanas pieejām, ir pieejamas konkrētiem sertificētiem aizsardzības profiliem, tehniskās jomas var būt balstītas uz šiem konkrētajiem aizsardzības profiliem.

(10) Lai panāktu augstu uzticamības un apliecinājuma līmeni sertificētiem IKT izstrādājumiem, saskaņā ar šo regulu nebūtu atļaujama pašnovērtēšana. Būtu jāatļauj tikai trešo personu veikta atbilstības novērtēšana, ko veic *ITSEF* un sertifikācijas struktūras.

(11) *SOG-IS* kopiena sniedza vienotu interpretāciju un pieejas vienoto kritēriju un vienotās izvērtēšanas metodikas piemērošanai sertificēšanā, it īpaši attiecībā uz apliecinājuma līmeni "augsts", kas sasniedzams tehniskajās jomās "viedkartes un tamlīdzīgas ierīces" un "aizsardzības ierīces ar drošības kastēm". Tādu pavaddokumentu atkalizmantošana *EUCC* shēmā nodrošina vienmērīgu pāreju no valsts īstenotajām *SOG-IS* shēmām uz saskaņoto *EUCC* shēmu. Tāpēc šajā regulā jāiekļauj saskaņota izvērtēšanas metodika, kas ir vispārēji piemērota visām sertifikācijas darbībām. Turklāt Komisijai jābūt iespējai pieprasīt Eiropas Kiberdrošības sertifikācijas grupai pieņemt atzinumu, ar ko apstiprina un iesaka piemērot izvērtēšanas metodiku, kura norādīta aktuālajos dokumentos IKT izstrādājuma vai aizsardzības profila sertifikācijai saskaņā ar *EUCC* shēmu. Tāpēc šīs regulas I pielikumā ir uzskaitīti aktuālie dokumenti, kas izmantojami atbilstības novērtēšanas struktūru veiktajām izvērtēšanas darbībām. Eiropas Kiberdrošības sertifikācijas grupai būtu jāapstiprina un jāuztur aktuālie dokumenti. Aktuālie dokumenti jāizmanto sertificēšanā. Tikai izņēmuma un pienācīgi pamatotos gadījumos atbilstības novērtēšanas struktūra var tos neizmantot, ja tiek ievēroti īpaši nosacījumi, it īpaši, ja dots valsts kiberdrošības sertifikācijas iestādes apstiprinājums.

(12) IKT izstrādājumu sertificēšana AVA_VAN 4. vai 5. līmenī būtu iespējama tikai ar īpašiem nosacījumiem un ja ir pieejama īpaša izvērtēšanas metodika. Konkrētā izvērtēšanas metodika var būt ietverta aktuālajos dokumentos, kas attiecas uz tehnisko jomu, vai īpašos aizsardzības profilos, kas pieņemti kā aktuālais dokuments un attiecas uz attiecīgo izstrādājumu kategoriju. Tikai izņēmuma un pienācīgi pamatotos gadījumos vajadzētu būt iespējamai sertifikācijai šajos apliecinājuma līmeņos, ja tiek ievēroti īpaši nosacījumi, jo īpaši, ja sniegts valsts kiberdrošības sertifikācijas iestādes apstiprinājums, arī attiecībā uz piemērojamo izvērtēšanas metodiku. Tādi ārkārtēji un pienācīgi pamatoti gadījumi var pastāvēt, ja Savienības vai valsts tiesību aktos ir noteikta prasība sertificēt IKT izstrādājumu AVA_VAN 4. vai 5. līmenī. Tāpat izņēmuma un pienācīgi pamatotos gadījumos aizsardzības profilus var sertificēt, nepiemērojot attiecīgos aktuālos dokumentus, ja tiek ievēroti īpaši nosacījumi, it īpaši, ja sniegts valsts kiberdrošības sertifikācijas iestādes apstiprinājums, arī attiecībā uz piemērojamo izvērtēšanas metodiku.

(13) *EUCC* ietvaros izmantoto zīmju un marķējumu mērķis ir uzskatāmi parādīt sertificētā IKT izstrādājuma uzticamību lietotājiem un dot tiem iespēju izdarīt informācijā balstītu izvēli, kad tie iegādājas IKT izstrādājumus. Uz zīmju un marķējumu izmantošanu būtu jāattiecina arī noteikumi un nosacījumi, kas izklāstīti ISO/IEC 17065 un attiecīgā gadījumā ISO/IEC 17030, ar piemērojamiem norādījumiem.

(14) Sertifikācijas struktūrām būtu jālemj par sertifikātu derīguma termiņu, ņemot vērā attiecīgā IKT izstrādājuma darbmūžu. Derīguma termiņam nebūtu jāpārsniedz 5 gadus. Valstu kiberdrošības sertifikācijas iestādēm būtu jāstrādā ar derīguma termiņu saskaņošanu Savienībā.

(15) Ja esošā *EUCC* sertifikāta darbības joma tiek sašaurināta, sertifikātu atsauc un jāizdod jauns sertifikāts ar jauno darbības jomu, lai nodrošinātu, ka lietotāji ir skaidri informēti par konkrētā IKT izstrādājuma sertifikāta pašreizējo darbības jomu un apliecinājuma līmeni.

(16) Aizsardzības profilu sertifikācija atšķiras no IKT izstrādājumu sertifikācijas, jo tā attiecas uz IKT procesu. Tā kā aizsardzības profils aptver kādu IKT izstrādājumu kategoriju, tā izvērtēšanu un sertificēšanu nevar veikt, pamatojoties uz vienu IKT izstrādājumu. Tā kā aizsardzības profils apvieno vispārīgās drošības prasības attiecībā uz kādu IKT izstrādājumu kategoriju un neatkarīgi no tā, kā to paziņo tā pārdevējs, aizsardzības profila *EUCC* sertifikāta derīguma termiņam principā būtu jāaptver vismaz 5 gadi un to var pagarināt līdz visam aizsardzības profila pastāvēšanas laikam.

(17) Atbilstības novērtēšanas struktūra ir definēta kā struktūra, kas veic atbilstības novērtēšanas darbības, ieskaitot kalibrēšanu, testēšanu, sertificēšanu un inspekciju. Lai nodrošinātu augstu pakalpojumu kvalitāti, šajā regulā noteikts, ka testēšanas darbības, no vienas puses, un sertifikācijas un inspicēšanas darbības, no otras puses, būtu jāveic struktūrām, kas darbojas neatkarīgi cita no citas, proti, attiecīgi informācijas tehnoloģiju drošības izvērtēšanas mehānismiem (*ITSEF*) un sertifikācijas struktūrām. Abu veidu atbilstības novērtēšanas struktūrām vajadzētu būt akreditētām un noteiktos gadījumos pilnvarotām.

(18) Valsts akreditācijas struktūrai jāakreditē sertifikācijas struktūra saskaņā ar standartu ISO/IEC 17065 attiecībā uz apliecinājuma līmeni "būtisks" un "augsts". Papildus akreditācijai saskaņā ar Regulu (ES) 2019/881 saistībā ar Regulu (EK) Nr. 765/2008 atbilstības novērtēšanas struktūrām būtu jāatbilst īpašām prasībām, lai garantētu, ka tām ir kiberdrošības prasību izvērtēšanai *EUCC* apliecinājuma līmenī "augsts" nepieciešamā tehniskā kompetence, ko apstiprina ar "atļauju". Lai atbalstītu atļauju piešķiršanas procesu, būtu jāizstrādā attiecīgie aktuālie dokumenti, kurus pēc apstiprināšanas Eiropas kiberdrošības sertifikācijas grupā publicē *ENISA*.

(19) *ITSEF* tehniskā kompetence būtu jānovērtē, akreditējot testēšanas laboratoriju saskaņā ar ISO/IEC 17025 un papildus ar ISO/IEC 23532-1 attiecībā uz visām izvērtēšanas darbībām, kas saistītas ar apliecinājuma līmeni un noteiktas ISO/IEC 18045 saistībā ar ISO/IEC 15408. Gan sertifikācijas struktūrai, gan *ITSEF* būtu jāizveido un jāuztur atbilstoša personāla kompetences pārvaldības sistēma, kuras pamatā ir ISO/IEC 19896-1 attiecībā uz kompetences elementiem un līmeņiem un kompetences novērtēšanu. Vērtētājiem piemērojamās prasības, kas attiecas uz zināšanu, prasmju, pieredzes un izglītības līmeni, jāņem no ISO/IEC 19896-3. Saskaņā ar sistēmas mērķiem būtu jānorāda līdzvērtīgi noteikumi un pasākumi, kas attiecas uz novirzēm no šādām kompetences pārvaldības sistēmām.

(20) Lai saņemtu atļauju, *ITSEF* būtu jāpierāda savas spējas noteikt zināmo vārīgo vietu neesību, pareizu un konsekventu jaunāko drošības funkciju īstenošanu attiecīgajai konkrētajai tehnoloģijai un to, vai konkrētais IKT izstrādājums ir noturīgs pret prasmīgiem uzbrucējiem. Turklāt attiecībā uz atļaujām tehniskajā jomā "Viedkartes un tamlīdzīgas ierīces" *ITSEF* būtu arī jāpierāda savas izvērtēšanas darbību un ar tām saistīto uzdevumu veikšanai nepieciešamās spējas, kā noteikts vienoto kritēriju pavaddokumentā "Minimālās prasībās, kurām *ITSEF* jāatbilst, lai varētu veikt viedkaršu un tamlīdzīgu ierīču drošības izvērtējumus" ([3]). Lai saņemtu atļauju tehniskajā jomā "aparatūras ierīces ar drošības kastēm", *ITSEF* būtu papildus jāpierāda atbilstība minimālajām tehniskajām prasībām, kas jāizpilda, lai veiktu izvērtēšanas darbības un ar tām saistītos uzdevumus aparatūras ierīču ar drošības kastēm jomā, kā ieteikusi *ECCG*. Minimālo prasību kontekstā *ITSEF* būtu jāspēj veikt dažāda veida uzbrukumus, kas izklāstīti vienoto kritēriju pavaddokumentā "Uzbrukumu potenciāla piemērošana aparatūras ierīcēm ar drošības kastēm". Šīs spējas ietver vērtētāja zināšanas un prasmes, kā arī aprīkojumu un izvērtēšanas metodes, kas vajadzīgas, lai noteiktu un novērtētu dažādu veidu uzbrukumus.

(21) Valsts kiberdrošības sertifikācijas iestādei jāpārrauga, vai sertifikācijas struktūras, *ITSEF* un sertifikātu turētāji pilda savus pienākumus, kas izriet no šīs regulas un Regulas (ES) 2019/881. Valsts kiberdrošības sertifikācijas iestādei šajā nolūkā būtu jāizmanto visi attiecīgie informācijas avoti, ieskaitot informāciju, kas saņemta no sertifikācijas procesa dalībniekiem un pašu veiktās izmeklēšanas.

(22) Sertifikācijas struktūrām būtu jāsadarbojas ar attiecīgajām tirgus uzraudzības iestādēm un jāņem vērā visa informācija par vārīgām vietām, kura var attiekties uz IKT izstrādājumiem, par kuriem tās ir izdevušas sertifikātus. Sertifikācijas struktūrām būtu jāpārrauga to sertificētie aizsardzības profili, lai noteiktu, vai drošības prasības, kas noteiktas IKT izstrādājumu kategorijai, joprojām atspoguļo jaunākās norises drošības apdraudējuma jomā.

(23) Lai atbalstītu atbilstības pārraudzību, valsts kiberdrošības sertifikācijas iestādēm būtu jāsadarbojas ar attiecīgajām tirgus uzraudzības iestādēm saskaņā ar Regulas (ES) 2019/881 58. pantu un Eiropas Parlamenta un Padomes Regulu (ES) 2019/1020 ([4]). Ekonomikas dalībniekiem Savienībā ir pienākums dalīties informācijā un sadarboties ar tirgus uzraudzības iestādēm saskaņā ar Regulas 2019/1020 4. panta 3. punktu.

([3]) "Joint Interpretation Library: Minimum ITSEF Requirements for Security Evaluations of Smart cards and similar devices", 2020. gada februāra 2.1. redakcija, pieejams: sogis.eu.

([4]) Eiropas Parlamenta un Padomes Regula (ES) 2019/1020 (2019. gada 20. jūnijs) par tirgus uzraudzību un produktu atbilstību un ar ko groza Direktīvu 2004/42/EK un Regulas (EK) Nr. 765/2008 un (ES) Nr. 305/2011 (OV L 169, 25.6.2019., 1. lpp.).

(24) Sertifikācijas struktūrām būtu jāpārrauga sertifikāta turētāju un visu saskaņā ar *EUCC* izdoto sertifikātu atbilstība. Pārraudzībai būtu jānodrošina, ka visi *ITSEF* iesniegtie izvērtējuma ziņojumi un tajos izdarītie secinājumi, kā arī izvērtēšanas kritēriji un metodes tiek konsekventi un pareizi piemēroti visās sertifikācijas darbībās.

(25) Ja tiek konstatētas potenciālas neatbilstības, kas ietekmē sertificētu IKT izstrādājumu, ir svarīgi nodrošināt samērīgu reakciju. Tāpēc sertifikātus var apturēt. Apturēšanai būtu jāietver daži ierobežojumi attiecībā uz attiecīgā IKT izstrādājuma popularizēšanu un izmantošanu, bet tā nedrīkst ietekmēt sertifikāta derīgumu. ES sertifikāta turētājam par apturēšanu būtu jāpaziņo skarto IKT izstrādājumu pircējiem, savukārt attiecīgajai valsts kiberdrošības sertifikācijas iestādei tas būtu jāpaziņo attiecīgajām tirgus uzraudzības iestādēm. Lai informētu sabiedrību, *ENISA* informācija par apturēšanu jāpublicē īpašā vietnē.

(26) *EUCC* sertifikāta turētājam būtu jāīsteno nepieciešamās vārīgo vietu pārvaldības procedūras un jānodrošina, ka minētās procedūras tiek ieviestas tā organizācijā. Uzzinot par potenciālu vārīgo vietu, *EUCC* sertifikāta turētājam būtu jāveic vārīgo vietu ietekmes analīze. Ja vārīgo vietu ietekmes analīze apstiprina, ka vārīgās vietas var izmantot, sertifikāta turētājam būtu jānosūta novērtējuma ziņojums sertifikācijas struktūrai, kurai savukārt būtu jāinformē valsts kiberdrošības sertifikācijas iestāde. Ziņojumā būtu jāinformē par vārīgo vietu ietekmi, nepieciešamajām izmaiņām vai korektīvajiem risinājumiem, kas ir nepieciešami, arī par iespējamu plašāku vārīgo vietu ietekmi, kā arī par korektīviem risinājumiem citiem izstrādājumiem. Vajadzības gadījumā vārīgo vietu uzrādīšanas procedūra būtu jāpapildina ar standartu EN ISO/IEC 29147.

(27) Sertifikācijas nolūkā atbilstības novērtēšanas struktūras un valsts kiberdrošības sertifikācijas iestādes iegūst konfidenciālus un sensitīvus datus un komercnoslēpumus, kas saistīti arī ar intelektuālo īpašumu vai atbilstības pārraudzību un kam nepieciešama pienācīga aizsardzība. Tādēļ tām būtu jābūt nepieciešamajai tehniskai kompetencei un zināšanām, un tām būtu jāizveido informācijas aizsardzības sistēmas. Informācijas aizsardzības prasībām un nosacījumiem būtu jābūt izpildītiem gan attiecībā uz akreditāciju, gan atļauju piešķiršanu.

(28) *ENISA* savā kiberdrošības sertifikācijas vietnē būtu jāsniedz sertificēto aizsardzības profilu saraksts un jānorāda to statuss saskaņā ar Regulu (ES) 2019/881.

(29) Šajā regulā ir izklāstīti nosacījumi savstarpējās atzīšanas nolīgumiem ar trešām valstīm. Šādi savstarpējās atzīšanas nolīgumi var būt divpusēji vai daudzpusēji, un tiem būtu jāaizstāj pašlaik spēkā esošie līdzīgie nolīgumi. Lai atvieglotu netraucētu pāreju uz šādiem savstarpējās atzīšanas nolīgumiem, dalībvalstis var uz ierobežotu laiku turpināt piemērot spēkā esošos sadarbības nolīgumus ar trešām valstīm.

(30) Sertifikācijas struktūrām, kas izdod *EUCC* sertifikātus apliecinājuma līmenī "augsts", kā arī attiecīgajiem saistītajiem *ITSEF* būtu jāveic profesionālās izvērtēšana. Profesionālā izvērtēšana būtu jāveic ar mērķi noteikt, vai profesionāli izvērtējamās sertifikācijas struktūras statūti un procedūras pastāvīgi atbilst *EUCC* shēmas prasībām. Profesionālā izvērtēšana atšķiras no valstu kiberdrošības sertifikācijas iestāžu profesionālās izvērtēšanas, kas noteikta Regulas (ES) 2019/881 59. pantā. Profesionālajā izvērtēšanā būtu jānoskaidro, vai sertifikācijas struktūras darbojas saskaņoti un nodrošina vienādas kvalitātes sertifikātus, un būtu jāapzina sertifikācijas struktūru darbības potenciāls vai trūkumi, arī nolūkā apmainīties ar paraugpraksi. Tā kā ir dažādi sertifikācijas struktūru veidi, būtu jāatļauj dažādi profesionālās izvērtēšanas veidi. Sarežģītākos gadījumos, piemēram, ja sertifikācijas struktūras izdod sertifikātus dažādos AVA_VAN līmeņos, var izmantot dažādus profesionālās izvērtēšanas veidus, ja ir izpildītas visas prasības.

(31) Eiropas Kiberdrošības sertifikācijas grupai būtu jāuzņemas nozīmīga loma shēmas uzturēšanā. Tai cita starpā, sadarbojoties ar privāto sektoru, būtu jāizveido specializētas apakšgrupas un jāveic attiecīgi sagatavošanas darbi un jāsniedz Komisijas prasītā palīdzība. Eiropas Kiberdrošības sertifikācijas grupai ir būtiska nozīme aktuālo dokumentu apstiprināšanā. Apstiprinot un pieņemot aktuālos dokumentus, būtu pienācīgi jāņem vērā Regulas (ES) 2019/881 54. panta 1. punkta c) apakšpunktā minētie elementi. Tehniskās jomas un aktuālie dokumenti būtu jāpublicē šīs regulas I pielikumā. Aizsardzības profili, kas pieņemti kā aktuālie dokumenti, būtu jāpublicē II

pielikumā. Lai nodrošinātu šo pielikumu elastīgumu, Komisija var tos grozīt saskaņā ar Regulas (ES) 2019/881 66. panta 2. punktā noteikto procedūru un ņemot vērā Eiropas kiberdrošības sertifikācijas grupas atzinumu. III pielikumā ir iekļauti ieteicamie aizsardzības profili, kas šīs regulas spēkā stāšanās brīdī nav aktuālie dokumenti. Tie būtu jāpublisko *ENISA* vietnē, kas minēta Regulas (ES) 2019/881 50. panta 1. punktā.

(32) Šī regula jāsāk piemērot 12 mēnešus pēc stāšanās spēkā. IV nodaļas un V pielikuma prasībām nav vajadzīgs pārejas periods, tāpēc tās jāpiemēro no šīs regulas spēkā stāšanās dienas.

(33) Šajā regulā noteiktie pasākumi ir saskaņā ar atzinumu, kuru sniegusi Eiropas Kiberdrošības sertifikācijas komiteja, kas izveidota ar Regulas (ES) 2019/881 66. pantu,

IR PIEŅĒMUSI ŠO REGULU.

I NODAĻA

VISPĀRĪGI NOTEIKUMI

1. pants

Priekšmets un darbības joma

Šī regula nosaka vienotos kritērijos balstītu Eiropas kiberdrošības sertifikācijas shēmu (*EUCC*).

Šī regula attiecas uz visiem informācijas un komunikācijas tehnoloģiju (IKT) izstrādājumiem, ieskaitot to dokumentāciju, kas iesniegti sertifikācijai saskaņā ar *EUCC*, un visiem aizsardzības profiliem, kuri iesniegti sertifikācijai kā daļa no IKT procesa, kas tiek veikts, lai sertificētu IKT izstrādājumus.

2. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "vienotie kritēriji" ir vienotie informācijas tehnoloģiju drošības izvērtēšanas kritēriji, kas noteikti ISO standartā ISO/IEC 15408;

2) "vienotā izvērtēšanas metodika" ir vienota informācijas tehnoloģiju drošības izvērtēšanas metodika, kas noteikta ISO/IEC standartā ISO/IEC 18045;

3) "izvērtēšanas objekts" ir tāds IKT izstrādājums vai tā daļa, vai aizsardzības profils kā daļa no IKT procesa, ko pakļauj kiberdrošības izvērtēšanai, lai tas varētu saņemt *EUCC* sertifikāciju;

4) "drošības mērķis" ir no īstenošanas atkarīgu drošības prasību pieprasījums konkrētam IKT izstrādājumam;

5) "aizsardzības profils" ir IKT process, ar ko nosaka kādas konkrētas IKT izstrādājumu kategorijas drošības prasības, ar ko risina no īstenošanas neatkarīgas drošības vajadzības un ko var izmantot, lai novērtētu konkrētajā kategorijā ietilpstošos IKT izstrādājumus to sertifikācijas nolūkā;

6) “izvērtēšanas tehniskais ziņojums” ir dokuments, ko sagatavo *ITSEF*, lai izklāstītu konstatējumus, spriedumus un pamatojumus, kuri gūti, saskaņā ar šajā regulā izklāstītajiem noteikumiem un pienākumiem izvērtējot IKT izstrādājumu vai aizsardzības profilu;

7) “*ITSEF*” ir informācijas tehnoloģiju drošības izvērtēšanas mehānisms, kas ir atbilstības novērtēšanas struktūra, kura definēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā un kura veic izvērtēšanas uzdevumus;

8) “AVA_VAN līmenis” ir apliecinājuma vārīgo vietu analīzes līmenis, kas norāda to kiberdrošības izvērtēšanas darbību pakāpi, kuras veic, lai noteiktu, kādā līmenī ir noturība pret izvērtēšanas objekta trūkumu vai nepilnību iespējamo izmantojamību darbības vidē, kā noteikts vienotajos kritērijos;

9) “*EUCC* sertifikāts” ir kiberdrošības sertifikāts, ko saskaņā ar *EUCC* izdod IKT izstrādājumiem vai aizsardzības profiliem, kurus var izmantot tikai IKT izstrādājumu sertifikācijas IKT procesā;

10) “salikts izstrādājums” ir IKT izstrādājums, ko izvērtē kopā ar citu IKT pamatizstrādājumu, kurš jau ir saņēmis *EUCC* sertifikātu un kura drošības funkcionalitāte ir atkarīga no saliktā IKT izstrādājuma;

11) “valsts kiberdrošības sertifikācijas iestāde” ir iestāde, kuru katra dalībvalsts izraudzījusies saskaņā ar Regulas (ES) 2019/881 58. panta 1. punktu;

12) “sertifikācijas struktūra” ir atbilstības novērtēšanas struktūra, kā definēts Regulas (EK) Nr. 765/2008 2. panta 13. punktā, kura veic tikai sertifikācijas darbības;

13) “tehniskā joma” ir kopīgs tehniskais satvars, kas saistīts ar kādu konkrētu tehnoloģiju saskaņotai sertifikācijai ar raksturīgu drošības prasību kopumu;

14) “aktuāls dokuments” ir dokuments, kurā norādītas izvērtēšanas metodes, paņēmieni un rīki, ko piemēro IKT izstrādājumu sertifikācijā, vai vispārīgās IKT izstrādājumu kategorijas drošības prasības, vai citas sertifikācijai nepieciešamas prasības, lai saskaņotu izvērtēšanu tehniskajās jomās vai aizsardzības profiliem;

15) “tirgus uzraudzības iestāde” ir iestāde, kas definēta Regulas (ES) 2019/1020 3. panta 4. punktā.

3. pants

Izvērtēšanas standarti

Izvērtēšanai, ko veic saskaņā ar *EUCC*, piemēro šādus standartus:

a) vienotos kritērijus;

b) vienoto izvērtēšanas metodiku.

4. pants

Apliecinājuma līmeņi

1. Sertifikācijas struktūras izdod *EUCC* sertifikātus apliecinājuma līmenī “būtisks” vai “augsts”.

2. *EUCC* sertifikāti apliecinājuma līmenī “būtisks” atbilst sertifikātiem, kas aptver AVA_VAN 1. vai 2. līmeni.

3. *EUCC* sertifikāti apliecinājuma līmenī “augsts” atbilst sertifikātiem, kas aptver AVA_VAN 3., 4. vai 5. līmeni.

4. Apliecinājuma līmenis, kas apstiprināts *EUCC* sertifikātā, nošķir apliecinājuma komponentu atbilstīgu un paplašinātu izmantošanu, kā norādīts vienotos kritērijos saskaņā ar VIII pielikumu.

5. Atbilstības novērtēšanas struktūras piemēro šos apliecinājuma komponentus, no kuriem ir atkarīgs izvēlētais AVA_VAN līmenis, saskaņā ar 3. pantā minētajiem standartiem.

5. pants

IKT izstrādājumu sertificēšanas metodes

1. IKT izstrādājuma sertificēšanu veic, ņemot vērā tā drošības mērķi:

a) kā noteicis pieteikuma iesniedzējs; vai

b) iekļaujot sertificētu aizsardzības profilu IKT procesā, ja IKT izstrādājums ietilpst tajā IKT izstrādājumu kategorijā, uz kuru attiecas minētais aizsardzības profils.

2. Aizsardzības profilus sertificē vienīgi tālab, lai sertificētu IKT izstrādājumus, kas ietilpst konkrētajā IKT izstrādājumu kategorijā, uz kuru attiecas aizsardzības profils.

6. pants

Atbilstības pašnovērtēšana

Atbilstības pašnovērtēšana Regulas (ES) 2019/881 53. panta nozīmē nav atļauta.

II NODAĻA

IKT IZSTRĀDĀJUMU SERTIFIKĀCIJA

I IEDAĻA

Īpaši izvērtēšanas standarti un prasības

7. pants

IKT izstrādājumu izvērtēšanas kritēriji un metodes

1. IKT izstrādājumu, kas iesniegts sertifikācijai, izvērtē, ņemot vērā vismaz šādus aspektus:

a) šīs regulas 3. pantā minēto standartu piemērojamos elementus;

b) vārīgo vietu novērtējuma drošības apliecinājuma prasību klases un neatkarīgu funkcionālo testēšanu, kā noteikts 3. pantā minētajos izvērtēšanas standartos;

c) ar IKT izstrādājumu paredzēto lietojumu saistītā riska līmeni saskaņā ar Regulas (ES) 2019/881 52. pantu un to drošības funkcijas, kas atbalsta Regulas (ES) 2019/881 51. pantā noteiktos drošības mērķus;

d) piemērojamos aktuālos dokumentus, kas uzskaitīti I pielikumā; un

e) piemērojamos sertificētos aizsardzības profilus, kas uzskaitīti II pielikumā.

2. Ārkārtējos un pienācīgi pamatotos gadījumos atbilstības novērtēšanas struktūra var pieprasīt nepiemērot attiecīgo aktuālo dokumentu. Tādos gadījumos atbilstības novērtēšanas struktūra informē valsts kiberdrošības sertifikācijas iestādi, pienācīgi pamatojot savu pieprasījumu. Valsts kiberdrošības sertifikācijas iestāde izvērtē izņēmuma pamatojumu un, ja tas ir pamatots, to apstiprina. Kamēr valsts kiberdrošības sertifikācijas iestāde nav pieņēmusi lēmumu, atbilstības novērtēšanas

struktūra sertifikātu neizdod. Valsts kiberdrošības sertifikācijas iestāde par apstiprināto izņēmumu bez liekas kavēšanās paziņo Eiropas kiberdrošības sertifikācijas grupai, kas var sniegt attiecīgu atzinumu. Valsts kiberdrošības sertifikācijas iestāde pēc iespējas rūpīgāk ņem vērā Eiropas kiberdrošības sertifikācijas grupas atzinumu.

3. IKT izstrādājumu sertifikācija AVA_VAN 4. vai 5. līmenī ir iespējama tikai šādos gadījumos:

a) ja uz IKT izstrādājumu attiecas kāda no I pielikumā uzskaitītajām tehniskajām jomām, to izvērtē saskaņā ar attiecīgajiem šo tehnisko jomu aktuālajiem dokumentiem;

b) ja IKT izstrādājums ietilpst IKT izstrādājumu kategorijā, uz kuru attiecas sertificēts aizsardzības profils, kas ietver AVA_VAN 4. vai 5. līmeni un ir iekļauts II pielikumā kā tehniskais aizsardzības profils, to izvērtē saskaņā ar izvērtēšanas metodiku, kas noteikta šim aizsardzības profilam;

c) ja šā punkta a) un b) apakšpunkts nav piemērojams un ja tehniskās jomas iekļaušana I pielikumā vai sertificēta aizsardzības profila iekļaušana II pielikumā tuvākajā nākotnē ir maz ticama, un tikai ārkārtējos un pienācīgi pamatotos gadījumos, ievērojot 4. punktā izklāstītos nosacījumus.

4. Ja atbilstības novērtēšanas struktūra uzskata, ka pastāv 3. punkta c) apakšpunktā minēts ārkārtējs un pienācīgi pamatots gadījums, tā par plānoto sertifikāciju paziņo valsts kiberdrošības sertifikācijas iestādei, norādot pamatojumu un izklāstot ierosināto izvērtēšanas metodiku. Valsts kiberdrošības sertifikācijas iestāde novērtē izņēmuma pamatojumu un, ja tas ir pamatoti, apstiprina vai groza izvērtēšanas metodiku, kas jāpiemēro atbilstības novērtēšanas struktūrai. Kamēr valsts kiberdrošības sertifikācijas iestāde nav pieņēmusi lēmumu, atbilstības novērtēšanas struktūra sertifikātu neizdod. Valsts kiberdrošības sertifikācijas iestāde bez liekas kavēšanās ziņo par plānoto sertifikāciju Eiropas kiberdrošības sertifikācijas grupai, kas var sniegt attiecīgu atzinumu. Valsts kiberdrošības sertifikācijas iestāde pēc iespējas rūpīgāk ņem vērā Eiropas kiberdrošības sertifikācijas grupas atzinumu.

5. Ja par kādu IKT izstrādājumu tiek veikta salikta izstrādājuma izvērtēšana saskaņā ar attiecīgajiem aktuālajiem dokumentiem, *ITSEF*, kas veicis IKT pamatizstrādājuma izvērtēšanu, attiecīgo informāciju sniedz *ITSEF*, kas veic saliktā IKT izstrādājuma izvērtēšanu.

II IEDAĻA

EUCC sertifikātu izdošana, atjaunošana un atsaukšana

8. pants

Sertifikācijai nepieciešamā informācija

1. *EUCC* sertifikācijas pieteikuma iesniedzējs iesniedz vai citādi dara pieejamu sertifikācijas struktūrai un ITSEF visu sertifikācijas darbībām nepieciešamo informāciju.

2. Šā panta 1. punktā minētajā informācijā iekļauj visus attiecīgos pierādījumus saskaņā ar iedaļām "Izstrādātāja darbības elementi" atbilstošā formā, kā noteikts vienoto kritēriju un vienotās izvērtēšanas metodikas iedaļās "Pierādījumu saturs un sniegšana" izvēlētajam apliecinājuma līmenim un saistītajām drošības apliecinājuma prasībām. Pierādījumos vajadzības gadījumā iekļauj ziņas par IKT izstrādājumu un tā pirmkodu saskaņā ar šo regulu, ievērojot aizsardzības pasākumus pret neatļautu uzrādīšanu.

3. Sertifikācijas pieteikuma iesniedzēji sertifikācijas struktūrai un *ITSEF* var iesniegt attiecīgos izvērtēšanas rezultātus no iepriekšējas sertifikācijas saskaņā ar:

a) šo regulu;

b) citu Eiropas kiberdrošības sertifikācijas shēmu, kas pieņemta saskaņā ar Regulas (ES) 2019/881 49. pantu;

c) valsts shēmu, kas minēta šīs regulas 49. pantā.

4. Ja izvērtēšanas rezultāti ir derīgi *ITSEF* uzdevumu izpildei, *ITSEF* var no jauna izmantot izvērtēšanas rezultātus, ja šādi rezultāti atbilst piemērojamajām prasībām un to autentiskums ir apstiprināts.

5. Ja sertifikācijas struktūra saistībā ar izstrādājumu atļauj veikt salikta izstrādājuma sertifikāciju, sertifikācijas pieteikuma iesniedzējs sertifikācijas struktūrai un *ITSEF* attiecīgā gadījumā dara pieejamus visus vajadzīgos elementus saskaņā ar aktuālo dokumentu.

6. Sertifikācijas pieteikuma iesniedzēji sertifikācijas struktūrai un *ITSEF* sniedz arī šādu informāciju:

a) saiti uz savu vietni, kurā ietverta Regulas (ES) 2019/881 55. pantā minētā papildu kiberdrošības informācija;

b) pieteikuma iesniedzēja vārīgo vietu pārvaldības un vārīgo vietu uzrādīšanas procedūru aprakstu.

7. Visu šajā pantā minēto attiecīgo dokumentāciju sertifikācijas struktūra, *ITSEF* un pieteikuma iesniedzējs glabā piecus gadus pēc sertifikāta derīguma termiņa beigām.

9. pants

EUCC sertifikāta izdošanas nosacījumi

1. Sertifikācijas struktūras izdod *EUCC* sertifikātu, ja ir izpildīti visi tālāk minētie nosacījumi:

a) IKT izstrādājuma kategorija ietilpst sertificēšanā iesaistītās sertifikācijas struktūras un *ITSEF* akreditācijas un attiecīgā gadījumā atļaujas tvērumā;

b) sertifikācijas pieteikuma iesniedzējs ir parakstījis paziņojumu, ar kuru uzņemas visas 2. punktā uzskaitītās saistības;

c) *ITSEF* izvērtējumu saskaņā ar 3. un 7. pantā minētajiem izvērtēšanas standartiem, kritērijiem un metodēm ir pabeidzis bez iebildumiem;

d) sertifikācijas struktūra ir pabeigusi izvērtēšanas rezultātu pārskatīšanu bez iebildumiem;

e) sertifikācijas iestāde ir verificējusi, ka *ITSEF* sniegtie izvērtēšanas tehniskie ziņojumi atbilst iesniegtajiem pierādījumiem un ka 3. un 7. pantā minētie izvērtēšanas standarti, kritēriji un metodes ir pareizi piemēroti.

2. Sertifikācijas pieteikuma iesniedzējs uzņemas šādas saistības:

a) sniegt sertifikācijas iestādei un *ITSEF* pilnīgu un pareizu visu nepieciešamo informāciju un vajadzības gadījumā sniegt vajadzīgo papildu informāciju;

b) nepopularizēt IKT izstrādājumu kā sertificētu saskaņā ar *EUCC* pirms *EUCC* sertifikāta izdošanas;

c) popularizēt IKT izstrādājumu kā sertificētu tikai *EUCC* sertifikātā noteiktajā darbības jomā;

d) nekavējoties beigt popularizēt IKT izstrādājumu kā sertificētu, ja *EUCC* sertifikāts tiek apturēts, atsaukts vai beidzies tā derīguma termiņš;

e) nodrošināt, ka IKT izstrādājumi, ko pārdod, atsaucoties uz *EUCC* sertifikātu, ir pilnīgi identiski IKT izstrādājumiem, kuriem veikta sertifikācija;

f) ievērot zīmes un marķējuma izmantošanas noteikumus, kas *EUCC* sertifikātam noteikti saskaņā ar 11. pantu.

3. Ja saistībā ar kādu IKT izstrādājumu tiek veikta salikta izstrādājuma sertificēšana saskaņā ar attiecīgajiem aktuālajiem dokumentiem, sertifikācijas struktūra, kas veikusi IKT pamatizstrādājuma sertificēšanu, sniedz attiecīgo informāciju sertifikācijas struktūrai, kura veic saliktā IKT izstrādājuma sertificēšanu.

10. pants

EUCC sertifikāta saturs un formāts

1. *EUCC* sertifikātā ietver vismaz V pielikumā noteikto informāciju.

2. *EUCC* sertifikātā vai sertifikācijas ziņojumā nepārprotami norāda sertificētā IKT izstrādājuma darbības jomu un robežas, norādot, vai ir sertificēts viss IKT izstrādājums vai tikai tā daļas.

3. Sertifikācijas struktūra *EUCC* sertifikātu pieteikuma iesniedzējam izdod vismaz elektroniskā veidā.

4. Sertifikācijas struktūra sagatavo sertifikācijas ziņojumu saskaņā ar V pielikumu par katru tās izdoto *EUCC* sertifikātu. Sertifikācijas ziņojumu sagatavo, pamatojoties uz *ITSEF* izdoto izvērtēšanas tehnisko ziņojumu. Izvērtēšanas tehniskajā ziņojumā un sertifikācijas ziņojumā norāda 7. pantā minētos īpašos izvērtēšanas kritērijus un metodes, kas izmantotas izvērtēšanā.

5. Sertifikācijas struktūra katru *EUCC* sertifikātu un katru sertifikācijas ziņojumu elektroniski iesniedz valsts kiberdrošības sertifikācijas iestādei un *ENISA*.

11. pants

Zīme un marķējums

1. Sertifikāta turētājs var sertificētam IKT izstrādājumam piestiprināt zīmi un marķējumu. Zīme un marķējums apliecina, ka IKT izstrādājums ir sertificēts saskaņā ar šo regulu. Zīmi un marķējumu piestiprina saskaņā ar šo pantu un IX pielikumu.

2. Zīmi un marķējumu redzami, salasāmi un neizdzēšami piestiprina sertificētajam IKT izstrādājumam vai tā datu plāksnei. Ja izstrādājuma veida dēļ tas nav iespējams vai nodrošināms, to uzliek iepakojumam un pavaddokumentiem. Ja sertificēts IKT izstrādājums tiek piegādāts programmatūras veidā, zīme un marķējums ir redzami, salasāmi un neizdzēšami norādīti tā pavaddokumentācijā vai arī šī dokumentācija ir viegli un tieši pieejama lietotājiem vietnē.

3. Zīmi un marķējumu veido tā, kā norādīts IX pielikumā, un tajos ietver šādu informāciju:

a) sertificētā IKT izstrādājuma apliecinājuma līmenis un AVA_VAN līmenis;

b) sertifikāta unikāla identifikācija, ko veido:

   1) shēmas nosaukums;

   2) sertifikātu izdevušās sertifikācijas struktūras akreditācijas nosaukumu un atsauces numurs;

   3) izdošanas gads un mēnesis;

   4) sertifikātu izdevušās sertifikācijas struktūras piešķirtais identifikācijas numurs.

4. Zīmei un marķējumam pievieno kvadrātkodu ar saiti uz vietni, kurā ir vismaz:

a) informācija par sertifikāta derīguma termiņu;

b) vajadzīgā sertifikācijas informācija, kas noteikta V un VII pielikumā;

c) informācija, kas sertifikāta turētājam jādara publiski pieejama saskaņā ar Regulas (ES) 2019/881 55. pantu; un

d) attiecīgā gadījumā vēsturiskā informācija, kas saistīta ar konkrētu IKT izstrādājuma sertifikāciju vai sertifikātiem, lai nodrošinātu izsekojamību.

12. pants

EUCC sertifikāta derīguma termiņš

1. Sertifikācijas struktūra katram izdotajam *EUCC* sertifikātam nosaka derīguma termiņu, ņemot vērā sertificētā IKT izstrādājuma īpašības.

2. *EUCC* sertifikāta derīguma termiņš nepārsniedz 5 gadus.

3. Atkāpjoties no 2. punkta, minētais laikposms var pārsniegt 5 gadus, ja iepriekš ir saņemts valsts kiberdrošības sertifikācijas iestādes apstiprinājums. Valsts kiberdrošības sertifikācijas iestāde bez liekas kavēšanās paziņo Eiropas Kiberdrošības sertifikācijas grupai par piešķirto apstiprinājumu.

13. pants

EUCC sertifikāta pārskatīšana

1. Pēc sertifikāta turētāja pieprasījuma vai citu pamatotu iemeslu dēļ sertifikācijas struktūra var nolemt pārskatīt IKT izstrādājuma *EUCC* sertifikātu. Pārskatīšanu veic saskaņā ar IV pielikumu. Sertifikācijas struktūra nosaka pārskatīšanas apjomu. Sertifikācijas struktūra pieprasa *ITSEF* atkārtot sertificētā IKT izstrādājuma izvērtēšanu, ja tas nepieciešams pārskatīšanai.

2. Pēc pārskatīšanas un attiecīgā gadījumā atkārtotas izvērtēšanas rezultātiem sertifikācijas struktūra:

a) apstiprina *EUCC* sertifikātu;

b) atsauc *EUCC* sertifikātu saskaņā ar 14. pantu;

c) atsauc *EUCC* sertifikātu saskaņā ar 14. pantu un izdod jaunu *EUCC* sertifikātu ar tādu pašu darbības jomu un pagarinātu derīguma termiņu; vai

d) atsauc *EUCC* sertifikātu saskaņā ar 14. pantu un izdod jaunu sertifikātu ar citu darbības jomu.

3. Sertifikācijas struktūra var nolemt bez liekas kavēšanās apturēt *EUCC* sertifikātu saskaņā ar 30. pantu, kamēr *EUCC* sertifikāta turētājs nav veicis korektīvus pasākumus.

14. pants

EUCC sertifikāta atsaukšana

1. Neskarot Regulas (ES) 2019/881 58. panta 8. punkta e) apakšpunktu, *EUCC* sertifikātu atsauc tā sertifikācijas struktūra, kas šo sertifikātu izdevusi.

2. Šā panta 1. punktā minētā sertifikācijas struktūra paziņo valsts kiberdrošības sertifikācijas iestādei par sertifikāta atsaukšanu. Tā arī paziņo *ENISA* par šādu atsaukšanu, lai atvieglotu tās uzdevuma izpildi saskaņā ar Regulas (ES) 2019/881 50. pantu. Valsts kiberdrošības sertifikācijas iestāde par to paziņo citām attiecīgajām tirgus uzraudzības iestādēm.

3. *EUCC* sertifikāta turētājs var pieprasīt sertifikāta atsaukšanu.

III NODAĻA

AIZSARDZĪBAS PROFILU SERTIFIKĀCIJA

I IEDAĻA

Īpaši izvērtēšanas standarti un prasības

15. pants

Izvērtēšanas kritēriji un metodes

1. Aizsardzības profilu izvērtē, ņemot vērā vismaz šādus aspektus:

a) šīs regulas 3. pantā minēto standartu piemērojamos elementus;

b) ar IKT izstrādājumu paredzēto lietojumu saistītā riska līmeni saskaņā ar Regulas (ES) 2019/881 52. pantu un to drošības funkcijas, kas atbalsta minētās regulas 51. pantā noteiktos drošības mērķus; un

c) piemērojamos aktuālos dokumentus, kas norādīti I pielikumā. Aizsardzības profilu, uz ko attiecas tehniskā joma, sertificē saskaņā ar minētajā tehniskajā jomā noteiktajām prasībām.

2. Ārkārtējos un pienācīgi pamatotos gadījumos atbilstības novērtēšanas struktūra var sertificēt aizsardzības profilu, nepiemērojot attiecīgos aktuālos dokumentus. Šādos gadījumos tā informē kompetento valsts kiberdrošības sertifikācijas iestādi un sniedz pamatojumu plānotajai sertifikācijai bez attiecīgo aktuālo dokumentu piemērošanas, kā arī izklāsta piedāvāto izvērtēšanas metodiku. Valsts kiberdrošības sertifikācijas iestāde novērtē pamatojumu un, ja tas ir pamatoti, apstiprina attiecīgo aktuālo dokumentu nepiemērošanu, kā arī vajadzības gadījumā apstiprina vai groza izvērtēšanas metodiku, kas jāpiemēro atbilstības novērtēšanas struktūrai. Kamēr valsts kiberdrošības sertifikācijas iestāde nav pieņēmusi lēmumu, atbilstības novērtēšanas struktūra aizsardzības profila sertifikātu neizdod. Valsts kiberdrošības sertifikācijas iestāde bez liekas kavēšanās paziņo par attiecīgo aktuālo dokumentu nepiemērošanas atļaušanu Eiropas kiberdrošības sertifikācijas grupai, kas var sniegt attiecīgu atzinumu. Valsts kiberdrošības sertifikācijas iestāde pēc iespējas rūpīgāk ņem vērā Eiropas kiberdrošības sertifikācijas grupas atzinumu.

II IEDAĻA

Aizsardzības profilu EUCC sertifikātu izdošana, atjaunošana un atsaukšana

16. pants

Aizsardzības profilu sertificēšanai nepieciešamā informācija

Aizsardzības profila sertifikācijas pieteikuma iesniedzējs sniedz vai citādi dara pieejamu sertifikācijas struktūrai un *ITSEF* visu sertifikācijas darbībām nepieciešamo informāciju. Pēc analoģijas piemēro šīs regulas 8. panta 2., 3., 4. un 7. punktu.

17. pants

Aizsardzības profilu *EUCC* sertifikātu izdošana

1. Sertifikācijas pieteikuma iesniedzējs sertifikācijas struktūrai un *ITSEF* sniedz pilnīgu un pareizu visu nepieciešamo informāciju.

2. Pēc analoģijas piemēro šīs regulas 9. un 10. pantu.

3. *ITSEF* izvērtē, vai aizsardzības profils ir pilnīgs, saskaņots, tehniski pamatots un lietderīgs paredzētajam lietojumam un drošības mērķiem, kas noteikti IKT izstrādājumu kategorijā, uz kuru attiecas attiecīgais aizsardzības profils.

4. Aizsardzības profilu sertificē tikai:

a) valsts kiberdrošības sertifikācijas iestāde vai cita publiska struktūra, kas akreditēta kā sertifikācijas struktūra; vai

b) sertifikācijas struktūra, iepriekš saņemot valsts kiberdrošības sertifikācijas iestādes apstiprinājumu par katru atsevišķu aizsardzības profilu.

18. pants

Aizsardzības profilu *EUCC* sertifikāta derīguma termiņš

1. Sertifikācijas struktūra katram *EUCC* sertifikātam nosaka derīguma termiņu.

2. Derīguma termiņš var būt viss attiecīgā aizsardzības profila pastāvēšanas laiks.

19. pants

Aizsardzības profilu *EUCC* sertifikāta pārskatīšana

1. Pēc sertifikāta turētāja pieprasījuma vai citu pamatotu iemeslu dēļ sertifikācijas struktūra var nolemt pārskatīt aizsardzības profila *EUCC* sertifikātu. Pārskatīšanu veic, piemērojot 15. pantā norādītos nosacījumus. Sertifikācijas struktūra nosaka pārskatīšanas apjomu. Sertifikācijas struktūra pieprasa *ITSEF* sertificēto aizsardzības profilu izvērtēt vēlreiz, ja tas nepieciešams pārskatīšanai.

2. Pēc pārskatīšanas un attiecīgā gadījumā otrreizējas izvērtēšanas rezultātiem sertifikācijas struktūra veic kādu no šīm darbībām:

a) apstiprina *EUCC* sertifikātu;

b) atsauc *EUCC* sertifikātu saskaņā ar 20. pantu;

c) atsauc *EUCC* sertifikātu saskaņā ar 20. pantu un izdod jaunu *EUCC* sertifikātu ar tādu pašu darbības jomu un pagarinātu derīguma termiņu;

d) atsauc *EUCC* sertifikātu saskaņā ar 20. pantu un izdod jaunu sertifikātu ar citādu darbības jomu.

20. pants

Aizsardzības profila *EUCC* sertifikāta atsaukšana

1. Neskarot Regulas (ES) 2019/881 58. panta 8. punkta e) apakšpunktu, aizsardzības profila *EUCC* sertifikātu atsauc tā sertifikācijas struktūra, kas šo sertifikātu izdevusi. Pēc analoģijas piemēro šīs regulas 14. pantu.

2. Aizsardzības profila sertifikātu, kas izdots saskaņā ar 17. panta 4. punkta b) apakšpunktu, atsauc valsts kiberdrošības sertifikācijas iestāde, kas sertifikātu apstiprinājusi.

IV NODAĻA

ATBILSTĪBAS IZVĒRTĒŠANAS STRUKTŪRAS

21. pants

Papildu vai īpašās prasības sertifikācijas struktūrām

1. Valsts kiberdrošības sertifikācijas iestāde pilnvaro sertifikācijas struktūru izdot *EUCC* sertifikātus apliecinājuma līmenī "augsts", ja minētā struktūra papildus Regulas (ES) 2019/881 60. panta 1. punktā un pielikumā noteiktajām prasībām attiecībā uz atbilstības novērtēšanas struktūru akreditāciju pierāda, ka:

a) tai ir lietpratība un kompetence, kas vajadzīgas, lai pieņemtu sertifikācijas lēmumu apliecinājuma līmenī "augsts";

b) tā veic sertifikācijas darbības sadarbībā ar *ITSEF*, kas apstiprināts saskaņā ar 22. pantu; un

c) papildus 43. pantā noteiktajām prasībām tai ir vajadzīgā kompetence un tā īsteno attiecīgus tehniskos un operatīvos pasākumus, ar kuriem rezultatīvi aizsargā konfidenciālu un sensitīvu informāciju apliecinājuma līmenim "augsts".

2. Valsts kiberdrošības sertifikācijas iestāde novērtē, vai sertifikācijas struktūra atbilst visām 1. punktā norādītajām prasībām. Novērtējums ietver vismaz strukturētas intervijas un vismaz viena tāda izmēģinājuma sertifikāta pārskatīšanu, ko sertifikācijas struktūra sagatavojusi saskaņā ar šo regulu.

Novērtēšanā valsts kiberdrošības sertifikācijas iestāde var atkalizmantot atbilstošus pierādījumus, kas iegūti saistībā ar iepriekšējām atļaujām vai tamlīdzīgām darbībām, kuras piešķirtas saskaņā ar:

a) šo regulu;

b) citu Eiropas kiberdrošības sertifikācijas shēmu, kas pieņemta saskaņā ar Regulas (ES) 2019/881 49. pantu;

c) valsts shēmu, kas minēta šīs regulas 49. pantā.

3. Valsts kiberdrošības sertifikācijas iestāde sagatavo atļaujas ziņojumu, uz ko attiecas profesionālā izvērtēšana saskaņā ar Regulas (ES) 2019/881 59. panta 3. punkta d) apakšpunktu.

4. Valsts kiberdrošības sertifikācijas iestāde norāda IKT izstrādājumu kategorijas un aizsardzības profilus, uz kuriem attiecas atļauja. Atļauja ir derīga ne ilgāk par akreditācijas derīguma termiņu. To pēc pieprasījuma var atjaunot, ja sertifikācijas struktūra joprojām atbilst šajā pantā izklāstītajām prasībām. Atļaujas atjaunošanai izmēģinājuma izvērtējumi nav nepieciešami.

5. Valsts kiberdrošības sertifikācijas iestāde atsauc sertifikācijas struktūras atļauju, ja tā vairs neatbilst šajā pantā izklāstītajiem nosacījumiem. Pēc atļaujas atsaukšanas sertifikācijas struktūra nekavējoties pārtrauc sevi popularizēt kā atļauju saņēmušu sertifikācijas struktūru.

22. pants

Papildu vai īpašās prasības *ITSEF*

1. Valsts kiberdrošības sertifikācijas iestāde pilnvaro ITSEF izvērtēt IKT izstrādājumus, uz kuriem attiecas sertifikācija apliecinājuma līmenī "augsts", ja ITSEF papildus Regulas (ES) 2019/881 60. panta 1. punktā un pielikumā noteiktajām prasībām attiecībā uz atbilstības novērtēšanas struktūru akreditāciju pierāda savu atbilstību visiem šiem nosacījumiem:

a) tam ir lietpratība, kas nepieciešama, lai veiktu izvērtēšanas darbības, ar ko nosaka noturību pret mūsdienīgiem kiberuzbrukumiem, kurus veic dalībnieki ar ievērojamām prasmēm un resursiem;

b) attiecībā uz tehniskajām jomām un aizsardzības profiliem, kas ir daļa no šo IKT izstrādājumu IKT procesa, tam ir:

1) lietpratība, kas nepieciešama, lai veiktu konkrētās izvērtēšanas darbības, kas vajadzīgas, lai metodiski noteiktu izvērtēšanas objekta noturību pret prasmīgiem uzbrucējiem tā darbības vidē, pieņemot, ka uzbrukuma potenciāls ir "mērens" vai "augsts", kā noteikts 3. pantā minētajos standartos;

2) tehniskā kompetence, kas noteikta I pielikumā norādītajos aktuālajos dokumentos;

c) papildus 43. pantā noteiktajām prasībām tai ir vajadzīgā kompetence un tā īsteno attiecīgus tehniskos un operatīvos pasākumus, ar kuriem rezultatīvi aizsargā konfidenciālu un sensitīvu informāciju apliecinājuma līmenim "augsts".

2. Valsts kiberdrošības sertifikācijas iestāde novērtē, vai *ITSEF* atbilst visām 1. punktā norādītajām prasībām. Novērtējums ietver vismaz strukturētas intervijas un vismaz viena tāda izmēģinājuma izvērtējuma pārskatīšanu, ko *ITSEF* sagatavojis saskaņā ar šo regulu.

3. Novērtēšanā valsts kiberdrošības sertifikācijas iestāde var atkalizmantot atbilstošus pierādījumus, kas iegūti saistībā ar iepriekšējām atļaujām vai tamlīdzīgām darbībām, kuras piešķirtas saskaņā ar:

a) šo regulu;

b) citu Eiropas kiberdrošības sertifikācijas shēmu, kas pieņemta saskaņā ar Regulas (ES) 2019/881 49. pantu;

c) valsts shēmu, kas minēta šīs regulas 49. pantā.

4. Valsts kiberdrošības sertifikācijas iestāde sagatavo atļaujas ziņojumu, uz ko attiecas profesionālā izvērtēšana saskaņā ar Regulas (ES) 2019/881 59. panta 3. punkta d) apakšpunktu.

5. Valsts kiberdrošības sertifikācijas iestāde norāda IKT izstrādājumu kategorijas un aizsardzības profilus, uz kuriem attiecas atļauja. Atļauja ir derīga ne ilgāk par akreditācijas derīguma termiņu. To pēc pieprasījuma var atjaunot, ja *ITSEF* joprojām atbilst šajā pantā izklāstītajām prasībām. Atļaujas atjaunošanai izmēģinājuma izvērtējumi nav nepieciešami.

6. Valsts kiberdrošības sertifikācijas iestāde atsauc *ITSEF* atļauju, ja tas vairs neatbilst šajā pantā izklāstītajiem nosacījumiem. Pēc atļaujas atsaukšanas *ITSEF* pārtrauc sevi popularizēt kā atļauju saņēmušu *ITSEF*.

23. pants

Sertifikācijas struktūru paziņošana

1. Valsts kiberdrošības sertifikācijas iestāde dara zināmas Komisijai tās teritorijā esošās sertifikācijas struktūras, kuras ir kompetentas sertificēt apliecinājuma līmenī "būtisks", pamatojoties uz to akreditāciju.

2. Valsts kiberdrošības sertifikācijas iestāde paziņo Komisijai tās teritorijā esošās sertifikācijas struktūras, kuras ir kompetentas sertificēt apliecinājuma līmenī "augsts", pamatojoties uz to akreditāciju un atļaujas piešķiršanas lēmumu.

3. Valsts kiberdrošības sertifikācijas iestāde, paziņojot Komisijai par sertifikācijas struktūrām, sniedz tai vismaz šādu informāciju:

a) apliecinājuma līmeni vai līmeņus, par kuriem sertifikācijas struktūra ir kompetenta izdot *EUCC* sertifikātus;

b) šādu ar akreditāciju saistītu informāciju:

1) akreditācijas datumu;

2) sertifikācijas iestādes nosaukumu un adresi;

3) sertifikācijas struktūras reģistrācijas valsti;

4) akreditācijas atsauces numuru;

5) akreditācijas tvērumu un derīguma termiņu;

6) valsts akreditācijas struktūras adresi, atrašanās vietu un saiti uz attiecīgo vietni; un

c) šādu ar apliecinājuma līmeni "augsts" saistītu informāciju:

1) atļaujas izdošanas datumu;

2) atļaujas atsauces numuru;

3) atļaujas derīguma termiņu;

4) atļaujas tvērumu, arī augstākajā AVA_VAN līmenī, un attiecīgā gadījumā aptverto tehnisko jomu.

4. Valsts kiberdrošības sertifikācijas iestāde 1. un 2. punktā minētā paziņojuma kopiju nosūta *ENISA*, lai tā varētu kiberdrošības sertifikācijas vietnē publicēt precīzu informāciju par sertifikācijas struktūru atbilstību.

5. Valsts kiberdrošības sertifikācijas iestāde bez liekas kavēšanās izskata visu informāciju par izmaiņām akreditācijas statusā, ko iesniegusi valsts akreditācijas struktūra. Ja akreditācija vai atļauja ir atsaukta, valsts kiberdrošības sertifikācijas iestāde par to informē Komisiju un var iesniegt Komisijai pieprasījumu saskaņā ar Regulas (ES) 2019/881 61. panta 4. punktu.

24. pants

ITSEF paziņošana

Valsts kiberdrošības sertifikācijas iestāžu paziņošanas pienākumi, kas noteikti 23. pantā, attiecas arī uz *ITSEF*. Paziņojumā norāda *ITSEF* adresi, derīgo akreditāciju un attiecīgā gadījumā derīgu attiecīgā *ITSEF* atļauju.

V NODAĻA

PĀRRAUDZĪBA, NEATBILSTĪBA VAI NEIZPILDE

I IEDAĻA

Atbilstības pārraudzība

25. pants

Valsts kiberdrošības sertifikācijas iestādes veiktās pārraudzības darbības

1. Neskarot Regulas (ES) 2019/881 58. panta 7. punktu, valsts kiberdrošības sertifikācijas iestāde pārrauga:

a) vai sertifikācijas struktūra un *ITSEF* izpilda savus pienākumus saskaņā ar šo regulu un Regulu (ES) 2019/881;

b) vai *EUCC* sertifikāta turētāji izpilda savus pienākumus saskaņā ar šo regulu un Regulu (ES) 2019/881;

c) vai sertificētie IKT izstrādājumi atbilst *EUCC* noteiktajām prasībām;

d) apliecinājuma līmeni, kas norādīts *EUCC* sertifikātā, ņemot vērā strauji mainīgo drošības apdraudējuma ainu.

2. Valsts kiberdrošības sertifikācijas iestāde veic pārraudzības darbības, jo īpaši, pamatojoties uz:

a) informāciju, ko sniedz sertifikācijas struktūras, valsts akreditācijas struktūras un attiecīgās tirgus uzraudzības iestādes;

b) informāciju, kas izriet no pašas vai citas iestādes veiktajām revīzijām un izmeklēšanām;

c) paraugu ņemšanu, ko veic saskaņā ar 3. punktu;

d) saņemtajām sūdzībām.

3. Valsts kiberdrošības sertifikācijas iestāde sadarbībā ar citām tirgus uzraudzības iestādēm katru gadu ņem paraugus saistībā ar vismaz 4 % *EUCC* sertifikātu, kā noteikts riska novērtējumā. Pēc kompetentās valsts kiberdrošības sertifikācijas iestādes pieprasījuma un tās vārdā sertifikācijas struktūras un, ja nepieciešams, *ITSEF* palīdz šai iestādei pārraudzīt atbilstību.

4. Valsts kiberdrošības sertifikācijas iestāde pārbaudāmo sertificēto IKT izstrādājumu izlasi atlasa, ņemot vērā objektīvus kritērijus, to starpā:

a) izstrādājuma kategoriju;

b) izstrādājumu apliecinājuma līmeņus;

c) sertifikāta turētāju;

d) sertifikācijas struktūru un attiecīgā gadījumā *ITSEF*, kas ir apakšuzņēmējs;

e) citu informāciju, kas darīta zināma iestādei.

5. Valsts kiberdrošības sertifikācijas iestāde informē *EUCC* sertifikāta turētājus par atlasītajiem IKT izstrādājumiem un atlases kritērijiem.

6. Sertifikācijas struktūra, kura sertificējusi izlasē iekļauto IKT izstrādājumu, pēc valsts kiberdrošības sertifikācijas iestādes pieprasījuma ar attiecīgā ITSEF palīdzību veic papildu pārskatīšanu saskaņā ar IV pielikuma IV.2. iedaļā noteikto procedūru un informē valsts kiberdrošības sertifikācijas iestādi par rezultātiem.

7. Ja valsts kiberdrošības sertifikācijas iestādei ir pietiekams iemesls uzskatīt, ka sertificēts IKT izstrādājums vairs neatbilst šīs regulas vai Regulas (ES) 2019/881 prasībām, tā var veikt izmeklēšanu vai izmantot citas pārraudzības pilnvaras, kas noteiktas Regulas (ES) 2019/881 58. panta 8. punktā.

8. Valsts kiberdrošības sertifikācijas iestāde informē attiecīgo sertifikācijas struktūru un *ITSEF* par notiekošo izmeklēšanu attiecībā uz atlasītajiem IKT izstrādājumiem.

9. Ja valsts kiberdrošības sertifikācijas iestāde konstatē, ka notiekošā izmeklēšana attiecas uz IKT izstrādājumiem, kurus sertificējušas citās dalībvalstīs izveidotas sertifikācijas struktūras, tā par to informē attiecīgo dalībvalstu kiberdrošības sertifikācijas iestādes, lai attiecīgā gadījumā sadarbotos izmeklēšanā. Tāda valsts kiberdrošības sertifikācijas iestāde arī paziņo Eiropas Kiberdrošības sertifikācijas grupai par pārrobežu izmeklēšanu un tās rezultātiem.

26. pants

Sertifikācijas struktūras veiktās pārraudzības darbības

1. Sertifikācijas struktūra pārrauga:

a) vai sertifikāta turētāji pilda šajā regulā un Regulā (ES) 2019/881 noteiktos pienākumus attiecībā uz *EUCC* sertifikātu, ko izdevusi sertifikācijas struktūra;

b) vai sertificētie IKT izstrādājumi atbilst tiem noteiktajām attiecīgajām drošības prasībām;

c) apliecinājuma līmeni, kas pausts sertificētajos aizsardzības profilos.

2. Sertifikācijas struktūra savas pārraudzības darbības veic, pamatojoties uz:

a) informāciju, kas sniegta, pildot 9. panta 2. punktā minētās sertifikācijas pieteikuma iesniedzēja saistības;

b) informāciju, kas iegūta citu attiecīgo tirgus uzraudzības iestāžu darbību rezultātā;

c) saņemtajām sūdzībām;

d) informāciju par vārīgajām vietām, kas var ietekmēt tās sertificētos IKT izstrādājumus.

3. Valsts kiberdrošības sertifikācijas iestāde var izstrādāt noteikumus periodiskam dialogam starp sertifikācijas struktūrām un *EUCC* sertifikātu turētājiem, lai pārbaudītu, kā tiek pildītas saistības, ko tie uzņēmušies saskaņā ar 9. panta 2. punktu, un ziņotu par to, neskarot darbības, kuras saistītas ar citām attiecīgām tirgus uzraudzības iestādēm.

27. pants

Sertifikāta turētāja veiktās pārraudzības darbības

1. *EUCC* sertifikāta turētājs veic šādus uzdevumus, lai pārraudzītu sertificētā IKT izstrādājuma atbilstību tā drošības prasībām:

a) pārrauga informāciju par vārīgajām vietām, kura attiecas uz sertificēto IKT izstrādājumu, arī par atkarībām, ar saviem līdzekļiem, kā arī ņemot vērā:

   1) galalietotāja vai drošības pētnieka publikāciju vai apsvērumus par informāciju par vārīgajām vietām, kā minēts Regulas (ES) 2019/881 55. panta 1. punkta c) apakšpunktā;

   2) citu avotu iesniegtu informāciju;

b) pārrauga *EUCC* sertifikātā pausto apliecinājuma līmeni.

2. *EUCC* sertifikāta turētājs sadarbojas ar sertifikācijas struktūru, *ITSEF* un attiecīgā gadījumā ar valsts kiberdrošības sertifikācijas iestādi, lai atbalstītu to veiktās pārraudzības darbības.

II IEDAĻA

Atbilstība un izpilde

28. pants

Sertificēta IKT izstrādājuma vai aizsardzības profila neatbilstības sekas

1. Ja sertificēts IKT izstrādājums vai aizsardzības profils neatbilst šajā regulā un Regulā (ES) 2019/881 noteiktajām prasībām, sertifikācijas struktūra informē EUCC sertifikāta turētāju par konstatēto neatbilstību un pieprasa korektīvus pasākumus.

2. Ja neatbilstība šīs regulas noteikumiem var ietekmēt atbilstību citiem attiecīgiem Savienības tiesību aktiem, kas paredz iespēju ar *EUCC* sertifikātu pierādīt pieņēmumu par atbilstību attiecīgā tiesību akta prasībām, sertifikācijas struktūra nekavējoties informē valsts kiberdrošības sertifikācijas iestādi. Valsts kiberdrošības sertifikācijas iestāde par konstatēto neatbilstību nekavējoties paziņo tirgus uzraudzības iestādei, kas atbild par citu attiecīgu Savienības tiesību aktu regulējumu.

3. Saņemot 1. punktā minēto informāciju, *EUCC* sertifikāta turētājs sertifikācijas struktūras noteiktajā termiņā, kas nepārsniedz 30 dienas, ierosina sertifikācijas struktūrai korektīvos pasākumus, kas nepieciešami neatbilstības novēršanai.

4. Ja ir ārkārtējs gadījums vai ja *EUCC* sertifikāta turētājs ar sertifikācijas struktūru nesadarbojas pienācīgi, sertifikācijas struktūra var bez liekas kavēšanās apturēt *EUCC* sertifikātu saskaņā ar 30. pantu.

5. Sertifikācijas struktūra veic pārskatīšanu saskaņā ar 13. un 19. pantu, novērtējot, vai korektīvais pasākums novērš neatbilstību.

6. Ja *EUCC* sertifikāta turētājs 3. punktā minētajā laikposmā neierosina atbilstošus korektīvus pasākumus, sertifikātu aptur saskaņā ar 30. pantu vai atsauc saskaņā ar 14. vai 20. pantu.

7. Šo pantu nepiemēro vārīgo vietu gadījumiem, kas skar sertificētu IKT izstrādājumu un ko risina saskaņā ar VI nodaļu.

29. pants

Sertifikāta turētāja pienākumu neizpildes sekas

1. Ja sertifikācijas struktūra konstatē, ka:

a) *EUCC* sertifikāta turētājs vai sertifikācijas pieteikuma iesniedzējs nav izpildījis savas saistības un pienākumus, kas noteikti 9. panta 2. punktā, 17. panta 2. punktā un 27. un 41. pantā, vai

b) *EUCC* sertifikāta turētājs neizpilda Regulas (ES) 2019/881 56. panta 8. punkta vai šīs regulas VI nodaļas prasības,

tā nosaka laikposmu, kas nepārsniedz 30 dienas, kurā *EUCC* sertifikāta turētājs veic korektīvus pasākumus.

2. Ja *EUCC* sertifikāta turētājs 1. punktā minētajā laikposmā neierosina atbilstošus korektīvus pasākumus, sertifikātu aptur saskaņā ar 30. pantu vai atsauc saskaņā ar 14. un 20. pantu.

3. Ja *EUCC* sertifikāta turētājs turpina nepildīt vai atkal neizpilda 1. punktā minētos pienākumus, *EUCC* sertifikātu atsauc saskaņā ar 14. vai 20. pantu.

4. Sertifikācijas struktūra informē valsts kiberdrošības sertifikācijas iestādi par 1. punktā minētajiem konstatējumiem. Ja neizpilde ietekmē citu attiecīgo Savienības tiesību aktu izpildi, valsts kiberdrošības sertifikācijas iestāde par konstatēto neizpildi nekavējoties informē tirgus uzraudzības iestādi, kura atbild par citiem attiecīgiem Savienības tiesību aktiem.

30. pants

***EUCC* sertifikāta apturēšana**

1. Kad šajā regulā ir minēta *EUCC* sertifikāta apturēšanu, sertifikācijas struktūra aptur attiecīgo *EUCC* sertifikātu uz laiku, kas atbilst apstākļiem, kuri izraisījuši apturēšanu, bet nepārsniedz 42 dienas. Apturēšanas laikposms sākas nākamajā dienā pēc sertifikācijas struktūras lēmuma pieņemšanas dienas. Apturēšana neietekmē sertifikāta derīguma termiņu.

2. Sertifikācijas struktūra par apturēšanu bez liekas kavēšanās paziņo sertifikāta turētājam un valsts kiberdrošības sertifikācijas iestādei un norāda apturēšanas iemeslus, pieprasītās darbības, kas jāveic, un apturēšanas laikposmu.

3. Sertifikāta turētāji informē attiecīgo IKT izstrādājumu pircējus par apturēšanu un sertifikācijas struktūras sniegtajiem apturēšanas iemesliem, izņemot tās iemeslu daļas, kuru kopīgošana radītu drošības risku vai kuras satur sensitīvu informāciju. Sertifikāta turētājs šo informāciju arī dara publiski pieejamu.

4. Ja citos attiecīgajos Savienības tiesību aktos ir paredzēts atbilstības pieņēmums, pamatojoties uz sertifikātiem, kuri izdoti saskaņā ar šīs regulas noteikumiem, valsts kiberdrošības sertifikācijas iestāde par apturēšanu informē tirgus uzraudzības iestādi, kas ir atbildīga par šādiem citiem attiecīgajiem Savienības tiesību aktiem.

5. Par sertifikāta apturēšanu paziņo *ENISA* saskaņā ar 42. panta 3. punktu.

6. Pienācīgi pamatotos gadījumos valsts kiberdrošības sertifikācijas iestāde var atļaut pagarināt *EUCC* sertifikāta apturēšanas laikposmu. Kopējais apturēšanas laikposms nedrīkst pārsniegt 1 gadu.

31. pants

Atbilstības novērtēšanas struktūras neizpildes sekas

1. Ja sertifikācijas struktūra nepilda savus pienākumus vai attiecīgā sertifikācijas struktūra konstatē *ITSEF* neizpildi, valsts kiberdrošības sertifikācijas iestāde bez liekas kavēšanās:

a) ar attiecīgā *ITSEF* atbalstu nosaka potenciāli skartos *EUCC* sertifikātus;

b) vajadzības gadījumā pieprasa, lai izvērtēšanas darbības vienam vai vairākiem IKT izstrādājumiem vai aizsardzības profiliem veiktu vai nu *ITSEF*, kas veicis izvērtēšanu, vai arī cits akreditēts un attiecīgā gadījumā pilnvarots *ITSEF*, kurš var būt tehniski labākās pozīcijās, lai atbalstītu minēto noteikšanu;

c) analizē prasību neizpildes ietekmi;

d) paziņo *EUCC* sertifikāta turētājam, kuru skar neizpilde.

2. Pamatojoties uz 1. punktā minētajiem pasākumiem, sertifikācijas struktūra attiecībā uz katru skarto *EUCC* sertifikātu pieņem kādu no šiem lēmumiem:

a) *EUCC* sertifikātu nemainīt;

b) atsaukt *EUCC* sertifikātu saskaņā ar 14. vai 20. pantu un attiecīgā gadījumā izdot jaunu *EUCC* sertifikātu.

3. Pamatojoties uz 1. punktā minētajiem pasākumiem, valsts kiberdrošības sertifikācijas iestāde:

a) vajadzības gadījumā ziņo valsts akreditācijas struktūrai par sertifikācijas struktūras vai saistītā *ITSEF* neizpildi;

b) attiecīgā gadījumā novērtē potenciālo ietekmi uz atļauju.

VI NODAĻA

VĀRĪGO VIETU PĀRVALDĪBA UN UZRĀDĪŠANA

32. pants

Vārīgo vietu pārvaldības tvērums

Šī nodaļa attiecas uz IKT izstrādājumiem, par kuriem izdots *EUCC* sertifikāts.

I IEDAĻA

Vārīgo vietu pārvaldība

33. pants

Vārīgo vietu pārvaldības procedūras

1. *EUCC* sertifikāta turētājs izveido un uztur visas nepieciešamās vārīgo vietu pārvaldības procedūras saskaņā ar šajā iedaļā izklāstītajiem noteikumiem un vajadzības gadījumā papildina ar procedūrām, kas izklāstītas EN ISO/IEC 30111.

2. *EUCC* sertifikāta turētājs uztur un publicē attiecīgās metodes, kuras izmantojamas, lai no ārējiem avotiem – arī lietotājiem, sertifikācijas struktūrām un drošības pētniekiem – saņemtu informāciju par vārīgajām vietām, kas saistīta ar tā izstrādājumiem.

3. Ja *EUCC* sertifikāta turētājs atklāj vai saņem informāciju par potenciālu vārīgo vietu, kas ietekmē sertificētu IKT izstrādājumu, tas to reģistrē un veic vārīgo vietu ietekmes analīzi.

4. Ja potenciālā vārīgā vieta ietekmē saliktu izstrādājumu, *EUCC* sertifikāta turētājs par potenciālo vārīgo vietu informē atkarīgo *EUCC* sertifikātu turētāju.

5. Atbildot uz sertifikācijas struktūras, kas izdevusi sertifikātu, pamatotu pieprasījumu, *EUCC* sertifikāta turētājs nosūta šai sertifikācijas struktūrai visu attiecīgo informāciju par potenciālām vārīgām vietām.

34. pants

Vārīgo vietu ietekmes analīze

1. Vārīgo vietu ietekmes analīze attiecas uz izvērtēšanas objektu un sertifikātā ietvertajām apliecinājumu deklarācijām. Vārīgo vietu ietekmes analīzi veic laikposmā, kas atbilst sertificētā IKT izstrādājuma potenciālās vārīgo vietu izmantošanas iespējām un kritiskumam.

2. Attiecīgā gadījumā uzbrukuma potenciālu aprēķina pēc attiecīgās metodikas, kas iekļauta 3. pantā minētajos standartos un attiecīgajos I pielikumā norādītajos aktuālajos dokumentos, lai noteiktu vārīgo vietu izmantojamību. Ņem vērā *EUCC* sertifikāta *AVA_VAN* līmeni.

35. pants

Vārīgo vietu ietekmes analīzes ziņojums

1. Turētājs sagatavo ziņojumu par vārīgo vietu ietekmes analīzi, ja ietekmes analīze liecina, ka vārīgajām vietām ir iespējama ietekme uz IKT izstrādājuma atbilstību tā sertifikātam.

2. Vārīgo vietu ietekmes analīzes ziņojumā iekļauj šādu elementu novērtējumu:

a) vārīgo vietu ietekme uz sertificēto IKT izstrādājumu;

b) iespējami riski, kas saistīti ar uzbrukuma tuvumu vai pieejamību;

c) vai vārīgās vietas var izlabot;

d) ja vārīgās vietas var izlabot, iespējamie vārīgo vietu risinājumi.

3. Vārīgo vietu ietekmes analīzes ziņojumā attiecīgā gadījumā iekļauj informāciju par iespējamiem vārīgo vietu izmantošanas veidiem. Informāciju par iespējamiem vārīgo vietu izmantošanas veidiem apstrādā saskaņā ar attiecīgajiem drošības pasākumiem, lai aizsargātu tās konfidencialitāti un vajadzības gadījumā nodrošinātu tās ierobežotu izplatīšanu.

4. *EUCC* sertifikāta turētājs bez liekas kavēšanās nosūta sertifikācijas struktūrai vai valsts kiberdrošības sertifikācijas iestādei ziņojumu par vārīgo vietu ietekmes analīzi saskaņā ar Regulas (ES) 2019/881 56. panta 8. punktu.

5. Ja vārīgo vietu ietekmes analīzes ziņojumā konstatēts, ka vārīgā vieta nav atlikusi vārīga vieta 3. pantā minēto standartu izpratnē un ka to var izlabot, piemēro 36. pantu.

6. Ja vārīgo vietu ietekmes analīzes ziņojumā konstatēts, ka vārīgā vieta nav atlikusi vārīga vieta un ka to nevar izlabot, *EUCC* sertifikātu atsauc saskaņā ar 14. pantu.

7. *EUCC* sertifikāta turētājs uzrauga visas atlikušās vārīgās vietas, lai nodrošinātu, ka tās nevar izmantot, ja mainās darbības vide.

36. pants

Vārīgo vietu izlabošana

EUCC sertifikāta turētājs sertifikācijas struktūrai iesniedz priekšlikumu par attiecīgu izlabošanas darbību. Sertifikācijas struktūra pārskata sertifikātu saskaņā ar 13. pantu. Pārskatīšanas tvērumu nosaka atkarībā no ierosinātā vārīgo vietu izlabošanas veida.

II IEDAĻA

Vārīgo vietu uzrādīšana

37. pants

Informācija, ko sniedz valsts kiberdrošības sertifikācijas iestādei

1. Informācijā, ko sertifikācijas struktūra sniedz valsts kiberdrošības sertifikācijas iestādei, iekļauj visus elementus, kas nepieciešami, lai valsts kiberdrošības sertifikācijas iestāde varētu izprast vārīgo vietu ietekmi, IKT izstrādājumā veicamās izmaiņas un attiecīgā gadījumā visu informāciju no sertifikācijas struktūras par vārīgo vietu plašāku ietekmi uz citiem sertificētiem IKT izstrādājumiem.

2. Saskaņā ar 1. punktu sniegtajā informācijā neietver sīku informāciju par vārīgo vietu izmantošanas veidiem. Šis noteikums neskar valsts kiberdrošības sertifikācijas iestādes izmeklēšanas pilnvaras.

38. pants

Sadarbība ar citām valsts kiberdrošības sertifikācijas iestādēm

1. Valsts kiberdrošības sertifikācijas iestāde attiecīgo saskaņā ar 37. pantu saņemto informāciju sniedz citām valsts kiberdrošības sertifikācijas iestādēm un *ENISA*.

2. Citas valsts kiberdrošības sertifikācijas iestādes var nolemt turpināt analizēt vārīgās vietas vai pēc *EUCC* sertifikāta turētāja informēšanas pieprasīt attiecīgajām sertifikācijas struktūrām novērtēt, vai vārīgā vieta var ietekmēt citus sertificētus IKT izstrādājumus.

39. pants

Vārīgo vietu publiskošana

Pēc sertifikāta atsaukšanas *EUCC* sertifikāta turētājs visas publiski zināmās un izlabotās IKT izstrādājuma vārīgās vietas uzrāda un reģistrē Eiropas vārīgo vietu datubāzē, kas izveidota saskaņā ar Eiropas Parlamenta un Padomes Direktīvas

(ES) 2022/2555 ([5]) 12. pantu, vai citos tiešsaistes reģistros, kuri norādīti Regulas (ES) 2019/881 55. panta 1. punkta d) apakšpunktā.

VII NODAĻA

INFORMĀCIJAS GLABĀŠANA, IZPAUŠANA UN AIZSARDZĪBA

40. pants

Sertifikācijas struktūru un *ITSEF* veikto ierakstu glabāšana

1. *ITSEF* un sertifikācijas struktūras uztur ierakstu sistēmu, kurā ir ietverti visi dokumenti, kas sagatavoti saistībā ar katru to veikto izvērtēšanu un sertifikāciju.

2. Sertifikācijas struktūras un *ITSEF* ierakstus glabā drošā veidā un tik ilgi, cik nepieciešams šīs regulas vajadzībām, bet vismaz piecus gadus pēc attiecīgā *EUCC* sertifikāta atsaukšanas. Ja sertifikācijas struktūra ir izdevusi jaunu *EUCC* sertifikātu saskaņā ar 13. panta 2. punkta c) apakšpunktu, tā kopā ar jauno *EUCC* sertifikātu un tikpat ilgi kā jauno *EUCC* sertifikātu glabā atsauktā *EUCC* sertifikāta dokumentāciju.

41. pants

Informācija, ko dara pieejamu sertifikāta turētājs

1. Regulas (ES) 2019/881 55. pantā minētā informācija ir pieejama lietotājiem viegli saprotamā valodā.

2. Sertifikāta turētājs glabā tālāk minēto informāciju drošā veidā un tik ilgi, cik nepieciešams šīs regulas vajadzībām, bet vismaz piecus gadus pēc attiecīgā *EUCC* sertifikāta atsaukšanas:

a) sertifikācijas procesa laikā sertifikācijas struktūrai un ITSEF sniegtās informācijas ierakstus;

b) sertificētā IKT izstrādājuma paraugu.

3. Ja sertifikācijas struktūra ir izdevusi jaunu *EUCC* sertifikātu saskaņā ar 13. panta 2. punkta c) apakšpunktu, tā turētājs kopā ar jauno *EUCC* sertifikātu un tikpat ilgi kā jauno *EUCC* sertifikātu glabā atsauktā *EUCC* sertifikāta dokumentāciju.

4. Pēc sertifikācijas struktūras vai valsts kiberdrošības sertifikācijas iestādes pieprasījuma *EUCC* sertifikāta turētājs dara pieejamus 2. punktā minētos ierakstus un kopijas.

42. pants

Informācija, ko pieejamu dara *ENISA*

1. *ENISA* Regulas (ES) 2019/881 50. panta 1. punktā minētajā vietnē publicē šādu informāciju:

a) visus *EUCC* sertifikātus;

b) informāciju par EUCC sertifikāta statusu, sevišķi par to, vai tas ir spēkā, apturēts, atsaukts vai beidzies;

c) katram *EUCC* sertifikātam attiecīgo sertifikācijas ziņojumu;

([5]) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris), ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva) (OV L 333, 27.12.2022., 80. lpp.).

d) akreditēto atbilstības novērtēšanas struktūru sarakstu;

e) pilnvaroto atbilstības novērtēšanas struktūru sarakstu;

f) aktuālos dokumentus, kas uzskaitīti I pielikumā;

g) Eiropas Kiberdrošības sertifikācijas grupas atzinumus, kas paredzēti Regulas (ES) 2019/881 62. panta 4. punkta c) apakšpunktā;

h) profesionālās izvērtēšanas ziņojumus, kas izdoti saskaņā ar 47. pantu.

2. Šā panta 1. punktā minēto informāciju dara pieejamu vismaz angļu valodā.

3. Sertifikācijas struktūras un attiecīgā gadījumā valsts kiberdrošības sertifikācijas iestādes nekavējoties informē *ENISA* par saviem lēmumiem, kas ietekmē 1. punkta b) apakšpunktā minētā *EUCC* sertifikāta saturu vai statusu.

4. *ENISA* nodrošina, ka informācijā, kas publicēta saskaņā ar 1. punkta a), b) un c) apakšpunktu, ir skaidri norādītas sertificētā IKT izstrādājuma versijas, uz kurām attiecas *EUCC* sertifikāts.

43. pants

Informācijas aizsardzība

Atbilstības novērtēšanas struktūras, valsta kiberdrošības sertifikācijas iestādes, *ECCG*, *ENISA*, Komisija un visas pārējās personas nodrošina komercnoslēpumu un citas konfidenciālas informācijas, arī tirdzniecības noslēpumu, drošību un aizsardzību, kā arī saglabā intelektuālā īpašuma tiesības, un veic nepieciešamos un pienācīgus tehniskos un organizatoriskos pasākumus.

VIII NODAĻA

SAVSTARPĒJAS ATZĪŠANAS NOLĪGUMI AR TREŠĀM VALSTĪM

44. pants

Nosacījumi

1. Trešās valstis, kuras vēlas savus izstrādājumus sertificēt saskaņā ar šo regulu un vēlas, lai sertifikācija tiktu atzīta Savienībā, noslēdz ar Savienību savstarpējas atzīšanas nolīgumu.

2. Savstarpējas atzīšanas nolīgums aptver sertificējamiem IKT izstrādājumiem piemērojamos apliecinājuma līmeņus un – attiecīgā gadījumā – aizsardzības profilus.

3. Šā panta 1. punktā minētos savstarpējās atzīšanas nolīgumus var noslēgt tikai ar trešām valstīm, kuras atbilst šādiem nosacījumiem:

a) tai ir iestāde:

   1) kura ir publiska struktūra, kas ir neatkarīga no vienībām, kuras tā uzrauga un pārrauga organizatoriskās un juridiskās struktūras, finanšu līdzekļu un lēmumu pieņemšanas ziņā;

   2) kurai ir attiecīgas pārraudzības un uzraudzības pilnvaras veikt izmeklēšanu, un tā ir pilnvarota veikt attiecīgus korektīvus pasākumus, kas nepieciešami, lai nodrošinātu atbilstību;

   3) kurai ir ieviesta iedarbīgu, samērīgu un atturošu sodu sistēma, ar ko nodrošina atbilstību;

   4) kura piekrīt sadarboties ar Eiropas Kiberdrošības sertifikācijas grupu un *ENISA*, lai apmainītos ar paraugpraksi un informāciju par attiecīgajām norisēm kiberdrošības sertifikācijas jomā un strādātu tā, lai vienādi interpretētu pašlaik piemērojamos izvērtēšanas kritērijus un metodes, cita starpā piemērojot saskaņotu dokumentāciju, kas ir līdzvērtīga I pielikumā uzskaitītajiem aktuālajiem dokumentiem;

b) kura ir neatkarīga akreditācijas struktūra, kas veic akreditāciju, izmantojot standartus, kuri ir līdzvērtīgi Regulā (EK) Nr. 765/2008 minētajiem standartiem;

c) kura apņēmusies izvērtēšanas un sertifikācijas procesus un procedūras īstenot pienācīgi profesionāli, ņemot vērā atbilstību starptautiskajiem standartiem, kas minēti šajā regulā, sevišķi 3. pantā;

d) kura spēj ziņot par iepriekš neatklātām vārīgām vietām un kurai ir izveidota atbilstoša vārīgo vietu pārvaldības un uzrādīšanas procedūra;

e) kura ir izveidojusi procedūras, kas nodrošina, ka sūdzības var faktiski iesniegt un izskatīt, un nodrošina rezultatīvu tiesiskās aizsardzības līdzekli sūdzības iesniedzējam;

f) kura ir izveidojusi mehānismu sadarbībai ar citām Savienības un dalībvalstu struktūrām, kas saistītas ar kiberdrošības sertifikāciju saskaņā ar šo regulu, kā arī apmaiņai ar informāciju par iespējamu sertifikātu neatbilstību, attiecīgo norišu pārraudzībai sertifikācijas jomā un kopīgas pieejas nodrošināšanai sertifikācijas uzturēšanas un pārskatīšanas jomā.

4. Papildus 3. punktā izklāstītajiem nosacījumiem 1. punktā minēto savstarpējās atzīšanas nolīgumu, kas attiecas uz apliecinājuma līmeni "augsts", ar trešām valstīm var noslēgt tikai tad, ja ir izpildīti arī šādi nosacījumi:

a) trešajai valstij ir neatkarīga un publiska kiberdrošības sertifikācijas iestāde, kas veic vai deleģē izvērtēšanas darbības, kuras vajadzīgas, lai varētu veikt sertifikāciju apliecinājuma līmenī "augsts", un kas atbilst līdzvērtīgām prasībām un procedūrām, kuras valsts kiberdrošības iestādēm noteiktas šajā regulā un Regulā (ES) 2019/881;

b) ar savstarpējās atzīšanas nolīgumu izveido kopīgu mehānismu, kas līdzvērtīgs *EUCC* sertifikācijas profesionālajai izvērtēšanai, lai uzlabotu prakses apmaiņu un kopīgi risinātu jautājumus izvērtēšanas un sertifikācijas jomā.

IX NODAĻA

SERTIFIKĀCIJAS STRUKTŪRU PROFESIONĀLĀ IZVĒRTĒŠANA

45. pants

Profesionālās izvērtēšanas procedūra

1. Saistībā ar sertifikācijas struktūru, kas izdod *EUCC* sertifikātus apliecinājuma līmenī "augsts", regulāri un vismaz reizi piecos gados veic profesionālo izvērtēšanu. Dažādie profesionālās izvērtēšanas veidi ir uzskaitīti VI pielikumā.

2. Eiropas Kiberdrošības sertifikācijas grupa izstrādā un uztur profesionālās izvērtēšanas grafiku, nodrošinot, ka tiek ievērota šāda regularitāte. Profesionālo izvērtēšanu veic uz vietas, izņemot pienācīgi pamatotus izņēmuma gadījumus.

3. Profesionālā izvērtēšana var būt balstīta uz pierādījumiem, kas savākti iepriekšējā profesionālajā izvērtēšanā, vai uz līdzvērtīgām procedūrām, kuras veikusi profesionāli izvērtējamā sertifikācijas struktūra vai valsts kiberdrošības sertifikācijas iestāde, ar noteikumu, ka:

a) rezultāti nav vecāki par pieciem gadiem;

b) rezultātiem ir pievienots apraksts par profesionālās izvērtēšanas procedūrām, kas izveidotas attiecīgajai shēmai, ja tās ir saistītas ar profesionālo izvērtēšanu, kuru veic saskaņā ar atšķirīgu sertifikācijas shēmu;

c) profesionālās izvērtēšanas ziņojumā, kas minēts 47. pantā, ir norādīts, kuri rezultāti ir atkalizmantoti ar papildu novērtējumu vai bez tā.

4. Ja profesionālā izvērtēšana aptver tehnisku jomu, novērtē arī attiecīgo *ITSEF*.

5. Sertifikācijas struktūra, kurai veic profesionālo izvērtēšanu, un vajadzības gadījumā valsts kiberdrošības sertifikācijas iestāde nodrošina, ka profesionālās izvērtēšanas grupai tiek darīta pieejama visa attiecīgā informācija.

6. Profesionālo izvērtēšanu veic profesionālās izvērtēšanas grupa, kas izveidota saskaņā ar VI pielikumu.

46. pants

Profesionālās izvērtēšanas posmi

1. Sagatavošanās posmā profesionālās izvērtēšanas grupas dalībnieki pārskata sertifikācijas struktūras dokumentāciju, kas aptver tās politiku un procedūras, kā arī aktuālo dokumentu izmantošanu.

2. Vietas apmeklējuma posmā profesionālās izvērtēšanas grupa novērtē struktūras tehnisko kompetenci un attiecīgā gadījumā tāda *ITSEF* kompetenci, kas veicis vismaz vienu tāda IKT izstrādājuma izvērtēšanu, uz kuru attiecas profesionālā izvērtēšana.

3. Vietas apmeklējuma posma ilgumu var pagarināt vai saīsināt atkarībā no tādiem faktoriem kā iespēja atkalizmantot esošos profesionālās izvērtēšanas pierādījumus un rezultātus vai no *ITSEF* un tehnisko jomu skaita, par kurām sertifikācijas struktūra izdevusi sertifikātus.

4. Attiecīgā gadījumā profesionālās izvērtēšanas grupa nosaka katra *ITSEF* tehnisko kompetenci, apmeklējot tā tehnisko laboratoriju vai laboratorijas un intervējot tā vērtētājus par tehnisko jomu un ar to saistītajām konkrētām uzbrukuma metodēm.

5. Ziņošanas posmā profesionālās izvērtēšanas grupa savus konstatējumus dokumentē profesionālās izvērtēšanas ziņojumā, ietverot slēdzienu un attiecīgā gadījumā sarakstu ar novērotajām neatbilstībām, kas sarindotas pēc to svarīguma pakāpes.

6. Profesionālās izvērtēšanas ziņojums vispirms jāapspriež ar sertifikācijas struktūru, kuras profesionālā izvērtēšana tiek veikta. Pēc šīm apspriedēm profesionāli novērtējamā sertifikācijas struktūra izveido grafiku ar pasākumiem, kas jāveic, lai risinātu konstatējumus.

47. pants

Profesionālās izvērtēšanas ziņojums

1. Profesionālās izvērtēšanas grupa profesionāli izvērtējamajai sertifikācijas struktūrai iesniedz profesionālās izvērtēšanas ziņojuma projektu.

2. Profesionāli izvērtējamā sertifikācijas struktūra iesniedz profesionālās izvērtēšanas grupai piezīmes par konstatējumiem un tādu saistību sarakstu, ar ko novērš profesionālās izvērtēšanas ziņojuma projektā konstatētos trūkumus.

3. Profesionālās izvērtēšanas grupa iesniedz Eiropas Kiberdrošības sertifikācijas grupai galīgo profesionālās izvērtēšanas ziņojumu, kurā ir ietvertas arī profesionāli izvērtējamās struktūras piezīmes un saistības. Profesionālās izvērtēšanas grupa iekļauj arī savu nostāju par piezīmēm un par to, vai minētās saistības ir pietiekamas, lai novērstu konstatētos trūkumus.

4. Ja profesionālās novērtēšanas ziņojumā ir konstatētas neatbilstības, Eiropas Kiberdrošības sertifikācijas grupa var noteikt attiecīgu termiņu profesionāli novērtējamās sertifikācijas struktūras neatbilstību novēršanai.

5. Eiropas Kiberdrošības sertifikācijas grupa pieņem atzinumu par profesionālās izvērtēšanas ziņojumu:

a) ja profesionālās novērtēšanas ziņojumā neatbilstības nav konstatētas vai ja profesionāli novērtējamā sertifikācijas struktūra neatbilstības ir pienācīgi risinājusi, Eiropas Kiberdrošības sertifikācijas grupa var sniegt pozitīvu atzinumu un visus attiecīgos dokumentus publicē *ENISA* sertifikācijas vietnē;

b) ja profesionāli izvērtējamā sertifikācijas struktūra noteiktajā termiņā neatbilstības pienācīgi nerisina, Eiropas Kiberdrošības sertifikācijas grupa var sniegt negatīvu atzinumu, ko publicē *ENISA* sertifikācijas vietnē, iekļaujot profesionālās izvērtēšanas ziņojumu un visus attiecīgos dokumentus.

6. Pirms atzinuma publicēšanas no publicējamiem dokumentiem izņem visu sensitīvo informāciju, personu datus un īpašniekinformāciju.

X NODAĻA

SHĒMAS UZTURĒŠANA

48. pants

***EUCC* uzturēšana**

1. Komisija var lūgt Eiropas Kiberdrošības sertifikācijas grupu pieņemt atzinumu ar mērķi uzturēt *EUCC* un veikt nepieciešamos priekšdarbus.

2. Eiropas Kiberdrošības sertifikācijas grupa var pieņemt atzinumu, lai apstiprinātu aktuālos dokumentus.

3. Aktuālos dokumentus, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa, publicē *ENISA*.

XI NODAĻA

NOBEIGUMA NOTEIKUMI

49. pants

Valstu shēmas, uz kurām attiecas *EUCC*

1. Saskaņā ar Regulas (ES) 2019/881 57. panta 1. punktu un neskarot minētās regulas 57. panta 3. punktu, visas valstu kiberdrošības sertifikācijas shēmas un saistītās procedūras attiecībā uz IKT izstrādājumiem un IKT procesiem, uz kuriem attiecas *EUCC*, zaudē spēku no dienas, kad pagājuši 12 mēneši pēc šīs regulas stāšanās spēkā.

2. Atkāpjoties no 50. panta, sertifikācijas procesu saskaņā ar valsts kiberdrošības sertifikācijas shēmu var sākt 12 mēnešu laikā pēc šīs regulas stāšanās spēkā, ja sertifikācijas process tiek pabeigts ne vēlāk kā 24 mēnešus pēc šīs regulas stāšanās spēkā.

3. Sertifikātiem, kas izdoti saskaņā ar valstu kiberdrošības sertifikācijas shēmām, var piemērot pārskatīšanu. Jaunus sertifikātus, kas aizstāj pārskatītos sertifikātus, izdod saskaņā ar šo regulu.

50. pants

Stāšanās spēkā

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

To piemēro no 2025. gada 27. februāra.

Bet IV nodaļu un V pielikumu piemēro no šīs regulas spēkā stāšanās brīža.

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

Briselē, 2024. gada 31. janvārī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

I PIELIKUMS

Tehniskās jomas un jaunākie dokumenti

1. Tehniskās jomas AVA_VAN 4. vai 5. līmenī:

   a) dokumenti, kas attiecas uz tehniskās jomas "Viedkartes un līdzīgas ierīces" saskaņoto izvērtēšanu, sevišķi šie dokumenti attiecīgajā redakcijā, kas ir spēkā no [spēkā stāšanās datuma]:

      1) "Minimālās *ITSEF* prasības viedkaršu un līdzīgu ierīču drošības izvērtēšanai", ko *ECCG* sākotnēji apstiprinājusi 2023. gada 20. oktobrī;

      2) "Minimālās objekta drošības prasības", ko *ECCG* sākotnēji apstiprinājusi 2023. gada 20. oktobrī;

      3) "Vienotu kritēriju piemērošana integrālajām shēmām", ko *ECCG* sākotnēji apstiprinājusi 2023. gada 20. oktobrī;

      4) "Drošības arhitektūras prasības (ADV_ARC) viedkartēm un līdzīgām ierīcēm", ko *ECCG* sākotnēji apstiprinājusi 2023. gada 20. oktobrī;

      5) ""Atvērto" viedkaršu izstrādājumu sertifikācija", ko *ECCG* sākotnēji apstiprinājusi 2023. gada 20. oktobrī;

      6) "Saliktu izstrādājumu izvērtēšana viedkartēm un līdzīgām ierīcēm", ko *ECCG* sākotnēji apstiprinājusi 2023. gada 20. oktobrī;

      7) "Uzbrukuma potenciāla piemērošana viedkartēm", ko *ECCG* sākotnēji apstiprinājusi 2023. gada 20. oktobrī;

   b) dokumenti, kas attiecas uz tehniskās jomas "aparatūras ierīces ar drošības kastēm" saskaņoto izvērtēšanu, sevišķi šie dokumenti attiecīgā redakcijā, kas ir spēkā no [spēkā stāšanās datuma]:

      1) "Minimālās *ITSEF* prasības aparatūras ierīču ar drošības kastēm drošības izvērtējumiem", ko *ECCG* sākotnēji apstiprinājusi 2023. gada 20. oktobrī;

      2) "Minimālās objekta drošības prasības", ko *ECCG* sākotnēji apstiprinājusi 2023. gada 20. oktobrī;

      3) "Uzbrukuma potenciāla piemērošana aparatūras ierīcēm ar drošības kastēm", ko *ECCG* sākotnēji apstiprinājusi 2023. gada 20. oktobrī.

2. Jaunākie dokumenti attiecīgajā redakcijā, kas ir spēkā no [spēkā stāšanās datuma]:

   a) dokuments, kas attiecas uz atbilstības novērtēšanas struktūru saskaņoto akreditāciju: "*ITSEF* akreditācija *EUCC* vajadzībām", ko *ECCG* sākotnēji apstiprinājusi 2023. gada 20. oktobrī.

II PIELIKUMS

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

1. Attiecībā uz kvalificēta paraksta un zīmoga tālradīšanas ierīču kategoriju:

1) EN 419241-2:2019. Uzticamas sistēmas, kas atbalsta servera parakstu. 2. daļa – Servera parakstu QSCD aizsardzības profili;

2) EN 419221-5:2018. Aizsardzības profili uzticamības pakalpojuma sniedzēja kriptogrāfijas moduļiem. 5. daļa – Uzticamības pakalpojumu kriptogrāfijas modulis

2. Aizsardzības profili, kas pieņemti kā jaunākie dokumenti:

[BLANK]

III PIELIKUMS

Ieteicamie aizsardzības profili (kas ilustrē I pielikuma tehniskās jomas)

Aizsardzības profili (*PP*), kas izmantojami tādu IKT izstrādājumu sertificēšanā, kuri ietilpst turpmāk norādītajās IKT izstrādājumu kategorijās:

a) mašīnlasāmu ceļošanas dokumentu kategorijā:

1) *PP* mašīnlasāmam ceļošanas dokumentam, kas izmanto standarta pārbaudes procedūru ar *PACE* (*PP Machine Readable Travel Document using Standard Inspection Procedure with PACE*), BSI-CC-PP-0068-V2-2011-MA-01;

2) *PP* mašīnlasāmam ceļošanas dokumentam ar "*ICAO* lietojumu", paplašinātā piekļuves kontrole (*PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control*), BSI-CC-PP-0056-2009;

3) *PP* mašīnlasāmam ceļošanas dokumentam ar "*ICAO* lietojumu", paplašinātā piekļuves kontrole ar *PACE* (*PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE*), BSI-CC-PP-0056-V2-2012-MA-02;

4) *PP* mašīnlasāmam ceļošanas dokumentam ar "*ICAO* lietojumu" (*PP for a Machine Readable Travel Document with "ICAO Application" Basic Access Control*), pamata piekļuves kontrole, BSI-CC-PP-0055-2009;

b) drošu paraksta radīšanas ierīču kategorijā:

1) EN 419211-1:2014. Aizsardzības profili drošām paraksta radīšanas ierīcēm. 1. daļa: Pārskats

2) EN 419211-2:2013. Aizsardzības profili drošām paraksta radīšanas ierīcēm. 2. daļa: Atslēgu ģenerēšanas ierīce;

3) EN 419211-3:2013. Aizsardzības profili drošām paraksta radīšanas ierīcēm. 3. daļa: Ierīce ar atslēgas importu;

4) EN 419211-4:2013. Aizsardzības profili drošām paraksta radīšanas ierīcēm. 4. daļa: Paplašinājums atslēgu ģenerēšanas ierīcei un uzticams kanāls sertifikāta ģenerēšanas lietotnei;

5) EN 419211-5:2013. Aizsardzības profili drošām paraksta radīšanas ierīcēm. 5. daļa: Paplašinājums atslēgu ģenerēšanas ierīcei un uzticams kanāls paraksta radīšanas lietotnei;

6) EN 419211-6:2014. Aizsardzības profili drošām paraksta radīšanas ierīcēm. 6. daļa: Paplašinājums atslēgu importēšanas ierīcei un uzticams kanāls paraksta radīšanas lietotnei;

c) digitālo tahogrāfu kategorijā:

1) Digitālais tahogrāfs – tahogrāfa karte, kā norādīts Komisijas 2016. gada 18. marta Īstenošanas regulā (ES) 2016/799, ar ko īsteno Regulu (ES) Nr. 165/2014 (1.C pielikums);

2) Digitālie tahogrāfi – transportlīdzekļu bloki, kā norādīts Komisijas Regulas (EK) Nr. 1360/2002 I.B pielikumā un ko paredzēts uzstādīt autotransporta līdzekļos;

3) Digitālais tahogrāfs – ārējā *GNSS* iekārta (*EGF PP*), kā norādīts 1.C pielikumā Komisijas 2016. gada 18. marta Īstenošanas regulā (ES) 2016/799, ar ko īsteno Eiropas Parlamenta un Padomes Regulu (ES) Nr. 165/2014;

4) Digitālais tahogrāfs – kustības sensors (*MS PP*), kā norādīts 1.C pielikumā Komisijas 2016. gada 18. marta Īstenošanas regulā (ES) 2016/799, ar ko īsteno Eiropas Parlamenta un Padomes Regulu (ES) Nr. 165/2014;

d) drošu integrālo shēmu (IS), viedkaršu un saistīto ierīču jomā:

1) Drošas IS platformas *PP* (*Security IC Platform PP*), BSI-CC-PP-0084-2014;

2) "Java" kartes sistēmas – atvērtā konfigurācija (*Java Card System – Open Configuration*), V3.0.5 BSI-CC-PP-0099-2017;

3) "Java" kartes sistēmas – slēgtā konfigurācija (*Java Card System – Closed Configuration*), BSI-CC-PP-0101-2017;

4) *PP PC* klienta uzticama platformas moduļa saime 2.0, līmenis 0 redakcija 1.16 (*PP for a PC Client Specific Trusted Platform Module Family 2.0 Level 0 Revision 1.16*), ANSSI-CC-PP-2015/07;

5) Universāla SIM karte (*Universal SIM card*), PU-2009-RT-79, ANSSI-CC-PP-2010/04;

6) Iegultais *UICC* (*eUICC*) mašīnas–mašīnas ierīcēm (*Embedded UICC (eUICC) for Machine-to-Machine Devices*), BSI-CC-PP-0089-2015;

e) (maksājumu) mijiedarbības punktu un maksājumu terminālu kategorijā;

1) Mijiedarbības punkts "POI-CHIP-ONLY" (*Point of Interaction "POI-CHIP-ONLY"*), ANSSI-CC-PP-2015/01;

2) Mijiedarbības punkts "POI-CHIP-ONLY un atvērtā protokola pakotne" (*Point of Interaction "POI-CHIP-ONLY and Open Protocol Package"*), ANSSI-CC-PP-2015/02;

3) Mijiedarbības punkts "POI-COMPREHENSIVEY" (*Point of Interaction "POI-COMPREHENSIVE"*), ANSSI-CC-PP-2015/03;

4) Mijiedarbības punkts "POI-COMPREHENSIVE un atvērtā protokola pakotne" (*Point of Interaction "POI-COMPREHENSIVE and Open Protocol Package"*), ANSSI-CC-PP-2015/04;

5) Mijiedarbības punkts "POI-PED-ONLY" (*Point of Interaction "POI-CHIP-ONLY"*), ANSSI-CC-PP-2015/05;

6) Mijiedarbības punkts "POI-PED-ONLY un atvērtā protokola pakotne" (*Point of Interaction "POI-CHIP-ONLY and Open Protocol Package"*), ANSSI-CC-PP-2015/06;

f) aparatūras ierīču ar drošības kastēm kategorijā:

1) Kriptogrāfisks modulis *CSP* parakstīšanas darbībām ar dublējumu – *PP CMCSOB, PP HSM CMCSOB* 14167-2 (*Cryptographic Module for CSP Signing Operations with Backup – PP CMCSOB, PP HSM CMCSOB 14167-2*), ANSSI-CC-PP-2015/08;

2) Kriptogrāfisks modulis *CSP* atslēgu ģenerēšanas pakalpojumiem – *PP CMCKG, PP HSM CMCKG* 14167-3 (*Cryptographic Module for CSP key generation services – PP CMCKG, PP HSM CMCKG 14167-3*), ANSSI-CC-PP-2015/09;

3) Kriptogrāfisks modulis *CSP* parakstīšanas darbībām bez dublējuma – *PP CMCSO, PP HSM CMCKG* 14167-4 (*Cryptographic Module for CSP Signing Operations without Backup – PP CMCSO, PP HSM CMCKG 14167-4*), ANSSI-CC-PP-2015/10.

IV PIELIKUMS

APLIECINĀJUMA PASTĀVĪGUMS UN SERTIFIKĀTA PĀRSKATĪŠANA

IV.1. **Apliecinājuma pastāvīgums. Tvērums**

1. Saistītajām uzturēšanas darbībām piemēro šādas apliecinājuma pastāvīguma prasības:

   a) otrreizēja novērtēšana, ja nemainīts sertificēts IKT izstrādājums joprojām atbilst tā drošības prasībām;

   b) sertificētā IKT izstrādājuma izmaiņu ietekmes uz sertifikāciju izvērtēšana;

   c) ielāpu izmantošana saskaņā ar novērtēto ielāpu pārvaldības procesu, ja tā ietilpst sertificēšanā;

   d) sertifikāta turētāja aprites cikla pārvaldības vai ražošanas procesu pārskatīšana, ja tā ietilpst.

2. *EUCC* sertifikāta turētājs var pieprasīt sertifikāta pārskatīšanu šādos gadījumos:

   a) *EUCC* sertifikāta derīguma termiņš beigsies deviņu mēnešu laikā;

   b) ir notikušas izmaiņas sertificētajā IKT izstrādājumā vai citā faktorā, kas var ietekmēt tā drošības funkcionalitāti;

   c) sertifikāta turētājs pieprasa vēlreiz veikt vārīgo vietu novērtēšanu, lai no jauna apstiprinātu *EUCC* sertifikāta apliecinājumu, kas saistīts ar IKT izstrādājuma noturīgumu pret tābrīža kiberuzbrukumiem.

IV.2. **Vēlreizēja novērtēšana**

1. Ja ir nepieciešams noteikt, kā apdraudējuma vides izmaiņas ietekmē neizmainītu sertificētu IKT izstrādājumu, sertifikācijas struktūrai iesniedz vēlreizējas novērtēšanas pieprasījumu.

2. Novērtēšanu atkārto tas pats *ITSEF*, kas bijis iesaistīts iepriekšējā izvērtēšanā, vēlreiz izmantojot visus tās rezultātus, kas joprojām ir spēkā. Novērtēšanā galveno uzmanību pievērš apliecināšanas darbībām, kuras ietekmēt varējušas sertificētā IKT izstrādājuma apdraudējuma vides izmaiņas, sevišķi attiecīgajai AVA_VAN saimei, kā arī apliecinājuma dzīves cikla (*ALC*) saimei, kur no jauna vāc pietiekamus pierādījumus par attīstības vides uzturēšanu.

3. *ITSEF* apraksta izmaiņas un sīki izklāsta vēlreizējās novērtēšanas rezultātus, atjauninot iepriekšējo izvērtējuma tehnisko ziņojumu.

4. Sertifikācijas struktūra pārskata atjaunināto izvērtēšanas tehnisko ziņojumu un sagatavo vēlreizējās novērtēšanas ziņojumu. Pēc tam sākotnējā sertifikāta statusu maina saskaņā ar 13. pantu.

5. Vēlreizējās novērtēšanas ziņojumu un atjaunināto sertifikātu iesniedz valsts kiberdrošības sertifikācijas iestādei un *ENISA* publicēšanai kiberdrošības sertifikācijas tīmekļa vietnē.

IV.3. **Izmaiņas sertificētā IKT izstrādājumā**

1. Ja sertificētā IKT izstrādājumā rodas izmaiņas, sertifikāta turētājs, kas vēlas saglabāt sertifikātu, iesniedz sertifikācijas struktūrai ietekmes analīzes ziņojumu.

2. Ietekmes analīzes ziņojumā iekļauj šādus elementus:

   a) ievadu, kurā ietverta informācija, kura vajadzīga, lai noteiktu ietekmes analīzes ziņojumu un izvērtēšanas objektu, uz ko attiecas izmaiņas;

b) izstrādājuma izmaiņu aprakstu;

c) ietekmēto izstrādātāja pierādījumu identifikāciju;

d) izstrādātāja pierādījumu grozījumu aprakstu;

e) konstatējumus un secinājumus par katras izmaiņas ietekmi uz apliecinājumu.

3. Sertifikācijas struktūra pārbauda ietekmes analīzes ziņojumā aprakstītās izmaiņas, lai apstiprinātu to ietekmi uz sertificētā izvērtēšanas objekta apliecinājumu, kā ierosināts ietekmes analīzes ziņojuma secinājumos.

4. Pēc pārbaudes sertifikācijas struktūra nosaka, vai izmaiņu apmērs ir nebūtisks vai būtisks atbilstoši to ietekmei.

5. Ja sertifikācijas struktūra ir apstiprinājusi, ka izmaiņas ir nebūtiskas, pārveidotajam IKT izstrādājumam izdod jaunu sertifikātu un sagatavo uzturēšanas ziņojumu papildus sākotnējam sertifikācijas ziņojumam, ievērojot šādus nosacījumus:

a) uzturēšanas ziņojumu iekļauj kā ietekmes analīzes ziņojuma apakškopu, kurā ir šādas iedaļas:

1) ievads;

2) izmaiņu apraksts;

3) ietekmētais izstrādātāja pierādījums;

b) jaunā sertifikāta derīguma termiņš nepārsniedz sākotnējā sertifikāta derīguma termiņu.

6. Jauno sertifikātu kopā ar uzturēšanas ziņojumu, iesniedz *ENISA* publicēšanai kiberdrošības sertifikācijas tīmekļa vietnē.

7. Ja tiek apstiprināts, ka izmaiņas ir būtiskas, veic vēlreizēju izvērtēšanu, ņemot vērā iepriekšējo izvērtēšanu un vēlreiz izmantojot visus iepriekšējās izvērtēšanas rezultātus, kas joprojām ir spēkā.

8. Pēc izmainītā novērtēšanas objekta izvērtēšanas pabeigšanas *ITSEF* sagatavo jaunu izvērtēšanas tehnisko ziņojumu. Sertifikācijas struktūra pārskata atjaunināto izvērtēšanas tehnisko ziņojumu un attiecīgā gadījumā sagatavo jaunu sertifikātu ar jaunu sertifikācijas ziņojumu.

9. Jauno sertifikātu un sertifikācijas ziņojumu iesniedz *ENISA* publicēšanai.

IV.4. **Ielāpu pārvaldība**

1. Ielāpu pārvaldības procedūra nodrošina strukturētu sertificēta IKT izstrādājuma atjaunināšanas procesu. Ielāpu pārvaldības procedūru, ieskaitot mehānismu, ko sertifikācijas pieteikuma iesniedzējs ir ieviesis IKT izstrādājumā, var izmantot pēc IKT izstrādājuma sertifikācijas atbilstības novērtēšanas struktūras atbildībā.

2. Sertifikācijas pieteikuma iesniedzējs var IKT izstrādājuma sertifikācijā iekļaut ielāpa mehānismu kā daļu no sertificētas pārvaldības procedūras IKT izstrādājumā, ja ir viens no šiem nosacījumiem:

a) funkcionalitāte, ko skar ielāps, ir ārpus sertificētā IKT izstrādājuma izvērtēšanas objekta;

b) ielāps attiecas uz iepriekš noteiktām nebūtiskām izmaiņām sertificētajā IKT izstrādājumā;

c) ielāps attiecas uz apstiprinātu vārīgu vietu, kas būtiski ietekmē sertificētā IKT izstrādājuma drošību.

3. Ja ielāps attiecas uz būtiskām izmaiņām sertificētā IKT izstrādājuma izvērtēšanas objektā saistībā ar iepriekš neatklātu vārīgu vietu, kam nav būtiskas ietekmes uz IKT izstrādājuma drošību, piemēro 13. panta noteikumus.

4. IKT izstrādājuma ielāpu pārvaldības procedūru veido šādi elementi:

   a) IKT izstrādājuma ielāpa izstrādes un izlaišanas process;

   b) tehniskais mehānisms un funkcijas ielāpa ieviešanai IKT izstrādājumā;

   c) tādu izvērtēšanas darbību kopums, kas saistītas ar tehniskā mehānisma efektivitāti un veiktspēju.

5. IKT izstrādājuma sertifikācijas laikā:

   a) IKT izstrādājuma sertifikācijas pieteikuma iesniedzējs iesniedz ielāpu pārvaldības procedūras aprakstu;

   b) *ITSEF* pārbauda šādus elementus:

      1) izstrādātājs ir ieviesis ielāpu mehānismus IKT izstrādājumā saskaņā ar ielāpu pārvaldības procedūru, kas tika iesniegta sertifikācijai;

      2) izvērtēšanas objekta robežas ir nodalītas tā, lai nodalītajos procesos veiktās izmaiņas neietekmētu izvērtēšanas objekta drošību;

      3) tehniskais ielāpa mehānisms darbojas saskaņā ar šīs iedaļas noteikumiem un pieteikuma iesniedzēja apgalvojumiem;

   c) sertifikācijas struktūra sertifikācijas ziņojumā iekļauj novērtētās ielāpu pārvaldības procedūras rezultātus.

6. Sertifikāta turētājs attiecīgajam sertificētajam IKT izstrādājumam var turpināt piemērot ielāpu, kas izgatavots saskaņā ar sertificēto ielāpu pārvaldības procedūru, un piecu darbdienu laikā veic šādus pasākumus:

   a) šīs iedaļas 2. punkta a) apakšpunktā minētajā gadījumā paziņo par attiecīgo ielāpu sertifikācijas struktūrai, kas nemaina attiecīgo *EUCC* sertifikātu;

   b) šīs iedaļas 2. punkta b) apakšpunktā minētajā gadījumā iesniedz attiecīgo ielāpu *ITSEF* pārskatīšanai. *ITSEF* pēc ielāpa saņemšanas informē sertifikācijas struktūru, un pēc tam sertifikācijas struktūra veic attiecīgos pasākumus, kas nepieciešami, lai attiecīgo *EUCC* sertifikātu izdotu jaunā redakcijā un atjauninātu sertifikācijas ziņojumu;

   c) šīs iedaļas 2. punkta c) apakšpunktā minētajā gadījumā iesniedz attiecīgo ielāpu *ITSEF* nepieciešamajai vēlreizējai izvērtēšanai, bet ielāpu var izmantot paralēli. *ITSEF* informē sertifikācijas struktūru, un pēc tam sertifikācijas struktūra sāk attiecīgās sertifikācijas darbības.

V PIELIKUMS

SERTIFIKĀCIJAS ZIŅOJUMA SATURS

V.1. **Sertifikācijas ziņojums**

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

2. Sertifikācijas ziņojums ir sīki izstrādātas un praktiskas informācijas avots par IKT izstrādājumu vai IKT izstrādājumu kategoriju un par IKT izstrādājuma drošu izvēršanu, un tāpēc tajā ietver visu publiski pieejamo un kopīgojamo informāciju, kas svarīga lietotājiem un ieinteresētajām personām. Sertifikācijas ziņojumā var atsaukties uz publiski pieejamo un kopīgojamo informāciju.

3. Sertifikācijas ziņojumā iekļauj vismaz šādas iedaļas:

   a) kopsavilkums;

   b) IKT izstrādājuma vai IKT izstrādājumu kategorijas identifikācija aizsardzības profiliem;

   c) drošības pakalpojumi;

   d) pieņēmumi un tvēruma precizēšana;

   e) arhitektūras informācija;

   f) attiecīgā gadījumā – papildinformācija par kiberdrošību;

   g) IKT izstrādājuma testēšana, ja tā veikta;

   h) attiecīgā gadījumā – sertifikāta turētāja aprites cikla pārvaldības procesu un ražošanas iekārtu identifikācija;

   i) izvērtēšanas rezultāti un informācija par sertifikātu;

   j) sertifikācijai iesniegtā IKT izstrādājuma drošības mērķa kopsavilkums;

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

   l) bibliogrāfija.

4. Kopsavilkums ir visa sertifikācijas ziņojuma īss kopsavilkums. Kopsavilkumā sniedz skaidru un kodolīgu pārskatu par izvērtēšanas rezultātiem un ietver šādu informāciju:

   a) izvērtētā IKT izstrādājuma nosaukumu, izstrādājuma to komponentu uzskaitījumu, ko aptver izvērtējums, un IKT izstrādājuma versiju;

   b) tā *ITSEF* nosaukumu, kas veicis izvērtēšanu, un attiecīgā gadījumā apakšuzņēmēju sarakstu;

   c) izvērtēšanas pabeigšanas datumu;

   d) atsauci uz *ITSEF* sagatavoto izvērtēšanas tehnisko ziņojumu;

   e) īsu sertifikācijas ziņojuma rezultātu aprakstu, ieskaitot:

      1) izvērtējumam piemēroto vienoto kritēriju redakciju un attiecīgā gadījumā laidienu;

      2) vienoto kritēriju apliecinājuma paketi un drošības apliecinājuma komponentus, arī AVA_VAN līmeni, kas piemērots izvērtēšanā, un tā attiecīgo apliecinājuma līmeni, kā noteikts Regulas (ES) 2019/881 52. pantā, uz kuru attiecas *EUCC* sertifikāts;

      3) izvērtētā IKT izstrādājuma drošības funkcionalitāti;

      4) izvērtētā IKT izstrādājuma apdraudējumu un organizatoriskās drošības politikas kopsavilkumu;

5) īpašas prasības attiecībā uz konfigurāciju;

6) pieņēmumus par darbības vidi;

7) attiecīgā gadījumā – apstiprinātu ielāpu pārvaldības procedūru saskaņā ar IV pielikuma IV.4. iedaļu;

8) atrunu(-as).

5. Izvērtēto IKT izstrādājumu skaidri identificē, norādot šādu informāciju:

a) izvērtētā IKT izstrādājuma nosaukumu;

b) IKT izstrādājuma to komponentu uzskaitījumu, ko aptver izvērtējums;

c) IKT izstrādājuma komponentu versijas numuru;

d) papildu prasību noteikšanu sertificētā IKT izstrādājuma darbības videi;

e) *EUCC* sertifikāta turētāja vārdu un kontaktinformāciju;

f) attiecīgā gadījumā ielāpu pārvaldības procedūru, kas ietverta sertifikātā;

g) saiti uz *EUCC* sertifikāta turētāja tīmekļa vietni, kurā ir sniegta papildu kiberdrošības informācija par sertificēto IKT izstrādājumu saskaņā ar Regulas (ES) 2019/881 55. pantu.

6. Šajā iedaļā iekļautā informācija ir pēc iespējas precīzāka, lai nodrošinātu pilnīgu un precīzu tā IKT izstrādājuma aprakstu, kuru var no jauna izmantot turpmākā izvērtēšanā.

7. Drošības politikas iedaļā iekļauj aprakstu par IKT izstrādājuma drošības politiku un kārtību vai noteikumiem, kas ar izvērtēto IKT izstrādājumu jāievieš vai jāievēro. Tajā iekļauj norādi un aprakstu par šādu politiku:

a) sertifikāta turētāja vārīgo vietu novēršanas politika;

b) sertifikāta turētāja apliecinājuma pastāvīguma politika;

8. Attiecīgā gadījumā politikā var iekļaut nosacījumus, kas saistīti ar ielāpu pārvaldības procedūras izmantošanu sertifikāta derīguma laikā.

9. Iedaļā par pieņēmumiem un tvēruma precizēšanu jābūt izsmeļošai informācijai par apstākļiem un mērķiem, kas saistīti ar izstrādājuma paredzēto lietojumu, kā minēts 7. panta 1. punkta c) apakšpunktā. Informācijā iekļauj šādus datus:

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

b) pieņēmumi par vidi IKT izstrādājuma atbilstīgai ekspluatācijai;

10. Šā pielikuma 9. punktā uzskaitītajai informācijai jābūt maksimāli saprotamai, lai sertificētā IKT izstrādājuma lietotāji var pieņemt pamatotus lēmumus par riskiem, kas saistīti ar tā lietošanu.

11. Arhitektūras informācijas iedaļā iekļauj IKT izstrādājuma un tā galveno komponentu augsta līmeņa aprakstu saskaņā ar vienoto kritēriju ADV_TDS apakšsistēmu projektu.

12. Sniedz pilnīgu IKT izstrādājuma kiberdrošības papildinformācijas sarakstu saskaņā ar Regulas (ES) 2019/881 55. pantu. Visus attiecīgos dokumentus apzīmē ar redakcijas numuru.

13. IKT izstrādājuma testēšanas iedaļā iekļauj šādu informāciju:

a) tās iestādes vai struktūras, kura izdevusi sertifikātu, kā arī atbildīgās valsts kiberdrošības sertifikācijas iestādes nosaukumu un kontaktpunktu;

b) tā *ITSEF* nosaukumu, kas veicis izvērtēšanu, ja tas atšķiras no sertifikācijas struktūras;

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

d) tehniskā dokumenta redakciju un papildu drošības izvērtēšanas kritērijus, kas izmantoti izvērtēšanā;

e) IKT izstrādājuma pilnīgus un precīzus iestatījumus un konfigurāciju izvērtēšanas laikā, ietverot operatīvās piezīmes un apsvērumus, ja tādi ir pieejami;

f) izmantoto aizsardzības profilu, ietverot šādu informāciju:

1) aizsardzības profila autoru;

2) aizsardzības profila nosaukumu un adresi;

3) aizsardzības profila sertifikāta identifikatoru;

4) aizsardzības profila izvērtēšanā iesaistītās sertifikācijas struktūras un *ITSEF* nosaukumu un kontaktinformāciju;

5) apliecinājuma paketi(-es), kas vajadzīga(-as) izstrādājumam, kurš atbilst aizsardzības profilam.

14. Izvērtēšanas rezultātos un informācijā par sertifikāta iedaļu ietver šādu informāciju:

a) iegūtā apliecinājuma līmeņa apstiprinājumu, kā minēts šīs regulas 4. pantā un Regulas (ES) 2019/881 52. pantā;

b) apliecinājuma prasības no 3. pantā minētajiem standartiem, kam IKT izstrādājums vai aizsardzības profils faktiski atbilst, ieskaitot AVA_VAN līmeni;

c) apliecinājuma prasību sīku aprakstu, kā arī sīku informāciju par to, kā izstrādājums atbilst katrai no tām;

d) sertifikāta izdošanas datumu un derīguma termiņu;

e) unikālu sertifikāta identifikatoru.

15. Drošības mērķi iekļauj sertifikācijas ziņojumā vai atsaucas uz to un sniedz tā kopsavilkumu sertifikācijas ziņojumā un iesniedz kopā ar saistīto sertifikācijas ziņojumu publicēšanas nolūkā.

16. Drošības mērķi var cenzēt saskaņā ar VI.2. iedaļu.

17. Ar *EUCC* saistīto zīmi vai marķējumu var iekļaut sertifikācijas ziņojumā saskaņā ar 11. pantā izklāstītajiem noteikumiem un procedūrām.

18. Bibliogrāfijas iedaļā iekļauj atsauces uz visiem dokumentiem, kas izmantoti sertifikācijas ziņojuma izstrādē. Šajā informācijā iekļauj vismaz šādas ziņas:

a) izmantotos drošības izvērtēšanas kritērijus, tehniskos dokumentus un attiecīgās papildu specifikācijas, kā arī to redakcijas numuru;

b) izvērtēšanas tehnisko ziņojumu;

c) attiecīgā gadījumā salikta izvērtējuma izvērtēšanas tehnisko ziņojumu;

d) tehnisko atsauces dokumentāciju;

e) izstrādātāja dokumentāciju, kas izmantota izvērtēšanā.

19. Lai nodrošinātu izvērtējuma atdarināmību, visa minētā dokumentācija ir unikāli jāidentificē, norādot pareizu izdošanas datumu un pareizu redakcijas numuru.

V.2. **Drošības mērķa cenzēšana publicēšanai**

1. Drošības mērķi, kas jāiekļauj vai jānorāda sertifikācijas ziņojumā saskaņā ar VI.1. iedaļas 1. punktu, var cenzēt, izņemot vai pārfrāzējot ar īpašumtiesībām aizsargāto tehnisko informāciju.

2. Pēc cenzēšanas noteiktais drošības mērķis ir tā pilnīgas sākotnējās redakcijas reāls atveidojums. Tas nozīmē, ka cenzētajā drošības mērķī nedrīkst būt izlaista informācija, kas ir nepieciešama, lai izprastu izvērtēšanas objekta drošības īpašības un izvērtēšanas tvērumu.

3. Cenzētā drošības mērķa saturs atbilst šādām minimālajām prasībām:

   a) tā ievads nav cenzēts, jo tas parasti neietver ar īpašumtiesībām aizsargātu informāciju;

   b) cenzētajam drošības mērķim jābūt ar unikālu identifikatoru, kas atšķiras no tā pilnās sākotnējās redakcijas;

   c) izvērtēšanas objekta aprakstu var samazināt, jo tas var ietvert ar īpašumtiesībām aizsargātu un sīku informāciju par izvērtēšanas objekta projektu, ko nevajadzētu publicēt;

   d) izvērtēšanas objekta drošības vides aprakstu (pieņēmumus, apdraudējumus, organizatoriskās drošības politikas) nesamazina, ciktāl šī informācija ir nepieciešama, lai izprastu izvērtēšanas tvērumu;

   e) informāciju par drošības mērķiem nesamazina, jo visa informācija ir jāpublisko, lai saprastu drošības mērķa un izvērtēšanas objekta nolūku;

   f) visas drošības prasības publisko. Lietojuma piezīmēs var sniegt informāciju par to, kā tiek izmantotas 3. pantā minēto vienoto kritēriju funkcionālās prasības, lai izprastu drošības mērķi;

   g) izvērtēšanas objekta kopsavilkuma specifikācija ietver visas izvērtēšanas objekta drošības funkcijas, bet papildu ar īpašumtiesībām aizsargāto informāciju var cenzēt;

   h) iekļauj atsauces uz aizsardzības profiliem, ko piemēro izvērtēšanas objektam;

   i) pamatojumu var cenzēt, lai izņemtu ar īpašumtiesībām aizsargātu informāciju.

4. Pat ja cenzētais drošības mērķis nav oficiāli izvērtēts saskaņā ar 3. pantā minētajiem izvērtēšanas standartiem, sertifikācijas struktūra nodrošina, ka tas atbilst pilnīgajam un izvērtētajam drošības mērķim, un sertifikācijas ziņojumā norāda gan pilno, gan cenzēto drošības mērķi.

VI PIELIKUMS

PROFESIONĀLĀS NOVĒRTĒŠANAS TVĒRUMS UN GRUPAS SASTĀVS

VI.1. **Profesionālās novērtēšanas tvērums**

1. Ir aptverti šādi profesionālās novērtēšanas veidi:

   a) veids. Sertifikācijas struktūra veic sertifikācijas darbības AVA_VAN.3 līmenī;

   b) veids. Sertifikācijas struktūra veic sertifikācijas darbības, kas atticas uz tehnisko jomu, kas I pielikumā uzskaitīta pie jaunākajiem dokumentiem;

   c) veids. Sertifikācijas struktūra veic sertifikācijas darbības virs AVA_VAN.3 līmeņa, izmantojot aizsardzības profilu, kas II vai III pielikumā uzskaitīts pie jaunākajiem dokumentiem.

2. Profesionāli novērtētā sertifikācijas struktūra iesniedz to sertificēto IKT izstrādājumu sarakstu, kuri varētu kandidēt uz profesionālās novērtēšanas grupas veikto izvērtēšanu, saskaņā ar šādiem noteikumiem:

   a) kandidātizstrādājumi aptver sertifikācijas struktūras atļaujas tehnisko tvērumu, un no tiem analizē vismaz divu dažādu izstrādājumu izvērtējumus apliecinājuma līmenī "augsts", izmantojot profesionālo novērtējumu, un vienu aizsardzības profilu, ja sertifikācijas struktūra ir izdevusi sertifikātu apliecinājuma līmenī "augsts";

   b) veida profesionālajai novērtēšanai sertifikācijas struktūra iesniedz vismaz vienu izstrādājumu katrā tehniskajā jomā un katram attiecīgajam *ITSEF*;

   c) veida profesionālai novērtēšanai vismaz vienu kandidātizstrādājumu izvērtē saskaņā ar piemērojamiem un attiecīgiem aizsardzības profiliem.

VI.2. **Profesionālās novērtēšanas grupa**

1. Novērtēšanas grupā ir vismaz divi eksperti, kas katrs izraudzīts no atšķirīgām dažādu dalībvalstu sertifikācijas struktūrām, kuras izsniedz sertifikātus apliecinājuma līmenī "augsts". Ekspertiem jāpierāda attiecīgās speciālās zināšanas par standartiem, kas minēti 3. pantā, un tehniskajiem dokumentiem, kuri ietilpst profesionālās novērtēšanas tvērumā.

2. Regulas (ES) 2019/881 56. panta 6. punktā minētās sertifikātu izdošanas deleģēšanas vai iepriekšēja apstiprinājuma gadījumā eksperts no valsts kiberdrošības sertifikācijas iestādes, kas saistīta ar attiecīgo sertifikācijas struktūru, papildus piedalās ekspertu grupā, kura izraudzīta saskaņā ar šīs iedaļas 1. punktu.

3. 2. veida profesionālajai novērtēšanai grupas dalībniekus izvēlas no sertifikācijas struktūrām, kas ir pilnvarotas attiecīgajā tehniskajā jomā.

4. Katram novērtēšanas grupas dalībniekam ir vismaz divu gadu pieredze sertifikācijas darbību veikšanā sertifikācijas struktūrā;

5. 2. vai 3. veida profesionālās novērtēšanas gadījumā katram novērtēšanas grupas dalībniekam ir vismaz divu gadu pieredze sertifikācijas darbību veikšanā attiecīgajā tehniskajā jomā vai aizsardzības profilā un pierādītas speciālās zināšanas un dalība *ITSEF* atļauju izsniegšanā.

6. Valsts kiberdrošības sertifikācijas iestāde, kas pārrauga un uzrauga profesionāli novērtējamo sertifikācijas struktūru, un vismaz viena valsts kiberdrošības sertifikācijas iestāde, kuras sertifikācijas struktūrai nav jāveic profesionālā novērtēšana, piedalās profesionālajā novērtēšanā kā novērotāja. *ENISA* arī var piedalīties profesionālajā novērtēšanā novērotāja statusā.

7. Profesionāli novērtējamo struktūru iepazīstināta ar profesionālās novērtēšanas grupas sastāvu. Pamatotos gadījumos tā var apstrīdēt profesionālās novērtēšanas grupas sastāvu un lūgt to pārskatīt.

VII PIELIKUMS

EUCC sertifikāta saturs

EUCC sertifikātā ir vismaz:

a) unikāls identifikators, ko noteikusi sertifikācijas struktūra, kas izdod sertifikātu;

b) informācija, kas saistīta ar sertificēto IKT izstrādājumu vai aizsardzības profilu un sertifikāta turētāju un kurā ietilpst:

   1) IKT izstrādājuma vai aizsardzības profila un attiecīgā gadījumā izvērtēšanas objekta nosaukums;

   2) IKT izstrādājuma vai aizsardzības profila un attiecīgā gadījumā izvērtēšanas objekta veids;

   3) IKT izstrādājuma vai aizsardzības profila versija;

   4) sertifikāta turētāja vārds/nosaukums, adrese un kontaktinformācija;

   5) saite uz sertifikāta turētāja tīmekļa vietni, kurā ietverta Regulas (ES) 2019/881 55. pantā minētā papildu kiberdrošības informācija;

c) informācija, kas saistīta ar IKT izstrādājuma vai aizsardzības profila izvērtēšanu un sertificēšanu un kurā ietilpst:

   1) tās sertifikācijas struktūras nosaukums, adrese un kontaktinformācija, kas izdevusi sertifikātu;

   2) tā *ITSEF* nosaukums, kas veicis izvērtēšanu, ja tas atšķiras no sertifikācijas struktūras;

   3) atbildīgās valsts kiberdrošības sertifikācijas iestādes nosaukums;

   4) atsauce uz šo regulu;

   5) atsauce uz sertifikācijas ziņojumu, kas saistīts ar V pielikumā minēto sertifikātu;

   6) piemērojamais apliecinājuma līmenis saskaņā ar 4. pantu;

   7) atsauce uz 3. pantā minēto izvērtēšanā izmantoto standartu redakciju;

   8) saskaņā ar 3. pantā minētajos standartos un VIII pielikumu noteiktā apliecinājuma līmeņa vai paketes identifikācija, arī izmantotie apliecinājuma komponenti un aptvertais AVA_VAN līmenis;

   9) attiecīgā gadījumā atsauce uz vienu vai vairākiem aizsardzības profiliem, kuriem atbilst IKT izstrādājums vai aizsardzības profils;

   10) izdošanas datums;

   11) sertifikāta derīguma termiņš;

d) ar sertifikātu saistītā zīme un marķējums saskaņā ar 11. pantu.

VIII PIELIKUMS

Apliecinājuma paketes deklarācija

1. Pretēji definīcijām vienotajos kritērijos palielinājumu:

a) nedrīkst apzīmēt ar saīsinājumu "+";

b) sīki apraksta visu attiecīgo komponentu sarakstā;

c) sīki izklāsta sertifikācijas ziņojumā.

2. Apliecinājuma līmeni, kas apstiprināts *EUCC* sertifikātā, var papildināt ar izvērtēšanas apliecinājuma līmeni, kā noteikts šīs regulas 3. pantā.

3. Ja apliecinājuma līmenis, kas apstiprināts *EUCC* sertifikātā, neattiecas uz palielinājumu, *EUCC* sertifikātā norāda vienu no šādām paketēm:

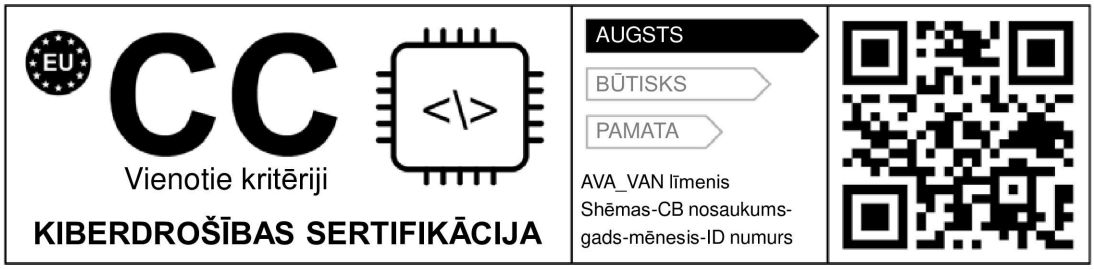
a) "īpašā apliecinājuma pakete";

b) "apliecinājuma pakete, kas atbilst aizsardzības profilam", ja atsaucas uz aizsardzības profilu bez izvērtēšanas apliecinājuma līmeņa.

IX PIELIKUMS

Zīme un marķējums

1. Zīmes un marķējuma attēls:



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

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