2024/2981

4.12.2024.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2024/2981

(2024. gada 28. novembris),

ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes maku sertifikāciju

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regulu (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK ([1]), jo īpaši tās 5.c panta 6. punktu,

tā kā:

(1) Saskaņā ar Regulas (ES) Nr. 910/2014 5.c pantu Eiropas digitālās identitātes maku ("maku") sertificēšana jāveic saskaņā ar funkcionālajām, kiberdrošības un datu aizsardzības prasībām, lai nodrošinātu augstu drošības līmeni un uzticēšanos makiem. Sertifikācijas prasības ir jāsaskaņo visās dalībvalstīs, lai novērstu tirgus sadrumstalotību un izveidotu stabilu satvaru.

(2) Visām šajā regulā paredzētajām personas datu apstrādes darbībām piemēro Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([2]) un, attiecīgā gadījumā, Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([3]).

(3) Komisija regulāri novērtē jaunās tehnoloģijas, praksi, standartus vai tehniskās specifikācijas. Lai nodrošinātu visaugstāko saskaņotības līmeni starp dalībvalstīm attiecībā uz maku izstrādi un sertifikāciju, šajā regulā izklāstīto tehnisko specifikāciju pamatā ir darbs, kas veikts, pamatojoties uz Komisijas 2021. gada 3. jūnija Ieteikumu (ES) 2021/946 par kopīgu Savienības rīkkopu koordinētai pieejai Eiropas digitālās identitātes satvaram ([4]) un jo īpaši arhitektūru un atsauces sistēmu, kas ir daļa no minētās rīkkopas. Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2024/1183 ([5]) 75. apsvērumu Komisijai šī īstenošanas regula būtu jāpārskata un vajadzības gadījumā jāatjaunina, lai tā atbilstu pasaules norisēm, arhitektūrai un atsauces sistēmai un tajā būtu ņemta vērā paraugprakse iekšējā tirgū.

(4) Lai apliecinātu atbilstību sertifikācijas satvarā iekļautajām kiberdrošības prasībām, maka risinājumu sertifikācijas ietvaros attiecīgā gadījumā būtu jāatsaucas uz Eiropas kiberdrošības sertifikācijas shēmām, kas izveidotas saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2019/881 ([6]). Gadījumiem, kad šādu shēmu nav vai tās kiberdrošības prasības aptver daļēji, šajā regulā ir noteiktas vispārīgās prasības, ko piemēro valsts sertifikācijas shēmām un kas aptver funkcionālās, kiberdrošības un datu aizsardzības prasības.

([1]) OV L 257, 28.8.2014., 73. lpp., ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp., ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([4]) OV L 210, 14.6.2021., 51. lpp., ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([5]) Eiropas Parlamenta un Padomes Regula (ES) 2024/1183 (2024. gada 11. aprīlis), ar ko groza Regulu (ES) Nr. 910/2014 attiecībā uz Eiropas digitālās identitātes satvara izveidi (OV L, 2024/1183, 30.4.2024., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([6]) Eiropas Parlamenta un Padomes Regula (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) (OV L 151, 7.6.2019., 15. lpp., ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) Saskaņā ar Regulas (ES) Nr. 910/2014 5.a panta 11. punktu maki ir jāsertificē atbilstoši augstam uzticamības līmenim, kā noteikts Regulā (ES) Nr. 910/2014, kā arī Komisijas Īstenošanas regulā (ES) 2015/1502 ([7]). Vispārējam maka risinājumam ir jāatbilst minētajam uzticamības līmenim. Saskaņā ar šo regulu dažus maka risinājuma komponentus var sertificēt arī tad, ja to uzticamības līmenis ir zemāks, ar nosacījumu, ka tas ir pienācīgi pamatoti un vispārējā risinājuma sasniegtais uzticamības līmenis joprojām ir augsts.

(6) Visām valsts sertifikācijas shēmām būtu jāieceļ shēmas īpašnieks, kas būs atbildīgs par sertifikācijas shēmas izstrādi un uzturēšanu. Shēmas īpašnieks var būt atbilstības novērtēšanas struktūra, valdības struktūra vai iestāde, tirdzniecības asociācija, atbilstības novērtēšanas struktūru grupa vai jebkura attiecīga struktūra, un tā var nebūt tā pati struktūra, kas pārvalda valsts sertifikācijas shēmu.

(7) Sertifikācijas priekšmetam būtu jāietver maka risinājuma programmatūras komponenti, piemēram, maka instance. Lai gan maka drošas kriptogrāfijas lietojumprogramma (*WSCA*), maka drošas kriptogrāfijas ierīce (*WSCD*) un platformas, kurās šīs programmatūras komponenti tiek izmantoti, ir daļa no darbības vides, tomēr sertifikācijas priekšmetā tās būtu jāiekļauj tikai tad, ja tās nodrošina maka risinājums. Citos gadījumos un jo īpaši tad, ja šīs ierīces un platformas nodrošina galalietotāji, pakalpojumu sniedzējiem būtu jāizdara pieņēmumi par maka risinājuma darbības vidi, tajā skaitā par šīm ierīcēm un platformām, un jāīsteno pasākumi, lai apstiprinātu, ka šie pieņēmumi tiek verificēti praksē. Lai ar aparatūru un sistēmas programmatūru, ko izmanto *WSCD* radīto, uzglabāto vai apstrādāto šifrēšanas atslēgu pārvaldībai un aizsardzībai, nodrošinātu kritiski svarīgo aktīvu aizsardzību, *WSCD* ir jāatbilst augstiem sertifikācijas standartiem, kādi atspoguļoti starptautiskajos standartos, piemēram, vienotajiem kritērijiem (*EUCC*), kuri iedibināti ar Komisijas Īstenošanas regulu (ES) 2024/482 ([8]), un vienotajiem kritērijiem, kuri izriet no izvērtējuma atbilstoši EAL4 un progresīvā metodiskā ievainojamības novērtējuma, kas salīdzināms ar AVA_VAN 5. līmeni. Šie sertifikācijas standarti būtu jāizmanto ne vēlāk kā tad, kad tiek veikta maku atbilstības sertifikācija saskaņā ar Eiropas kiberdrošības sertifikācijas shēmu, kura pieņemta saskaņā ar Regulu (ES) 2019/881.

(8) Pilnībā mobilus, drošus un lietotājdraudzīgus makus atbalsta ar standartizētiem un sertificētiem risinājumiem, kas ir noturīgi pret nesankcionētām manipulācijām, piemēram, iegultiem aizsardzības elementiem, tādām ārējām ierīcēm kā viedkartes vai iegultas SIM platformas mobilajās ierīcēs. Ir svarīgi nodrošināt, ka valstu eID līdzekļiem un makiem ir savlaicīga piekļuve iegultajiem aizsardzības elementiem, un koordinēt dalībvalstu centienus šajā jomā. Tāpēc Eiropas digitālās identitātes sadarbības grupai, kas izveidota saskaņā ar Regulas (ES) Nr. 910/2014 46.e panta 1. punktu ("Sadarbības grupa"), šajā nolūkā būtu jāizveido īpaša apakšgrupa. Apspriežoties ar attiecīgajām ieinteresētajām personām, šai apakšgrupai būtu jāvienojas par kopīgu ceļvedi attiecībā uz piekļuvi iegultiem aizsardzības elementiem, un Komisijai šis ceļvedis būtu jāapsver Regulas (ES) Nr. 910/2014 pārskatīšanas ziņojumā. Lai atvieglotu maka apguvi valsts līmenī, Komisijai sadarbībā ar dalībvalstīm būtu arī jāizstrādā un pastāvīgi jāatjaunina lietošanas gadījumu rokasgrāmata kā daļa no arhitektūras un atsauces satvara.

(9) Valsts sertifikācijas shēmu sertifikācijas priekšmetā būtu jāiekļauj arī procesi, ko izmanto maka risinājuma nodrošināšanai un darbībai, pat ja par šo procesu definēšanu vai izpildi ir noslēgts apakšlīgums ar trešām personām. Lai pierādītu, ka procesi atbilst shēmu prasībām, kā pierādījumu ir atļauts izmantot uzticamības informāciju ar noteikumu, ka, lai noteiktu, vai apliecinājuma informācija ir pietiekama, izmanto atkarības analīzi. Uzticamības informācija tiek sniegta daudzās dažādās formās, tajā skaitā ziņojumu un atbilstības sertifikātu veidā, kas var būt privāti, valsts, Eiropas vai starptautiski, pamatojoties uz standartiem vai tehniskajām specifikācijām. Atkarības analīzes mērķis ir novērtēt par maka komponentiem pieejamās uzticamības informācijas kvalitāti.

([7]) Komisijas Īstenošanas regula (ES) 2015/1502 (2015. gada 8. septembris), kas saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 8. panta 3. punktu nosaka elektroniskās identifikācijas līdzekļu uzticamības līmeņu minimālās tehniskās specifikācijas un procedūras (OV L 235, 9.9.2015., 7. lpp., ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

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

(10) Ievērojot šim nolūkam izveidotās procedūras, sadarbības grupai vajadzētu būt iespējai sniegt atzinumus un ieteikumus par tai iesniegtajiem valsts sertifikācijas shēmu projektiem. Šīm valsts sertifikācijas shēmām būtu jābūt atbilstošām maka arhitektūrai, un katrai konkrētajai atbalstītajai arhitektūrai vajadzētu būt īpašiem profiliem.

(11) Lai nodrošinātu vienotu izpratni par visbūtiskākajiem riskiem, kas varētu skart maku nodrošināšanu un darbību, un saskaņotu pieeju to novērtēšanai, būtu jāizveido to risku un apdraudējumu reģistrs, kuri jāņem vērā, izstrādājot maku risinājumus neatkarīgi no to konkrētās arhitektūras. Nosakot, kādi riski būtu jāiekļauj reģistrā, būtu jāņem vērā Regulā (ES) Nr. 910/2014 aprakstītie kiberdrošības mērķi, piemēram, maka risinājuma konfidencialitāte, integritāte un pieejamība, kā arī lietotāju un datu privātums. Valsts sertifikācijas shēmu prasībās būtu pienācīgi jāņem vērā šajā risku reģistrā iekļautie riski un apdraudējumi. Lai nodrošinātu atbilstību pastāvīgi mainīgajai apdraudējumu ainai, sadarbībā ar Sadarbības grupu risku reģistrs būtu jāuztur un regulāri jāatjaunina.

(12) Shēmu īpašniekiem, izveidojot savas sertifikācijas shēmas, būtu jāveic riska novērtējums, lai precizētu un papildinātu reģistrā uzskaitītos riskus un apdraudējumus, iekļaujot riskus un apdraudējumus, kas attiecas uz maka risinājuma arhitektūru vai īstenošanu. Riska novērtējumā būtu jāizvērtē, kā pienācīgi novērst attiecīgos riskus un apdraudējumus. Maka nodrošinātājiem būtu jāpapildina shēmas riska novērtējums, lai apzinātu visus riskus un apdraudējumus, kas raksturīgi to īstenošanai, un jāierosina piemēroti novēršanas pasākumi, kas sertifikācijas struktūrai jāizvērtē.

(13) Lai pierādītu, ka maka risinājuma arhitektūra atbilst piemērojamajām drošības prasībām, katrā arhitektūrai specifiskajā shēmā vai profilā būtu jāietver vismaz maka risinājuma arhitektūras apraksts, maka risinājuma arhitektūrai piemērojamo drošības prasību saraksts, izvērtēšanas plāns nolūkā apstiprināt, ka maka risinājums, kura pamatā ir šī arhitektūra, atbilst minētajām prasībām, un riska novērtējums. Valsts sertifikācijas shēmu ietvaros būtu jānosaka prasība, ka maku nodrošinātājiem jāparāda, kā to nodrošinātais maka risinājums atbilst atsauces arhitektūrai, un sīki jāizklāsta konkrētā maka risinājuma drošības kontroles un validācijas plāni. Valsts sertifikācijas shēmās būtu arī jānosaka atbilstības novērtēšanas darbība, lai verificētu, vai maka koncepcija pienācīgi atspoguļo izvēlētā profila atsauces arhitektūru. Valsts sertifikācijas shēmām būtu jāatbilst prasībām, kas noteiktas Regulas (ES) 2019/881 51. pantā, izņemot tā e) un f) apakšpunktu saistībā ar reģistrēšanu.

(14) Attiecībā uz produktu sertifikāciju būtu jāatļauj izmantot atbilstības sertifikātus, kas izdoti saskaņā ar Eiropas kiberdrošības sertifikācijas shēmu (*EUCC*), un atbilstības sertifikātus, kas izdoti saskaņā ar valsts sertifikācijas shēmām *SOG-IS* Savstarpējās atzīšanas nolīguma kontekstā. Turklāt attiecībā uz mazāk sensitīviem produktu komponentiem būtu jāatļauj izmantot citas valsts sertifikācijas shēmas, piemēram, shēmas, kas izveidotas saskaņā ar standartu CEN EN 17640 attiecībā uz kiberdrošības noteikta laika izvērtēšanas metodiku.

(15) ES digitālās identitātes maka uzticamības marķējums ("uzticamības marķējums") būtu jāizmanto, lai skaidrā, vienkāršā un atpazīstamā veidā norādītu, ka maks tiek nodrošināts saskaņā ar Regulu (ES) Nr. 910/2014. Tāpēc tas būtu jāuzskata par tāda maka risinājuma atbilstības zīmi, kas sertificēts saskaņā ar valsts sertifikācijas shēmām. Valsts sertifikācijas shēmās nebūtu jānosaka citas atbilstības zīmes.

(16) Krāpšanas novēršanas nolūkā valsts sertifikācijas shēmās būtu jānosaka darbības, kādas jāveic, ja nepatiesi tiek apgalvots, ka ir iegūta sertifikācija saskaņā ar shēmu.

(17) Lai nodrošinātu paziņojumu par ievainojamību efektīvu pārvaldību, maka risinājumu un tās elektroniskās identifikācijas shēmas nodrošinātājiem, kuras ietvaros šie risinājumi tiek sniegti, būtu jānosaka un jāīsteno procesi nolūkā novērtēt ievainojamību nopietnību un iespējamo ietekmi. Valsts sertifikācijas shēmās būtu jānosaka robeža, kuras pārsniegšanas gadījumā ir jāziņo sertifikācijas struktūrai. Šādai paziņošanas prasībai nevajadzētu skart kritērijus, kas noteikti datu aizsardzības tiesību aktos un dalībvalstu datu aizsardzības iestādēs attiecībā uz paziņošanu par personas datu aizsardzības pārkāpumiem. Ir iespējams veidot sinerģiju starp obligāto paziņošanu par maka risinājumu aizsardzības pārkāpumiem vai kompromitējumu un paziņošanu par personas datu aizsardzības pārkāpumiem saskaņā ar Regulu (ES) 2016/679. Sertifikācijas struktūras novērtējumam par ievainojamības ietekmes analīzes ziņojumu nevajadzētu skart datu aizsardzības iestādes novērtējumu par ietekmes uz datu aizsardzību novērtējumu saskaņā ar Regulas (ES) 2016/679 35. un 36. pantu.

(18) Maka risinājumu un tās elektroniskās identifikācijas shēmas nodrošinātājiem, saskaņā ar kuru tie tiek nodrošināti, būtu jāpaziņo shēmas īpašniekam visi pamatojumi izņēmumiem ievainojamības novērtējumā, kas vajadzīgi *WSCD* un *WSCA* izvērtēšanai, kā izklāstīts IV pielikumā.

(19) Atbilstības sertifikāta anulēšanai var būt nopietnas sekas, piemēram, visu izvietoto maka vienību atsaukšana. Tāpēc sertifikācijas struktūrām anulēšana būtu jāapsver tikai tad, ja nenovērsta ievainojamība varētu būtiski skart maka risinājuma uzticamību vai cita maka risinājuma uzticamību.

(20) Būtu jāievieš īpašs process valsts sertifikācijas shēmu atjaunināšanai, lai pārvaldītu pāreju starp secīgām shēmu versijām, jo īpaši attiecībā uz darbībām, kas sertifikāta turētājam jāveic saistībā ar gaidāmu izvērtēšanu, uzturēšanu, resertifikāciju un īpašu izvērtēšanu.

(21) Lai veicinātu pārredzamību, maku nodrošinātājiem būtu jāpublisko drošības informācija par savu maka risinājumu.

(22) Ja valsts sertifikācijas shēmas balstās uz uzticamības informāciju no citām sertifikācijas shēmām vai avotiem, būtu jāveic atkarības analīze, lai verificētu uzticamības dokumentācijas, piemēram, uzticamības ziņojumu un atbilstības sertifikātu, pieejamību un piemērotību maka risinājumiem un elektroniskās identifikācijas shēmai, saskaņā ar kuru tie tiek nodrošināti. Šīs atkarības analīzes pamatā vajadzētu būt maka risinājumu un elektroniskās identifikācijas shēmas, saskaņā ar kuru tie tiek nodrošināti, riska novērtējumam. Izvērtēšanā būtu jānosaka, vai par attiecīgo maka risinājumu pieejamā uzticamības dokumentācija un elektroniskās identifikācijas shēma, saskaņā ar kuru tas tiek nodrošināts, ir pietiekama, lai nodrošinātu uzticamību, kas atbilst vēlamajam izvērtēšanas līmenim. Veicot izvērtēšanu, būtu arī jāatjaunina atkarības analīze vai vajadzības gadījumā jāveic atkārtota izsmeļoša atkarības izvērtēšana.

(23) Sertifikācijas struktūrām būtu jāizdod atbilstības sertifikāti valsts sertifikācijas shēmu ietvaros kopā ar publiski pieejamu sertifikācijas ziņojumu, kā minēts Regulas (ES) Nr. 910/2014 5.d panta 2. punkta a) apakšpunktā. Saistītais sertifikācijas novērtējuma ziņojums būtu jādara pieejams Sadarbības grupai.

(24) Valsts sertifikācijas shēmās būtu jāparedz ikgadēja uzraudzības izvērtēšana, lai nodrošinātu, ka ar maku pārvaldību un uzturēšanu saistītie procesi darbojas rezultatīvi, proti, tie darbojas atbilstīgi procedūrām, ar kurām nosaka procesus. Ik pēc diviem gadiem veicamais ievainojamības novērtējums ir prasība, kas izriet no Regulas (ES) Nr. 910/2014, lai nodrošinātu, ka maka risinājums turpina pienācīgi aptvert risku reģistrā identificētos kiberdrošības riskus un apdraudējumus, tajā skaitā jebkādu apdraudējumu ainas attīstību. Uzraudzības izvērtēšanas, resertifikācijas izvērtēšanas un īpašas izvērtēšanas jēdzieniem būtu jāatbilst standartam EN ISO/IEC 17021-1:2015.

(25) Sertifikācijas cikls noslēdzas ar atbilstības sertifikāta termiņa beigām vai ar jauna atbilstības sertifikāta izdošanu pēc resertifikācijas izvērtēšanas sekmīga noslēguma. Resertifikācijas izvērtēšanā būtu jāiekļauj visu sertifikācijas priekšmeta komponentu izvērtēšana, tajā skaitā efektivitātes izvērtēšana un attiecīgā gadījumā ievainojamības novērtējums. Resertifikācijas laikā vajadzētu būt iespējai atkārtoti izmantot iepriekšējo izvērtēšanu rezultātus attiecībā uz komponentiem, kas nav mainījušies.

(26) Pēc Eiropas kiberdrošības sertifikācijas shēmas pieņemšanas valsts sertifikācijas shēmām ar tādu pašu tvērumu pēc noteikta pārejas perioda būtu jāpārtrauc sertifikātu izdošana, kā minēts Regulas (ES) 2019/881 57. panta 1. punktā.

(27) Lai nodrošinātu saskaņotību un sadarbspēju, valsts sertifikācijas shēmām attiecīgā gadījumā būtu jābalstās uz esošajiem satvariem un atkārtoti jāizmanto pierādījumi. Dalībvalstis var slēgt nolīgumus par sertifikācijas shēmu vai to daļu pārrobežu atkalizmantošanu. Eiropas Komisijai un *ENISA* kopā ar Sadarbības grupu būtu jāatbalsta dalībvalstis to valsts sertifikācijas shēmu izstrādē un uzturēšanā, nodrošinot zināšanu apmaiņu un paraugpraksi.

(28) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([9]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2024. gada 30. septembrī sniedza atzinumu.

(29) Šajā regulā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi Regulas (ES) Nr. 910/2014 48. panta 1. punktā minētā komiteja,

IR PIEŅĒMUSI ŠO REGULU.

I NODAĻA

VISPĀRĪGIE NOTEIKUMI

1. pants

Priekšmets un darbības joma

Šajā regulā ir aprakstīti atsauces standarti un noteiktas specifikācijas un procedūras ar nolūku izveidot stabilu maku sertifikācijas satvaru, kas regulāri jāatjaunina, lai nodrošinātu atbilstību tehnoloģiju un standartu pārmaiņām un ņemtu vērā darbu, kas veikts, pamatojoties uz Komisijas Ieteikumu (ES) 2021/946 par kopīgu Savienības rīkkopu koordinētai pieejai Eiropas digitālās identitātes satvaram, un jo īpaši arhitektūru un atsauces sistēmu.

2. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "maka risinājums" ir programmatūras, aparatūras, pakalpojumu, iestatījumu un konfigurāciju kombinācija, kas ietver maka instances, vienu vai vairākas maka drošas kriptogrāfijas lietojumprogrammas un vienu vai vairākas maka drošas kriptogrāfijas ierīces;

2) "shēmas īpašnieks" ir organizācija, kas ir atbildīga par sertifikācijas shēmas izstrādi un uzturēšanu;

3) "sertifikācijas priekšmets" ir produkti, procesi un pakalpojumi vai to kombinācija, uz ko attiecas noteiktas prasības;

4) "maka drošas kriptogrāfijas lietojumprogramma" ir lietojumprogramma, kura sasaistē ar kriptogrāfiskām un nekriptogrāfiskām funkcijām, ko nodrošina maka drošas kriptogrāfijas ierīce, un, izmantojot šīs funkcijas, pārvalda kritiski svarīgus aktīvus;

5) "maka instance" ir lietojumprogramma, kas uzstādīta un konfigurēta maka lietotāja ierīcē vai vidē, tā ir daļa no maka vienības un maka lietotājs to izmanto, lai mijiedarbotos ar maka vienību;

([9]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

6) “maka drošas kriptogrāfijas ierīce” ir pret nesankcionētām manipulācijām noturīga ierīce, kas nodrošina vidi, kura ir sasaistīta ar maka drošas kriptogrāfijas lietojumprogrammu, kas šo vidi izmanto, lai aizsargātu kritiski svarīgus aktīvus un nodrošinātu kriptogrāfijas funkcijas kritiski svarīgu operāciju drošai izpildei;

7) “risku reģistrs” ir tādas informācijas reģistrs, kura attiecas uz apzinātajiem riskiem un ir būtiska sertifikācijas procesam;

8) “maka nodrošinātājs” ir fiziska vai juridiska persona, kas nodrošina maka risinājumus;

9) “sertifikācijas struktūra” ir atbilstības novērtēšanas struktūra, kas ir trešā persona un kas īsteno sertifikācijas shēmas;

10) “maka vienība” ir maka risinājuma unikāla konfigurācija, kas ietver maka instances, maka drošas kriptogrāfijas lietojumprogrammas un maka drošas kriptogrāfijas ierīces, ko maka nodrošinātājs nodrošina individuālam maka lietotājam;

11) “kritiski svarīgi aktīvi” ir aktīvi maka vienībā vai saistībā ar to, kas ir tik ārkārtīgi svarīgi, ka, ja to pieejamība, konfidencialitāte vai integritāte tiktu kompromitēta, tas ļoti nopietni un negatīvi ietekmētu spēju paļauties uz maka vienību;

12) “maka lietotājs” ir lietotājs, kas kontrolē maka vienību;

13) “incidents” ir incidents, kas definēts Eiropas Parlamenta un Padomes Direktīvas (ES) 2022/2555 ([10]) 6. panta 6. punktā;

14) “iegultā informācijas izpaušanas procedūra” ir noteikumu kopums, kuru atribūtu elektroniskajā apliecinājumā iegūlis tā izsniedzējs un kurā norādīti nosacījumi, kas maka atkarīgajai pusei ir jāizpilda, lai piekļūtu atribūtu elektroniskajam apliecinājumam.

II NODAĻA

VALSTS SERTIFIKĀCIJAS SHĒMAS

3. pants

Valsts sertifikācijas shēmu izveide

1. Dalībvalstis katrai valsts sertifikācijas shēmai norīko shēmas īpašnieku.

2. Valsts sertifikācijas shēmās noteiktais sertifikācijas priekšmets ir maka risinājumu un to elektroniskās identifikācijas shēmu nodrošināšana un darbība, saskaņā ar kurām tie tiek nodrošināti.

3. Saskaņā ar Īstenošanas regulu (ES) 2015/1502 valsts sertifikācijas shēmu sertifikācijas priekšmets ietver šādus elementus:

a) programmatūras komponenti, tajā skaitā maka risinājuma un tās elektroniskās identifikācijas shēmas iestatījumi un konfigurācijas, saskaņā ar kuru maka risinājumi tiek nodrošināti;

b) aparatūras komponenti un platformas, kuros darbojas vai uz kuriem balstās b) punktā minētās programmatūras komponenti kritiski svarīgu operāciju veikšanai gadījumos, kad tos tieši vai netieši nodrošina maka risinājums un elektroniskās identifikācijas shēma, saskaņā ar kuru tas tiek nodrošināts, un ja tie ir nepieciešami, lai panāktu šo programmatūras komponentu vēlamo uzticamības līmeni. Ja maka nodrošinātājs nenodrošina aparatūras komponentus un platformas, valsts sertifikācijas shēmas šai aparatūras komponentu un platformu izvērtēšanai formulē pieņēmumus, saskaņā ar kuriem var nodrošināt noturību pret uzbrucējiem ar augstu uzbrukuma potenciālu saskaņā ar Īstenošanas regulu (ES) 2015/1502, un precizē izvērtēšanas darbības šo pieņēmumu apstiprināšanai, kā minēts IV pielikumā;

([10]) 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., ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

c) procesi, kas atbalsta maka risinājuma nodrošināšanu un darbību, tajā skaitā lietotāju pievienošanas process, kā minēts Regulas (ES) Nr. 910/2014 5.a pantā, aptverot vismaz reģistrāciju, elektronisko līdzekļu pārvaldību un organizāciju saskaņā ar Īstenošanas regulas (ES) 2015/1502 I pielikuma 2.1., 2.2. un 2.4. iedaļu.

4. Valsts sertifikācijas shēmās iekļauj maka risinājuma konkrētās arhitektūras aprakstu un elektroniskās identifikācijas shēmas aprakstu, saskaņā ar kuru tas tiek nodrošināts. Ja valsts sertifikācijas shēmas aptver vairāk nekā vienu konkrētu arhitektūru, tajās iekļauj katras konkrētās arhitektūras profilu.

5. Attiecībā uz katru profilu valsts sertifikācijas shēmās norāda vismaz šādu informāciju:

a) maka risinājuma un tās elektroniskās identifikācijas shēmas īpašo arhitektūru, saskaņā ar kuru tas tiek nodrošināts;

b) drošības kontroles, kas saistītas ar Regulas (ES) Nr. 910/2014 8. pantā noteiktajiem uzticamības līmeņiem;

c) izvērtēšanas plānu, kas izstrādāts saskaņā ar 7.4.1. iedaļu standartā EN ISO/IEC 17065:2012;

d) drošības prasības, kas vajadzīgas, lai risinātu kiberdrošības riskus un apdraudējumus, kuri uzskaitīti šīs regulas I pielikumā paredzētajā risku reģistrā, nodrošinot prasīto uzticamības līmeni, un lai attiecīgā gadījumā sasniegtu Regulas (ES) 2019/881 51. pantā noteiktos mērķus;

e) šā punkta b) apakšpunktā minēto kontroļu kartēšanu atbilstīgi arhitektūras komponentiem;

f) aprakstu par to, kā b) līdz c) apakšpunktā minētās drošības kontroles, kartēšana, drošības prasības un izvērtēšanas plāns ļauj maka risinājumu un tās elektroniskās identifikācijas shēmas nodrošinātājiem, saskaņā ar kuru tie tiek nodrošināti, pienācīgi novērst kiberdrošības riskus un apdraudējumus, kas uzskaitīti d) apakšpunktā minētajā risku reģistrā, nodrošinot nepieciešamo uzticamības līmeni, pamatojoties uz riska novērtējumu, lai risku reģistrā uzskaitītos riskus un apdraudējumus precizētu un papildinātu ar arhitektūrai specifiskiem riskiem un apdraudējumiem.

6. Panta 5. punkta c) apakšpunktā minētajā izvērtēšanas plānā uzskaita izvērtēšanas darbības, kas jāiekļauj maka risinājumu un tās elektroniskās identifikācijas shēmas izvērtēšanā, saskaņā ar kuru tas tiek nodrošināts.

7. Panta 6. punktā minētā izvērtēšanas darbība paredz, ka maka risinājumu un tās elektroniskās identifikācijas shēmas nodrošinātājiem, saskaņā ar kuru tie tiek nodrošināti, jāsniedz informācija, kas atbilst II pielikumā uzskaitītajām prasībām.

4. pants

Vispārīgās prasības

1. Valsts sertifikācijas shēmas aptver funkcionālās, kiberdrošības un datu aizsardzības prasības, un, ja ir pieejamas un piemērojamas, izmanto šādas sertifikācijas shēmas:

a) Eiropas kiberdrošības sertifikācijas shēmas, kas izveidotas saskaņā ar Regulu (ES) 2019/881, tajā skaitā *EUCC*;

b) valsts kiberdrošības sertifikācijas shēmas, uz kurām attiecas *EUCC*, saskaņā ar Īstenošanas regulas (ES) 2024/482 49. pantu.

2. Valsts sertifikācijas shēmās papildus var atsaukties uz šādām shēmām (ja tās ir pieejamas un piemērojamas):

a) citām attiecīgām valsts sertifikācijas shēmām;

b) starptautiskiem, Eiropas un valstu standartiem;

c) tehniskām specifikācijām, kas atbilst Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1025/2012 ([11]) II pielikumā izklāstītajām prasībām.

3. Valsts sertifikācijas shēmas:

a) norāda EN ISO/IEC 17067:2013 6.5. iedaļā uzskaitītos elementus;

b) īsteno kā 6. tipa shēmu saskaņā ar standarta EN ISO/IEC 17067:2013 5.3.8. iedaļu.

4. Valsts sertifikācijas shēmas atbilst šādām prasībām:

a) saskaņā ar valsts sertifikācijas shēmām saņemt sertifikātus ir tiesīgi tikai Regulas (ES) Nr. 910/2014 5.a panta 2. punktā minētie nodrošinātāji;

b) par atbilstības zīmi izmanto tikai uzticamības marķējumu;

c) maka risinājumu un tās elektroniskās identifikācijas shēmas nodrošinātāji, saskaņā ar kuru tie tiek nodrošināti, atsaucoties uz shēmu, ietver atsauces uz Regulu (ES) Nr. 910/2014 un šo regulu;

d) maka risinājumu un tās elektroniskās identifikācijas shēmas nodrošinātāji, saskaņā ar kuru tie tiek nodrošināti, papildina shēmas riska novērtējumu, kā minēts 3. panta 5. punkta f) apakšpunktā, lai identificētu riskus un apdraudējumus, kas raksturīgi to īstenošanai, un ierosinātu atbilstošus visu attiecīgo risku un apdraudējumu novēršanas pasākumus;

e) ir noteikti pienākumi un tiesiskās darbības, un tie ietver atsauces uz piemērojamiem valsts tiesību aktiem, kuros noteikti pienākumi un iespējamās tiesiskās darbības gadījumos, kad sertifikācija saskaņā ar shēmu tiek izmantota krāpnieciski.

5. Šā panta 4. punkta d) apakšpunktā minēto novērtējumu dara zināmu sertifikācijas struktūrai izvērtēšanai.

5. pants

Incidentu un ievainojamības pārvaldība

1. Valsts sertifikācijas shēmas ietver incidentu un ievainojamības pārvaldības prasības saskaņā ar 2.–9. punktu.

2. Maka risinājuma un tās elektroniskās identifikācijas shēmas atbilstības sertifikāta turētājs, saskaņā ar kuru tas tiek nodrošināts, bez liekas kavēšanās paziņo savai sertifikācijas struktūrai par jebkādiem maka risinājuma vai elektroniskās identifikācijas shēmas, saskaņā ar kuru tas tiek nodrošināts, drošības pārkāpumiem vai kompromitējumiem, kas varētu ietekmēt tā atbilstību valsts sertifikācijas shēmas prasībām.

3. Atbilstības sertifikāta turētājs izstrādā, uztur un īsteno ievainojamības pārvaldības politiku un procedūras, ņemot vērā procedūras, kas izklāstītas spēkā esošajos Eiropas un starptautiskajos standartos, to vidū EN ISO/IEC 30111:2019.

4. Atbilstības sertifikāta turētājs paziņo izdevējai sertifikācijas struktūrai par ievainojamībām un izmaiņām, kas skar maka risinājumu, pamatojoties uz noteiktiem kritērijiem par šo ievainojamību un izmaiņu ietekmi.

5. Atbilstības sertifikāta turētājs sagatavo ievainojamības ietekmes analīzes ziņojumu par jebkuru ievainojamību, kas skar maka risinājuma programmatūras komponentus. Ziņojumā norāda šādu informāciju:

a) ievainojamības ietekme uz sertificēto maka risinājumu;

b) iespējamie riski, kas saistīti ar uzbrukuma tuvumu vai varbūtību;

([11]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1025/2012 (2012. gada 25. oktobris) par Eiropas standartizāciju, ar ko groza Padomes Direktīvas 89/686/EEK un 93/15/EEK un Eiropas Parlamenta un Padomes Direktīvas 94/9/EK, 94/25/EK, 95/16/EK, 97/23/EK, 98/34/EK, 2004/22/EK, 2007/23/EK, 2009/23/EK un 2009/105/EK, un ar ko atceļ Padomes Lēmumu 87/95/EEK un Eiropas Parlamenta un Padomes Lēmumu Nr. 1673/2006/EK (OV L 316, 14.11.2012., 12. lpp., ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

c) to, vai ievainojamību var novērst ar pieejamajiem līdzekļiem;

d) ja ievainojamību var novērst ar pieejamajiem līdzekļiem, – iespējamie veidi, kā ievainojamību novērst.

6. Ja 4. punktā ir prasīta paziņošana, atbilstības sertifikāta turētājs bez liekas kavēšanās sertifikācijas struktūrai nosūta 5. punktā minēto ievainojamības ietekmes analīzes ziņojumu.

7. Atbilstības sertifikāta turētājs izstrādā, uztur un īsteno ievainojamības pārvaldības politiku, kas atbilst Kibernoturības akta ([12]) I pielikumā noteiktajām prasībām.

8. Valsts sertifikācijas shēmas nosaka ievainojamības atklāšanas prasības, kas piemērojamas sertifikācijas struktūrām.

9. Atbilstības sertifikāta turētājs atklāj un reģistrē visas publiski zināmās un novērstās ievainojamības maka risinājumā vai kādā no V pielikumā minētajiem tiešsaistes repozitorijiem.

6. pants

Valsts sertifikācijas shēmu uzturēšana

1. Valsts sertifikācijas shēmās iekļauj procedūru to darbības periodiskai pārskatīšanai. Minētās procedūras mērķis ir apstiprināt to atbilstību un apzināt aspektus, kas jāuzlabo, ņemot vērā ieinteresēto personu atsauksmes.

2. Valsts sertifikācijas shēmās iekļauj noteikumus par to uzturēšanu. Šī procedūra ietver vismaz šādas prasības:

a) noteikumus par valsts sertifikācijas shēmu noteikšanas un prasību pārvaldību;

b) sertifikātu izdošanas termiņu noteikšanu pēc valstu sertifikācijas shēmu atjauninātu versiju pieņemšanas gan attiecībā uz jauniem, gan iepriekš izdotiem atbilstības sertifikātiem;

c) valsts sertifikācijas shēmu periodisku pārskatīšanu, lai nodrošinātu, ka valsts sertifikācijas shēmu prasības tiek piemērotas konsekventi, ņemot vērā vismaz šādus aspektus:

— shēmas īpašniekam adresētus pieprasījumus veikt precizējumus saistībā ar valsts sertifikācijas shēmas prasībām,

— atsauksmes no ieinteresētajām personām un citām ieinteresētajām pusēm,

— valsts sertifikācijas shēmas īpašnieka atsaucību uz informācijas pieprasījumiem;

d) noteikumus par atsauces dokumentu un procedūru pārraudzību attiecībā uz valsts sertifikācijas shēmu atsauces versiju izstrādi, iekļaujot vismaz pārejas periodus;

e) procedūru, ar ko nodrošina, ka tiek aptverti jaunākie kiberdrošības riski un apdraudējumi, kuri uzskaitīti šīs regulas I pielikumā noteiktajā risku reģistrā;

f) procedūru citu izmaiņu pārvaldībai valsts sertifikācijas shēmās.

([12]) Eiropas Parlamenta un Padomes Regula (ES) 2024/2847 (2024. gada 23. oktobris) par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulas (ES) Nr. 168/2013 un (ES) 2019/1020 un Direktīvu (ES) 2020/1828 (Kibernoturības akts) (OV L, 2024/2847, 20.11.2024., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. Valsts sertifikācijas shēmās ietver prasības veikt patlaban sertificēto produktu izvērtēšanu noteiktā laikposmā pēc shēmas pārskatīšanas vai pēc tādu jaunu specifikāciju vai standartu, vai to jaunu versiju publiskošanas, kurām maka risinājumiem un elektroniskās identifikācijas shēmai, saskaņā ar kuru tie tiek nodrošināti, ir jāatbilst.

III NODAĻA

PRASĪBAS ATTIECĪBĀ UZ SHĒMU ĪPAŠNIEKIEM

7. pants

Vispārīgās prasības

1. Shēmu īpašnieki izstrādā un uztur valsts sertifikācijas shēmas un pārvalda to darbību.

2. Shēmas īpašnieki var slēgt apakšuzņēmuma līgumus ar trešām personām par visiem vai daļu no saviem uzdevumiem. Slēdzot apakšuzņēmuma līgumus ar privātpersonu, shēmas īpašnieki, pamatojoties uz līgumu, nosaka visu pušu pienākumus un atbildību. Shēmu īpašnieki joprojām ir atbildīgi par visām darbībām, par kurām to apakšuzņēmēji slēdz apakšuzņēmuma līgumus.

3. Shēmu īpašnieki attiecīgā gadījumā veic pārraudzības darbības, pamatojoties vismaz uz šādu informāciju:

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) sūdzībām un pārsūdzībām, kas saņemtas saskaņā ar 15. pantu.

4. Shēmu īpašnieki informē Sadarbības grupu par valsts sertifikācijas shēmu pārskatīšanu. Minētajā paziņojumā Sadarbības grupai sniedz pietiekamu informāciju, lai tā varētu sniegt ieteikumus shēmu īpašniekiem un atzinumus par atjauninātajām valsts sertifikācijas shēmām.

IV NODAĻA

PRASĪBAS ATTIECĪBĀ UZ MAKA RISINĀJUMU UN TĀS ELEKTRONISKĀS IDENTIFIKĀCIJAS SHĒMAS NODROŠINĀTĀJIEM, SASKAŅĀ AR KURU TIE TIEK NODROŠINĀTI

8. pants

Vispārīgās prasības

1. Valsts sertifikācijas shēmas ietver kiberdrošības prasības, kuru pamatā ir katras konkrētās atbalstītās arhitektūras analīze. Minēto kiberdrošības prasību mērķis ir novērst apzinātos kiberdrošības riskus un apdraudējumus, kā noteikts I pielikumā izklāstītajā risku reģistrā.

2. Saskaņā ar Regulas (ES) Nr. 910/2014 5.a panta 23. punktu valsts sertifikācijas shēmās ir noteikta prasība, ka maku risinājumiem un elektroniskās identifikācijas shēmām, saskaņā ar kurām tie tiek nodrošināti, jābūt noturīgiem pret uzbrucējiem ar augstu uzbrukuma potenciālu, nodrošinot uzticamības līmeni "augsts", kā minēts Īstenošanas regulā (ES) 2015/1502.

3. Valsts sertifikācijas shēmas nosaka drošības kritērijus, kas ietver šādas prasības:

a) attiecīgā gadījumā – Kibernoturības akts vai prasības, kas atbilst Regulas (ES) 2019/881 51. pantā noteiktajiem drošības mērķiem;

b) politikas un procedūru izstrāde un īstenošana attiecībā uz to risku pārvaldību, kas saistīti ar maka risinājuma darbību, ieskaitot risku apzināšanu un novērtēšanu un apzināto risku mazināšanu;

c) tādas politikas un procedūru izveide un īstenošana, kas saistītas ar izmaiņu pārvaldību un ievainojamību pārvaldību saskaņā ar šīs regulas 5. pantu;

d) cilvēkresursu pārvaldības politikas un procedūru izstrāde un īstenošana, ieskaitot prasības attiecībā uz maka risinājuma izstrādē vai darbībā iesaistītā personāla kompetenci, uzticamību, pieredzi, apmācību drošības jomā un kvalifikāciju;

e) prasības attiecībā uz maka risinājuma darbības vidi, arī pieņēmumu veidā par to ierīču un platformu drošību, kurās darbojas maka risinājuma programmatūras komponenti, arī par *WSCD*, un attiecīgā gadījumā atbilstības novērtēšanas prasības nolūkā apstiprināt, ka minētie pieņēmumi ir verificēti attiecīgajās ierīcēs un platformās;

f) par katru pieņēmumu, kas nav pamatots ar atbilstības sertifikātu vai citu pieņemamu uzticamības informāciju, – tā mehānisma apraksts, ko maka nodrošinātājs izmanto, lai panāktu pieņēmuma izpildi, kā arī pamatojums, ka ar mehānismu pietiek, lai nodrošinātu pieņēmuma verifikāciju;

g) pasākumu noteikšana un īstenošana, lai nodrošinātu, ka tiek izmantota patlaban sertificēta maka risinājuma versija.

4. Valsts sertifikācijas shēmas ietver funkcionālās prasības attiecībā uz atjaunināšanas mehānismiem katram maka risinājumu programmatūras komponentam un elektroniskās identifikācijas shēmai, saskaņā ar kuru maka risinājumi tiek nodrošināti, saistībā ar III pielikumā uzskaitītajām darbībām.

5. Valsts sertifikācijas shēmās ir noteikta prasība, ka sertifikācijas pieteikuma iesniedzējam sertifikācijas struktūrai jāsniedz vai citādi jādara pieejama šāda informācija un dokumentācija:

a) pierādījumi, kas saistīti ar IV pielikuma 1. punktā minēto informāciju, un vajadzības gadījumā arī ziņas par maka risinājumu un tā pirmkodu, ieskaitot:

— *arhitektūras informāciju*: par katru maka risinājuma komponentu (ieskaitot produktu, procesu un pakalpojumu komponentus) – tā būtisko drošības īpašību apraksts, ieskaitot ārējās atkarības,

— *kontroles un uzticamības līmeņus*: par katru maka risinājuma drošības kontroli – kontroles apraksts un nepieciešamais uzticamības līmenis, pamatojoties uz Īstenošanas regulas (ES) 2015/1502 pielikumu, kurā izklāstītas vairākas tehniskās specifikācijas un procedūras, kas attiecas uz dažādām kontrolēm, kuras īsteno ar elektroniskās identifikācijas līdzekļiem,

— *kontroļu kartēšanu atbilstoši arhitektūras komponentiem*: apraksts par to, kā ar dažādiem maka risinājuma komponentiem tiek īstenotas maka kontroles, pamatojoties uz argumentāciju, kāpēc ir nepieciešams konkrēts uzticamības līmenis, un kā kontrole tiek īstenota ar visiem nepieciešamajiem drošības aspektiem attiecīgajā līmenī,

— *riska seguma pamatojumu un argumentāciju*: pamatojums attiecībā uz:

— kontroļu kartēšanu atbilstoši to komponentiem,

— ierosinātā izvērtēšanas plāna piemērotību pienācīgi aptvert visas kontroles,

— kontroļu nodrošināto tvērumu attiecībā uz riska reģistrā identificētajiem kiberdrošības riskiem un apdraudējumiem, ko papildina ar īstenošanai specifisko risku un apdraudējumu kontrolēm, atbilstošā uzticamības līmenī.

b) V pielikumā minētā informācija;

c) pilnīgs saraksts ar atbilstības sertifikātiem un citu uzticamības informāciju, kas izmantota kā pierādījums izvērtēšanas darbībās;

d) jebkāda cita informācija, kas attiecas uz izvērtēšanas darbībām.

V NODAĻA

PRASĪBAS ATTIECĪBĀ UZ SERTIFIKĀCIJAS STRUKTŪRĀM

9. pants

Vispārīgās prasības

1. Sertifikācijas struktūras saņem akreditāciju no valsts akreditācijas struktūrām, kas ieceltas saskaņā ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 765/2008 ([13]), saskaņā ar EN ISO/IEC 17065:2012, ar noteikumu, ka tās atbilst prasībām, kuras noteiktas valsts sertifikācijas shēmās saskaņā ar 2. punktu.

2. Akreditācijas nolūkā sertifikācijas struktūras atbilst visām turpmākajām kompetences prasībām:

a) detalizētas un tehniskas zināšanas par maka risinājuma attiecīgajām arhitektūrām un par elektroniskās identifikācijas shēmu, saskaņā ar kuru tās tiek nodrošinātas, kā arī par apdraudējumiem un riskiem, kas attiecas uz minētajām arhitektūrām;

b) zināšanas par pieejamajiem drošības risinājumiem un to īpašībām saskaņā ar Īstenošanas regulas (ES) 2015/1502 pielikumu;

c) zināšanas par darbībām, kas veiktas, pamatojoties uz atbilstības sertifikātiem, kurus piemēro maka risinājuma komponentiem un elektroniskās identifikācijas shēmai, saskaņā ar kuru tie tiek nodrošināti, kā sertifikācijas priekšmetam;

d) detalizētas zināšanas par piemērojamo valsts sertifikācijas shēmu, kas izveidota saskaņā ar II nodaļu.

3. Sertifikācijas struktūras veic uzraudzības darbības, jo īpaši pamatojoties uz šādu informāciju:

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

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

c) sūdzībām un pārsūdzībām, kas saņemtas saskaņā ar 15. pantu.

10. pants

Apakšuzņēmumu līgumu slēgšana

Sertifikācijas struktūras var slēgt apakšuzņēmuma līgumus ar trešām personām par izvērtēšanas darbībām, kā noteikts 13. pantā. Ja par izvērtēšanas darbībām ir noslēgti apakšuzņēmuma līgumi, valsts sertifikācijas shēmas nosaka:

1) ka visi tās sertifikācijas struktūras apakšuzņēmēji, kas veic izvērtēšanas darbības, attiecīgā gadījumā un atbilstoši veicamajām darbībām atbilst tādu saskaņoto standartu prasībām kā EN ISO/IEC 17025:2017 attiecībā uz testēšanu, EN ISO/IEC 17020:2012 attiecībā uz inspekciju, EN ISO/IEC 17021-1:2015 attiecībā uz revīziju un EN ISO/IEC 17029:2019 attiecībā uz validēšanu un verifikāciju;

2) ka sertifikācijas struktūras uzņemas atbildību par visām izvērtēšanas darbībām, kas uzticētas citām struktūrām, un pierāda, ka akreditācijas laikā tās ir veikušas atbilstīgus pasākumus, attiecīgā gadījumā arī paļaujoties uz pašu apakšuzņēmēju akreditāciju;

3) cik lielā mērā ārpakalpojumu vajadzībām ir jāsaņem iepriekšēja piekrišana no shēmas īpašniekiem vai klienta, kura maka risinājums tiek sertificēts saskaņā ar sertifikācijas shēmu.

([13]) Eiropas Parlamenta un Padomes Regula (EK) Nr. 765/2008 (2008. gada 9. jūlijs), ar ko nosaka akreditācijas un tirgus uzraudzības prasības attiecībā uz produktu tirdzniecību un atceļ Regulu (EEK) Nr. 339/93 (OV L 218, 13.8.2008., 30. lpp., ELI: http://data.europa.eu/eli/reg/2008/765/oj).

11. pants

Paziņošana uzraudzības iestādei

Sertifikācijas struktūras paziņo Regulas (ES) Nr. 910/2014 46.a panta 1. punktā minētajai uzraudzības iestādei par to, ka tās izdod, aptur un anulē atbilstības sertifikātus maka risinājumiem un elektroniskās identifikācijas shēmai, saskaņā ar kuru tie tiek nodrošināti.

12. pants

Incidentu un ievainojamības pārvaldība

1. Sertifikācijas struktūras bez liekas kavēšanās aptur atbilstības sertifikātu maka risinājumiem un elektroniskās identifikācijas shēmai, saskaņā ar kuru tie tiek nodrošināti, pēc tam, kad struktūra, kurai incidents vai ievainojamība tika paziņota, ir apstiprinājusi maka risinājuma vai elektroniskās identifikācijas shēmas, saskaņā ar kuru tas tiek nodrošināts, drošības pārkāpumu vai kompromitējumu, kas ietekmē tā atbilstību valsts sertifikācijas shēmu prasībām.

2. Sertifikācijas struktūras anulē atbilstības sertifikātu, kas apturēts laikus nenovērsta drošības pārkāpuma vai kompromitējuma dēļ.

3. Sertifikācijas struktūras saskaņā ar Regulas (ES) Nr. 910/2014 5.c panta 4. punktu un 5.e panta 2. punktu anulē atbilstības sertifikātus, ja identificētā ievainojamība nav laikus novērsta atbilstoši tās nopietnībai un iespējamajai ietekmei.

VI NODAĻA

ATBILSTĪBAS NOVĒRTĒŠANAS DARBĪBAS

13. pants

Izvērtēšanas darbības

1. Valsts sertifikācijas shēmās ietver metodes un procedūras, kas atbilstības novērtēšanas struktūrām jāizmanto, veicot izvērtēšanas darbības saskaņā ar EN ISO/IEC 17065:2012, un kas aptver vismaz šādus aspektus:

a) metodes un procedūras izvērtēšanas darbību veikšanai, to vidū tās, kas saistītas ar *WSCD*, kā izklāstīts IV pielikumā;

b) maka risinājuma un tās elektroniskās identifikācijas shēmas, īstenošanas revīzija, saskaņā ar kuru tas tiek nodrošināts, pamatojoties uz riska reģistru, kas izklāstīts I pielikumā un vajadzības gadījumā papildināts ar īstenošanai specifiskiem riskiem;

c) funkcionālās testēšanas darbības, pamatojoties uz testu kompleksiem (ja tie ir pieejami un atbilstoši), kas noteikti saskaņā ar tehniskajām specifikācijām vai standartiem;

d) uzturēšanas procesu esības un piemērotības novērtējums, ieskaitot vismaz versiju pārvaldību, atjaunināšanas pārvaldību un ievainojamības pārvaldību;

e) uzturēšanas procesu darbības efektivitātes novērtējums, ieskaitot vismaz versiju pārvaldību, atjaunināšanas pārvaldību un ievainojamības pārvaldību;

f) maka nodrošinātāja sniegtā atkarības analīze, ieskaitot uzticamības informācijas pieņemamības novērtēšanas metodiku, kas ietver VI pielikumā izklāstītos elementus;

g) ievainojamības novērtējums atbilstošā līmenī, ieskaitot:

— maka risinājuma koncepcijas un attiecīgā gadījumā tā pirmkoda pārskatīšanu,

— maka risinājuma noturības testēšanu pret uzbrucējiem ar augstu uzbrukuma potenciālu attiecībā uz uzticamības līmeni "augsts" atbilstīgi Īstenošanas regulas (ES) 2015/1502 pielikuma 2.2.1. iedaļai;

h) novērtējumu par apdraudējuma vides attīstību un tās ietekmi uz maka risinājuma risku segumu, lai noteiktu, kādas izvērtēšanas darbības ir nepieciešamas maka risinājuma dažādajiem komponentiem.

2. Valsts sertifikācijas shēmas ietver izvērtēšanu, kuras nolūks ir noteikt, vai maka risinājumu un tās elektroniskās identifikācijas shēmas īstenošana, saskaņā ar kuru tiek nodrošināti minētie maka risinājumi, atbilst 3. panta 5. punkta a) apakšpunktā noteiktajai arhitektūrai, kā arī izvērtēšanu nolūkā noteikt, vai ierosinātais izvērtēšanas plāns kopā ar īstenošanu atbilst 3. panta 5. punkta c) apakšpunktā minētajam izvērtēšanas plānam.

3. Lai izvairītos no identisku izvērtēšanas darbību atkārtošanās un koncentrētos uz darbībām, kas ir specifiskas konkrētajam variantam, valsts sertifikācijas shēmās paredz izlases veidošanas noteikumus. Minētie izlases veidošanas noteikumi ļauj veikt funkcionālos un drošības testus tikai maka risinājuma un tās elektroniskās identifikācijas shēmas, saskaņā ar kuru tas tiek nodrošināts, mērķa komponenta variantu izlasei un mērķa ierīču izlasei. Valsts sertifikācijas shēmās nosaka, ka visām sertifikācijas struktūrām jāpamato izlases izmantošana.

4. Valsts sertifikācijas shēmas paredz, ka sertifikācijas struktūrai ir jāizvērtē *WSCA*, pamatojoties uz IV pielikumā izklāstītajām metodēm un procedūrām.

14. pants

Sertifikācijas darbības

1. Valsts sertifikācijas shēmās nosaka apliecināšanas darbības, ko veic atbilstības sertifikāta izdošanas nolūkā saskaņā ar EN ISO/IEC 17067:2013 V iedaļas a) punktu, 1. tabulu, to vidū šādus aspektus:

a) atbilstības sertifikāta saturu, kā noteikts VII pielikumā;

b) to, kā izvērtēšanas rezultāti ir jāpaziņo publiskajā sertifikācijas ziņojumā, iekļaujot vismaz sākotnējās revīzijas un validācijas plāna kopsavilkumu, kā izklāstīts VIII pielikumā;

c) sertifikācijas novērtējuma ziņojumā paziņoto izvērtēšanas rezultātu saturu, ieskaitot VIII pielikumā noteiktos elementus.

2. Sertifikācijas novērtējuma ziņojumu var darīt pieejamu Sadarbības grupai un Komisijai.

15. pants

Sūdzības un apelācijas

Valsts sertifikācijas shēmas ietver procedūras vai atsauces uz piemērojamiem valsts tiesību aktiem, kuros noteikts mehānisms efektīvai sūdzību un pārsūdzību iesniegšanai saistībā ar to veikto sertifikācijas shēmas īstenošanu vai izdoto atbilstības sertifikātu. Šīs procedūras ietver informācijas sniegšanu sūdzības iesniedzējam par procesa gaitu un pieņemto lēmumu, kā arī informāciju sūdzības iesniedzējam par tiesībām uz efektīvu tiesību aizsardzību tiesā. Valsts sertifikācijas shēmas paredz, ka visas sūdzības un pārsūdzības, ko sertifikācijas struktūra nav atrisinājusi vai nevar atrisināt, nosūta shēmas īpašniekam novērtēšanai un atrisināšanai.

16. pants

Uzraudzības pasākumi

1. Valsts sertifikācijas shēmās nosaka, ka sertifikācijas iestādēm jāīsteno uzraudzības darbības, kas ietver procesu uzraudzības izvērtēšanu apvienojumā ar izlases veida testiem vai inspekcijām.

2. Valsts sertifikācijas shēmās ietver prasības shēmu īpašniekiem uzraudzīt, kā sertifikācijas struktūras pilda savus pienākumus saskaņā ar Regulu (ES) Nr. 910/2014 un attiecīgā gadījumā saskaņā ar valsts sertifikācijas shēmām.

3. Valsts sertifikācijas shēmās ietver prasības sertifikācijas struktūrām uzraudzīt:

a) saskaņā ar valsts sertifikācijas shēmām izdota atbilstības sertifikāta turētāju atbilstību sertifikācijas pienākumiem saskaņā ar Regulu (ES) Nr. 910/2014 un valsts sertifikācijas shēmām;

b) sertificētā maka risinājuma atbilstību prasībām, kas noteiktas valsts sertifikācijas shēmās.

17. pants

Neatbilstības sekas

Valsts sertifikācijas shēmās nosaka, kādas sekas ir tam, ka kāds sertificēts maka risinājums un tā elektroniskā identifikācijas shēma, saskaņā ar kuru tas tiek nodrošināts, neatbilst šajā regulā noteiktajām prasībām. Minētās sekas ietver šādus aspektus:

1) sertifikācijas struktūras pienākums informēt atbilstības sertifikāta turētāju un pieprasīt atbilstības sertifikāta turētājam veikt korektīvas darbības;

2) sertifikācijas struktūras pienākums informēt citas attiecīgās tirgus uzraudzības iestādes, ja neatbilstība ir saistīta ar attiecīgajiem Savienības tiesību aktiem;

3) nosacījumi, ar kādiem atbilstības sertifikāta turētājs veic korektīvas darbības;

4) nosacījumi atbilstības sertifikāta apturēšanai, ko veic sertifikācijas struktūra, un atbilstības sertifikāta atjaunošanai pēc neatbilstības novēršanas;

5) nosacījumi, saskaņā ar kuriem sertifikācijas struktūra anulē atbilstības sertifikātu;

6) kādas sekas ir tam, ka sertifikācijas struktūra neatbilst valsts sertifikācijas shēmas prasībām.

VII NODAĻA

SERTIFIKĀCIJAS CIKLS

18. pants

Sertifikācijas cikls

1. Valsts sertifikācijas shēmu ietvaros izdoto atbilstības sertifikātu derīgumu regulāri izvērtē sertifikācijas struktūra saskaņā ar IX pielikumā izklāstītajām prasībām.

2. Valsts sertifikācijas shēmās ietver resertifikācijas procesu attiecībā uz maka risinājumiem un elektroniskās identifikācijas shēmu, saskaņā ar kuru tie tiek nodrošināti, un to veic pēc atbilstības sertifikāta turētāja pieprasījuma pirms sākotnējā atbilstības sertifikāta termiņa beigām. Minētais resertifikācijas process ietver maka risinājuma un tās elektroniskās identifikācijas shēmas pilnīgu izvērtējumu, saskaņā ar kuru tas tiek nodrošināts, ieskaitot ievainojamības novērtējumu, balstoties uz IX pielikumā izklāstītajiem principiem.

3. Valsts sertifikācijas shēmas ietver procesu tādu izmaiņu pārvaldībai, kas skar sertificētā maka risinājumu un elektroniskās identifikācijas shēmu, saskaņā ar kuru tas tiek nodrošināts. Minētais process ietver noteikumus, pēc kuriem nosaka, vai uz izmaiņām attiecas 4. punktā minētā īpašā izvērtēšana vai IV pielikumā minēto uzturēšanas procesu darbības efektivitātes verificēšana.

4. Valsts sertifikācijas shēmās ietver īpašas izvērtēšanas procesu saskaņā ar EN ISO/IEC 17065:2012. Minētajā īpašās izvērtēšanas procesā iekļauj veicamo darbību izlasi, kas vajadzīgas, lai risinātu konkrēto problēmu, kura radīja nepieciešamību pēc īpašā izvērtējuma.

5. Valsts sertifikācijas shēmās paredz noteikumus par atbilstības sertifikāta anulēšanu.

VIII NODAĻA

UZSKAITE UN INFORMĀCIJAS AIZSARDZĪBA

19. pants

Uzskaites datu saglabāšana

1. Valsts sertifikācijas shēmas ietver prasības sertifikācijas struktūrām attiecībā uz uzskaites sistēmu, kurā glabā visu attiecīgo informāciju, kas sagatavota saistībā ar to veiktajām atbilstības novērtēšanas darbībām, ieskaitot datus, ko izdevuši un saņēmuši maku risinājumu un to elektronisko identifikācijas shēmu nodrošinātāji, saskaņā ar kurām tie tiek nodrošināti. Šādas informācijas ierakstus glabā drošā veidā. Dokumentāciju var glabāt elektroniski, un tā ir pieejama tik ilgi, cik to prasa Savienības vai valsts tiesību akti, un vismaz piecus gadus pēc attiecīgā atbilstības sertifikāta anulēšanas vai derīguma termiņa beigām.

2. Valsts sertifikācijas shēmās šīs regulas vajadzībām nosaka prasības atbilstības sertifikāta turētājam vismaz piecus gadus pēc attiecīgā atbilstības sertifikāta anulēšanas vai derīguma termiņa beigām droši glabāt šādu informāciju:

a) reģistru ar sertifikācijas struktūrai vai jebkuram tās apakšuzņēmējam sertifikācijas procesā sniegto informāciju;

b) maka risinājuma sertifikācijas tvērumā iekļauto aparatūras komponentu paraugus.

3. Valsts sertifikācijas shēmās iekļauj prasību, ka atbilstības sertifikāta turētājam 1. punktā minētā informācija pēc pieprasījuma jādara pieejama sertifikācijas struktūrai vai uzraudzības iestādei, kas minēta Regulas (ES) Nr. 910/2014 46.a panta 1. punktā.

20. pants

Informācijas aizsardzība

Saskaņā ar valsts sertifikācijas shēmām visām personām vai organizācijām, kurām ir piešķirta piekļuve informācijai saistībā ar darbību veikšanu saskaņā ar valsts sertifikācijas shēmu, ir jānodrošina komercnoslēpumu un citas konfidenciālas informācijas drošība un aizsardzība, kā arī jāievēro intelektuālā īpašuma tiesības un jāveic vajadzīgie un atbilstīgie tehniskie un organizatoriskie pasākumi, lai nodrošinātu šo konfidencialitāti.

IX NODAĻA

NOBEIGUMA NOTEIKUMI

21. pants

Pāreja uz Eiropas kiberdrošības sertifikācijas shēmu

Pēc pirmās Eiropas kiberdrošības sertifikācijas shēmas pieņemšanas attiecībā uz maku risinājumiem un elektroniskās identifikācijas shēmām, saskaņā ar kurām tie tiek nodrošināti, šo regulu pārskata, lai ņemtu vērā šādas Eiropas kiberdrošības sertifikācijas shēmas ieguldījumu maka risinājumu un to elektroniskās identifikācijas shēmu vispārējā sertificēšanā, saskaņā ar kurām tie tiek nodrošināti.

22. pants

Stāšanās spēkā

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

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

Briselē, 2024. gada 28. novembrī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

I PIELIKUMS

EIROPAS DIGITĀLĀS IDENTITĀTES MAKU RISKU REĢISTRS

Ievads

Risku reģistrā ir aprakstīti galvenie drošības un privātuma riski un apdraudējumi, kas attiecas uz makiem un ko pienācīgi ņem vērā katrā maku arhitektūrā un īstenošanā. **Augsta līmeņa riski** (I iedaļa) ir saistīti ar maku izmantošanu, ko veic lietotāji un atkarīgās puses, un tie ir saistīti ar tiešiem draudiem, kas vērsti pret maku aktīviem. Turklāt ir konstatēti daži **sistēmas līmeņa riski** (II iedaļa) attiecībā uz makiem, kas parasti izrietētu no apdraudējumu kombinācijas, kura attiecas uz visu maku sistēmu kopumā.

Riska veids	Riska ID	Saistītie riska nosaukumi
Augsta līmeņa riski attiecībā uz makiem	R1	Esošas elektroniskās identitātes izveide vai izmantošana
	R2	Viltotas elektroniskās identitātes izveide vai izmantošana
	R3	Viltotu atribūtu izveide vai izmantošana
	R4	Identitātes zādzība
	R5	Datu zādzība
	R6	Datu izpaušana
	R7	Manipulācijas ar datiem
	R8	Datu zudums
	R9	Neatļauts darījums
	R10	Manipulācijas ar darījumiem
	R11	Noliegšana
	R12	Darījumu datu atklāšana
	R13	Pakalpojuma pārtraukums
	R14	Novērošana
Ar sistēmu saistīti riski	SR1	Masveida novērošana
	SR2	Kaitējums reputācijai
	SR3	Juridiska neatbilstība

Reģistrā ir uzskaitīti arī **tehniskie apdraudējumi** (III iedaļa), kas vērsti pret maka risinājuma īstenošanu. Šie apdraudējumi ir saistīti ar augsta līmeņa riskiem tādā nozīmē, ka katru no tiem varētu izmantot, lai izraisītu daudzus augsta līmeņa riskus.

Apdraudējuma veids	Apdraudējuma ID	Saistītie apdraudējumu nosaukumi	Apdraudējumu apakškategorijas
Tehnisks apdraudējums	TT1	Fiziski uzbrukumi	1.1. *Zādzība*
			1.2. *Informācijas noplūde*
			1.3. *Nesankcionēta manipulācija*
	TT2	Kļūdas un nepareizas konfigurācijas	2.1. *Kļūdas, kas pieļautas, pārvaldot IT sistēmu*
			2.2. *Lietojumprogrammas līmeņa kļūdas vai lietošanas kļūdas*
			2.3. *Izstrādes laikā pieļautās kļūdas un sistēmas nepareizas konfigurācijas*

Apdraudējuma veids	Apdraudējuma ID	Saistītie apdraudējumu nosaukumi	Apdraudējumu apakškategorijas
	TT3	Neuzticamu resursu izmantošana	3.1. *Maka komponentu nepareiza izmantošana vai konfigurācija*
	TT4	Atteice un nepieejamība	4.1. *Iekārtu, ierīču vai sistēmu atteice vai disfunkcija*
			4.2. *Resursu zudums*
			4.3. *Atbalsta pakalpojumu zudums*
	TT5	Ļaunprātīgas darbības	5.1. *Informācijas pārtveršana*
			5.2. *Pikšķerēšana un viltošana*
			5.3. *Ziņojumu reproducēšana*
			5.4. *Pārlases uzbrukums*
			5.5. *Programmatūras ievainojamības*
			5.6. *Uzbrukumi piegādes ķēdēm*
			5.7. *Ļaunprogrammatūra*
			5.8. *Gadījumskaitļu prognozēšana*

Visbeidzot, reģistrā ir **uzskaitīti tieši draudi makiem**, un katrs no tiem ir saistīts ar (neizsmeļošu) risku izlasi (IV iedaļa).

I IEDAĻA

Augsta līmeņa riski attiecībā uz makiem

R1. Esošas elektroniskās identitātes izveide vai izmantošana

Esošas elektroniskās identitātes izveide vai izmantošana ir definēta kā tādas elektroniskas identitātes radīšana makā, kas pastāv reālajā pasaulē un ir piešķirta citam lietotājam. Būtībā šis risks rada identitātes zādzības (R4) un neatļautu darījumu (R9) riskus.

R2. Viltotas elektroniskās identitātes izveide vai izmantošana

Viltotas elektroniskās identitātes izveide vai izmantošana ir definēta kā tādas elektroniskas identitātes radīšana makā, kas reālajā pasaulē nepastāv.

R3. Viltotu atribūtu izveide vai izmantošana

Viltotu atribūtu izveide vai izmantošana ir tādu atribūtu radīšana vai izmantošana, attiecībā uz kuriem nav iespējams pārbaudīt, vai tos ir izdevis apgalvotais pakalpojumu sniedzējs, un kuriem nevar uzticēties.

R4. Identitātes zādzība

Identitātes zādzību definē kā maka vienības neatļautu ieguvi vai tādu autentifikācijas faktoru zudumu, kas ļauj uzdoties par attiecīgo personu.

R5. Datu zādzība

Datu zādzību definē kā datu neatļautu iegūšanu. Datu zādzība ir saistīta arī tādiem apdraudējumiem kā datu pārtveršana (neatļauta nosūtītu datu tveršana) un datu atšifrēšana (neatļauta šifrētu datu dekodēšana), kas dažos gadījumos varētu novest pie datu izpaušanas (R6).

R6. Datu izpaušana

Datu izpaušana ir definēta kā neatļauta personas datu, to vidū īpašu kategoriju personas datu, izpaušana. Privātuma pārkāpuma risks ir ļoti līdzīgs, ja to aplūko no privātuma, nevis drošības viedokļa.

R7. Manipulācijas ar datiem

Manipulācijas ar datiem definē kā datu neatļautu pārveidošanu.

R8. Datu zudums

Datu zudumu definē kā situāciju, kad makā glabātie dati tiek zaudēti nepareizas izmantošanas vai ļaunprātīgas rīcības rezultātā. Šis risks bieži vien ir sekundārs risks pēc manipulācijas ar datiem (R7) vai pakalpojuma pārtraukuma (R13), kad nav iespējams atjaunot visus datus vai to daļu.

R9. Neatļauts darījums

Neatļauti darījumi tiek definēti kā operacionālas darbības, ko veic bez maka lietotāja atļaujas vai ziņas. Daudzos gadījumos neatļauts darījums var izraisīt identitātes zādzību (R4) vai datu izpaušanu (R6). Tas ir saistīts arī ar tādiem neatļautiem darījumiem kā šifrēšanas atslēgu ļaunprātīgu izmantošana.

R10. Manipulācijas ar darījumiem

Manipulācijas ar darījumiem definē kā maka darbību neatļautu pārveidošanu. Manipulācijas ar darījumiem ir uzbrukums integritātei, un tās ir saistītas ar datu integritātes pārkāpumu.

R11. Noliegšana

Noliegšana ir definēta kā situācija, kad ieinteresētā persona var noliegt, ka tā veikusi kādu darbību vai bijusi iesaistīta darījumā, un citu ieinteresēto personu rīcībā nav pienācīgu pierādījumu, lai to atspēkotu.

R12. Darījumu datu atklāšana

Darījumu datu atklāšana ir informācijas atklāšana saistībā ar informāciju par darījumu starp ieinteresētajām personām.

R13. Pakalpojuma pārtraukums

Pakalpojuma pārtraukumu definē kā maka normālās darbības pārtraukumu vai pasliktināšanos. Īpašs pakalpojuma pārtraukums ir lietotāja bloķēšana, ko definē kā lietotāja nespēju piekļūt savam kontam vai makam.

R14. Novērošana

Novērošana vai monitorēšana ir maka lietotāja darbību, saziņas vai datu neatļauta izsekošana vai novērošana. Novērošana bieži vien ir saistīta ar izsecināšanu, ko definē kā sensitīvas vai personas informācijas iegūšanu no šķietami nekaitīgiem datiem.

II IEDAĻA

Ar sistēmu saistīti riski

Šie riski nav iekļauti apdraudējumu sarakstā, jo tie parasti ir vairāku apdraudējumu sekas, kas atkārtojas tādā veidā, ka tiek apdraudēta visa sistēma.

SR1. Masveida novērošana

Masveida novērošana ir daudzu lietotāju darbību izsekošana vai novērošana, izmantojot viņu maka saziņas darbības vai datus. Masveida novērošana bieži vien ir saistīta ar novērošanu (R14) un izsecināšanu vispārējā mērogā, kad informācija par daudziem lietotājiem tiek apvienota, lai iegūtu sensitīvus vai personas datus par lietotājiem vai lai noteiktu statistikas tendences, ko var izmantot turpmāku uzbrukumu izstrādei.

SR2. Kaitējums reputācijai

Kaitējumu reputācijai definē kā kaitējumu, kas nodarīts organizācijas vai valdības struktūras reputācijai. Reputācijai nodarītais kaitējums izrietēs arī no citiem riskiem, ja pārkāpumu vai incidentu atspoguļos plašsaziņas līdzekļi un attēlos organizāciju nelabvēlīgā gaismā. Kaitējums reputācijai var radīt papildu riskus, piemēram, uzticības zudumu, kas izriet no lietotāja pamatotām šaubām, un ekosistēmas zudumu, sabrūkot visai ekosistēmai.

SR3. Juridiska neatbilstība

Juridiska neatbilstība tiek definēta kā situācija, kad nav iespējams ievērot attiecīgos tiesību aktus vai standartus. Maka kontekstā, tā kā risinājuma drošība un privātums ir juridiskas prasības, visi apdraudējumi varētu izraisīt zināmu juridisku neatbilstību.

III IEDAĻA

Tehniskie apdraudējumi

Ne visi tehniskie apdraudējumi ir saistīti ar konkrētiem riskiem attiecībā uz makiem, jo daudzus no tiem varētu izmantot, lai īstenotu uzbrukumus, kas atbilst daudziem dažādiem riskiem.

TT1. Fiziski uzbrukumi

1.1. *Zādzība*

Zādzība ir tādu ierīču zādzība, kas var mainīt maka pareizu darbību (ja ierīce ir nozagta un maka vienība nav pietiekami aizsargāta). Tas var veicināt daudzus riskus, to vidū identitātes zādzību (R4), datu zādzību (R5) un neatļautus darījumus (R9).

1.2. *Informācijas noplūde*

Informācijas noplūde ir neatļauta piekļuve, informācijas nopludināšana vai kopīgošana pēc fiziskas piekļuves makam. Tas jo īpaši var veicināt datu izpaušanu (R6) un datu zādzību (R5).

1.3. *Nesankcionēta manipulācija*

Nesankcionēta manipulācija ir viena vai vairāku maka vienības komponentu integritātes pārkāpšana, vai to komponentu integritātes pārkāpšana, uz kuriem balstās maka vienība, piemēram, lietotāja ierīces vai tās operētājsistēmas integritātes pārkāpšana. Tas jo īpaši var veicināt manipulācijas ar datiem (R7), datu zudumu (R8) un manipulācijas ar darījumiem (R10). Ja nesankcionēta manipulācija ir vērsta uz programmatūras komponentiem, tā var veicināt daudzus riskus.

TT2. Kļūdas un nepareizas konfigurācijas

2.1. *Kļūdas, kas pieļautas, pārvaldot IT sistēmu*

Kļūdas, kas pieļautas, pārvaldot IT sistēmu, ir informācijas noplūde, kopīgošana vai kaitējums, ko rada lietotāju veikta IT aktīvu nepareiza izmantošana (lietojumprogrammas iespēju izpratnes trūkums) vai IT aktīvu nepareiza konfigurācija vai pārvaldība.

2.2. *Lietojumprogrammas līmeņa kļūdas vai lietošanas kļūdas*

Lietojumprogrammas līmeņa kļūdas vai lietošanas kļūdas ir lietojumprogrammas disfunkcija, kuras iemesls ir kļūda pašā lietojumprogrammā vai kāda lietotāja (maka lietotāju un atkarīgo pušu) kļūda.

2.3. *Izstrādes laikā pieļautās kļūdas un sistēmas nepareizas konfigurācijas*

Izstrādes laikā pieļautās kļūdas un sistēmas nepareizas konfigurācijas ir disfunkcija vai ievainojamības, ko izraisa nepareizi izstrādāti vai konfigurēti IT aktīvi vai uzņēmējdarbības procesi (neatbilstīgas IT produktu specifikācijas, neatbilstoša lietojamība, nedrošas saskarnes, neatbilstošas politikas un procedūru plūsmas, izstrādes kļūdas).

TT3. Neuzticamu resursu izmantošana

Neuzticamu resursu izmantošana ir darbība, kas noved pie netīša kaitējuma, kas radies nepareizi definētu uzticamības attiecību dēļ, piemēram, bez pietiekamām garantijām uzticoties pakalpojumu sniedzējam, kas ir trešā persona.

3.1. *Maka komponentu kļūdaina izmantošana vai konfigurācija*

Maka komponentu kļūdaina izmantošana vai konfigurācija ir maka komponentu netīšs bojājums, kas izriet no tā, ka maka lietotāji vai nepietiekami apmācīti izstrādātāji kļūdaini izmanto nepareizu konfigurāciju vai nav nodrošināta pietiekama pielāgošanās apdraudējumu ainas izmaiņām, parasti izmantojot neaizsargātus trešo personu komponentus vai izpildes platformas.

TT4. Atteice un nepieejamība

4.1. *Aprīkojuma, ierīču vai sistēmu atteice vai nepieejamība*

Aprīkojuma atteice vai disfunkcija ir netīšs kaitējums IT aktīviem aprīkojuma, arī nodrošinātāja infrastruktūras un lietotāju ierīču, atteices vai disfunkcijas dēļ.

4.2. *Resursu zudums*

Resursu zudums ir nepieejamība vai disfunkcija šādu resursu nepieejamības dēļ, piemēram, apkopes darbu dēļ.

4.3. *Atbalsta pakalpojumu zudums*

Atbalsta pakalpojumu zudums ir nepieejamība vai disfunkcija, jo nav pieejami atbalsta pakalpojumi, kas vajadzīgi sistēmas pienācīgai darbībai, to vidū pakalpojumu sniedzēja infrastruktūras un lietotāja ierīces tīkla savienojums.

TT5. Ļaunprātīgas darbības

5.1. *Informācijas pārtveršana*

Informācijas pārtveršana ir tādas informācijas tveršana, kas ir nepienācīgi aizsargāta, pārsūtot informāciju, ieskaitot pārtvērējuzbrukumus.

5.2. *Pikšķerēšana un viltošana*

Pikšķerēšana ir lietotāja sniegtās informācijas iegūšana pēc maldinošas mijiedarbības, kas bieži vien ir saistīta ar likumīgu saziņas līdzekļu un tīmekļa vietņu viltošanu. Šie apdraudējumi ir vērsti pret lietotāju un parasti veicina identitātes zādzību (R4) un neatļautus darījumus (R9), bieži vien izmantojot datu zādzību (R5) vai datu izpaušanu (R6).

5.3. *Ziņojumu reproducēšana*

Ziņojumu reproducēšana ir iepriekš pārtvertu ziņojumu atkārtota izmantošana neatļautu darījumu veikšanai, bieži vien protokola līmenī. Šis tehniskais apdraudējums galvenokārt veicina neatļautus darījumus, kas atkarībā no darījuma var radīt citus riskus.

5.4. *Pārlases uzbrukums*

Pārlases uzbrukums ir drošības, bieži vien konfidencialitātes pārkāpums, veicot lielu skaitu mijiedarbību, līdz atbildes sniedz vērtīgu informāciju.

5.5. *Programmatūras ievainojamības*

Apdraudējums, kas saistīts ar programmatūras ievainojamībām, ir drošības pārkāpums, kas izriet no programmatūras ievainojamības maka komponentos vai maka ieviešanā izmantotajā programmatūrā un aparatūras komponentos, ieskaitot publicētās ievainojamības un nepublicētās (nulles dienas) ievainojamības.

5.6. *Uzbrukumi piegādes ķēdēm*

Uzbrukums piegādes ķēdei ir drošības pārkāpums, ko izraisa uzbrukumi maka nodrošinātājam vai tā lietotājiem, lai varētu veikt turpmākus uzbrukumus pašam makam.

5.7. *Ļaunprogrammatūra*

Ļaunprogrammatūra ir drošības pārkāpums, izmantojot ļaunprātīgiem nolūkiem paredzētas lietojumprogrammas, kas makā veic nevēlamas un nelikumīgas darbības.

5.8. *Gadījumskaitļu prognozēšana*

Gadījumskaitļu prognozēšana ir pārlases uzbrukuma iespējas sekmēšana, daļēji vai pilnībā prognozējot ģenerētos gadījumskaitļus.

IV IEDAĻA

Apdraudējumi attiecībā uz makiem

Šajā pēdējā iedaļā ir sniegti vairāki makiem raksturīgi tipiski apdraudējumu scenāriji, kas ir attiecināti uz galvenajiem saistītajiem augsta līmeņa riskiem, kuri uzskaitīti iepriekš. Šajā sarakstā ir norādīti apdraudējumi, kas ir jāaptver, taču tas nav izsmeļošs apdraudējumu saraksts, kas lielā mērā ir atkarīgs no izvēlētā maka risinājuma arhitektūras un apdraudējuma vides attīstības. Turklāt riska novērtējumā un ierosinātajos pasākumos maka nodrošinātājs var būt atbildīgs tikai par tiem komponentiem, kas ietilpst sertifikācijas tvērumā (*).

ID *Identifikators*	Apdraudējuma apraksts *Identificētā apdraudējuma apraksts* (*)	Riska nosaukums *Saistītie riski*
TR1	Uzbrucējs bez pamatota iemesla var atsaukt pseidonīmus.	Viltotas elektroniskās identitātes (R2) izveide vai izmantošana
TR2	Uzbrucējs var izsniegt viltotas elektroniskas identitātes, kuras nepastāv.	Viltotas elektroniskās identitātes (R2) izveide vai izmantošana
TR3	Uzbrucējs var sākt izsniegt neatļautus PID.	Viltotas elektroniskās identitātes (R2) izveide vai izmantošana
TR4	Uzbrucējs var panākt, ka administrators uzticamo PID pakalpojumu sniedzēju sarakstā ievada nepareizu PID sniedzēju.	Viltotas elektroniskās identitātes (R2) izveide vai izmantošana
TR5	Uzbrucējs var apiet attālinātās identitātes apliecināšanas pakalpojumu.	Esošas elektroniskās identitātes izveide vai izmantošana (R1) / viltotas elektroniskās identitātes izveide vai izmantošana (R2)
TR6	Uzbrucējs var apiet fiziskās identitātes apliecināšanas pakalpojumu.	Esošas elektroniskās identitātes izveide vai izmantošana (R1) / viltotas elektroniskās identitātes izveide vai izmantošana (R2)
TR7	Uzbrucējs var apiet identitātes apliecināšanas pakalpojumus, kas saistīti ar attālināta (kvalificēta) sertifikāta izmantošanu.	Esošas elektroniskās identitātes izveide vai izmantošana (R1) / viltotas elektroniskās identitātes izveide vai izmantošana (R2)
TR8	Uzbrucējs var piekļūt makam, kas nav piesaistīts kādai personai.	Esošas elektroniskās identitātes izveide vai izmantošana (R1) / viltotas elektroniskās identitātes izveide vai izmantošana (R2)
TR9	Uzbrucējs var izvairīties no tehniskās un procesuālās kontroles, lai radītu nepareizus PID.	Esošas elektroniskās identitātes izveide vai izmantošana (R1) / viltotas elektroniskās identitātes izveide vai izmantošana (R2)
TR10	Uzbrucējs var aktivizēt jaunu maku uz nederīgas *WSCD*.	Esošas elektroniskās identitātes izveide vai izmantošana (R1) / viltotas elektroniskās identitātes izveide vai izmantošana (R2)
TR11	Uzbrucējs var apiet identitātes pārbaudes pakalpojumu, kas saistīts ar pastāvošu eID līdzekļu izmantošanu.	Esošas elektroniskās identitātes izveide vai izmantošana (R1) / identitātes zādzība (R4) / neatļauts darījums (R9)
TR12	Uzbrucējs var apiet PID nodrošinātāja veikto verifikāciju attiecībā uz to, vai maku kontrolē lietotājs, un izsniegt PID uzbrucēja kontrolētā kompromitētā makā.	Esošas elektroniskās identitātes izveide vai izmantošana (R1) / identitātes zādzība (R4) / neatļauts darījums (R9)

ID *Identifikators*	Apdraudējuma apraksts *Identificētā apdraudējuma apraksts* (*)	Riska nosaukums *Saistītie riski*
TR13	Uzbrucējs var iegūt derīgu PID nederīgā maka vienībā.	Esošas elektroniskās identitātes izveide vai izmantošana (R1) / identitātes zādzība (R4) / neatļauts darījums (R9)
TR14	PID sniedzējs var izdot viltotas identitātes, ja identitāte ir saistīta ar esošu personu.	Esošas elektroniskās identitātes izveide vai izmantošana (R1) / identitātes zādzība (R4) / neatļauts darījums (R9)
TR15	Uzbrucējs var sasaistīt PID ar nepareizu maku, jo PID sniedzējs nespēj sasaistīt PID ar pareizo maku.	Esošas elektroniskās identitātes izveide vai izmantošana (R1) / identitātes zādzība (R4) / neatļauts darījums (R9)
TR16	Uzbrucējs var likt lietotājam apstiprināt jaunas uzbrucēja kontrolē esošas maka vienības/instances aktivizēšanu, kā arī pēc tam kontrolēt apliecinājumus.	Esošas elektroniskās identitātes (R1) izveide vai izmantošana / viltotas elektroniskās identitātes (R2) izveide vai izmantošana / identitātes zādzība (R4) / neatļauts darījums (R9)
TR17	Uzbrucējs var izdot citas valsts PID, lai piekļūtu par uzbrukuma mērķi izvēlēto iedzīvotāju datiem / digitālajiem aktīviem.	Esošas elektroniskās identitātes izveide vai izmantošana (R1) / identitātes zādzība (R4) / neatļauts darījums (R9)
TR18	Uzbrucējs var izvairīties no tehniskās un procesuālās kontroles, lai izveidotu viltus *(Q)EAA*.	Viltotu atribūtu izveide vai izmantošana (R3)
TR19	Uzbrucējs var uzrādīt *(Q)EAA*, kas viņam nav likumīgi izdoti.	Viltotu atribūtu izveide vai izmantošana (R3)
TR20	Uzbrucējs var uzbrukt maka kriptogrāfiskās sasaistes mehānismam starp PID un *(Q)EAA*, kuri viņam nebūtu jāizdod.	Viltotu atribūtu izveide vai izmantošana (R3)
TR21	Uzbrucējs var izmantot *(Q)EAA* makā, lai gan *(Q)EAA* fiziskajam ekvivalentam ir beidzies derīguma termiņš vai tas ir nederīgs.	Viltotu atribūtu izveide vai izmantošana (R3)
TR22	Uzbrucējs var apiet *(Q)EAA* pakalpojumu sniedzēja veikto verifikāciju attiecībā uz to, vai maks ir lietotāja kontrolē, un panākt *(Q)EAA* izdošanu kompromitētā makā, ko kontrolē uzbrucējs.	Viltotu atribūtu izveide vai izmantošana (R3)
TR23	Uzbrucējs var viltot atribūtu elektroniskos apliecinājumus.	Viltotu atribūtu izveide vai izmantošana (R3)
TR24	Uzbrucējs makā var ievadīt viltotus atribūtu elektroniskos apliecinājumus.	Viltotu atribūtu izveide vai izmantošana (R3)
TR25	Maks var uzrādīt atribūtus atkarīgajai pusei bez lietotāja piekrišanas.	Datu izpaušana (R6)
TR26	PID, *(Q)EAA* vai pseidonīmus var uzrādīt nepareizai atkarīgajai pusei.	Datu izpaušana (R6)
TR27	Uzbrucējs var ierosināt atribūtu elektronisko apliecinājumu ļaunprātīgu atjaunošanu.	Datu izpaušana (R6)
TR28	Uzbrucējs var panākt, ka lietotājs nepamatoti apstiprina atribūtu elektronisko apliecinājumu pieprasījumu (pikšķerēšanas ceļā vai citādi).	Datu izpaušana (R6)

ID *Identifikators*	Apdraudējuma apraksts *Identificētā apdraudējuma apraksts* (*)	Riska nosaukums *Saistītie riski*
TR29	Uzbrucējs var nopludināt atribūtus no maka un identificēt maka lietotāju gadījumos, kad identifikācija nav nepieciešama/ atļauta.	Datu izpaušana (R6)
TR30	Uzbrucējs var izvairīties no tehniskās un procesuālās kontroles, lai iegūtu datus.	Datu izpaušana (R6)
TR31	Pieprasījums var tikt nopludināts uzbrucējam.	Datu izpaušana (R6)
TR32	Uzbrucējs var iegūt informāciju par iegulto informācijas izpaušanas procedūru attiecībā uz atribūtiem un iesniegt pašreizējā pieprasījumā ietvertos atribūtus, izmantojot maku vienības.	Datu izpaušana (R6)
TR33	Uzbrucējs var izgūt žurnālus vai to daļas.	Datu izpaušana (R6)
TR34	Uzbrucējs var uzzināt, vai maks ir instalēts tajā pašā ierīcē, ko viņš izmanto, vai citā ierīcē, un iegūt informāciju par to.	Datu izpaušana (R6)
TR35	Uzbrucējs var iegūt informāciju par zināšanu faktoru, ko izmanto, lai lietotājs autentificētos *WSCA*.	Datu izpaušana (R6)
TR36	Atribūtu elektroniskais apliecinājums par personu, kas tiek uzrādīts vairākos darījumos ar atkarīgo pusi vai starp dažādām atkarīgajām pusēm, netīši ļauj sasaistīt vairākus darījumus ar attiecīgo personu.	Datu izpaušana (R6)
TR37	Publiskā atsaukto apliecinājumu / atkarīgu pušu sarakstā var būt informācija par to, kā lietotājs izmanto apliecinājumu (piemēram, atrašanās vieta, IP adrese...).	Datu izpaušana (R6)
TR38	Nespējot pierādīt lietotāja piekrišanu kopīgotiem atribūtiem, atkarīgās puses var ietekmēt žurnālu integritāti.	Datu izpaušana (R6)
TR39	Uzbrucējs var nelikumīgi izsekot maku lietotājus, izmantojot unikālus/izsekojamus identifikatorus.	Datu atklāšana (R6) / novērošana (R14)
TR40	Atkarīgā puse, kas sastāv no vairākām vienībām/struktūrām, kurām katrai ir atšķirīgs tvērums attiecībā uz to, ko tām ir atļauts pieprasīt/apstrādāt, var pieprasīt un apstrādāt datus bez likumīga pamata.	Datu atklāšana (R6) / neatļauts darījums (R9)
TR41	Uzbrucējs var vājināt PID maka veiktās integritātes un autentiskuma pārbaudes, lai to rezultāts vienmēr būtu apstiprinošs.	Manipulācijas ar datiem (R7)
TR42	Uzbrucējs var apiet vai vājināt maka veiktās pārbaudes, ar kurām verificē pieprasīto atribūtu integritāti un autentiskumu, tā, lai pārbaužu rezultāts vienmēr būtu apstiprinošs.	Manipulācijas ar datiem (R7)
TR43	Uzbrucējs var apiet vai vājināt maka veiktās pārbaudes, ar kurām verificē visus pieprasītos viena un tā paša lietotāja atribūtus, tā, lai pārbaužu rezultāts vienmēr būtu apstiprinošs.	Manipulācijas ar datiem (R7)
TR44	Uzbrucējs var apiet vai vājināt maka veiktās pārbaudes, ar kurām verificē, vai PID ir derīgs un to ir izsniedzis uzticams PID sniedzējs, tā, lai pārbaužu rezultāts vienmēr būtu apstiprinošs.	Manipulācijas ar datiem (R7)

ID *Identifikators*	Apdraudējuma apraksts *Identificētā apdraudējuma apraksts* (*)	Riska nosaukums *Saistītie riski*
TR45	Uzbrucējs var apiet vai vājināt maka veiktās pārbaudes, ar kurām verificē, vai *QEAA* ir derīgs un to ir izsniedzis kvalificēts uzticamības pakalpojumu sniedzējs, kas ir reģistrēts kā *QEAA* izdevējs, tā, lai pārbaužu rezultāts vienmēr būtu apstiprinošs.	Manipulācijas ar datiem (R7)
TR46	Uzbrucējs var apiet vai vājināt maka veiktās pārbaudes, ar kurām verificē, vai PID sniedzējs nav atsaucis PID, tā, lai pārbaužu rezultāts vienmēr būtu apstiprinošs.	Manipulācijas ar datiem (R7)
TR47	Uzbrucējs var apiet vai vājināt maka veiktās pārbaudes, ar kurām verificē, vai *(Q)EAA* sniedzējs nav atsaucis *(Q)EAA*, tā, lai pārbaužu rezultāts vienmēr būtu apstiprinošs.	Manipulācijas ar datiem (R7)
TR48	Uzbrucējs var mainīt dublējuma un atgūto datu saturu, kam vajadzētu būt tikai lietotāja kontrolē.	Manipulācijas ar datiem (R7) / datu zudums (R8)
TR49	Uzbrucējs var mainīt konkrētās maka instances darījumu vēsturi darbību žurnālos.	Manipulācijas ar datiem (R7) / datu zudums (R8)
TR50	Uzbrucējs var veikt noklausīšanos maka savienojuma laikā ar atkarīgajām pusēm.	Datu zādzība (R5) / Datu atklāšana (R6)
TR51	Uzbrucējs var pārliecināt lietotāju kopīgot personas datus (t. i., PID, atribūtu elektroniskos apliecinājumus, pseidonīmus, elektroniskos parakstus, reģistrus un citus datus) ar uzbrucēju vai ar trešo personu, ko lietotājs nebija plānojis darīt.	Datu zādzība (R5) / Datu atklāšana (R6)
TR52	Uzbrucējs darbību žurnālos var izlasīt darījumu vēsturi attiecībā uz konkrēto maka instanci.	Datu zādzība (R5) / Datu atklāšana (R6)
TR53	Uzbrucējs var eksportēt vai iegūt šifrēšanas atslēgas materiālus ārpus *WSCD*.	Datu zādzība (R5) / datu atklāšana (R6) / neatļauts darījums (R9)
TR54	Uzbrucējs var nolasīt dublējuma un atgūto datu saturu, kam vajadzētu būt tikai lietotāja kontrolē.	Datu zādzība (R5) / Datu atklāšana (R6)
TR55	Uzbrucējs var apiet lietotāja autentifikācijas metodi, lai izmantotu maka vienības ģenerētu pseidonīmu.	Identitātes zādzība (R4)
TR56	Uzbrucējs var piedāvāt lietotājiem lietojumprogrammu, kas imitē noteiktu likumīgu maku.	Identitātes zādzība (R4)
TR57	Uzbrucējs var eksportēt maka datus, to vidū PID, *(Q)EAA* vai žurnālus.	Identitātes zādzība (R4)
TR58	Uzbrucējs var eksportēt kriptogrāfiskos sasaistes materiālus.	Identitātes zādzība (R4)
TR59	Uzbrucējs var pārņemt identitātes, izmantojot maka šifrēšanas atslēgas.	Identitātes zādzība (R4)
TR60	Uzbrucējs var dublēt cita lietotāja personīgo maka vienību savā personīgajā ierīcē un izmantot to.	Identitātes zādzība (R4) / esošas elektroniskās identitātes izveide vai izmantošana (R1)

ID *Identifikators*	Apdraudējuma apraksts *Identificētā apdraudējuma apraksts* (*)	Riska nosaukums *Saistītie riski*
TR61	Kādas citas valsts iestādes var lūgt lietotāju parādīt un/vai kopīgot visus maka datus tuva attāluma situācijā, piemēram, šķērsojot attiecīgās valsts robežu.	Identitātes zādzība (R4) / novērošana (R14)
TR62	Lietotāji nevar pārsūtīt savus darījumu žurnālus pēc lietotāja ierīces atteices, kā rezultātā tiek zaudēta iepriekšējo darījumu izsekojamība jaunajā makā.	Noliegšana (R11)
TR63	Lietotāji nevar atgūt savus darījumu žurnālus pēc lietotāja ierīces atteices, kā rezultātā tiek zaudēta izsekojamība jaunajā makā.	Noliegšana (R11)
TR64	Atkarīgajām pusēm var būt grūtības pierādīt piekrišanu saistībā ar attālinātiem elektroniskajiem parakstiem.	Noliegšana (R11)
TR65	Uzbrucējs savienojuma laikā ar atkarīgajām personām var pārpludināt savienojumu(-us) ar pieprasījumiem.	Pakalpojuma pārtraukums (R13)
TR66	Uzbrucējs var pārpludināt statusa nodrošināšanas pakalpojumu ar savienojumiem ar atkarīgajām pusēm.	Pakalpojuma pārtraukums (R13)
TR67	Uzbrucējs var panākt, ka atribūta attēlojums parādās kā apstrīdēts/noraidīts, neskatoties uz to, ka atribūta attēlojumā ir norādīts tā derīgums.	Pakalpojuma pārtraukums (R13)
TR68	Uzbrucējs var atsaukt PID bez pamatota iemesla.	Pakalpojuma pārtraukums (R13)
TR69	Uzbrucējs var atsaukt PID bez lietotāja piekrišanas.	Pakalpojuma pārtraukums (R13)
TR70	Uzbrucējs var atsaukt *(Q)EAA* bez pamatota iemesla.	Pakalpojuma pārtraukums (R13)
TR71	Uzbrucējs var atsaukt *(Q)EAA* bez lietotāja piekrišanas.	Pakalpojuma pārtraukums (R13)
TR72	Uzbrucējs var ierosināt vairākus identifikācijas pieprasījumus, un tie netiek atpazīti kā tīši nezināmu autoru pieprasījumi.	Pakalpojuma pārtraukums (R13)
TR73	Uzbrucējs var nosūtīt vairākus pieprasījumus bez turpmāka darījuma.	Pakalpojuma pārtraukums (R13)
TR74	Uzbrucējs var ļaut atkarīgajai pusei pieprasīt identifikāciju bez atbilstošas identifikācijas (atbildes) un pilnīgu kontroli.	Pakalpojuma pārtraukums (R13)
TR75	Uzbrucējs var nosūtīt atbildi uz pieprasījumu pēc tā izpildes laika beigām vai līdzīgas situācijas, kas izraisa pakalpojuma pārtraukumu.	Pakalpojuma pārtraukums (R13)
TR76	Atkarīgā puse var nosūtīt vairākus nederīgus pieprasījumus.	Pakalpojuma pārtraukums (R13)
TR77	Uzbrucējs var nosūtīt vairākus nederīgus pieprasījumus maka nodrošinātājam.	Pakalpojuma pārtraukums (R13)
TR78	Uzbrucējs var liegt dalībvalstij iespēju atsaukt neuzticamu PID sniedzēju no uzticamo PID pakalpojumu sniedzēja saraksta.	Pakalpojuma pārtraukums (R13)
TR79	Uzbrucējs var novērst maka apturēšanu vai atsaukšanu.	Pakalpojuma pārtraukums (R13)

ID *Identifikators*	Apdraudējuma apraksts *Identificētā apdraudējuma apraksts* (*)	Riska nosaukums *Saistītie riski*
TR80	Uzbrucējs var bloķēt atkarīgo pušu, lietotāju un/vai PID sniedzēja darījumus.	Pakalpojuma pārtraukums (R13)
TR81	Uzbrucējs var atspējot *WSCD* vai padarīt to nepieejamu.	Pakalpojuma pārtraukums (R13)
TR82	Uzbrucējs var liegt PID pakalpojumu sniedzējam iespēju atsaukt vai apturēt PID.	Pakalpojuma pārtraukums (R13) / neatļauts darījums (R9)
TR83	Atkarīgā puse papildus datiem, kas ar tiem tiek kopīgoti, var iegūt lietotāja identitātes datus.	Novērošana (R14)
TR84	Slepeni vienojoties, atkarīgo pušu vai PID sniedzēju grupa var iegūt lietotāja identitātes datus papildus tiem zināmajiem datiem.	Novērošana (R14)
TR85	Uzbrucējs var izsekot un identificēt lietotāju, izmantojot lietotāja personas identifikācijas datus tur, kur lietotāja identifikācija nav nepieciešama.	Novērošana (R14)
TR86	Uzbrucējs var izveidot uzrādīšanai viltotu *(Q)EAA* kombināciju.	Manipulācijas ar darījumiem (R10)
TR87	Uzbrucējs var aktivizēt/pārņemt maku attālināti (piemēram, bankas lietotne, kurā iegults autentifikācijas vai apliecinājuma pieprasījums) bez lietotāja nepārprotamas piekrišanas vai ekskluzīvas kontroles situācijās, kad lietotājs par to nezina (piemēram, guļ) vai nevar redzēt atkarīgo pusi.	Manipulācijas ar darījumiem (R10)
TR88	Uzbrucēji var mainīt pieprasījuma metadatus (pakalpojuma nosaukumu, lietojumu utt.).	Manipulācijas ar darījumiem (R10)
TR89	Uzbrucēji var mainīt atbildes informāciju (pakalpojuma stāvoklis, vienreizējais kods u. c.).	Manipulācijas ar darījumiem (R10)
TR90	Uzbrucēji var mainīt pieprasījuma atribūta informāciju (prasīt par daudz informācijas utt.).	Manipulācijas ar darījumiem (R10)
TR91	Atkarīgā puse var reproducēt elementus no iepriekšējās sesijas citā sesijā.	Manipulācijas ar darījumiem (R10)
TR92	Uzbrucējs var aizstāt vai pārveidot PID laikā, kad tas tiek pārsūtīts no PID sniedzēja uz maka vienību.	Manipulācijas ar darījumiem (R10)
TR93	Uzbrucējs var aizstāt vai pārveidot PID laikā, kad tas tiek pārsūtīts no maka vienības uz tiešsaistes atkarīgo pusi.	Manipulācijas ar darījumiem (R10)
TR94	Uzbrucējs var aizstāt vai pārveidot PID laikā, kad to pārsūta no maka vienības uz bezsaistes atkarīgo pusi.	Manipulācijas ar darījumiem (R10)
TR95	Uzbrucējs var izdot PID bez lietotāja piekrišanas.	Neatļauts darījums (R9)
TR96	Uzbrucējs var izmantot atsauktas vai nederīgas iegultās informācijas izpaušanas procedūras, iespējams, bez atkarīgo pušu ziņas.	Neatļauts darījums (R9)
TR97	Uzbrucējs var manipulēt maku, lai tas verificētu nepareizus elektroniskos parakstus.	Neatļauts darījums (R9)
TR98	Uzbrucējs var izmantot maku ārpus lietotāja kontroles.	Neatļauts darījums (R9)

ID *Identifikators*	Apdraudējuma apraksts *Identificētā apdraudējuma apraksts* (*)	Riska nosaukums *Saistītie riski*
TR99	Uzbrucējs var pārliecināt lietotāju autentificēt un apstiprināt darījumus ar uzbrucēju vai neatļautu trešo personu.	Neatļauts darījums (R9)
TR100	Uzbrucējs var elektroniski parakstīties bez satura uzrādīšanas lietotājam vai pēc nepareiza satura uzrādīšanas.	Neatļauts darījums (R9)
TR101	Uzbrucējs var apiet piekļuves kontroli lietotāja kontā pie maka nodrošinātāja.	Neatļauts darījums (R9)
TR102	Uzbrucējs var uzdoties par atkarīgajām pusēm savienojuma ar atkarīgajām pusēm laikā.	Neatļauts darījums (R9) / datu izpaušana (R6)
TR103	Lietotājs aiz pārlūkprogrammas pieslēguma atkarīgās puses var atšķirties no lietotāja, kas atrodas aiz maka pieslēguma atkarīgās puses.	Neatļauts darījums (R9) / datu izpaušana (R6) / identitātes zādzība (R4)
TR104	Uzbrucējs var pārliecināt lietotāju bez iemesla atsaukt lietotāja maku.	Neatļauts darījums (R9) / pakalpojuma pārtraukums (R13)
TR105	Uzbrucējs var veikt pārtvērējuzbrukumus.	Neatļauts darījums (R9) / datu izpaušana (R6) / novērošana (R14)
TR106	Uzbrucējs var uzrādīt nederīgus vai atsauktus atribūtus no maka, kas regulāri neveido savienojumu ar tīklu.	Ietekme uz dažādiem riskiem
TR107	Uzbrucējs var nozagt informāciju no lietotāja, viltojot maku.	Ietekme uz dažādiem riskiem
TR108	Uzbrucējs var uzdoties par lietotāju, reproducējot/imitējot datu pieprasījumu (piemēram, autentificēšanu), kas izskatītos derīgs.	Ietekme uz dažādiem riskiem
TR109	Uzbrucējs var reproducēt iegulto informācijas izpaušanas procedūru attiecībā uz lietotāju, lai imitētu apstiprinātu pieprasījumu.	Ietekme uz dažādiem riskiem
TR110	Uzbrucējs var izmantot maka lietotāju informācijas trūkumu vai nepamatotu kavēšanos pēc drošības pārkāpuma vai kompromitējuma.	Ietekme uz dažādiem riskiem
TR111	Uzbrucējs var pārveidot iepriekš instalētu likumīgu maka instanci, lai pievienotu ļaunprātīgus elementus.	Ietekme uz dažādiem riskiem
TR112	Uzbrucējs var mainīt likumīgu maka instanci un piedāvāt to lietotājiem kā likumīgu.	Ietekme uz dažādiem riskiem
TR113	Uzbrucējs var neitralizēt pašu lietotāja autentifikācijas mehānismu, lai apietu maka lietotāja autentifikāciju.	Ietekme uz dažādiem riskiem
TR114	Kad maka kods tiek instalēts lietotāja ierīcē, uzbrucējs tajā var ievadīt ļaunprātīgu kodu vai slepenpiekļuves.	Ietekme uz dažādiem riskiem
TR115	Uzbrucējs maka kodā tā izstrādes laikā var ievadīt ļaunprātīgu kodu vai slepenpiekļuves.	Ietekme uz dažādiem riskiem
TR116	Uzbrucējs var manipulēt ar gadījumskaitļu ģenerēšanu, lai pietiekami samazinātu to entropiju, tādējādi ļaujot veikt uzbrukumus.	Ietekme uz dažādiem riskiem

ID *Identifikators*	Apdraudējuma apraksts *Identificētā apdraudējuma apraksts* (*)	Riska nosaukums *Saistītie riski*
TR117	Uzbrucējs var veikt manipulācijas ar lietotāja ierīcēm piegādes ķēdē, lai iekļautu kodu vai konfigurācijas, kas neatbilst maka lietošanas nosacījumiem.	Ietekme uz dažādiem riskiem
TR118	Uzbrucējs var aktivizēt maka vienību, izmantojot uzbrucēju kontrolētu viltotu *WSCD*.	Ietekme uz dažādiem riskiem
TR119	Uzbrucējs var izlasīt *WSCA* un/vai *WSCD* nosūtīto informāciju.	Ietekme uz dažādiem riskiem
TR120	Uzbrucējs var nosūtīt patvaļīgi iegūtu informāciju *WSCA*.	Ietekme uz dažādiem riskiem
TR121	Uzbrucējs var nozagt informāciju, pārtverot informācijas apmaiņu starp *WSCA* un *WSCD*.	Ietekme uz dažādiem riskiem
TR122	Uzbrucējs var nosūtīt patvaļīgi iegūtu informāciju *WSCD*.	Ietekme uz dažādiem riskiem
TR123	Uzbrucējs var nosūtīt informāciju *WSCD*, apejot *WSCA*.	Ietekme uz dažādiem riskiem
TR124	Uzbrucējs var izmantot pikšķerēšanu, lai piesaistītu lietotājus viltotam makam un PID pārvaldības tīmekļa lietotnei.	Ietekme uz dažādiem riskiem
TR125	Uzbrucējs maka atslēgas var aizstāt ar citām atslēgām, lai radītu ziņojumus, ko izmantot citā uzbrukumā.	Ietekme uz dažādiem riskiem
TR126	Uzbrucējs var pārveidot vai iznīcināt maka atslēgas, padarot dažas maka funkcijas neizmantojamas.	Ietekme uz dažādiem riskiem
TR127	Uzbrucējs var kontrolēt ļaunprogrammatūru, lai piekļūtu makā glabātajiem datiem.	Ietekme uz dažādiem riskiem
TR128	Uzbrucējs var piekļūt makā ģenerētiem pierādījumiem.	Ietekme uz dažādiem riskiem
TR129	Maku nodrošinātāji var piekļūt objektiem makā.	Ietekme uz dažādiem riskiem
TR130	Maku nodrošinātāji var piekļūt makā ģenerētiem pierādījumiem.	Ietekme uz dažādiem riskiem
TR131	Uzbrucējs var nozagt neaizslēgtu maka ierīci.	Ietekme uz dažādiem riskiem
TR132	Uzbrucējs var manipulēt ar sistēmu, lai nepieļautu konkrētu notikumu reģistrēšanu.	Ietekme uz dažādiem riskiem
TR133	Uzbrucējs var pārtvert saziņu starp maku un *WSCA* vai reproducēt/imitēt lietotāju (piemēram, pārņemot autentifikācijas mehānismu).	Ietekme uz dažādiem riskiem

II PIELIKUMS

KRITĒRIJI UZTICAMĪBAS INFORMĀCIJAS PIEŅEMAMĪBAS NOVĒRTĒŠANAI

Nosaukums	Priekšmets	Aspekti, kam būtu jāpievērš uzmanība
EUCC	IKT produkti	Par izdevēju: nav (akreditētas sertifikācijas struktūras) Par darbības jomu: — pārbauda aizsardzības profilu un drošības mērķi — pārbauda izvērtējuma uzticamības līmeni un papildinājumus Par uzticamību: — pārbauda ierobežojumus lietotāja dokumentācijā — Attiecībā uz sastāvu var pieprasīt piekļuvi izvērtēšanas tehniskajam ziņojumam
EUCS (ja pieejams)	Mākoņpakalpojumi	Par izdevēju: nav (akreditētas sertifikācijas struktūras) Par darbības jomu: — pārbauda mākoņpakalpojumu aprakstu — pārbauda izvērtējuma līmeni un paplašinājuma profilus Par uzticamību: — pārbauda informāciju par pārredzamību un vajadzības gadījumā informāciju par sastāvu
Uz vienotajiem kritērijiem balstītas sertifikācijas shēmas, kas darbojas ES, to vidū *SOG-IS* shēmas	IKT produkti	Par izdevēju: nav (dalībvalstis) Par darbības jomu: — pārbauda aizsardzības profilu un drošības mērķi — pārbauda izvērtējuma uzticamības līmeni un papildinājumus Par uzticamību: — pārbauda ierobežojumus lietotāja dokumentācijā — Attiecībā uz sastāvu var pieprasīt piekļuvi izvērtēšanas tehniskajam ziņojumam
EN 17640:2018 (*FITCEM*, ieskaitot *CSPN, BSZ, LINCE, BSZA*)	IKT produkti	Par izdevēju: — pārbauda shēmu un prasības attiecībā uz sertifikācijas struktūrām Par darbības jomu: — pārbauda produkta aprakstu — pārbauda drošības apgalvojumus — pārbauda uzticamības līmeņus Par uzticamību: — pārbauda veiktās darbības un konstatējumus ziņojumā
Kvalificētu paraksta radīšanas ierīču sertifikācijas shēmas saskaņā ar Regulas (ES) Nr. 910/2014 30. pantu.	*QSCD*	Par izdevēju: — pārbauda shēmu un prasības attiecībā uz sertifikācijas struktūrām Par darbības jomu: — pārbauda produkta aprakstu — pārbauda drošības apgalvojumus — pārbauda uzticamības līmeņus Par uzticamību: — pārbauda veiktās darbības

Nosaukums	Priekšmets	Aspekti, kam būtu jāpievērš uzmanība
EN ISO/IEC 27001:2022	*ISMS*	Par izdevēju: nav (akreditētās sertifikācijas struktūras) Par darbības jomu: — pārbauda pārvaldības sistēmas aprakstu — pārbauda paziņojumu par piemērojamību Par uzticamību: — pārbauda veiktās darbības
SOC2	Organizācijas	Par izdevēju: — pārbauda izdevēja publiskā konta statusu Par darbības jomu: — pārbauda pārvaldības pārskatu un kontroļu aprakstu — pārbauda paziņojumu par piemērojamību Par uzticamību: — pārbauda ziņojuma konstatējumus — Vajadzības gadījumā pārbaudīt saskaņošanas vēstules
MDSCert (*GSMA*) (ja pieejams)	Mobilās ierīces	Par izdevēju: — pārbauda prasības attiecībā uz sertifikācijas struktūrām Par darbības jomu: — pārbauda drošības uzticamības līmeni — pārbauda shēmas prasības Par uzticamību: — pārbauda ziņojumā iekļautās darbības un konstatējumus
Citas shēmas	Jebkurš komponents	Par shēmu: — pārbauda shēmas atbilstību un noteikumus Par izdevēju: — pārbauda prasības attiecībā uz sertifikācijas struktūrām Par darbības jomu: — pārbauda shēmas prasības — pārbauda drošības mērķi vai līdzīgu dokumentu, kurā aprakstītas drošības funkcionālās un uzticamības prasības — pārbauda produkta aprakstu un atlasītās drošības funkcionālās prasības Par uzticamību: — pārbauda ziņojumā iekļautās darbības un konstatējumus

III PIELIKUMS

FUNKCIONĀLĀS PRASĪBAS MAKA RISINĀJUMIEM

Saskaņā ar Regulas (ES) Nr. 910/2014 5.a panta 4., 5., 8. un 14. punktu funkcionālie kritēriji, kuriem jāatbilst sertificēta maka risinājumam un elektroniskās identifikācijas shēmai, saskaņā ar kuru tas tiek nodrošināts, ietver funkcionālās prasības attiecībā uz darbībām, kas uzskaitītas turpmāk minētajos aktos:

1) Komisijas Īstenošanas regulā (ES) 2024/2979, ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz integritāti un pamatfunkcijām ([1]);

2) Komisijas Īstenošanas regulā (ES) 2024/2982, ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes satvara atbalstāmajiem protokoliem un saskarnēm ([2]);

3) Komisijas Īstenošanas regulā (ES) 2024/2977, ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes makiem izsniegtajiem personas identifikācijas datiem un atribūtu elektroniskajiem apliecinājumiem ([3]).

([1]) Komisijas Īstenošanas regula (ES) 2024/2979 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz integritāti un pamatfunkcijām (OV L, 2024/2979, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([2]) Komisijas Īstenošanas regula (ES) 2024/2982 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes satvara atbalstāmajiem protokoliem un saskarnēm (OV L, 2024/2982, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([3]) Komisijas Īstenošanas regula (ES) 2024/2977 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes makiem izsniegtajiem personas identifikācijas datiem un atribūtu elektroniskajiem apliecinājumiem (OV L, 2024/2977, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

IV PIELIKUMS

METODES UN PROCEDŪRAS IZVĒRTĒŠANAS DARBĪBU VEIKŠANAI

1. **Maka risinājuma īstenošanas revīzija**

Atbilstības novērtēšanas darbība ietver konkrētu izvērtēšanas darbību atlasi.

Valsts sertifikācijas shēmās norāda izvērtēšanas darbību nolūkā novērtēt sniegto informāciju, ietverot vismaz šādus aspektus:

a) sniegtās informācijas analīze ar mērķi apstiprināt, ka tā ir piemērota kādai no valsts sertifikācijas shēmās noteiktajām arhitektūrām;

b) analīze par to kiberdrošības risku un apdraudējumu aptvērumu, kas noteikti I pielikuma risku reģistrā, veicot aprakstītos drošības kontroles pasākumus.

Šā punkta a) un b) apakšpunktā minētās analīzes pamatā ir maka nodrošinātāja sniegtais pamatojums un argumentācija.

2. **Izvērtēšanas darbības, kas saistītas ar maka drošas kriptogrāfijas ierīci**

1) Kritiski svarīgas operācijas, to vidū kriptogrāfiskie aprēķini, nav pilnībā jāīsteno *WSCD*. Tomēr *WSCD* īstenotā daļa, kad tā darbojas kā daļa no maka risinājuma, saskaņā ar Komisijas Īstenošanas regulu (ES) 2015/1502 ([1]) garantē tās veikto kritiski svarīgo operāciju aizsardzību pret uzbrukumiem, ko veic uzbrucēji ar augstu uzbrukuma potenciālu.

2) *WSCD* vai tā daļa var ietilpt sertifikācijas priekšmetā, ja to nodrošina sertifikāta turētājs vai pieteikuma iesniedzējs, vai būt ārpus tā tvēruma, ja tā ir iegulta galalietotāja nodrošinātā ierīcē. Turklāt valsts sertifikācijas shēmās precizē izvērtēšanas darbības, lai verificētu *WSCD* piemērotību, divos šādos gadījumos:

   a) ja *WSCA* ir atkarīga no konkrētā *WSCD* (t. i., ja tā ir jānovērtē kā salikts produkts, kura pamatā ir *WSCD*), *WSCA* izvērtēšanā ir vajadzīga piekļuve papildu informācijai, kas saistīta ar *WSCD* sertifikāciju, tajā skaitā jo īpaši tās izvērtēšanas tehniskajam ziņojumam;

   b) ja shēmā aplūkotajā arhitektūrā tiek izmantotas vairākas *WSCD* vai ja dažas darbības ar kritiski svarīgiem aktīviem tiek veiktas ārpus *WSCD*, tad valsts sertifikācijas shēmās iekļauj izvērtēšanas darbības, lai nodrošinātu, ka vispārējais risinājums nodrošina vēlamo drošības līmeni.

3) Priekšnoteikums sertifikācijai saskaņā ar valsts sertifikācijas shēmām ir *WSCD* novērtēšana atbilstoši Īstenošanas regulā (ES) 2015/1502 izklāstītajām uzticamības līmeņa "augsts" prasībām.

   Ja ir izpildīti 3. panta 3. punkta b) apakšpunkta nosacījumi, *WSCD* vai tās daļas izvērtēšanā iekļauj ievainojamības novērtējumu saskaņā ar standartu EN ISO/IEC 15408-3:2022 AVA_VAN 5. līmenī, kā noteikts Komisijas Īstenošanas regulas (ES) 2024/482 ([2]) I pielikumā, ja vien sertifikācijas struktūrai nav pienācīgi pamatots, ka *WSCA* drošības raksturlielumi ļauj izmantot zemāku novērtējuma līmeni, vienlaikus saglabājot tādu pašu vispārējo uzticamības līmeni, kāds noteikts Īstenošanas regulā (ES) 2015/1502.

([1]) Komisijas Īstenošanas regula (ES) 2015/1502 (2015. gada 8. septembris), kas saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 8. panta 3. punktu nosaka elektroniskās identifikācijas līdzekļu uzticamības līmeņu minimālās tehniskās specifikācijas un procedūras (OV L 235, 9.9.2015., 7. lpp., ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

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

4) Turklāt ar katru konkrēto arhitektūru saistītajā dokumentācijā valsts sertifikācijas shēmas formulē pieņēmumus šai *WSCD* izvērtēšanai, ar kuriem var nodrošināt noturību pret uzbrucējiem ar augstu uzbrukuma potenciālu saskaņā ar Īstenošanas regulu (ES) 2015/1502, un norāda izvērtēšanas darbības, ar kurām šos pieņēmumus apstiprina un pēc sertifikāta izsniegšanas apstiprina, ka pieņēmumi joprojām ir verificēti. Valsts shēmās arī nosaka, ka sertifikācijas kandidātiem ir jāprecizē šie pieņēmumi attiecībā uz konkrēto īstenošanu un jāapraksta pasākumi, kas ieviesti, lai garantētu, ka pieņēmumi tiek verificēti visā sertifikācijas ciklā.

5) Visos gadījumos valsts sertifikācijas shēmas ietver izvērtēšanas darbību, ar kuru verificē, vai pieejamā uzticamības informācija par *WSCD* ir piemērota maka risinājumam, analizējot uzticamības informāciju, piemēram, *EUCC* sertifikātu drošības mērķi, ieskaitot šādas darbības:

   a) verifikāciju attiecībā uz izvērtēšanas tvēruma piemērotību, kas, piemēram, *EUCC* sertifikātu gadījumā nozīmē verificēt, vai drošības mērķis apliecina atbilstību kādam no *EUCC* ieteiktajiem aizsardzības profiliem;

   b) verifikāciju attiecībā uz pieņēmumu par darbības vidi saderību ar maka risinājumu, kas, piemēram, *EUCC* sertifikātu gadījumā nozīmē, ka šos pieņēmumus var atrast drošības mērķī;

   c) verifikāciju attiecībā uz to, vai ieteikumi lietotāja norādījumos vai dokumentācijā ir saderīgi ar nosacījumiem, saskaņā ar kuriem *WSCD* ir jāizmanto maka risinājumā;

   d) verifikāciju attiecībā uz to, vai valsts sertifikācijas shēmā izdarītie pieņēmumi par *WSCD* ir verificēti un ietverti uzticamības informācijā.

6) Gadījumos, kad dažas verifikācijas nav pilnībā pārliecinošas, valsts sertifikācijas shēmas nosaka, ka sertifikācijas struktūrām jānorāda kompensējošas prasības attiecībā uz maka drošas kriptogrāfijas lietojumprogrammu (*WSCA*), pamatojoties uz *WSCD*, kura jāiekļauj *WSCA* izvērtēšanā. Ja tas nav iespējams, valsts sertifikācijas shēmas uzskata *WSCD* par nepiemērotu, kas nozīmē, ka maka risinājumam neizdod atbilstības sertifikātu.

3. **Izvērtēšanas darbības, kas saistītas ar maka drošas kriptogrāfijas lietojumprogrammu (*WSCA*)**

1) Valsts sertifikācijas shēmas paredz, ka *WSCA* kā daļa no maka risinājuma ir jāizvērtē, ņemot vērā vismaz uzticamības līmeņa "augsts" prasības, kā noteikts Īstenošanas regulā (ES) 2015/1502.

2) Šajā izvērtēšanā iekļauj ievainojamības novērtējumu saskaņā ar standartu EN ISO/IEC 15408-3:2022 AVA_VAN 5. līmenī, kā noteikts Īstenošanas regulas (ES) 2024/482 I pielikumā, ja vien sertifikācijas struktūrai nav pienācīgi pamatots, ka *WSCA* drošības raksturlielumi ļauj izmantot zemāku novērtējuma līmeni, vienlaikus saglabājot tādu pašu vispārējo uzticamības līmeni, kāds noteikts Īstenošanas regulā (ES) 2015/1502.

3) Gadījumos, kad *WSCA* nenodrošina maka nodrošinātājs, valsts sertifikācijas shēmas šai *WSCA* izvērtēšanai formulē pieņēmumus, saskaņā ar kuriem var nodrošināt noturību pret uzbrucējiem ar augstu uzbrukuma potenciālu saskaņā ar Īstenošanas regulu (ES) 2015/1502, un precizē izvērtēšanas darbības, ar kurām šos pieņēmumus apstiprina un pēc sertifikāta izsniegšanas apstiprina, ka pieņēmumi joprojām ir verificēti. Valsts shēmās arī nosaka, ka sertifikācijas kandidātiem ir jāprecizē šie pieņēmumi attiecībā uz konkrēto īstenošanu un jāapraksta pasākumi, kas ieviesti, lai garantētu, ka pieņēmumi tiek verificēti visā sertifikācijas ciklā.

4) Visos gadījumos valsts sertifikācijas shēmas ietver izvērtēšanas darbību, ar kuru verificē, vai pieejamā uzticamības informācija par *WSCA* ir piemērota maka risinājumam, analizējot uzticamības informāciju, piemēram, *EUCC* sertifikātu drošības mērķi, ieskaitot šādas darbības:

   a) verifikāciju attiecībā uz izvērtēšanas tvēruma piemērotību, kas, piemēram, *EUCC* sertifikātu gadījumā nozīmē verificēt, vai drošības mērķis apliecina atbilstību kādam no *EUCC* ieteiktajiem aizsardzības profiliem;

   b) verifikāciju attiecībā uz pieņēmumu par darbības vidi saderību ar maka risinājumu, kas, piemēram, *EUCC* sertifikātu gadījumā nozīmē, ka šos pieņēmumus var atrast drošības mērķī;

c) verifikāciju attiecībā uz to, vai ieteikumi lietotāja norādījumos vai dokumentācijā ir saderīgi ar nosacījumiem, saskaņā ar kuriem *WSCA* ir jāizmanto maka risinājumā;

d) verifikāciju attiecībā uz to, vai valsts sertifikācijas shēmā izdarītie pieņēmumi par *WSCA* ir verificēti un ietverti uzticamības informācijā.

5) Valsts sertifikācijas shēmās nosaka prasību, ka WSCA izvērtēšana aptver visas drošības kontroles, ko šī WSCA īsteno.

4. **Ar galalietotāja ierīci saistītās izvērtēšanas darbības**

Tā kā riska reģistrā, kas noteikts šīs regulas I pielikumā, ir uzskaitīti riski, kas ir tieši saistīti ar galalietotāja ierīces drošību, valsts sertifikācijas shēmās precizē drošības prasības attiecībā uz galalietotāja ierīcēm. Tomēr, tā kā šīs ierīces nodrošina galalietotājs, nevis maku nodrošinātājs, uz šīm prasībām attiecas pieņēmumi.

Attiecībā uz katru pieņēmumu maka risinājumā iekļauj mehānismu, ar ko attiecībā uz katru maka vienību verificē pamatā esošās galalietotāja ierīces atbilstību pieņēmumam. Šādus mehānismus uzskata par drošības kontroli, un uz tiem attiecas izvērtēšanas darbības, lai pierādītu gan to piemērotību, gan efektivitāti atbilstošā uzticamības līmenī.

Tālāk ir sniegti divi piemēri:

a) galalietotāja ierīcē var būt sertificēta *WSCD*, kas ir jāpierāda. Parasti tas tiktu darīts, izmantojot kriptogrāfijas mehānismu, lai verificētu, vai sertificētajā *WSCD* ir kriptogrāfisks noslēpums, kas ir pieejams tikai sertificētajā *WSCD*. Šajā gadījumā šis kriptogrāfiskais noslēpums būtu jāuzskata par kritiski svarīgu aktīvu, un uz to būtu jāattiecina *WSCD* un/vai *WSCA* sertifikācija;

b) tipiska prasība attiecībā uz galalietotāja ierīcēm būtu tāda, ka ierīcēm ir jānodrošina drošības atjauninājumi. Tā kā šī prasība ir saistīta ar maka instanci, mehānisms, ko izmanto drošības atjauninājumu pieejamības verificēšanai, ir jāiekļauj izvērtēšanas darbībās tikai tādā uzticamības līmenī, kāds ir piemērots maka instancei, jo īpaši tāpēc, ka tas, visticamāk, tiks integrēts maka instancē.

5. **Izvērtēšanas darbības, kas saistītas ar maka instanci**

1) Maka instances izvērtēšanā ņem vērā šādas divas galvenās problēmas:

a) maka instance, visticamāk, pastāv viena un tā paša pamatlietojuma variantu kopumā, un katrs variants ir specializēts konkrētai galalietotāju ierīču kategorijai;

b) dažādi maka instances varianti, visticamāk, būs regulāri jāatjaunina, lai sekotu pamatā esošās drošības platformas attīstībai, piemēram, ja tiks konstatētas ievainojamības, kuru dēļ lietojumprogrammās ir jāveic izmaiņas.

2) Maka izvērtēšanā ņem vērā šīs konkrētās problēmas. Viena no tūlītējām sekām ir tāda, ka vienoto kritēriju sistēma var nebūt piemērota visos gadījumos. Tādēļ vajadzības gadījumā jāapsver alternatīvas izvērtēšanas metodes. Valsts sertifikācijas shēmās izvērtē EN 17640:2018 metodikas izmantošanu:

a) kā daļu no pašas shēmas;

b) izmantojot valsts shēmas, kuru pamatā ir metodika;

c) izmantojot valsts shēmas, kuru pamatā ir līdzīgi principi, bet kuras izveidotas pirms EN 17640:2018 metodikas izstrādes.

3) Turklāt, tā kā katra varianta pilnīgas īpašas izvērtēšanas pievienotā vērtība var būt ierobežota, valsts sertifikācijas shēmās jāizvērtē iespēja precizēt kritērijus, kas ļauj veidot izlasi nolūkā izvairīties no identisku izvērtēšanas darbību atkārtošanās un koncentrēties uz darbībām, kas ir specifiskas konkrētam variantam. Valsts sertifikācijas shēmās nosaka, ka visām sertifikācijas struktūrām jāpamato izlases izmantošana.

4) Valsts sertifikācijas shēmās maka instances atjauninājumus iekļauj vispārējā izmaiņu pārvaldības procesā, kas noteikts maka risinājumam. Tajās paredz arī noteikumus par procedūrām, kas maka nodrošinātājam jāveic katram atjauninājumam (piemēram, analīze par izmaiņu ietekmi uz drošības kontrolēm), un par izvērtēšanas darbībām, ko sertifikācijas struktūra veic attiecībā uz atjauninājumiem noteiktos apstākļos (piemēram, grozītās drošības kontroles darbības efektivitātes novērtēšana). Izmaiņu pārvaldības process ir viens no procesiem, kura darbības efektivitāte ir jāpārbauda katru gadu saskaņā ar 18. panta 3. punktu.

6. **Izvērtēšanas darbības saistībā ar pakalpojumiem un procesiem, ko izmanto maka risinājuma nodrošināšanai un darbībai**

1) Lai novērtētu pakalpojumus un procesus, kam ir nozīme maka risinājuma un tās elektroniskās identifikācijas shēmas nodrošināšanā un darbībā, saskaņā ar kuru tas tiek nodrošināts, izvērtēšanas grupa vāc pierādījumus, veicot izvērtēšanas darbības, kas var ietvert revīzijas, pārbaudes, verifikācijas un validācijas darbības.

2) Sertifikācijas struktūra apstiprina pierādījumu pietiekamību un piemērotību tam, lai nodrošinātu pietiekamu uzticamību, ka pakalpojumi un procesi atbilst sertifikācijas prasībām, apstiprinot:

   a) procesu un pakalpojumu aprakstā sniegtās informācijas pareizību;

   b) procesu un pakalpojumu izstrādes un kontroles piemērotību izvērtēšanas kritēriju izpildei;

   c) šo kontroļu īstenošanas darbības efektivitāti noteiktā laikposmā pirms izvērtēšanas.

3) Apraksta pareizību un kontroles pasākumu īstenošanas darbības efektivitāti var uzskatīt par verifikācijas mērķiem ISO/IEC 17000:2020 nozīmē attiecībā uz attiecīgajiem maka nodrošinātāja apgalvojumiem (t. i., apstiprinājumu par jau notikušo notikumu vai jau iegūto rezultātu godīgumu), savukārt pakalpojumu un procesu izstrādes un kontroles piemērotību izvērtēšanas kritēriju izpildei var uzskatīt par attiecīgā maka nodrošinātāja apgalvojuma validācijas mērķi ISO/IEC 17000:2020 nozīmē (t. i., apstiprinājumu par ticamību attiecībā uz paredzēto turpmāko izmantošanu vai prognozēto iznākumu).

4) Ņemot vērā to, ka maka risinājumam nav atļauts darboties pirms tā sertificēšanas, darbības efektivitāti nevar apstiprināt, pamatojoties uz risinājuma faktisko darbību. Tāpēc to apstiprina, izmantojot izmēģinājumu vai testu laikā savāktos pierādījumus.

5) Valsts sertifikācijas shēmas, iespējams, jau ir izveidotas attiecībā uz konkrētiem pakalpojumiem un procesiem, piemēram, lietotāju pievienošanu. Attiecīgā gadījumā valstu sertifikācijas shēmās izvērtē šādu shēmu izmantošanu.

7. **Izvērtēšanas darbības saistībā ar IKT pakalpojumiem, ko izmanto maka risinājuma nodrošināšanai un darbībai**

1) Dažas maku arhitektūras var būt atkarīgas no specializētiem IKT pakalpojumiem, to vidū mākoņpakalpojumiem maka risinājuma nodrošināšanai un darbībai, un šie pakalpojumi var mitināt sensitīvus datus, kā arī sensitīvas darbības. Šādā gadījumā valsts sertifikācijas shēmās nosaka drošības prasības attiecībā uz šiem IKT pakalpojumiem.

2) Jau pastāv daudzas sertifikācijas shēmas IKT pakalpojumiem, mākoņpakalpojumiem un citiem uzticamības informācijas avotiem, arī tiem, kas uzskaitīti II pielikumā. Valsts sertifikācijas shēmas, ja tās ir pieejamas un piemērojamas, paļaujas uz minētajiem pastāvošajiem mehānismiem, izmantojot vienu no šādiem mehānismiem:

   a) tiek dots pilnvarojums izmantot konkrētu shēmu vai shēmu izlasi, precizējot nosacījumus, saskaņā ar kuriem IKT vai mākoņpakalpojumi jānovērtē šo shēmu ietvaros;

   b) novērtējuma izvēle tiek atstāta maka nodrošinātāja ziņā un šajos novērtējumos iegūtās uzticamības informācijas piemērotība tiek analizēta, izmantojot atkarības analīzes darbību.

3) Abos gadījumos valsts sertifikācijas shēmās, ja nepieciešams, norāda papildu izvērtēšanas darbības, lai analizētu vai papildinātu informāciju, kura iegūta, izmantojot šīs shēmas.

V PIELIKUMS

SARAKSTS AR PUBLISKI PIEEJAMU INFORMĀCIJU PAR MAKIEM

1. Informācijā, ko publisko saskaņā ar 8. panta 5. punktu, iekļauj vismaz šādas ziņas:

   a) maka risinājuma izmantošanas ierobežojumi;

   b) maka nodrošinātāja norādījumi un ieteikumi nolūkā palīdzēt galalietotājiem droši konfigurēt, instalēt, izvērst, lietot un uzturēt makus;

   c) laikposms, kādā galalietotājiem tiks piedāvāts drošības atbalsts, jo īpaši attiecībā uz atjauninājumu pieejamību saistībā ar kiberdrošību;

   d) ražotāja vai sniedzēja kontaktinformācija un akceptētās metodes informācijas par ievainojamību saņemšanai no galalietotājiem un drošības pētniekiem;

   e) atsauce uz tiešsaistes repozitorijiem, kuros uzskaitītas publiski atklātās ar makiem saistītās ievainojamības, un uz visiem attiecīgiem kiberdrošības padomdevējiem.

2. Šā panta 1. punktā minēto informāciju skaidrā, visaptverošā un viegli pieejamā veidā publiski pieejamā vietā dara pieejamu jebkurai personai, kas vēlas izmantot maka risinājumu.

VI PIELIKUMS

UZTICAMĪBAS INFORMĀCIJAS PIEŅEMAMĪBAS NOVĒRTĒŠANAS METODIKA

1. **Uzticamības dokumentācijas pieejamības novērtēšana**

Izvērtētāji norāda uzticamības dokumentāciju, kas pieejama par katru attiecīgo maka risinājuma komponentu un elektroniskās identifikācijas shēmu, saskaņā ar kuru tas tiek nodrošināts. Pēc tam izvērtētāji novērtē katra uzticamības dokumenta vispārējo atbilstību atkarības pārbaudei.

Analīzē ņem vērā šādus aspektus:

1) attiecībā uz pašu uzticamības dokumentāciju:

   a) uzticamības dokumentācijas veids ar visām vajadzīgajām ziņām,

      (šādu dokumentu piemēri ir atbilstības sertifikāti saskaņā ar EN ISO/IEC 27001:2022 vai 1. vai 2. tipa *ISAE* ziņojumi);

   b) aptvertais laikposms vai derīguma termiņš, (šo periodu var papildināt ar saskaņošanas vēstuli (dokumentu, kas aptver laikposmu no pašreizējā *ISAE* ziņojuma pārskata perioda beigu datuma līdz jauna *ISAE* ziņojuma publiskošanai) vai līdzīgu paziņojumu);
   c) piemērojamais regulējums (piemēram, spēkā esošais standarts);

   d) tas, vai uzticamības dokumentācija ietver shēmas prasību kartēšanu;

2) attiecībā uz uzticamības ziņojuma izdevēja profesionālo kompetenci un objektivitāti:

   a) sertifikācijas struktūras nosaukums un, ja pieejams, galvenā vērtētāja vārds;

   b) pierādījumi par sertifikācijas struktūras un vērtētāja kompetenci (piemēram, akreditācija, personīgā sertifikācija u. c.);

   c) pierādījumi par sertifikācijas struktūras un vērtētāja objektivitāti (piemēram, akreditācija u. c.).

2. **Uzticamības novērtēšana saistībā ar individuālām prasībām**

Izvērtētāji verificē, vai pieejamā uzticamības dokumentācija par maka risinājumu un elektroniskās identifikācijas shēmu, saskaņā ar kuru tie tiek nodrošināti, ir pietiekama, lai noteiktu, vai maka risinājums atbilst gaidām attiecībā uz sertifikācijas shēmas individuālajām prasībām.

Šo novērtēšanu veic par katru attiecīgo maka risinājuma komponentu un elektroniskās identifikācijas shēmu, saskaņā ar kuru tas tiek nodrošināts, formulējot pieņēmumu par maka risinājuma drošības kontrolēm.

Attiecībā uz katru šādu pieņēmumu izvērtēšanas grupa nosaka, vai pieejamā uzticamības dokumentācija nodrošina pietiekamu uzticamību.

Lai noteiktu, vai uzticamība ir pietiekama, ņem vērā turpmāk minēto:

1) prasītā informācija ir pieejama uzticamības dokumentācijā un ir norādīts sagaidāmais uzticamības līmenis;

2) uzticamības dokumentācijā pieejamā informācija neaptver visu prasības darbības jomu, bet papildu kontroles vai kompensējošas kontroles (t. i., iekšējās kontroles, kas samazina esošo vai potenciālo kontroles nepilnību risku), kuras īsteno maka risinājumā vai elektroniskās identifikācijas shēmā, saskaņā ar kuru to nodrošina, ļauj izvērtētājiem noteikt, vai informācija ir pietiekama;

3) uzticamības dokumentācijā pieejamā informācija nesniedz gaidīto uzticamības līmeni, bet kontroles pasākumi, kas īstenoti, lai novērtētu un uzraudzītu maka nodrošināju, ļauj vērtētājiem noteikt, vai informācija ir pietiekama;

4) ja uzticamības dokumentācijā ir minētas neatbilstības to kontroļu izstrādē vai īstenošanā, kuras izmantotas, lai izpildītu pieņēmumu, maka nodrošinātāja ierosinātās un īstenotās korektīvās darbības, ko novērtējuši tā izvērtētāji, ir pietiekamas, lai garantētu, ka pieņēmums patiešām ir izpildīts.

VII PIELIKUMS

ATBILSTĪBAS SERTIFIKĀTA SATURS

1. Unikāls identifikators, ko piešķīrusi sertifikācijas struktūra, kura izdod atbilstības sertifikātu.

2. Informācija saistībā ar sertificētu maka risinājumu un elektroniskās identifikācijas shēmu, saskaņā ar kuru tas tiek nodrošināts, un par atbilstības sertifikāta turētāju, ieskaitot šādas ziņas:
   a) maka risinājuma nosaukums;
   b) to elektroniskās identifikācijas shēmu nosaukums, saskaņā ar kurām tiek nodrošināts maka risinājums;
   c) maka risinājuma versija, kura tika izvērtēta;
   d) atbilstības sertifikāta turētāja vārds/nosaukums, adrese un kontaktinformācija;
   e) saite uz atbilstības sertifikāta turētāja tīmekļa vietni, kurā ietverta informācija, kas ir jādara publiski pieejama.

3. Informācija saistībā ar maka risinājuma un tās elektroniskās identifikācijas shēmas izvērtēšanu un sertificēšanu, saskaņā ar kurām tas tiek nodrošināts, ieskaitot šādas ziņas:
   a) tās sertifikācijas struktūras nosaukums, adrese un kontaktinformācija, kas izdevusi atbilstības sertifikātu;
   b) tās atbilstības novērtēšanas struktūras nosaukums, kas veikusi izvērtēšanu, kā arī informācija par tās akreditāciju (gadījumos, kad tā nav tā pati sertifikācijas struktūra);
   c) shēmas īpašnieka vārds/nosaukums;
   d) atsauces uz Regulu (ES) Nr. 910/2014 un šo regulu;
   e) atsauce uz sertifikācijas ziņojumu, kas saistīts ar atbilstības sertifikātu;
   f) atsauce uz sertifikācijas novērtējuma ziņojumu, kas saistīts ar atbilstības sertifikātu;
   g) atsauce uz izvērtēšanā izmantotajiem standartiem, arī to versijām;
   h) atbilstības sertifikāta izdošanas datums,
   i) atbilstības sertifikāta derīguma termiņš.

VIII PIELIKUMS

PUBLISKĀ SERTIFIKĀCIJAS ZIŅOJUMA UN SERTIFIKĀCIJAS NOVĒRTĒJUMA ZIŅOJUMA SATURS

1. Publiskajā sertifikācijas ziņojumā iekļauj vismaz šādu informāciju:
   a) kopsavilkums;
   b) maka risinājuma un tās elektroniskās identifikācijas shēmas identifikācija, saskaņā ar kuru tas tiek nodrošināts;
   c) maka risinājuma un tās elektroniskās identifikācijas shēmas apraksts, saskaņā ar kuru tas tiek nodrošināts;
   d) drošības informācija, kas jādara publiski pieejama, kā aprakstīts V pielikumā, vai norāde uz šo informāciju;
   e) provizoriskās revīzijas un validācijas plāna kopsavilkums;
   f) pārskatīšanas un sertifikācijas lēmuma kopsavilkums.

2. Sertifikācijas novērtējuma ziņojumā iekļauj vismaz:
   a) maka risinājuma koncepcijas, identifikācijas sistēmas un pievienošanas procesa aprakstu kopā ar riska novērtējumu un īpašo validācijas plānu;
   b) aprakstu par to, kā maka risinājums atbilst augsta uzticamības līmeņa prasībām un kā to pierāda saskaņā ar šo regulu veiktā maka risinājuma sertifikācijas novērtējuma rezultāti;
   c) aprakstu par to, kā novērtēta maka risinājuma un tās elektroniskās identifikācijas shēmas atbilstība, saskaņā ar kuru attiecīgās maka vienības ir nodrošinātas, jo īpaši atbilstība šādām prasībām:
      — prasības, kas izklāstītas Regulas (ES) Nr. 910/2014 5.a panta 4., 5. un 8. punktā,
      — prasības attiecībā uz loģisko nošķiršanu, kas noteiktas Regulas (ES) Nr. 910/2014 5.a panta 14. punktā,
      — attiecīgā gadījumā – Regulas (ES) Nr. 910/2014 5.a panta 24. punktā minētie standarti un tehniskās specifikācijas, vienlaikus aprakstot, kā šīs prasības ir saistītas ar attiecīgajām normatīvajām prasībām, ko nosaka valsts sertifikācijas shēmas;
   d) kopsavilkums par validācijas plāna izpildes rezultātiem, tajā skaitā par visām konstatētajām neatbilstībām.

IX PIELIKUMS

OBLIGĀTĀS UZRAUDZĪBAS IZVĒRTĒŠANAS GRAFIKS

1. Regulas 18. pantā ir noteiktas prasības attiecībā uz sertifikācijas ciklu, jo īpaši regulāras izvērtēšanas darbību veikšanu. Minētās darbības ietver vismaz šādus pasākumus:

   a) atbilstības novērtēšanas priekšmeta pilnīgu izvērtēšanu sākotnējās izvērtēšanas ietvaros un katras resertifikācijas izvērtēšanas ietvaros, ieskaitot jebkura produkta komponenta atjaunināšanas funkciju;

   b) ievainojamības novērtējumu sākotnējās izvērtēšanas ietvaros un katras resertifikācijas izvērtēšanas ietvaros, un vismaz reizi divos gados uzraudzības izvērtējumos, aptverot vismaz izmaiņas atbilstības novērtējuma priekšmetā un izmaiņas apdraudējuma vidē kopš pēdējā ievainojamības novērtējuma;

   c) papildu darbības, piemēram, ielaušanās testēšanu paaugstināta riska līmeņa vai jaunu apdraudējumu rašanās gadījumā;

   d) vismaz reizi gadā uzraudzības un resertifikācijas izvērtējumos izvērtē uzturēšanas procesu darbības efektivitāti, aptverot vismaz versiju kontroles, atjaunināšanas un ievainojamības pārvaldības procesus;

   e) pēc sekmīga pārskatīšanas un sertifikācijas lēmuma – atbilstības sertifikāta izdošanu pēc sākotnējās izvērtēšanas un pēc katras resertifikācijas izvērtēšanas.

2. Atsauces grafiks ir noteikts 1. tabulā, pamatojoties uz četru gadu ciklu, kur:

   a) pirmais gads sākas, kad pirmo reizi tiek izdots atbilstības sertifikāts, un

   b) visas izvērtēšanas darbības veic 12 mēnešu laikā pēc iepriekšējā gada izvērtēšanas.

3. Turpmāk 1. tabulā noteiktais grafiks ir ieteikums, kas paredzēts, lai nodrošinātu savlaicīgu resertifikāciju un izvairītos no traucējumiem maka risinājuma nodrošināšanā. Var būt iespējami citi grafiki, ja vien atbilstības sertifikāta derīguma termiņš nepārsniedz piecus gadus, kā noteikts Regulas (ES) Nr. 910/2014 5.c panta 4. punktā.

4. Papildus regulārajai izvērtēšanai, ja notiek būtiskas sertifikācijas subjekta vai apdraudējuma vides izmaiņas, pēc sertifikācijas struktūras vai atbilstības sertifikāta turētāja pieprasījuma var sākt īpašu izvērtēšanu.

5. Jebkura izvērtēšana, ieskaitot uzraudzības izvērtējumus un īpašus izvērtējumus, var būt par pamatu jauna atbilstības sertifikāta izdošanai, jo īpaši tad, ja sertifikācijas subjektā tiek veiktas būtiskas izmaiņas, bet ar tādu pašu derīguma termiņu, kāds ir sākotnējam atbilstības sertifikātam.

1. tabula

Pilns četru gadu izvērtēšanas cikls

Laiks	Izvērt. tips	Darbības
0. gads	Sākotnējā izvērtēšana	— Sertifikācijas priekšmeta pilnīga izvērtēšana, arī ievainojamības novērtējums — Arī funkcija, kas ļauj veikt atjauninājumus katrā programmatūras komponentā — Uzturēšanas procesu izvērtēšana, izņemot to darbības efektivitāti — Atbilstības sertifikāta izdošana un četru gadu cikla sākums
1. gads	Uzraudzība	— Uzturēšanas procesu darbības efektivitātes izvērtējums — Vismaz versijas pārbaude, atjaunināšana, ievainojamības pārvaldība — To izmaiņu izvērtējums, kas ietekmē produkta drošību

Laiks	Izvērt. tips	Darbības
2. gads	Uzraudzība	— Visa risinājuma ievainojamības novērtējums — Uzturēšanas procesu darbības efektivitātes izvērtējums — Vismaz versiju kontrole, atjaunināšana, ievainojamības pārvaldība — To izmaiņu izvērtējums, kas ietekmē produkta drošību
3. gads	Uzraudzība	— Uzturēšanas procesu darbības efektivitātes izvērtējums — Vismaz versijas pārbaude, atjaunināšana, ievainojamības pārvaldība — To izmaiņu izvērtējums, kas ietekmē produkta drošību
4. gads	Resertifikācija	1) Sertifikācijas priekšmeta pilnīga izvērtēšana, arī ievainojamības novērtējums 2) Vienkāršota tādu iezīmju/procesu izvērtēšana, kas nav mainījušies 3) Arī funkcija, kas ļauj veikt atjauninājumus katrā programmatūras komponentā 4) Uzturēšanas procesu izvērtējums, ieskaitot to darbības efektivitāti 5) Jauna atbilstības sertifikāta izdošana