Europos Sąjungos
oficialusis leidinys

LT
L serija

2024/2981

2024 12 4

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2024/2981

2024 m. lapkričio 28 d.

kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 nuostatų dėl europinių skaitmeninės tapatybės dėklių sertifikavimo taikymo taisyklės

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB ([1]), ypač į jo 5c straipsnio 6 dalį,

kadangi:

(1) pagal Reglamento (ES) Nr. 910/2014 5c straipsnį europinės skaitmeninės tapatybės dėklės (toliau – dėklės) turi būti sertifikuojamos laikantis funkcinių, kibernetinio saugumo ir duomenų apsaugos reikalavimų, kad būtų užtikrintas aukšto lygio dėklių saugumas ir pasitikėjimas jomis. Sertifikavimo reikalavimai turi būti suderinti visose valstybėse narėse, siekiant išvengti rinkos susiskaidymo ir sukurti patikimą sistemą;

(2) asmens duomenų tvarkymo veiklai pagal šį reglamentą taikomi Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 ([2]) ir, kai aktualu, Europos Parlamento ir Tarybos direktyva 2002/58/EB ([3]);

(3) Komisija reguliariai vertina naujas technologijas, praktiką, standartus ar technines specifikacijas. Siekiant užtikrinti aukščiausią valstybių narių suderinimo lygį kuriant ir sertifikuojant dėkles, šiame reglamente nustatytos techninės specifikacijos grindžiamos darbu, atliktu remiantis 2021 m. birželio 3 d. Komisijos rekomendacija (ES) 2021/946 dėl bendro Sąjungos priemonių rinkinio darniam Europos skaitmeninės tapatybės sistemos kūrimui užtikrinti ([4]), visų pirma jos architektūra ir pamatine sistema. Pagal Europos Parlamento ir Tarybos reglamento (ES) 2024/1183 ([5]) 75 konstatuojamąją dalį, Komisija prireikus turėtų šį įgyvendinimo reglamentą peržiūrėti ir atnaujinti, kad jis atitiktų pasaulinius pokyčius, architektūrą ir pamatinę sistemą ir būtų laikomasi geriausios vidaus rinkos praktikos;

(4) siekiant patvirtinti atitiktį į sertifikavimo sistemą įtrauktiems kibernetinio saugumo reikalavimams, dėklių sprendiniai, kai tai įmanoma ir svarbu, turėtų būti sertifikuojami pagal Europos kibernetinio saugumo sertifikavimo schemas, sukurtas pagal Europos Parlamento ir Tarybos reglamentą (ES) 2019/881 ([6]). Jei tokių schemų nėra arba jei jos apima kibernetinio saugumo reikalavimus tik iš dalies, šiame reglamente nustatomi bendrieji reikalavimai, taikomi nacionalinėms sertifikavimo schemoms, apimančioms funkcinius, kibernetinio saugumo ir duomenų apsaugos reikalavimus;

([1]) OL L 257, 2014 8 28, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).
([3]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).
([4]) OL L 210, 2021 6 14, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.
([5]) 2024 m. balandžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1183, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014, kiek tai susiję su Europos skaitmeninės tapatybės sistemos nustatymu, (OL L, 2024/1183, 2024 4 30, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).
([6]) 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) pagal Reglamento (ES) Nr. 910/2014 5a straipsnio 11 dalį, dėklės turi būti sertifikuojamos taikant aukštą saugumo užtikrinimo lygį, nustatytą Reglamente (ES) Nr. 910/2014 ir Komisijos įgyvendinimo reglamente (ES) 2015/1502 ([7]). Tokį saugumo užtikrinimo lygį turi pasiekti bendras dėklės sprendinys. Pagal šį reglamentą kai kurie dėklės sprendinio komponentai gali būti sertifikuojami taikant žemesnio saugumo užtikrinimo lygio reikalavimą, jei tai bus deramai pagrįsta ir nedarys poveikio aukštam saugumo užtikrinimo lygiui, kurį pasiekė bendras sprendinys;

(6) turėtų būti paskirtas kiekvienos nacionalinės sertifikavimo schemos savininkas, kuris bus atsakingas už sertifikavimo schemos kūrimą ir priežiūrą. Sertifikavimo schemos savininkas gali būti atitikties vertinimo įstaiga, valdžios įstaiga ar institucija, prekybos asociacija, atitikties vertinimo įstaigų grupė arba bet kuri atitinkama įstaiga, kuri nebūtinai turi būti nacionalinės sertifikavimo schemos vykdytoja;

(7) sertifikavimo objektas turėtų apimti dėklės sprendinio programinės įrangos komponentus, pavyzdžiui, dėklės egzempliorių. saugi dėklės šifravimo programa, saugus dėklės šifravimo įrenginys ir platformos, kuriose veikia šie programinės įrangos komponentai, nors ir yra operacinės aplinkos dalis, turėtų būti įtraukti į sertifikavimo objektą tik jei jie įtraukti į dėklės sprendinį. Kitais atvejais, ypač kai šiuos įrenginius ir platformas teikia galutiniai naudotojai, teikėjai turėtų nustatyti prielaidas dėl dėklės sprendinio operacinės aplinkos, be kita ko, dėl šių įrenginių ir platformų, ir įgyvendinti priemones, kuriomis būtų patvirtinta, kad šios prielaidos yra patikrintos praktiškai. Siekiant užtikrinti ypatingos svarbos turto apsaugą pasitelkiant aparatinę ir sisteminę programinę įrangą, naudojamą saugaus dėklės šifravimo įrenginio sukurtiems, saugomiems arba apdorojamiems kriptografiniams raktams valdyti ir apsaugoti, saugus dėklės šifravimo įrenginys turi atitikti aukštas sertifikavimo normas, nustatytas tarptautiniuose standartuose, pavyzdžiui, Komisijos įgyvendinimo reglamentu (ES) 2024/482 ([8]) nustatytuose bendruosiuose kriterijuose (toliau – EKSSS) pagal EAL4 vertinimą ir pažangioje metodinėje pažeidžiamumo analizėje, palyginamoje, pavyzdžiui, su AVA_VAN.5. Šios sertifikavimo normos turėtų būti taikomos ne vėliau kaip sertifikuojant dėklių atitiktį pagal Europos kibernetinio saugumo sertifikavimo schemą, priimtą pagal Reglamentą (ES) 2019/881;

(8) visiškai mobilioms, saugioms ir patogioms naudoti dėklėms reikia standartizuotų ir sertifikuotų manipuliavimui atsparių sprendinių, pavyzdžiui, įmontuotų saugių elementų, išorinių įrenginių, tokių kaip lustinės kortelės, arba mobiliuosiuose įrenginiuose integruotų SIM platformų; svarbu užtikrinti, kad nacionalinėms e. atpažinties priemonėms ir dėklėms būtų laiku suteikta prieiga prie įmontuotų saugių elementų, ir koordinuoti valstybių narių pastangas šioje srityje. Todėl pagal Reglamento (ES) Nr. 910/2014 46e straipsnio 1 dalį įsteigta Bendradarbiavimo dėl Europos skaitmeninės tapatybės grupė (toliau – Bendradarbiavimo grupė) šiuo tikslu turėtų įsteigti specialų pogrupį. Konsultuodamasis su atitinkamais suinteresuotaisiais subjektais, šis pogrupis turėtų susitarti dėl bendrų veiksmų gairių dėl prieigos prie įmontuotų saugių elementų, į kurias Komisija turėtų atsižvelgti rengdama Reglamento (ES) Nr. 910/2014 peržiūros ataskaitą. Siekdama palengvinti dėklės diegimą nacionaliniu lygmeniu, Komisija, bendradarbiaudama su valstybėmis narėmis, taip pat turėtų parengti ir nuolat atnaujinti naudojimo vadovą, kuris būtų architektūros ir pamatinės sistemos dalis;

(9) sertifikavimo pagal nacionalines sertifikavimo schemas objektas taip pat turėtų apimti procesus, kurie naudojami dėklės sprendiniui teikti ir naudoti, net jei tų procesų apibrėžimas ar vykdymas subrangos sutarties pagrindu pavedami trečiosioms šalims. Siekiant parodyti, kad procesai atitinka schemų reikalavimus, kaip įrodymą leidžiama naudoti saugumo užtikrinimo informaciją, su sąlyga, kad nustatant, ar tokios saugumo užtikrinimo informacijos pakanka, naudojama priklausomybės analizė. Saugumo užtikrinimo informacija gali būti įvairių formų, įskaitant ataskaitas ir atitikties sertifikatus, kurie gali būti privatūs, nacionaliniai, Europos ar tarptautiniai, grindžiami standartais arba techninėmis specifikacijomis. Priklausomybės analize siekiama įvertinti esamos saugumo užtikrinimo informacijos apie dėklės komponentus kokybę;

([7]) 2015 m. rugsėjo 8 d. Komisijos įgyvendinimo reglamentas (ES) 2015/1502, kuriuo pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 8 straipsnio 3 dalį nustatomos minimalios techninės specifikacijos ir procedūros dėl elektroninės atpažinties priemonių saugumo užtikrinimo lygių, (OL L 235, 2015 9 9, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([8]) 2024 m. sausio 31 d. Komisijos įgyvendinimo reglamentas (ES) 2024/482, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2019/881 taikymo taisyklės dėl bendraisiais kriterijais grindžiamos Europos kibernetinio saugumo sertifikavimo schemos (EKSSS) priėmimo, (OL L, 2024/482, 2024 2 7, ELI: http://data.europa.eu/eli/reg/2024/482/oj).

(10) vykdydama šiuo tikslu nustatytas procedūras, Bendradarbiavimo grupė turėtų galėti teikti nuomones ir rekomendacijas dėl jai pateiktų nacionalinių sertifikavimo schemų projektų. Šios nacionalinės sertifikavimo schemos turėtų būti pritaikytos dėklės architektūrai, nustatant kiekvienos konkrečios palaikomos architektūros konkrečius profilius;

(11) siekiant užtikrinti bendrą supratimą ir suderintą požiūrį į didžiausios rizikos, kuri gali turėti įtakos dėklių teikimui ir veikimui, vertinimą, turėtų būti sudarytas rizikos ir grėsmių, į kurias reikėtų atsižvelgti kuriant dėklių sprendinius nepriklausomai nuo jų konkrečios architektūros, registras. Nustatant, kokia rizika turėtų būti įtraukta į registrą, reikėtų atsižvelgti į Reglamente (ES) Nr. 910/2014 aprašytus kibernetinio saugumo tikslus, pavyzdžiui, dėklės sprendinio konfidencialumą, vientisumą ir prieinamumą, taip pat naudotojų ir duomenų privatumą. Kuriant nacionalinių sertifikavimo schemų reikalavimus reikėtų deramai atsižvelgti į riziką ir grėsmes, kurios įtrauktos į šį rizikos registrą. Siekiant neatsilikti nuo nuolat kintančios grėsmių padėties, rizikos registras turėtų būti tvarkomas ir reguliariai atnaujinamas bendradarbiaujant su Bendradarbiavimo grupe;

(12) kurdami savo sertifikavimo schemas, schemų savininkai turėtų atlikti rizikos vertinimą, kad galėtų patikslinti į registrą jau įtrauktą riziką ir grėsmes ir jas papildyti dėklės sprendinio architektūrai ar įgyvendinimui būdinga rizika ir grėsmėmis. Atliekant rizikos vertinimą reikėtų apsvarstyti, kaip būtų galima tinkamai reaguoti į taikytiną riziką ir grėsmes. Dėklės teikėjai turėtų papildyti schemos rizikos vertinimą, kad nustatytų bet kokią su jos įgyvendinimu susijusią riziką bei grėsmes ir pasiūlytų sertifikavimo įstaigai įvertinti tinkamas rizikos priežiūros priemones;

(13) siekiant įrodyti, kad dėklės sprendinio architektūra atitinka taikomus saugumo reikalavimus, į kiekvieną konkrečiai architektūrai skirtą schemą ar profilį turėtų būti įtrauktas bent dėklės sprendinio architektūros aprašymas, dėklės sprendinio architektūrai taikomų saugumo reikalavimų sąrašas, vertinimo planas, kuriuo patvirtinama, kad šios architektūros dėklės sprendinys atitinka tuos reikalavimus, ir rizikos vertinimas. Nacionalinėse sertifikavimo schemose turėtų būti reikalaujama, kad dėklės teikėjai parodytų, kaip jų teikiamo dėklės sprendinio projektas atitinka pamatinę architektūrą, ir išsamiai apibūdintų konkretaus dėklės sprendinio saugumo kontrolės priemones ir patvirtinimo planus. Nacionalinėse sertifikavimo schemose taip pat turėtų būti apibrėžta atitikties vertinimo veikla, siekiant patikrinti, ar dėklės projektas tinkamai atspindi pasirinkto profilio bazinę architektūrą. Nacionalinės sertifikavimo schemos turėtų atitikti Reglamento (ES) 2019/881 51 straipsnyje (išskyrus jo e ir f punktus) nustatytus reikalavimus, susijusius su duomenų registravimu;

(14) produktų sertifikavimo srityje turėtų būti leidžiama naudoti pagal EKSSS išduotus atitikties sertifikatus ir atitikties sertifikatus, išduotus pagal nacionalines sertifikavimo schemas, atitinkančias vyresniųjų pareigūnų grupės informacinių sistemų saugumo klausimais (SOG-IS) tarpusavio pripažinimo susitarimą. Be to, ne tokiems jautriems produktų komponentams turėtų būti leidžiama taikyti kitas nacionalines sertifikavimo schemas, pavyzdžiui, nustatytas pagal standartą CEN EN 17640 dėl kibernetinės saugos įvertinimo nustatytu laiku metodikos;

(15) ES skaitmeninės tapatybės dėklės patikimumo ženklas (toliau – patikimumo ženklas) turėtų būti naudojamas siekiant aiškiai, paprastai ir atpažįstamai nurodyti, kad dėklė buvo pateikta pagal Reglamentą (ES) Nr. 910/2014. Todėl jis turėtų būti laikomas pagal nacionalines sertifikavimo schemas sertifikuotos dėklės sprendinio atitikties ženklu. Nacionalinėse sertifikavimo schemose neturėtų būti apibrėžti jokie kiti atitikties ženklai;

(16) siekiant atgrasyti nuo sukčiavimo, nacionalinėse sertifikavimo schemose turėtų būti nurodyti veiksmai, kurių reikia imtis pasirodžius melagingiems teiginiams apie sertifikavimą;

(17) kad būtų užtikrintas veiksmingas pranešimų apie pažeidžiamumą valdymas, dėklės sprendinių ir elektroninės atpažinties schemos, pagal kurią jie teikiami, teikėjai turėtų apibrėžti ir įgyvendinti procesus, skirtus pažeidžiamumo kritiškumui ir galimam jo poveikiui įvertinti. Nacionalinėse sertifikavimo schemose turėtų būti nustatyta riba, kurią peržengus privaloma informuoti sertifikavimo įstaigą. Toks informavimo reikalavimas neturėtų daryti poveikio duomenų apsaugos teisės aktuose ir valstybių narių duomenų apsaugos institucijų nustatytiems pranešimo apie asmens duomenų saugumo pažeidimus kriterijams. Galėtų būti nustatyta galima privalomo pranešimo apie dėklės sprendinių saugumo ar patikimumo pažeidimą ir pranešimo apie asmens duomenų saugumo pažeidimus pagal Reglamentą (ES) 2016/679 sinergija. Sertifikavimo įstaigos atliekamas pažeidžiamumo poveikio vertinimo ataskaitos auditas neturėtų daryti poveikio duomenų apsaugos institucijos atliekamam poveikio duomenų apsaugai vertinimo patikrinimui pagal Reglamento (ES) 2016/679 35 ir 36 straipsnius;

(18) dėklės sprendinių ir elektroninės atpažinties schemos, pagal kurią jie teikiami, teikėjai schemos savininkui turėtų pranešti apie visus pažeidžiamumo vertinimo išimčių, reikalingų saugiam dėklės šifravimo įrenginiui ir saugiai dėklės šifravimo programai įvertinti, pagrindimus, nustatytus IV priede;

(19) atitikties sertifikato anuliavimas gali turėti rimtų pasekmių, pavyzdžiui, gali būti atšaukti visi įdiegti dėklės vienetai. Todėl sertifikavimo įstaigos sertifikato anuliavimo galimybę turėtų svarstyti tik jei nepašalintas pažeidžiamumas gali turėti didelį poveikį sertifikuoto dėklės sprendinio patikimumui arba kito dėklės sprendinio patikimumui;

(20) reikėtų nustatyti specialų nacionalinių sertifikavimo schemų atnaujinimo procesą, kad būtų galima valdyti perėjimą nuo vienos schemos versijos prie kitos, visų pirma kiek tai susiję su veiksmais, kurių sertifikato turėtojas turi imtis ruošdamasis būsimiems vertinimams, priežiūros, pakartotinio sertifikavimo ir specialiesiems vertinimams;

(21) siekiant sudaryti palankesnes sąlygas užtikrinti skaidrumą, dėklės teikėjai turėtų viešai dalytis savo dėklės sprendinio saugumo informacija;

(22) kai nacionalinės sertifikavimo schemos grindžiamos saugumo užtikrinimo informacija, gauta iš kitų sertifikavimo schemų ar šaltinių, turėtų būti atliekama priklausomybės analizė, siekiant patikrinti, ar saugumo užtikrinimo dokumentai, pavyzdžiui, saugumo užtikrinimo ataskaitos ir atitikties sertifikatai, yra prieinami ir tinkami atsižvelgiant į dėklės sprendinius ir elektroninės atpažinties schemą, pagal kurią jie teikiami. Tokios priklausomybės analizės pagrindas turėtų būti dėklės sprendinių ir elektroninės atpažinties schemos, pagal kurią jie teikiami, rizikos vertinimas. Atliekant vertinimą turėtų būti nustatyta, ar turimi konkretaus dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, saugumo užtikrinimo dokumentai yra pakankami, kad būtų suteiktas saugumo užtikrinimas, atitinkantis tikslingo vertinimo lygį. Atliekant vertinimą taip pat turėtų būti atnaujinta arba, jei būtina, iš naujo įvertinta priklausomybės analizė;

(23) sertifikavimo įstaigos turėtų išduoti atitikties sertifikatus pagal nacionalines sertifikavimo schemas kartu su viešai prieinama sertifikavimo ataskaita, nurodyta Reglamento (ES) Nr. 910/2014 5d straipsnio 2 dalies a punkte. Susijusi sertifikavimo vertinimo ataskaita turėtų būti pateikta Bendradarbiavimo grupei;

(24) nacionalinėse sertifikavimo schemose turėtų būti nustatytas metinis priežiūros vertinimas, siekiant užtikrinti, kad su dėklių valdymu ir priežiūra susiję procesai būtų veiksmingi, t. y. kad jie veiktų taip, kaip apibrėžta procesų nustatymo politikoje. Reglamente (ES) Nr. 910/2014 nustatytu reikalavimu kas dvejus metus atlikti pažeidžiamumo vertinimą siekiama užtikrinti, kad dėklės sprendiniu būtų nuolat tinkamai atsižvelgiama į rizikos registre nustatytą kibernetinio saugumo riziką ir grėsmes, įskaitant bet kokią grėsmių padėties raidą. Priežiūros vertinimų, pakartotinio sertifikavimo vertinimų ir specialiųjų vertinimų sąvokos turėtų atitikti standartą EN ISO/IEC 17021-1:2015;

(25) sertifikavimo ciklas baigiasi pasibaigus atitikties sertifikato galiojimui arba išdavus naują atitikties sertifikatą po sėkmingo pakartotinio sertifikavimo vertinimo. Pakartotinio sertifikavimo vertinimas turėtų apimti visų į sertifikavimo objektą įtrauktų komponentų vertinimą, įskaitant veiksmingumo vertinimą ir, kai taikytina, pažeidžiamumo vertinimą. Pakartotinio sertifikavimo metu turėtų būti įmanoma pakartotinai naudoti ankstesnių komponentų vertinimų rezultatus, jei tokie komponentai nepasikeitė;

(26) priėmus Europos kibernetinio saugumo sertifikavimo schemą, sertifikatai pagal nacionalines sertifikavimo schemas, kurių taikymo sritis tokia pati, nebeišduodami pasibaigus pereinamajam laikotarpiui, nurodytam Reglamento (ES) 2019/881 57 straipsnio 1 dalyje;

(27) nacionalinės sertifikavimo schemos turėtų būti grindžiamos esamomis sistemomis ir prireikus jose turėtų būti pakartotinai naudojami įrodymai, kad būtų užtikrintas suderinimas ir sąveikumas. Valstybės narės gali sudaryti susitarimus dėl tarpvalstybinio sertifikavimo schemų ar jų dalių pakartotinio naudojimo. Europos Komisija ir ENISA, bendradarbiaudamos su Bendradarbiavimo grupe, turėtų padėti valstybėms narėms kurti ir prižiūrėti savo nacionalines sertifikavimo schemas, taip užtikrindamos dalijimąsi žiniomis ir geriausia praktika;

(28) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([9]) 42 straipsnio 1 dalimi, buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis pateikė nuomonę 2024 m. rugsėjo 30 d.;

(29) šiame reglamente numatytos priemonės atitinka Reglamento (ES) Nr. 910/2014 48 straipsnio 1 dalyje nurodyto komiteto nuomonę,

PRIĖMĖ ŠĮ REGLAMENTĄ:

I SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas ir taikymo sritis

Šiuo reglamentu nustatomi pamatiniai standartai ir specifikacijos bei procedūros, siekiant sukurti patikimą dėklių sertifikavimo sistemą, kuri turi būti reguliariai atnaujinama, kad atitiktų su technologijomis ir standartais susijusius pokyčius ir darbą, atliktą pagal Rekomendaciją (ES) 2021/946 dėl bendro Sąjungos priemonių rinkinio darniam Europos skaitmeninės tapatybės sistemos kūrimui užtikrinti, visų pirma architektūrai ir pamatinei sistemai kurti.

2 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) dėklės sprendinys – programinės ir aparatinės įrangos, paslaugų, nuostačių ir konfigūracijų derinys, apimantis dėklės egzempliorius, vieną ar daugiau saugių dėklės šifravimo programų ir vieną ar daugiau saugių dėklės šifravimo įrenginių;

2) schemos savininkas – organizacija, atsakinga už sertifikavimo schemos kūrimą ir priežiūrą;

3) sertifikavimo objektas – produktai, procesai ir paslaugos arba jų derinys, kuriems taikomi konkretūs reikalavimai;

4) saugi dėklės šifravimo programa – taikomoji programa ypatingos svarbos turtui valdyti, susieta su saugiu dėklės šifravimo įrenginiu ir naudojanti jo teikiamas šifravimo ir kitas funkcijas;

5) dėklės egzempliorius – dėklės naudotojo įrenginyje arba aplinkoje įdiegta ir sukonfigūruota taikomoji programa, kuri yra dėklės vieneto dalis ir kurią dėklės naudotojas naudoja sąveikai su dėklės vienetu;

([9]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB, (OL L 295, 2018 11 21, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

6) saugus dėklės šifravimo įrenginys – manipuliavimui atsparus įrenginys, suteikiantis aplinką, kuri susieta su saugia dėklės šifravimo programa ir kurią ši programa naudoja ypatingos svarbos turtui apsaugoti ir šifravimo funkcijoms atlikti, kad būtų galima saugiai vykdyti ypatingos svarbos operacijas;

7) rizikos registras – su sertifikavimo procesu susijusios informacijos apie nustatytą riziką registras;

8) dėklės teikėjas – fizinis arba juridinis asmuo, teikiantis dėklės sprendinius;

9) sertifikavimo įstaiga – trečiosios šalies atitikties vertinimo įstaiga, administruojanti sertifikavimo schemas;

10) dėklės vienetas – unikalios konfigūracijos dėklės sprendinys, apimantis dėklės egzempliorius, saugias dėklės šifravimo programas ir saugius dėklės šifravimo įrenginius, kuriuos dėklės teikėjas teikia atskiram dėklės naudotojui;

11) ypatingos svarbos turtas – dėklės vienetui priklausantis arba su juo susijęs turtas, kurio svarba tokia didelė, kad pažeistas jo prieinamumas, konfidencialumas ar vientisumas turėtų labai didelį neigiamą poveikį patikimam dėklės vieneto naudojimui;

12) dėklės naudotojas – naudotojas, valdantis dėklės vienetą;

13) incidentas – incidentas, apibrėžtas Europos Parlamento ir Tarybos direktyvos (ES) 2022/2555 ([10]) 6 straipsnio 6 punkte;

14) integruota informacijos atskleidimo politika – taisyklių rinkinys, kurį elektroninio požymių liudijimo teikėjas įtraukia į elektroninį požymių liudijimą ir kuriame nurodomos sąlygos, kurias turi atitikti dėklės pasikliaujančioji šalis, kad gautų prieigą prie elektroninio požymių liudijimo.

II SKYRIUS

NACIONALINĖS SERTIFIKAVIMO SCHEMOS

3 straipsnis

Nacionalinių sertifikavimo schemų kūrimas

1. Valstybės narės paskiria kiekvienos nacionalinės sertifikavimo schemos savininką.

2. Apibrėžtas sertifikavimo pagal nacionalines sertifikavimo schemas objektas yra dėklės sprendinių ir elektroninės atpažinties schemų, pagal kurias jie teikiami, teikimas ir veikimas.

3. Pagal Įgyvendinimo reglamentą (ES) 2015/1502, į sertifikavimo pagal nacionalines sertifikavimo schemas objektą įtraukiami šie elementai:

a) programinės įrangos komponentai, įskaitant dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią dėklės sprendiniai teikiami, nuostačius ir konfigūracijas;

b) aparatinės įrangos komponentai ir platformos, kuriuose b punkte nurodyti programinės įrangos komponentai veikia arba kuriais jie naudojasi vykdant ypatingos svarbos operacijas, kai tokie aparatinės įrangos komponentai ir platformos tiesiogiai ar netiesiogiai teikiami dėklės sprendinyje ir elektroninės atpažinties schemoje, pagal kurią jis teikiamas, ir kai reikalaujama, kad jie atitiktų pageidaujamą tų programinės įrangos komponentų saugumo užtikrinimo lygį. Kai dėklės teikėjas neteikia aparatinės įrangos komponentų ir platformų, nacionalinėse sertifikavimo schemose suformuluojamos aparatinės įrangos komponentų ir platformų vertinimo prielaidos, pagal kurias gali būti užtikrinta apsauga nuo išpuolių vykdytojų su dideliu išpuolių vykdymo potencialu pagal Įgyvendinimo reglamentą (ES) 2015/1502, ir nustatomi vertinimo veiksmai šioms prielaidoms patvirtinti, nurodyti IV priede;

([10]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva), (OL L 333, 2022 12 27, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

c) procesai, kuriais palaikomas dėklės sprendinio teikimas ir veikimas, įskaitant naudotojo prisijungimo procesą, nurodytą Reglamento (ES) Nr. 910/2014 5a straipsnyje, apimantys bent registraciją, elektroninių priemonių valdymą ir organizavimą pagal Įgyvendinimo reglamento (ES) 2015/1502 I priedo 2.1, 2.2 ir 2.4 skirsnius.

4. Į nacionalines sertifikavimo schemas įtraukiamas dėklės sprendinių ir elektroninės atpažinties schemos, pagal kurią jie teikiami, konkrečios architektūros aprašymas. Kai nacionalinės sertifikavimo schemos apima daugiau nei vieną konkrečią architektūrą, jose nurodomas kiekvienos konkrečios architektūros profilis.

5. Kiekvienam profiliui nacionalinėse sertifikavimo schemose pateikiama bent ši informacija:

a) konkreti dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, architektūra;

b) saugumo kontrolės priemonės, susijusios su Reglamento (ES) Nr. 910/2014 8 straipsnyje nustatytais saugumo užtikrinimo lygiais;

c) vertinimo planas, parengtas pagal standarto EN ISO/IEC 17065:2012 7.4.1 skirsnį;

d) saugumo reikalavimai, būtini siekiant sumažinti kibernetinę riziką ir grėsmes, išvardytas šio reglamento I priede aprašytame rizikos registre, iki reikalaujamo saugumo užtikrinimo lygio, ir, kai taikytina, įgyvendinti Reglamento (ES) 2019/881 51 straipsnyje apibrėžtus tikslus;

e) šios dalies b punkte nurodytų kontrolės priemonių sąsaja su architektūros komponentais;

f) aprašymas, kuriame paaiškinama, kaip, pasitelkdami saugumo kontrolės priemones, jų sąsają, saugumo reikalavimus ir vertinimo planą, nurodytus b ir c punktuose, dėklių sprendinių ir elektroninės atpažinties schemos, pagal kurią jie teikiami, teikėjai gali tinkamai sumažinti kibernetinę riziką ir grėsmes, nustatytas d punkte nurodytame rizikos registre, iki reikalaujamo saugumo užtikrinimo lygio, ir, atlikę rizikos vertinimą, patikslinti į registrą jau įtrauktą riziką ir grėsmes ir jas papildyti dėklės sprendinio architektūrai būdinga rizika ir grėsmėmis.

6. 5 dalies c punkte nurodytame vertinimo plane išvardijami vertinimo veiksmai, kuriuos būtina įtraukti į dėklės sprendinių ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, vertinimą.

7. Atliekant 6 dalyje nurodytus vertinimo veiksmus dėklės sprendinių ir elektroninės atpažinties schemos, pagal kurią jie teikiami, teikėjai privalo pateikti informaciją, atitinkančią II priede išvardytus reikalavimus.

4 straipsnis

Bendrieji reikalavimai

1. Nacionalinės sertifikavimo schemos apima funkcinius, kibernetinio saugumo ir duomenų apsaugos reikalavimus, pasitelkiant, jei įmanoma ir taikytina, šias sertifikavimo schemas:

a) Europos kibernetinio saugumo sertifikavimo schemas, sukurtas pagal Reglamentą (ES) 2019/881, įskaitant EKSSS;

b) nacionalines kibernetinio saugumo sertifikavimo schemas, kurioms taikoma EKSSS, pagal Įgyvendinimo reglamento (ES) 2024/482 49 straipsnį.

2. Be to, kai įmanoma ir taikytina, nacionalinės sertifikavimo schemos gali būti grindžiamos:

a) kitomis susijusiomis nacionalinėmis sertifikavimo schemomis;

b) tarptautiniais, Europos ir nacionaliniais standartais;

c) techninėmis specifikacijomis, atitinkančiomis Europos Parlamento ir Tarybos reglamento (ES) Nr. 1025/2012 ([11]) II priede pateiktus reikalavimus.

3. Nacionalinėse sertifikavimo schemose:

a) nurodomi standarto EN ISO/IEC 17067:2013 6.5 skirsnyje išvardyti elementai;

b) jos įgyvendinamos kaip 6 tipo schemos pagal standarto EN ISO/IEC 17067:2013 5.3.8 skirsnį.

4. Nacionalinės sertifikavimo schemos atitinka šiuos reikalavimus:

a) sertifikatai pagal nacionalines sertifikavimo schemas gali būti išduodami tik Reglamento (ES) Nr. 910/2014 5a straipsnio 2 dalyje nurodytiems teikėjams;

b) kaip atitikties ženklas gali būti naudojamas tik patikimumo ženklas;

c) nurodydami schemą, dėklės sprendinių ir elektroninės atpažinties schemos, pagal kurią jie teikiami, teikėjai pateikia nuorodas į Reglamentą (ES) Nr. 910/2014 ir šį reglamentą;

d) dėklės sprendinių ir elektroninės atpažinties schemos, pagal kurią jie teikiami, teikėjai papildo schemos rizikos vertinimą, nurodytą 3 straipsnio 5 dalies f punkte, kad nustatytų bet kokią su jų įgyvendinimu susijusią riziką bei grėsmes ir pasiūlytų tinkamas rizikos priežiūros priemones;

e) nustatoma atsakomybė bei teisiniai veiksmai ir pateikiamos nuorodos į taikytinus nacionalinės teisės aktus, kuriuose apibrėžiama atsakomybė ir galimi teisiniai veiksmai, kai sertifikavimas pagal schemą naudojamas sukčiaujant.

5. 4 dalies d punkte nurodyti vertinimo rezultatai pateikiami sertifikavimo įstaigai išorės vertinimo tikslais.

5 straipsnis

Incidentų ir pažeidžiamumų valdymas

1. Nacionalinėse sertifikavimo schemose pateikiami incidentų ir pažeidžiamumų valdymo reikalavimai pagal 2–9 dalis.

2. Dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, atitikties sertifikato turėtojas nedelsdamas praneša savo sertifikavimo įstaigai apie bet kokį dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, saugumo ar patikimumo pažeidimą, dėl kurio, tikėtina, bus paveikta jo atitiktis nacionalinių sertifikavimo schemų reikalavimams.

3. Atitikties sertifikato turėtojas sukuria, prižiūri ir taiko pažeidžiamumų valdymo politiką ir procedūras, atsižvelgdamas į procedūras, aprašytas galiojančiuose Europos ir tarptautiniuose standartuose, įskaitant EN ISO/IEC 30111:2019.

4. Atitikties sertifikato turėtojas praneša sertifikatą išdavusiai sertifikavimo įstaigai apie pažeidžiamumus ir pokyčius, turinčius įtakos dėklės sprendiniui, pagal nustatytus tokių pažeidžiamumų ir pokyčių kriterijus.

5. Atitikties sertifikato turėtojas parengia bet kurio pažeidžiamumo, kuris turi įtakos dėklės sprendinio programinės įrangos komponentams, poveikio vertinimo ataskaitą. Ataskaitoje pateikiama tokia informacija:

a) pažeidžiamumo poveikis sertifikuotam dėklės sprendiniui;

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

([11]) 2012 m. spalio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1025/2012 dėl Europos standartizacijos, kuriuo iš dalies keičiamos Tarybos direktyvos 89/686/EEB ir 93/15/EEB ir Europos Parlamento ir Tarybos direktyvos 94/9/EB, 94/25/EB, 95/16/EB, 97/23/EB, 98/34/EB, 2004/22/EB, 2007/23/EB, 2009/23/EB ir 2009/105/EB ir panaikinamas Tarybos sprendimas 87/95/EEB ir Europos Parlamento ir Tarybos sprendimas Nr. 1673/2006/EB (OL L 316, 2012 11 14, p. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

c) informacija, ar pažeidžiamumą galima pašalinti turimomis priemonėmis;

d) galimi pažeidžiamumo pašalinimo būdai, kai pažeidžiamumą galima pašalinti turimomis priemonėmis.

6. Kai pagal 4 dalį reikalaujamas pranešimas, atitikties sertifikato turėtojas nepagrįstai nedelsdamas perduoda 5 dalyje nurodytą pažeidžiamumo poveikio vertinimo ataskaitą sertifikavimo įstaigai.

7. Atitikties sertifikato turėtojas parengia, prižiūri ir taiko pažeidžiamumų valdymo politiką atitinkančią Kibernetinio atsparumo akto ([12]) I priede nustatytus reikalavimus.

8. Nacionalinėse sertifikavimo schemose nustatomi sertifikavimo įstaigoms taikytini pažeidžiamumo problemų atskleidimo reikalavimai.

9. Atitikties sertifikato turėtojas atskleidžia ir registruoja bet kokį viešai žinomą ir ištaisytą dėklės sprendinio arba vienos iš V priede nurodytų internetinių saugyklų pažeidžiamumą.

6 straipsnis

Nacionalinių sertifikavimo schemų priežiūra

1. Nacionalinėse sertifikavimo schemose nustatomas periodinės jų veikimo peržiūros procesas. Tuo procesu siekiama patvirtinti jų tinkamumą ir nustatyti tobulintinus aspektus, atsižvelgiant į suinteresuotųjų subjektų atsiliepimus.

2. Nacionalinėse sertifikavimo schemose pateikiamos nuostatos dėl jų priežiūros. Į šį procesą įtraukiami bent tokie reikalavimai:

a) nacionalinių sertifikavimo schemų apibrėžties ir reikalavimų valdymo taisyklės;

b) naujų atitikties sertifikatų išdavimo ir jau galiojančių sertifikatų atnaujinimo terminų nustatymas priėmus naujas nacionalinių sertifikavimo schemų versijas;

c) periodinė nacionalinių sertifikavimo schemų peržiūra, siekiant užtikrinti, kad nacionalinių sertifikavimo schemų reikalavimai būtų taikomi nuosekliai, atsižvelgiant bent į šiuos aspektus:

— schemos savininkui skirtus prašymus pateikti paaiškinimus, susijusius su nacionalinės sertifikavimo schemos reikalavimais,

— suinteresuotųjų subjektų ir kitų suinteresuotųjų šalių atsiliepimus,

— nacionalinės sertifikavimo schemos savininko gebėjimą reaguoti į prašymus pateikti informaciją;

d) pamatinių dokumentų stebėsenos taisyklės ir nacionalinių sertifikavimo schemų pamatinių versijų keitimo procedūros, įskaitant bent pereinamuosius laikotarpius;

e) procesas, kuriuo užtikrinama informacija apie naujausią kibernetinę riziką ir grėsmes, išvardytas šio reglamento I priede aprašytame rizikos registre;

f) kitokių nacionalinių sertifikavimo schemų pakeitimų valdymo procesas.

([12]) 2024 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828, (Kibernetinio atsparumo aktas) (OL L, 2024/2847, 2024 11 20, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. Nacionalinėse sertifikavimo schemose pateikiami reikalavimai, pagal kuriuos atliekamas jau sertifikuotų produktų vertinimas praėjus nustatytam laikotarpiui po schemos atnaujinimo arba išleidus naujas specifikacijas ar standartus arba jų naujas versijas, kurių reikalavimus turi atitikti dėklės sprendiniai ar elektroninės atpažinties schema, pagal kurią jie teikiami.

III SKYRIUS

REIKALAVIMAI, SUSIJĘ SU SCHEMOS SAVININKAIS

7 straipsnis

Bendrieji reikalavimai

1. Schemų savininkai parengia ir prižiūri nacionalines sertifikavimo schemas ir reglamentuoja jų veikimą.

2. Schemos savininkai visas savo užduotis arba jų dalį gali pavesti atlikti trečiajai šaliai. Kai su privačia šalimi sudaroma subrangos sutartis, schemos savininkai joje nustato visų šalių pareigas ir atsakomybę. Schemos savininkai yra atsakingi už visą pagal subrangos sutartis vykdomą veiklą, kuri pavedama subrangovams.

3. Savo stebėsenos veiklą schemos savininkai, jei taikoma, grindžia bent šia informacija:

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

b) informacija, gauta jiems patiems ar kitai institucijai atlikus auditą ir tyrimus;

c) apeliaciniais ir kitais skundais, gautais pagal 15 straipsnį.

4. Schemų savininkai informuoja Bendradarbiavimo grupę apie nacionalinių sertifikavimo schemų pakeitimus. Pranešime pateikiama pakankama informacija Bendradarbiavimo grupei, kad ji galėtų teikti rekomendacijas schemų savininkams ir nuomones apie atnaujintas nacionalines sertifikavimo schemas.

IV SKYRIUS

REIKALAVIMAI, SUSIJĘ SU DĖKLĖS SPRENDINIŲ IR ELEKTRONINĖS ATPAŽINTIES SCHEMOS, PAGAL KURIĄ JIE TEIKIAMI, TEIKĖJAIS

8 straipsnis

Bendrieji reikalavimai

1. Nacionalinėse sertifikavimo schemose nustatomi kibernetinio saugumo reikalavimai, grindžiami kiekvienos konkrečios palaikomos architektūros rizikos vertinimu. Šiais kibernetinio saugumo reikalavimais siekiama valdyti nustatytą kibernetinę riziką ir grėsmes, kurios nurodytos I priede aprašytame rizikos registre.

2. Pagal Reglamento (ES) Nr. 910/2014 5a straipsnio 23 dalį nacionalinėse sertifikavimo schemose reikalaujama, kad aukšto saugumo užtikrinimo lygio, apibrėžto Įgyvendinimo reglamente (ES) 2015/1502, dėklių sprendiniai ir elektroninės atpažinties schemos, pagal kurias jie teikiami, būtų apsaugoti nuo išpuolių vykdytojų su dideliu išpuolių vykdymo potencialu.

3. Nacionalinėse sertifikavimo schemose nustatomi saugumo kriterijai, kurie apima šiuos reikalavimus:

a) Kibernetinio atsparumo aktą, kai taikytina, arba reikalavimus, kuriais siekiama Reglamento (ES) 2019/881 51 straipsnyje nustatytų saugumo tikslų;

b) rizikos, susijusios su dėklės sprendinio veikimu valdymo, įskaitant rizikos nustatymą bei vertinimą ir nustatytos rizikos mažinimą, politikos ir procedūrų kūrimą ir įgyvendinimą;

c) politikos ir procedūrų, susijusių su pokyčių valdymu ir pažeidžiamumų valdymu pagal šio reglamento 5 straipsnį, kūrimą ir įgyvendinimą;

d) žmogiškųjų išteklių valdymo politikos ir procedūrų, įskaitant personalo, dalyvaujančio kuriant ir naudojant dėklės sprendinį, kompetencijos, patikimumo, patirties, saugumo mokymo ir kvalifikacijos reikalavimus, kūrimą ir įgyvendinimą;

e) reikalavimus, susijusius su dėklės sprendinio operacine aplinka, įskaitant prielaidas dėl įrenginių ir platformų, kuriuose veikia dėklės sprendinio programinės įrangos komponentai, įskaitant saugų dėklės šifravimo įrenginį, saugumo, ir, kai taikytina ir svarbu, atitikties vertinimo reikalavimus, kuriais patvirtinama, kad tos prielaidos yra patikrintos naudojant atitinkamus įrenginius ir platformas;

f) mechanizmo, kurį dėklės teikėjas naudoja prielaidai užtikrinti, aprašymą, taip pat pagrindimą, kad mechanizmo pakanka prielaidai patikrinti, taikytiną kiekvieną kartą, kai prielaida nėra pagrįsta atitikties sertifikatu ar kita priimtina saugumo užtikrinimo informacija;

g) priemonių, kuriomis siekiama užtikrinti, kad būtų naudojama naujausia sertifikuota dėklės sprendinio versija, kūrimą ir įgyvendinimą.

4. Nacionalinėse sertifikavimo schemose nurodomi funkciniai reikalavimai, susiję su kiekvieno dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, programinės įrangos komponento atnaujinimo mechanizmais, atsižvelgiant į III priede išvardytus veiksmus.

5. Nacionalinėse sertifikavimo schemose reikalaujama, kad sertifikavimo paslaugos pareiškėjas sertifikavimo įstaigai pateiktų ar kitaip paviešintų šią informaciją ir dokumentus:

a) įrodymus, susijusius su IV priedo 1 punkte nurodyta informacija, taip pat, jei reikia, išsamią informaciją apie dėklės sprendinį ir jo pirminį kodą, įskaitant:

— *informaciją apie architektūrą* – kiekvieno dėklės sprendinio komponento (įskaitant produkto, proceso ir paslaugos komponentus) esminių saugumo savybių, įtraukiant išorės tarpusavio priklausomybės ryšius, aprašymą;

— *kontrolės priemones ir saugumo užtikrinimo lygius* – kiekvienos dėklės sprendinio saugumo kontrolės priemonės aprašymą ir reikalaujamą saugumo užtikrinimo lygį pagal Įgyvendinimo reglamento (ES) 2015/1502 priedą, kuriame aprašomos įvairios techninės specifikacijos ir procedūros, taikomos skirtingoms elektroninės atpažinties priemonėmis įgyvendinamoms kontrolės priemonėms;

— *kontrolės priemonių sąsają su architektūros komponentais* – dėklės kontrolės priemonių įgyvendinimo aprašymą naudojant įvairius dėklės sprendinio komponentus, pagrindžiant, kodėl reikia tam tikro saugumo užtikrinimo lygio ir kaip kontrolės priemonė įgyvendinama atitinkamu lygmeniu, atsižvelgiant į visus reikiamus saugumo aspektus;

— *rizikos valdymo loginį pagrindą ir pagrindimą*, pagrindžiant:

— kontrolės priemonių sąsają su komponentais;

— siūlomo vertinimo plano tinkamumą visoms kontrolės priemonėms įtraukti;

— rizikos registre nurodytos kibernetinės rizikos ir grėsmių valdymą kontrolės priemonėmis, kurios papildomos įgyvendinimui būdingos rizikos ir grėsmių kontrolės priemonėmis, atsižvelgiant į tinkamą saugumo užtikrinimo lygį;

b) V priede išvardytą informaciją;

c) išsamų atitikties sertifikatų ir kitos saugumo užtikrinimo informacijos, kuri naudojama kaip įrodymai atliekant vertinimo veiksmus, sąrašą;

d) visą kitą su vertinimo veiksmais susijusią informaciją.

V SKYRIUS

REIKALAVIMAI, SUSIJĘ SU SERTIFIKAVIMO ĮSTAIGOMIS

9 straipsnis

Bendrieji reikalavimai

1. Sertifikavimo įstaigas akredituoja nacionalinės akreditacijos įstaigos, paskirtos pagal Europos Parlamento ir Tarybos reglamentą (EB) Nr. 765/2008 ([13]); akreditacija suteikiama pagal standartą EN ISO/IEC 17065:2012, jei sertifikavimo įstaigos atitinka reikalavimus, nustatytus nacionalinėse sertifikavimo schemose, pagal 2 dalį.

2. Siekdamos akreditacijos, sertifikavimo įstaigos įvykdo visus šiuos kompetencijos reikalavimus:

a) išsamios ir techninės žinios apie atitinkamas dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, architektūrą, taip pat apie tai architektūrai aktualias grėsmes ir riziką;

b) žinios apie esamus saugumo sprendimus ir jų savybes pagal Įgyvendinimo reglamento (ES) 2015/1502 priedą;

c) žinios apie sertifikuojamą veiklą, susijusią su dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, komponentais, t. y. apie sertifikavimo objektą;

d) išsamios žinios apie taikomą nacionalinę sertifikavimo schemą, sukurtą pagal II skyrių.

3. Savo priežiūros veiklą sertifikavimo įstaigos visų pirma grindžia šia informacija:

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

b) informacija, gauta joms pačioms ar kitai institucijai atlikus auditą ir tyrimus;

c) apeliaciniais ir kitais skundais, gautais pagal 15 straipsnį.

10 straipsnis

Subranga

Sertifikavimo įstaigos su trečiosiomis šalimis gali sudaryti subrangos sutartis dėl vertinimo veiklos, aprašytos 13 straipsnyje. Kai vertinimo veikla pavedama subrangovams, nacionalinėse sertifikavimo schemose nustatoma, kad:

1) visi vertinimo veiklą atliekantys sertifikavimo įstaigos subrangovai atitinka darniųjų standartų, pavyzdžiui EN ISO/IEC 17025:2017 dėl bandymų, EN ISO/IEC 17020:2012 dėl tikrinimo, EN ISO/IEC 17021–1:2015 dėl audito ir EN ISO/IEC 17029:2019 dėl validavimo ir verifikavimo, reikalavimus, kai taikytina ir tinkama, atsižvelgiant į vykdytiną veiklą;

2) sertifikavimo įstaigos prisiima atsakomybę už visą kitoms įstaigoms perduotą vertinimo veiklą ir įrodo, kad akreditavimo proceso metu ėmėsi tinkamų priemonių, be kita ko, pasikliaudamos savo subrangovų akreditacija, kai taikytina;

3) tam tikrais atvejais gaunamas išankstinis schemos savininkų arba kliento, kurio dėklės sprendinys sertifikuojamas pagal sertifikavimo schemą, sutikimas dėl veiklos rangos.

([13]) 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 765/2008, nustatantis su gaminių prekyba susijusius akreditavimo ir rinkos priežiūros reikalavimus ir panaikinantis Reglamentą (EEB) Nr. 339/93 (OL L 218, 2008 8 13, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

11 straipsnis

Pranešimas priežiūros institucijai

Sertifikavimo įstaigos praneša Reglamento (ES) Nr. 910/2014 46a straipsnio 1 dalyje nurodytai priežiūros institucijai apie dėklės sprendinių ir elektroninės atpažinties schemos, pagal kurią jie teikiami, atitikties sertifikatų išdavimą, galiojimo sustabdymą ir anuliavimą.

12 straipsnis

Incidentų ir pažeidžiamumų valdymas

1. Sertifikavimo įstaigos nepagrįstai nedelsdamos sustabdo dėklės sprendinių ir elektroninės atpažinties schemos, pagal kurią jie teikiami, atitikties sertifikato galiojimą po to, kai jos įsitikina, kad saugumo ar patikimumo pažeidimas, apie kurį pranešta, daro poveikį nacionalinių sertifikavimo schemų, dėklės sprendinio arba elektroninės atpažinties schemos, pagal kurią jis teikiamas, atitikčiai nacionalinių sertifikavimo schemų reikalavimams.

2. Sertifikavimo įstaigos anuliuoja atitikties sertifikatą, kurio galiojimas buvo sustabdytas dėl saugumo ar patikimumo pažeidimo, kuris nebuvo laiku ištaisytas.

3. Sertifikavimo įstaigos anuliuoja atitikties sertifikatus, jei nustatytas pažeidžiamumas nebuvo laiku pašalintas atsižvelgiant į jo sunkumą ir galimą poveikį pagal Reglamento (ES) Nr. 910/2014 5c straipsnio 4 dalį ir 5e straipsnio 2 dalį.

VI SKYRIUS

ATITIKTIES VERTINIMO VEIKLA

13 straipsnis

Vertinimo veikla

1. Nacionalinėse sertifikavimo schemose nurodomi metodai ir procedūros, kuriuos atitikties vertinimo įstaigos taiko vykdydamos vertinimo veiklą pagal EN ISO/IEC 17065:2012 ir kurie apima bent šiuos aspektus:

a) vertinimo veiklos vykdymo metodus ir procedūras, įskaitant veiksmus, susijusius su saugiu dėklės šifravimo įrenginiu, aprašytu IV priede;

b) dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, įgyvendinimo auditą, atsižvelgiant į I priede aprašytą rizikos registrą, kuris prireikus papildomas su įgyvendinimu susijusia rizika;

c) funkcinių bandymų veiklą, pagrįstą, kai įmanoma ir tinkama, bandymų rinkiniais, apibūdintais pagal technines specifikacijas arba standartus;

d) priežiūros procesų nustatymo ir tinkamumo vertinimą, įskaitant bent jų versijų valdymą, atnaujinimo valdymą ir pažeidžiamumų valdymą;

e) priežiūros procesų veiksmingumo vertinimą, įskaitant bent jų versijų valdymą, atnaujinimo valdymą ir pažeidžiamumų valdymą;

f) dėklės teikėjo pateiktą priklausomybės analizę, įskaitant saugumo užtikrinimo informacijos priimtinumo vertinimo metodiką, kuri apima VI priede aprašytus elementus;

g) pažeidžiamumo vertinimą tinkamu lygmeniu, įskaitant:

— dėklės sprendinio ir, kai taikytina, jo pirminio kodo projekto apžvalgą,

— aukšto saugumo užtikrinimo lygio, nustatyto Įgyvendinimo reglamento (ES) 2015/1502 priedo 2.2.1 skirsnyje, dėklės sprendinio apsaugos nuo išpuolių vykdytojų su dideliu išpuolių vykdymo potencialu, testavimą;

h) grėsmės aplinkos raidos ir jos poveikio dėklės sprendinio rizikos valdymui vertinimą, siekiant nustatyti, kokių veiksmų reikia imtis vertinant įvairius dėklės sprendinio komponentus.

2. Nacionalinėse sertifikavimo schemose apibūdinamas vertinimas, kuriuo siekiama nustatyti, ar dėklės sprendinių ir elektroninės atpažinties schemos, pagal kurią jie teikiami, įgyvendinimas atitinka 3 straipsnio 5 dalies a punkte aprašytą architektūrą, taip pat vertinimas siekiant nustatyti, ar siūlomas vertinimo planas kartu su jo įgyvendinimu atitinka 3 straipsnio 5 dalies c punkte nurodytą vertinimo planą.

3. Nacionalinėse sertifikavimo schemose aprašytos imties sudarymo taisyklės, siekiant išvengti identiškos vertinimo veiklos pasikartojimo ir susitelkti į veiksmus, būdingus atitinkamam variantui. Pagal tas imties sudarymo taisykles galima atlikti tik dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, tikslinio komponento variantų mėginio ir tikslinių įrenginių mėginio funkcinius ir saugumo bandymus. Nacionalinėse sertifikavimo schemose reikalaujama, kad visos sertifikavimo įstaigos pagrįstų savo imties sudarymą.

4. Nacionalinėse sertifikavimo schemose reikalaujama, kad sertifikavimo įstaiga atliktų saugios dėklės šifravimo programos vertinimą, taikydama IV priede nustatytus metodus ir procedūras.

14 straipsnis

Sertifikavimo veikla

1. Nacionalinėse sertifikavimo schemose aprašyta atestavimo veikla siekiant išduoti atitikties sertifikatą pagal standarto EN ISO/IEC 17067:2013 V skyriaus a punkto 1 lentelę, įskaitant šiuos aspektus:

a) atitikties sertifikato turinį, aprašytą VII priede;

b) vertinimo rezultatų pateikimą viešoje sertifikavimo ataskaitoje, įskaitant bent preliminaraus audito santrauką ir patvirtinimo planą, aprašytą VIII priede;

c) sertifikavimo vertinimo ataskaitoje pateiktų vertinimo rezultatų turinį, įskaitant VIII priede nurodytus elementus.

2. Sertifikavimo vertinimo ataskaita gali būti pateikta Bendradarbiavimo grupei ir Komisijai.

15 straipsnis

Apeliaciniai ir kiti skundai

Nacionalinėse sertifikavimo schemose nustatomos procedūros arba pateikiamos nuorodos į taikytinus nacionalinės teisės aktus, kuriais apibrėžiamas veiksmingo apeliacinių ir kitų skundų teikimo bei nagrinėjimo mechanizmas, susijęs su sertifikavimo schemos įgyvendinimu arba išduotu atitikties sertifikatu. Šios procedūros apima informaciją skundo pateikėjui apie proceso eigą ir priimtą sprendimą, taip pat informaciją skundo pateikėjui apie teisę į veiksmingą teisminę teisių gynimo priemonę. Nacionalinėse sertifikavimo schemose reikalaujama, kad visi apeliaciniai ir kiti skundai, kurių sertifikavimo įstaiga neišsprendė arba kurių ji negali išspręsti, būtų perduodami schemos savininkui įvertinti ir išspręsti.

16 straipsnis

Priežiūros veikla

1. Nacionalinėse sertifikavimo schemose reikalaujama, kad sertifikavimo įstaigos įgyvendintų priežiūros veiklą, kurią sudaro procesų priežiūros vertinimas kartu su atsitiktiniais bandymais ar patikrinimais.

2. Nacionalinėse sertifikavimo schemose nustatomi reikalavimai, pagal kuriuos schemų savininkai stebi, kaip sertifikavimo įstaigos laikosi savo pareigų pagal Reglamentą (ES) Nr. 910/2014 ir, jei taikytina, pagal nacionalines sertifikavimo schemas.

3. Nacionalinėse sertifikavimo schemose nustatomi reikalavimai sertifikavimo įstaigoms stebėti:

a) atitikties sertifikato, išduoto pagal nacionalines sertifikavimo schemas, turėtojų atitiktį reikalavimams, susijusiems su sertifikavimu pagal Reglamentą (ES) Nr. 910/2014 ir pagal nacionalines sertifikavimo schemas;

b) sertifikuoto dėklės sprendinio atitiktį nacionalinėse sertifikavimo schemose nustatytiems reikalavimams.

17 straipsnis

Pareigų nevykdymo pasekmės

Nacionalinėse sertifikavimo schemose nustatomos sertifikuoto dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, neatitikties šiame reglamente nustatytiems reikalavimams pasekmės. Tokios pasekmės apima šiuos aspektus:

1) sertifikavimo įstaigos pareigą informuoti atitikties sertifikato turėtoją ir pareikalauti, kad atitikties sertifikato turėtojas imtųsi taisomųjų veiksmų;

2) sertifikavimo įstaigos pareigą informuoti kitas atitinkamas rinkos priežiūros institucijas, kai neatitiktis yra susijusi su atitinkamais Sąjungos teisės aktais;

3) atitikties sertifikato turėtojo taisomųjų veiksmų vykdymo sąlygas;

4) atitikties sertifikato galiojimo sustabdymo, kurį inicijuoja sertifikavimo įstaiga, ir atitikties sertifikato atnaujinimo po neatitikties ištaisymo sąlygas;

5) atitikties sertifikato anuliavimo, kurį inicijuoja sertifikavimo įstaiga, sąlygas;

6) sertifikavimo įstaigos neatitikties nacionalinės sertifikavimo schemos reikalavimams pasekmes.

VII SKYRIUS

SERTIFIKAVIMO CIKLAS

18 straipsnis

Sertifikavimo ciklas

1. Atitikties sertifikatų, išduotų pagal nacionalines sertifikavimo schemas, galiojimas priklauso nuo reguliarios vertinimo veiklos, kurią vykdo sertifikavimo įstaiga pagal IX priede aprašytus reikalavimus.

2. Nacionalinėse sertifikavimo schemose numatomas dėklės sprendinių ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, pakartotinio sertifikavimo procesas atitikties sertifikato turėtojo prašymu, kuris atliekamas iki pirminio atitikties sertifikato galiojimo pabaigos. Toks pakartotinio sertifikavimo procesas apima išsamų dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, vertinimą, įskaitant pažeidžiamumo vertinimą, laikantis IX priede nustatytų principų.

3. Nacionalinėse sertifikavimo schemose nustatytas sertifikuoto dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, pakeitimų valdymo procesas. Tas procesas apima taisykles, pagal kurias nustatoma, ar pakeitimas turi būti įvertinamas atliekant specialųjį vertinimą, nurodytą 4 dalyje, ar tikrinant priežiūros procesų veiksmingumą, nurodytą IV priede.

4. Nacionalinėse sertifikavimo schemose nustatomas specialiųjų vertinimų procesas pagal standartą EN ISO/IEC 17065:2012. Toks specialiųjų vertinimų procesas apima veiksmų, kurie turi būti atliekami siekiant patikrinti konkrečią sritį, dėl kurios reikalingas specialusis vertinimas, atranką.

5. Nacionalinėse sertifikavimo schemose nustatomos taisyklės, susijusios su atitikties sertifikato anuliavimu.

VIII SKYRIUS

ĮRAŠŲ SAUGOJIMAS IR INFORMACIJOS APSAUGA

19 straipsnis

Įrašų saugojimas

1. Nacionalinėse sertifikavimo schemose nustatyti reikalavimai sertifikavimo įstaigoms dėl visų svarbių įrašų, gautų vykdant atitikties vertinimo veiklą, sistemos, įskaitant dėklės sprendinių ir elektroninės atpažinties schemų, pagal kurias jie teikiami, teikėjų pateiktus ir gautus duomenis. Tokių duomenų įrašai saugomi saugiai. Įrašai gali būti saugomi elektroniniu būdu ir yra prieinami tol, kol to reikalaujama pagal Sąjungos arba nacionalinę teisę, ir bent penkerius metus po atitinkamo atitikties sertifikato anuliavimo arba galiojimo pabaigos.

2. Nacionalinėse sertifikavimo schemose atitikties sertifikato turėtojui nustatomi reikalavimai saugiai saugoti toliau nurodytą informaciją šio reglamento taikymo tikslais ir bent penkerius metus po atitinkamo atitikties sertifikato anuliavimo arba galiojimo pabaigos:

a) sertifikavimo įstaigai arba bet kuriam jos subrangovui sertifikavimo proceso metu pateiktos informacijos įrašus;

b) aparatinės įrangos komponentų, įtrauktų į dėklės sprendinio sertifikavimo taikymo sritį, mėginius.

3. Nacionalinėse sertifikavimo schemose reikalaujama, kad atitikties sertifikato turėtojas, gavęs prašymą, pateiktų 1 dalyje nurodytą informaciją sertifikavimo įstaigai arba priežiūros institucijai, nurodytai Reglamento (ES) Nr. 910/2014 46a straipsnio 1 dalyje.

20 straipsnis

Informacijos apsauga

Pagal nacionalines sertifikavimo schemas reikalaujama, kad visi asmenys ar organizacijos, kuriems suteikta prieiga prie informacijos vykdant veiklą pagal nacionalinę sertifikavimo schemą, užtikrintų verslo paslapčių ir kitos konfidencialios informacijos, saugumą ir apsaugą, taip pat saugotų intelektinės nuosavybės teises ir imtųsi būtinų bei tinkamų techninių ir organizacinių priemonių šiam konfidencialumo įsipareigojimui užtikrinti.

IX SKYRIUS

BAIGIAMOSIOS NUOSTATOS

21 straipsnis

Perėjimas prie Europos kibernetinio saugumo sertifikavimo schemos

Šis reglamentas bus peržiūrėtas priėmus pirmąją dėklių sprendiniams ir elektroninės atpažinties schemoms, pagal kurias jie teikiami, taikomą Europos kibernetinio saugumo sertifikavimo schemą, siekiant atsižvelgti į tokios Europos kibernetinio saugumo sertifikavimo schemos vaidmenį sertifikuojant dėklių sprendinius ir elektroninės atpažinties schemas, pagal kurias jie teikiami.

22 straipsnis

Įsigaliojimas

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

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2024 m. lapkričio 28 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN

I PRIEDAS

EUROPINIŲ SKAITMENINĖS TAPATYBĖS DĖKLIŲ RIZIKOS REGISTRAS

Įžanga

Rizikos registre aprašoma pagrindinė su dėklėmis susijusi saugumo ir privatumo rizika ir grėsmės, į kurias tinkamai atsižvelgiama kuriant kiekvieną dėklių architektūrą ir jas diegiant. **Didelė rizika** (I skirsnis) yra susijusi su naudotojų ir pasikliaujančiųjų šalių naudojimusi dėklėmis ir siejama su tiesioginėmis grėsmėmis, kurios kyla dėklių turtui. Be to, nustatyta tam tikra **sistemos lygmens rizika** (II skirsnis) dėklėms, kuri paprastai atsiranda dėl grėsmių, kylančių visai dėklės sistemai, derinio.

Rizikos rūšis	Rizikos ID	Susijusios rizikos pavadinimai
Didelė rizika dėklėms	R1	Esamos elektroninės tapatybės sukūrimas arba naudojimas
	R2	Netikros elektroninės tapatybės kūrimas arba naudojimas
	R3	Netikrų požymių kūrimas arba naudojimas
	R4	Tapatybės vagystė
	R5	Duomenų vagystė
	R6	Duomenų atskleidimas
	R7	Manipuliavimas duomenimis
	R8	Duomenų praradimas
	R9	Neleistinas sandoris
	R10	Manipuliavimas sandoriu
	R11	Veiksmų nepripažinimas
	R12	Sandorio duomenų atskleidimas
	R13	Paslaugos nutraukimas
	R14	Sekimas
Sistemos lygmens rizika	SR1	Masinis sekimas
	SR2	Žala reputacijai
	SR3	Teisinė neatitiktis

Registre taip pat nustatomos **techninės grėsmės** (III skirsnis), susijusios su dėklės sprendinio įgyvendinimu. Šios grėsmės yra susijusios su didele rizika, t. y. kiekviena iš jų galėtų būti panaudota siekiant sukelti įvairaus pobūdžio riziką.

Grėsmės rūšis	Grėsmės ID	Susijusių grėsmių pavadinimai	Grėsmių pakategorės
Techninė grėsmė	TT1	Fiziniai išpuoliai	1.1. *Vagystė*
			1.2. *Informacijos nutekėjimas*
			1.3. *Klastojimas*
	TT2	Klaidos ir klaidingas konfigūravimas	2.1. *IT sistemos valdymo klaidos*
			2.2. *Taikomosios programos lygmens klaidos arba naudojimo klaidos*
			2.3. *Kūrimo laikotarpio klaidos ir klaidingas sistemos konfigūravimas*

Grėsmės rūšis	Grėsmės ID	Susijusių grėsmių pavadinimai	Grėsmių pakategorės
	TT3	Nepatikimų išteklių naudojimas	3.1. *Klaidingas dėklės komponentų naudojimas arba konfigūravimas*
	TT4	Gedimas ir atjungimas	4.1. *Įrangos, įrenginių ar sistemų gedimas arba veikimo sutrikimas*
			4.2. *Išteklių praradimas*
			4.3. *Pagalbinių paslaugų praradimas*
	TT5	Piktavališki veiksmai	5.1. *Informacijos perėmimas*
			5.2. *Duomenų viliojimas ir apsimetinėjimas*
			5.3. *Pranešimų pakartojimas*
			5.4. *Brutalioji ataka*
			5.5. *Programinės įrangos pažeidžiamumas*
			5.6. *Tiekimo grandinės atakos*
			5.7. *Kenkimo programinė įranga*
			5.8. *Atsitiktinių skaičių numatymas*

Galiausiai registre **išvardijamos tiesioginės grėsmės dėklėms** ir kiekviena iš jų susiejama su (nebaigtiniu) rizikos rūšių sąrašu (IV skirsnis).

I SKIRSNIS

Didelė rizika dėklėms

R1. Esamos elektroninės tapatybės sukūrimas arba naudojimas

Esamos elektroninės tapatybės sukūrimas arba naudojimas – elektroninės tapatybės, kuri realiai egzistuoja ir yra priskirta kitam naudotojui, kūrimas dėklėje. Iš esmės dėl šios rizikos kyla tapatybės vagystės (R4) ir neleistinų sandorių (R9) rizika.

R2. Netikros elektroninės tapatybės kūrimas arba naudojimas

Netikros elektroninės tapatybės sukūrimas arba naudojimas – neegzistuojančios elektroninės tapatybės kūrimas dėklėje.

R3. Netikrų požymių kūrimas arba naudojimas

Netikrų požymių kūrimas arba naudojimas – požymių kūrimas arba naudojimas, kai negalima patvirtinti, kad tuos požymius išdavė deklaruojamas teikėjas ir jais negalima pasitikėti.

R4. Tapatybės vagystė

Tapatybės vagystė – neteisėtas dėklės vieneto tapatumo nustatymo veiksnių gavimas arba praradimas, dėl kurių galimas sukčiavimas naudojant kito asmens dokumentą.

R5. Duomenų vagystė

Duomenų vagystė – neteisėtas duomenų rinkimas. Duomenų vagystė taip pat yra susijusi su tokiomis grėsmėmis kaip duomenų perėmimas (neleistinas perduodamų duomenų rinkimas) ir duomenų iššifravimas (neleistinas šifruotų duomenų dekodavimas), dėl kurių kai kuriais atvejais gali būti atskleisti duomenys (R6).

R6. Duomenų atskleidimas

Duomenų atskleidimas – neleistinas asmens duomenų, įskaitant specialių kategorijų asmens duomenis, atskleidimas. Labai panaši yra privatumo pažeidimo rizika, kai ji vertinama atsižvelgiant į privatumą, o ne į saugumą.

R7. Manipuliavimas duomenimis

Manipuliavimas duomenimis – neleistinas duomenų pakeitimas.

R8. Duomenų praradimas

Duomenų praradimas – situacija, kai dėklėje saugomi duomenys prarandami dėl netinkamo naudojimo arba piktavališkų veiksmų. Ši rizika dažnai yra antrinė manipuliavimo duomenimis (R7) arba paslaugos nutraukimo (R13) rizika, kai neįmanoma atkurti visų duomenų ar jų dalies.

R9. Neleistinas sandoris

Neleistini sandoriai – operacinė veikla, vykdoma be dėklės naudotojo leidimo ar žinios. Daugeliu atvejų dėl neleistino sandorio galima tapatybės vagystė (R4) arba duomenų atskleidimas (R6). Jis taip pat susijęs su tokiomis neleistinomis operacijomis kaip netinkamas kriptografinių raktų naudojimas.

R10. Manipuliavimas sandoriu

Manipuliavimas sandoriu – neleistinas dėklės operacijų pakeitimas. Manipuliavimas sandoriu yra prieš vientisumą nukreipta ataka ir yra susijęs su duomenų vientisumo pažeidimu.

R11. Veiksmų nepripažinimas

Veiksmų nepripažinimas – tai situacija, kai suinteresuotasis subjektas gali neigti, jog jis atliko veiksmą arba dalyvavo vykdant sandorį, o kiti suinteresuotieji subjektai neturi tinkamų įrodymų jam prieštarauti.

R12. Sandorio duomenų atskleidimas

Sandorio duomenų atskleidimas – informacijos, susijusios su suinteresuotųjų subjektų sandorio duomenimis, atskleidimas.

R13. Paslaugos nutraukimas

Paslaugos nutraukimas – įprasto dėklės veikimo sutrikimas arba pablogėjimas. Konkretus paslaugos nutraukimo pavyzdys yra naudotojo blokavimas, kai naudotojas negali prisijungti prie savo paskyros ar dėklės.

R14. Sekimas

Sekimas arba stebėjimas – neteisėtas dėklės naudotojo veiklos, ryšių ar duomenų sekimas arba stebėjimas. Sekimas dažnai yra susijęs su numanymu, t. y. neskelbtinų ar asmens duomenų išvedimu pasinaudojant informacija, kuri nelaikoma jautria.

II SKIRSNIS

Sistemos lygmens rizika

Ši rizika nėra įtraukta į grėsmių sąrašą, nes paprastai ji yra daugelio pasikartojančių grėsmių, keliančių pavojų visai sistemai, pasekmė.

SR1. Masinis sekimas

Masinis sekimas – daugelio naudotojų veiklos sekimas arba stebėjimas naudojantis jų dėklės ryšiais ar duomenimis. Masinis sekimas dažnai siejamas su sekimu (R14) ir numanymu pasauliniu mastu, kai informacija apie daugelį naudotojų sujungiama siekiant gauti naudotojų neskelbtinus ar asmens duomenis arba nustatyti statistines tendencijas, kurios gali būti naudojamos rengiant tolesnius išpuolius.

SR2. Žala reputacijai

Žala reputacijai – žala organizacijos ar Vyriausybinės įstaigos reputacijai. Žala reputacijai taip pat kyla dėl kitos rizikos, kai pažeidimą ar incidentą paviešina žiniasklaida, nepalankiai pristatydama organizaciją. Žala reputacijai gali sukelti papildomą riziką, pavyzdžiui, pasitikėjimo praradimą dėl pagrįstų naudotojo abejonių ir ekosistemos praradimą, kai žlunga visa ekosistema.

SR3. Teisinė neatitiktis

Teisinė neatitiktis – situacija, kai neįmanoma laikytis atitinkamų įstatymų, kitų teisės aktų ar standartų reikalavimų. Kadangi dėklės sprendinio saugumas ir privatumas yra teisiniai reikalavimai, tikėtina, kad tam tikra teisinė neatitiktis atsiras dėl visų grėsmių.

III SKIRSNIS

Techninės grėsmės

Ne visos techninės grėsmės yra susijusios su konkrečia dėklėms kylančia rizika, nes daugelis jų yra priemonės, kurias būtų galima panaudoti išpuoliams, atitinkantiems įvairių rūšių riziką, vykdyti.

TT1. Fiziniai išpuoliai

1.1. *Vagystė*

Vagystė – įrenginių, kuriais galima pakeisti tinkamą dėklės veikimą, vagystė (kai įrenginys pavogtas ir dėklės vienetas nėra tinkamai apsaugotas). Vagystė gali prisidėti prie įvairių rūšių rizikos, įskaitant tapatybės vagystę (R4), duomenų vagystę (R5) ir neleistinus sandorius (R9).

1.2. *Informacijos nutekėjimas*

Informacijos nutekėjimas – neleistina prieiga, informacijos atskleidimas arba paviešinimas gavus fizinę prieigą prie dėklės. Ši grėsmė visų pirma gali prisidėti prie duomenų atskleidimo (R6) ir duomenų vagystės (R5).

1.3. *Klastojimas*

Klastojimas – vienos ar kelių dėklės vieneto komponentų arba komponentų, nuo kurių priklauso dėklės vieneto veikimas, pvz., naudotojo įrenginio arba jo operacinės sistemos, vientisumo pažeidimas. Ši grėsmė visų pirma gali prisidėti prie manipuliavimo duomenimis (R7), duomenų praradimo (R8) ir manipuliavimo sandoriu (R10). Programinės įrangos komponentų klastojimas gali sukelti įvairių rūšių riziką.

TT2. Klaidos ir klaidingas konfigūravimas

2.1. *IT sistemos valdymo klaidos*

IT sistemos valdymo klaidos – informacijos nutekėjimas, dalijimasis informacija arba žala, padaryta dėl naudotojų netinkamo IT išteklių naudojimo (dėl jų nepakankamo informuotumo apie taikomosios programos funkcijas) arba netinkamo IT išteklių konfigūravimo ar valdymo.

2.2. *Taikomosios programos lygmens klaidos arba naudojimo klaidos*

Taikomosios programos lygmens klaidos arba naudojimo klaidos – taikomosios programos veikimo sutrikimai dėl klaidos pačioje programoje arba dėl vieno iš naudotojų (dėklės naudotojų ir pasikliaujančiųjų šalių) padarytos klaidos.

2.3. *Kūrimo laikotarpio klaidos ir klaidingas sistemos konfigūravimas*

Kūrimo laikotarpio klaidos ir klaidingas sistemos konfigūravimas – veikimo sutrikimas arba pažeidžiamumas, atsiradęs dėl netinkamai sukurto ar konfigūruoto IT turto arba veiklos procesų (netinkamų IT produktų specifikacijų, nepakankamo tinkamumo naudoti, nesaugių sąsajų, netinkamų politikos ir procedūrų srautų, projektavimo klaidų).

TT3. Nepatikimų išteklių naudojimas

Nepatikimų išteklių naudojimas – veikla, dėl kurios atsiranda netyčinė dėl netinkamai nustatytų pasitikėjimo santykių, pavyzdžiui, pasitikėjimas paslaugas teikiančia trečiąja šalimi, nesant pakankamo patikimumo lygio.

3.1. *Klaidingas dėklės komponentų naudojimas arba konfigūravimas*

Klaidingas dėklės komponentų naudojimas arba konfigūravimas – netyčinė žala dėklės komponentams dėl dėklės naudotojų arba nepakankamai kvalifikuotų kūrėjų klaidingo komponentų naudojimo ar netinkamo konfigūravimo arba dėl nepakankamo prisitaikymo prie besikeičiančios grėsmių padėties, paprastai naudojant pažeidžiamus trečiųjų šalių komponentus arba vykdymo platformas.

TT4. Gedimas ir atjungimas

4.1. *Įrangos, įrenginių ar sistemų gedimas arba veikimo sutrikimas*

Įrangos, įrenginių ar sistemų gedimas arba veikimo sutrikimas – netyčinė žala IT turtui dėl įrangos, įskaitant teikėjo infrastruktūrą ir naudotojo įrenginius, gedimo arba veikimo sutrikimo.

4.2. *Išteklių praradimas*

Išteklių praradimas – atjungimas arba veikimo sutrikimas dėl išteklių, pvz., techninės priežiūros dalių, trūkumo.

4.3. *Pagalbinių paslaugų praradimas*

Pagalbinių paslaugų praradimas – atjungimas arba veikimo sutrikimas dėl to, kad nėra galimybės naudotis pagalbinėmis paslaugomis, reikalingomis tinkamam sistemos veikimui, įskaitant paslaugų teikėjo infrastruktūros ir naudotojo įrenginio tinklo junglumą.

TT5. Piktavališki veiksmai

5.1. *Informacijos perėmimas*

Informacijos perėmimas – netinkamai apsaugotos perduodamos informacijos pasisavinimas, įskaitant komunikacijos perėmimo išpuolį.

5.2. *Duomenų viliojimas ir apsimetinėjimas*

Duomenų viliojimas – informacijos išviliojimas iš naudotojo apgaulės būdu, dažnai siejamas su teisėtų ryšių priemonių ir interneto svetainių klastojimu. Šios grėsmės nukreiptos prieš naudotoją ir paprastai prisideda prie tapatybės vagystės (R4) ir neleistinų sandorių (R9), dažnai vykdomos vagiant duomenis (R5) arba atskleidžiant duomenis (R6).

5.3. *Pranešimų pakartojimas*

Pranešimų pakartojimas – pakartotinis anksčiau perimtų pranešimų naudojimas neteisėtoms operacijoms atlikti, dažnai protokolo lygmeniu. Ši techninė grėsmė daugiausia prisideda prie neleistinų sandorių, dėl kurių, priklausomai nuo sandorio, gali kilti kita rizika.

5.4. *Brutalioji ataka*

Brutalioji ataka – saugumo, dažnai konfidencialumo, pažeidimas, kai vyksta intensyvus bendravimas, kol iš atsakymų gaunama vertingos informacijos.

5.5. *Programinės įrangos pažeidžiamumas*

Su programinės įrangos pažeidžiamumu susijusi grėsmė yra saugumo pažeidimas išnaudojant dėklės komponentų programinės įrangos pažeidžiamumą arba programinės ir aparatinės įrangos komponentų, naudojamų diegiant dėklę, pažeidžiamumą, įskaitant paskelbtus ir nepaskelbtus (ką tik nustatytus) pažeidžiamumus.

5.6. *Tiekimo grandinės atakos*

Tiekimo grandinės ataka – saugumo pažeidimas vykdant išpuolius prieš dėklės teikėją arba jos naudotojus, kad būtų galima vykdyti tolesnius išpuolius, nukreiptus prieš pačią dėklę.

5.7. *Kenkimo programinė įranga*

Kenkimo programinė įranga – saugumo pažeidimas, susijęs su kenkimo taikomosiomis programomis, atliekančiomis nepageidaujamus ir neteisėtus veiksmus dėklėje.

5.8. *Atsitiktinių skaičių numatymas*

Atsitiktinis skaičių numatymas – galimybė vykdyti brutaliąsias atakas, iš dalies arba visiškai numačius sugeneruotus atsitiktinius skaičius.

IV SKIRSNIS

Dėklėms kylančios grėsmės

Šiame paskutiniame skirsnyje pateikiami tam tikri tipiški grėsmių scenarijai, susiję su dėklėmis, kurie yra susieti su pirmiau išvardytomis pagrindinėmis didelės rizikos rūšimis. Šiame sąraše nurodytos grėsmės, į kurias reikia atsižvelgti, tačiau jis nėra baigtinis ir labai priklauso nuo pasirinkto dėklės sprendinio architektūros ir grėsmės aplinkos raidos. Be to, atlikdamas rizikos vertinimą ir siūlydamas priemones, dėklės teikėjas gali būti atsakingas tik už tuos komponentus, kurie įtraukti į sertifikavimo taikymo sritį (*).

ID *Identifikatorius*	Grėsmės aprašymas *Nustatytos grėsmės aprašymas* (*)	Rizikos pavadinimas *Susijusi rizika*
TR1	Išpuolių vykdytojas gali be pagrįstos priežasties atšaukti slapyvardžius.	Netikros elektroninės tapatybės sukūrimas arba naudojimas (R2)
TR2	Išpuolių vykdytojas gali išduoti suklastotas, neegzistuojančias elektronines tapatybes.	Netikros elektroninės tapatybės sukūrimas arba naudojimas (R2)
TR3	Išpuolių vykdytojas gali pradėti išduoti neteisėtus asmens tapatybės duomenis.	Netikros elektroninės tapatybės sukūrimas arba naudojimas (R2)
TR4	Išpuolių vykdytojas gali kreiptis į administratorių, kad šis į asmens tapatybės duomenų teikėjų patikimą sąrašą įtrauktų neteisingą asmens tapatybės duomenų teikėją.	Netikros elektroninės tapatybės sukūrimas arba naudojimas (R2)
TR5	Išpuolių vykdytojas gali apeiti nuotolinio tapatybės įrodymo paslaugą.	Esamos elektroninės tapatybės sukūrimas arba naudojimas (R1) / netikros elektroninės tapatybės sukūrimas arba naudojimas (R2)
TR6	Išpuolių vykdytojas gali apeiti fizinio tapatybės įrodymo paslaugą.	Esamos elektroninės tapatybės sukūrimas arba naudojimas (R1) / netikros elektroninės tapatybės sukūrimas arba naudojimas (R2)
TR7	Išpuolių vykdytojas gali apeiti tapatybės įrodymo paslaugas, susijusias su nuotolinio (kvalifikuoto) pažymėjimo naudojimu.	Esamos elektroninės tapatybės sukūrimas arba naudojimas (R1) / netikros elektroninės tapatybės sukūrimas arba naudojimas (R2)
TR8	Išpuolių vykdytojas gali gauti prieigą prie dėklės, kuri nėra susieta su asmeniu.	Esamos elektroninės tapatybės sukūrimas arba naudojimas (R1) / netikros elektroninės tapatybės sukūrimas arba naudojimas (R2)
TR9	Išpuolių vykdytojas gali išderinti technines ir procedūrines kontrolės priemones, kad sukurtų neteisingus asmens tapatybės duomenis.	Esamos elektroninės tapatybės sukūrimas arba naudojimas (R1) / netikros elektroninės tapatybės sukūrimas arba naudojimas (R2)
TR10	Išpuolių vykdytojas gali aktyvinti naują dėklę negaliojančiame saugiame dėklės šifravimo įrenginyje.	Esamos elektroninės tapatybės sukūrimas arba naudojimas (R1) / netikros elektroninės tapatybės sukūrimas arba naudojimas (R2)
TR11	Išpuolių vykdytojas gali apeiti tapatybės įrodymo paslaugą, susijusią su esamų elektroninės tapatybės priemonių naudojimu.	Esamos elektroninės tapatybės sukūrimas arba naudojimas (R1) / tapatybės vagystė (R4) / neleistinas sandoris (R9)
TR12	Išpuolių vykdytojas gali pergudrauti asmens tapatybės duomenų teikėjo atliekamą patikrą, siekiant patvirtinti, kad dėklę kontroliuoja naudotojas, ir išduoti asmens tapatybės duomenis išpuolių vykdytojo užvaldytoje dėklėje.	Esamos elektroninės tapatybės sukūrimas arba naudojimas (R1) / tapatybės vagystė (R4) / neleistinas sandoris (R9)

ID *Identifikatorius*	Grėsmės aprašymas *Nustatytos grėsmės aprašymas* (*)	Rizikos pavadinimas *Susijusi rizika*
TR13	Išpuolių vykdytojas gali įkelti galiojančius asmens tapatybės duomenis į negaliojantį dėklės vienetą.	Esamos elektroninės tapatybės sukūrimas arba naudojimas (R1) / tapatybės vagystė (R4) / neleistinas sandoris (R9)
TR14	Asmens tapatybės duomenų teikėjas gali išduoti suklastotus tapatybės duomenis, kai tapatybė yra susijusi su realiu asmeniu.	Esamos elektroninės tapatybės sukūrimas arba naudojimas (R1) / tapatybės vagystė (R4) / neleistinas sandoris (R9)
TR15	Išpuolių vykdytojas gali susieti asmens tapatybės duomenis su neteisinga dėkle, nes asmens tapatybės duomenų teikėjas negali jų susieti su teisinga dėkle.	Esamos elektroninės tapatybės sukūrimas arba naudojimas (R1) / tapatybės vagystė (R4) / neleistinas sandoris (R9)
TR16	Išpuolių vykdytojas gali priversti naudotoją patvirtinti naujo dėklės vieneto / egzemplioriaus, kurį kontroliuoja išpuolių vykdytojas, aktyvinimą, o vėliau kontroliuoti ir liudijimus.	Esamos elektroninės tapatybės sukūrimas arba naudojimas (R1) / netikros elektroninės tapatybės sukūrimas arba naudojimas / (R2) tapatybės vagystė (R4) / neleistinas sandoris (R9)
TR17	Išpuolių vykdytojas gali išduoti kitos valstybės asmens tapatybės duomenis, kad gautų prieigą prie piliečių, prieš kuriuos nukreiptas išpuolis, prieigos duomenų / skaitmeninio turto.	Esamos elektroninės tapatybės sukūrimas arba naudojimas (R1) / tapatybės vagystė (R4) / neleistinas sandoris (R9)
TR18	Išpuolių vykdytojas gali išderinti technines ir procedūrines kontrolės priemones, kad sukurtų netikrus kvalifikuotus elektroninius požymių liudijimus.	Netikrų požymių kūrimas arba naudojimas (R3)
TR19	Išpuolių vykdytojas gali pateikti kvalifikuotus elektroninius požymių liudijimus, kurie nėra jam teisėtai išduoti.	Netikrų požymių kūrimas arba naudojimas (R3)
TR20	Išpuolių vykdytojas gali nusitaikyti į dėklės kriptografinį sąsajos tarp asmens tapatybės duomenų ir kvalifikuoto elektroninio požymių liudijimo mechanizmą, kuris jam neturėtų būti išduotas.	Netikrų požymių kūrimas arba naudojimas (R3)
TR21	Išpuolių vykdytojas gali naudoti kvalifikuotą elektroninį požymių liudijimą dėklėje, nors fizinis kvalifikuotas elektroninio požymių liudijimas negalioja.	Netikrų požymių kūrimas arba naudojimas (R3)
TR22	Išpuolių vykdytojas gali pergudrauti kvalifikuoto elektroninio požymių liudijimo teikėjo atliekamą patikrą, siekiant patvirtinti, kad dėklę kontroliuoja naudotojas, ir išduoti kvalifikuotą elektroninį požymių liudijimą išpuolių vykdytojo užvaldytoje dėklėje.	Netikrų požymių kūrimas arba naudojimas (R3)
TR23	Išpuolių vykdytojas gali suklastoti elektroninius požymių liudijimus.	Netikrų požymių kūrimas arba naudojimas (R3)
TR24	Išpuolių vykdytojas gali įdiegti suklastotus elektroninius požymių liudijimus dėklėje.	Netikrų požymių kūrimas arba naudojimas (R3)
TR25	Dėklė gali pateikti požymius pasikliaujančiajai šaliai be naudotojo patvirtinimo.	Duomenų atskleidimas (R6)
TR26	Asmens tapatybės duomenys, kvalifikuoti elektroniniai požymių liudijimai arba slapyvardžiai gali būti pateikti ne tai pasikliaujančiajai šaliai.	Duomenų atskleidimas (R6)
TR27	Išpuolių vykdytojas gali inicijuoti piktavališką elektroninio požymių liudijimo atnaujinimą.	Duomenų atskleidimas (R6)
TR28	Išpuolių vykdytojas gali priversti naudotoją neteisingai patvirtinti elektroninių požymių liudijimų prašymą (pasitelkiant duomenų viliojimą ar kt.).	Duomenų atskleidimas (R6)

ID *Identifikatorius*	Grėsmės aprašymas *Nustatytos grėsmės aprašymas* (*)	Rizikos pavadinimas *Susijusi rizika*
TR29	Išpuolių vykdytojas nutekinti dėklės požymius ir identifikuoti dėklės naudotoją, jei tapatybės nustatymas nebūtinas / neleidžiamas.	Duomenų atskleidimas (R6)
TR30	Išpuolių vykdytojas gali išderinti technines ir procedūrines kontrolės priemones, kad gautų duomenis.	Duomenų atskleidimas (R6)
TR31	Užklausa gali būti nutekinta išpuolių vykdytojui.	Duomenų atskleidimas (R6)
TR32	Išpuolių vykdytojas gali gauti žinių apie integruotą informacijos apie požymius atskleidimo politiką ir požymius, esančius naujausiame dėklės vieneto užklausoje.	Duomenų atskleidimas (R6)
TR33	Išpuolių vykdytojas gali gauti žurnalus arba jų dalis.	Duomenų atskleidimas (R6)
TR34	Išpuolių vykdytojas gali žinoti, ar dėklė įdiegta tame pačiame įrenginyje, kuriuo jis naudojasi, ar kitame įrenginyje, ir gauti apie ją informacijos.	Duomenų atskleidimas (R6)
TR35	Išpuolių vykdytojas gali išsiaiškinti žinomą veiksnį, naudojamą naudotojo tapatybei nustatyti saugioje dėklės šifravimo programoje.	Duomenų atskleidimas (R6)
TR36	Asmens elektroninis požymių liudijimas, kuris pateikiamas keliuose sandoriuose su pasikliaujančiąja šalimi arba tarp skirtingų pasikliaujančiųjų šalių, netyčia padeda susieti daugybinius sandorius su atitinkamu asmeniu.	Duomenų atskleidimas (R6)
TR37	Viešame liudijimų / pasikliaujančiųjų šalių atšaukimo sąraše gali būti pateikta informacijos apie tai, kaip naudotojas naudoja savo liudijimą, (pvz., buvimo vieta, IP adresas ir kt.).	Duomenų atskleidimas (R6)
TR38	Negalėdamos įrodyti naudotojo sutikimo dėl bendrų požymių, pasikliaujančiosios šalys gali daryti poveikį žurnalų vientisumui.	Duomenų atskleidimas (R6)
TR39	Išpuolių vykdytojas gali neteisėtai atsekti dėklės naudotojus, naudojančius unikalius / atsekamus identifikatorius.	Duomenų atskleidimas (R6) / sekimas (R14)
TR40	Pasikliaujančioji šalis, kurią sudaro keli vienetai / subjektai su skirtinga leistina užklausų / apdorojimo apimtimi, gali prašyti duomenų, kurių prašyti ji neturi teisėto pagrindo, ir juos apdoroti.	Duomenų atskleidimas (R6) / neleistinas sandoris (R9)
TR41	Išpuolių vykdytojas gali iškreipti dėklės vykdomas asmens tapatybės duomenų vientisumo ir autentiškumo patikras, kad jų rezultatai visada būtų sėkmingi.	Manipuliavimas duomenimis (R7)
TR42	Išpuolių vykdytojas gali apeiti arba iškreipti dėklės atliekamas patikras, kuriomis tikrinamas prašomų požymių vientisumas ir autentiškumas, kad jų rezultatai visada būtų sėkmingi.	Manipuliavimas duomenimis (R7)
TR43	Išpuolių vykdytojas gali apeiti arba iškreipti dėklės atliekamas patikras, kuriomis tikrinami visi tam pačiam naudotojui priklausantys prašomi požymiai, kad jų rezultatai visada būtų sėkmingi.	Manipuliavimas duomenimis (R7)
TR44	Išpuolių vykdytojas gali apeiti arba iškreipti dėklės atliekamas patikras, kuriomis tikrinama, ar galioja asmens tapatybės duomenys ir ar juos išdavė patikimas asmens tapatybės duomenų teikėjas, kad jų rezultatai visada būtų sėkmingi.	Manipuliavimas duomenimis (R7)

ID *Identifikatorius*	Grėsmės aprašymas *Nustatytos grėsmės aprašymas* (*)	Rizikos pavadinimas *Susijusi rizika*
TR45	Išpuolių vykdytojas gali apeiti arba iškreipti dėklės atliekamas patikras, kuriomis tikrinama, ar galioja kvalifikuotas elektroninis požymių liudijimas ir ar jį išdavė kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, registruotas išduoti kvalifikuotus elektroninius požymių liudijimus, kad jų rezultatai visada būtų sėkmingi.	Manipuliavimas duomenimis (R7)
TR46	Išpuolių vykdytojas gali apeiti arba iškreipti dėklės atliekamas patikras, kuriomis tikrinama, ar asmens tapatybės duomenų teikėjas neatšaukė asmens tapatybės duomenų, kad jų rezultatai visada būtų sėkmingi.	Manipuliavimas duomenimis (R7)
TR47	Išpuolių vykdytojas gali apeiti arba iškreipti dėklės atliekamas patikras, kuriomis tikrinama, ar kvalifikuoto elektroninio požymių liudijimo teikėjas neatšaukė kvalifikuoto elektroninio požymių liudijimo, kad jų rezultatai visada būtų sėkmingi.	Manipuliavimas duomenimis (R7)
TR48	Išpuolių vykdytojas gali pakeisti atsarginių kopijų ir atkūrimo duomenų, kuriuos išimtinai turėtų kontroliuoti naudotojas, turinį.	Manipuliavimas duomenimis (R7) / duomenų praradimas (R8)
TR49	Išpuolių vykdytojas gali pakeisti konkretaus dėklės egzemplioriaus sandorio istoriją veiklos žurnaluose.	Manipuliavimas duomenimis (R7) / duomenų praradimas (R8)
TR50	Išpuolių vykdytojas gali neteisėtai perimti informaciją, kai užmezgamas ryšys tarp dėklės ir pasikliaujančiųjų šalių.	Duomenų vagystė (R5) / duomenų atskleidimas (R6)
TR51	Išpuolių vykdytojas gali įtikinti naudotoją atskleisti savo asmens duomenis (t. y. asmens tapatybės duomenis, elektroninį požymių liudijimą, slapyvardžius, elektroninius parašus, žurnalus ir kitus duomenis) išpuolių vykdytojui arba trečiajai šaliai, kuriai duomenų atskleisti naudotojas neketino.	Duomenų vagystė (R5) / duomenų atskleidimas (R6)
TR52	Išpuolių vykdytojas gali perskaityti konkretaus dėklės egzemplioriaus sandorio istoriją veiklos žurnaluose.	Duomenų vagystė (R5) / duomenų atskleidimas (R6)
TR53	Išpuolių vykdytojas gali eksportuoti arba atskleisti kriptografinio rakto medžiagą už saugaus dėklės šifravimo įrenginio ribų.	Duomenų vagystė (R5) / duomenų atskleidimas (R6) / neteisėtas sandoris (R9)
TR54	Išpuolių vykdytojas gali perskaityti atsarginių kopijų ir atkūrimo duomenų, kuriuos išimtinai turėtų kontroliuoti naudotojas, turinį.	Duomenų vagystė (R5) / duomenų atskleidimas (R6)
TR55	Išpuolių vykdytojas gali apeiti naudotojo tapatumo nustatymo metodą, kad galėtų naudoti dėklės vieneto sugeneruotą slapyvardį.	Tapatybės vagystė (R4)
TR56	Išpuolių vykdytojas gali pasiūlyti naudotojams taikomąją programą, kuria imituojama konkreti teisėta dėklė.	Tapatybės vagystė (R4)
TR57	Išpuolių vykdytojas gali eksportuoti dėklės duomenis, įskaitant asmens tapatybės duomenis, kvalifikuotus elektroninius požymių liudijimus arba žurnalus.	Tapatybės vagystė (R4)
TR58	Išpuolių vykdytojas gali eksportuoti kriptografinio susiejimo medžiagą.	Tapatybės vagystė (R4)
TR59	Išpuolių vykdytojas gali perimti tapatybę naudodamas dėklės kriptografinius raktus.	Tapatybės vagystė (R4)
TR60	Išpuolių vykdytojas gali nukopijuoti kito naudotojo asmeninės dėklės vienetą į savo asmeninį įrenginį ir juo naudotis.	Tapatybės vagystė (R4) / esamos elektroninės tapatybės sukūrimas arba naudojimas (R1)

ID *Identifikatorius*	Grėsmės aprašymas *Nustatytos grėsmės aprašymas* (*)	Rizikos pavadinimas *Susijusi rizika*
TR61	Kitos valstybės institucijos gali betarpiškai paprašyti naudotojo parodyti ir (arba) atskleisti visus dėklės duomenis, pavyzdžiui, jam kertant tos valstybės sieną.	Tapatybės vagystė (R4) / sekimas (R14)
TR62	Sugedus naudotojo įrenginiui, naudotojai negali perduoti savo sandorių žurnalų, todėl naujojoje dėklėje prarandamas ankstesnių sandorių atsekamumas.	Veiksmų nepripažinimas (R11)
TR63	Sugedus naudotojo įrenginiui, naudotojai negali atgauti savo sandorių žurnalų, todėl naujojoje dėklėje prarandamas atsekamumas.	Veiksmų nepripažinimas (R11)
TR64	Pasikliaujančiosioms šalims gali būti sunku įrodyti nuotolinių elektroninių parašų patvirtinimą.	Veiksmų nepripažinimas (R11)
TR65	Išpuolių vykdytojas gali perkrauti ryšį užklausomis, kai užmezgamas ryšys su pasikliaujančiosiomis šalimis.	Paslaugos nutraukimas (R13)
TR66	Išpuolių vykdytojas gali perkrauti padėties užtikrinimo paslaugą ryšio su pasikliaujančiosiomis šalimis bandymais.	Paslaugos nutraukimas (R13)
TR67	Išpuolių vykdytojas gali sudaryti įspūdį, kad požymių pateikimas yra užginčytas / atmestas, nepaisant pateikiamų požymių galiojimo.	Paslaugos nutraukimas (R13)
TR68	Išpuolių vykdytojas gali atšaukti asmens tapatybės duomenis be pagrįstos priežasties.	Paslaugos nutraukimas (R13)
TR69	Išpuolių vykdytojas gali atšaukti asmens tapatybės duomenis be naudotojo sutikimo.	Paslaugos nutraukimas (R13)
TR70	Išpuolių vykdytojas gali atšaukti kvalifikuotą elektroninį požymių liudijimą be pagrįstos priežasties.	Paslaugos nutraukimas (R13)
TR71	Išpuolių vykdytojas gali atšaukti kvalifikuotą elektroninį požymių liudijimą be naudotojo sutikimo.	Paslaugos nutraukimas (R13)
TR72	Išpuolių vykdytojas gali inicijuoti kelias tapatybės nustatymo užklausas taip, kad jos nebus atpažintos kaip generuotos ne naudotojo.	Paslaugos nutraukimas (R13)
TR73	Išpuolių vykdytojas gali išsiųsti keletą užklausų ir neatlikti tolesnių veiksmų.	Paslaugos nutraukimas (R13)
TR74	Išpuolių vykdytojas gali leisti pasikliaujančiajai šaliai prašyti tapatybės nustatymo be atitinkamo atsakymo (tapatybės nustatymo) ir visiškos kontrolės.	Paslaugos nutraukimas (R13)
TR75	Išpuolių vykdytojas gali išsiųsti atsakymą į užklausą jau pasibaigus jai skirtam laikui arba atlikti kitokius veiksmus, dėl kurių sutrinka paslaugos teikimas.	Paslaugos nutraukimas (R13)
TR76	Pasikliaujančioji šalis gali siųsti kelias negaliojančias užklausas.	Paslaugos nutraukimas (R13)
TR77	Išpuolių vykdytojas gali siųsti kelias negaliojančias užklausas dėklės teikėjui.	Paslaugos nutraukimas (R13)
TR78	Išpuolių vykdytojas gali sukliudyti valstybei narei pašalinti nepatikimo asmens tapatybės duomenų teikėjo iš patikimų asmens tapatybės duomenų teikėjų sąrašo.	Paslaugos nutraukimas (R13)
TR79	Išpuolių vykdytojas gali sukliudyti dėklės galiojimo sustabdymui ar atšaukimui.	Paslaugos nutraukimas (R13)

ID *Identifikatorius*	Grėsmės aprašymas *Nustatytos grėsmės aprašymas* (*)	Rizikos pavadinimas *Susijusi rizika*
TR80	Išpuolių vykdytojas gali blokuoti pasikliaujančiųjų šalių, naudotojų ir (arba) asmens tapatybės duomenų teikėjo vykdomus sandorius.	Paslaugos nutraukimas (R13)
TR81	Išpuolių vykdytojas gali išjungti saugų dėklės šifravimo įrenginį arba padaryti jį neprieinamą.	Paslaugos nutraukimas (R13)
TR82	Išpuolių vykdytojas gali sukliudyti asmens tapatybės duomenų teikėjui atšaukti asmens tapatybės duomenis arba sustabdyti jų galiojimą.	Paslaugos nutraukimas (R13) / neleistinas sandoris (R9)
TR83	Pasikliaujančioji šalis gali gauti ne tik duomenis, kurie su ja bendrinami, bet ir naudotojo tapatybės duomenis.	Sekimas (R14)
TR84	Nelegaliai bendradarbiaujančių pasikliaujančiųjų šalių arba asmens tapatybės duomenų teikėjų grupė gali gauti ne tik duomenis, kurie jiems žinomi, bet ir naudotojo tapatybės duomenis.	Sekimas (R14)
TR85	Išpuolių vykdytojas gali sekti ir atsekti naudotoją naudodamas naudotojo asmens tapatybės duomenis, kai nereikalaujamas naudotojo tapatybės nustatymas.	Sekimas (R14)
TR86	Išpuolių vykdytojas gali sukurti „suklastotą“ kvalifikuotų elektroninių požymių liudijimų derinių pateiktį.	Manipuliavimas sandoriu (R10)
TR87	Išpuolių vykdytojas gali aktyvinti / perimti dėklę nuotoliniu būdu (pvz., per banko mobiliąją programėlę su integruota elektroninio tapatumo nustatymo arba liudijimo užklausa) be aiškaus naudotojo sutikimo arba išskirtinės naudotojo kontrolės, kai naudotojas neįtaria, kad pasikliaujančioji šalis veikia, (pvz., miega) arba jos nemato.	Manipuliavimas sandoriu (R10)
TR88	Išpuolių vykdytojai gali keisti užklausos metaduomenis (paslaugos pavadinimą, naudojimo būdus ir kt.).	Manipuliavimas sandoriu (R10)
TR89	Išpuolių vykdytojai gali keisti atsako informaciją (paslaugos valstybę, vienkartinę saugos frazę ir pan.).	Manipuliavimas sandoriu (R10)
TR90	Išpuolių vykdytojai gali keisti užklausos požymio informaciją (kartotinai prašant informacijos ir kt.).	Manipuliavimas sandoriu (R10)
TR91	Pasikliaujančioji šalis gali pakartoti ankstesnės sesijos elementus kitoje sesijoje.	Manipuliavimas sandoriu (R10)
TR92	Išpuolių vykdytojas gali modifikuoti asmens tapatybės duomenis arba pakeisti juos kitais, kai jie perduodami iš asmens tapatybės duomenų teikėjo į dėklės vienetą.	Manipuliavimas sandoriu (R10)
TR93	Išpuolių vykdytojas gali modifikuoti asmens tapatybės duomenis arba pakeisti juos kitais, kai jie perduodami iš dėklės vieneto internetinei pasikliaujančiajai šaliai.	Manipuliavimas sandoriu (R10)
TR94	Išpuolių vykdytojas gali modifikuoti asmens tapatybės duomenis arba pakeisti juos kitais, kai jie perduodami iš dėklės vieneto neprisijungusiai pasikliaujančiajai šaliai.	Manipuliavimas sandoriu (R10)
TR95	Išpuolių vykdytojas gali išduoti asmens tapatybės duomenis be naudotojo sutikimo.	Neleistinas sandoris (R9)
TR96	Išpuolių vykdytojas gali naudoti atšauktą arba negaliojančią integruotą informacijos atskleidimo politiką galimai be pasikliaujančiųjų šalių žinios.	Neleistinas sandoris (R9)
TR97	Išpuolių vykdytojas gali suklaidinti dėklę, kad ji patvirtintų neteisingus elektroninius parašus.	Neleistinas sandoris (R9)
TR98	Išpuolių vykdytojas gali naudoti dėklę be naudotojo kontrolės.	Neleistinas sandoris (R9)

ID *Identifikatorius*	Grėsmės aprašymas *Nustatytos grėsmės aprašymas* (*)	Rizikos pavadinimas *Susijusi rizika*
TR99	Išpuolių vykdytojas gali įtikinti naudotoją patvirtinti savo tapatybę ir patvirtinti sandorius su išpuolių vykdytoju arba leidimo neturinčia trečiąja šalimi.	Neleistinas sandoris (R9)
TR100	Išpuolių vykdytojas gali priversti naudotoją pasirašyti elektroniniu parašu, nepateikęs naudotojui turinio arba pateikęs neteisingą turinį.	Neleistinas sandoris (R9)
TR101	Išpuolių vykdytojas gali apeiti dėklės teikėjo prieigos prie naudotojo paskyros kontrolės priemones.	Neleistinas sandoris (R9)
TR102	Išpuolių vykdytojas gali apsimesti pasikliaujančiosiomis šalimis užmezgant ryšį su pasikliaujančiosiomis šalimis.	Neleistinas sandoris (R9) / duomenų atskleidimas (R6)
TR103	Pasikliaujančiosios šalies ir naršyklės ryšio naudotojas gali skirtis nuo pasikliaujančiosios šalies ir dėklės ryšio naudotojo.	Neleistinas sandoris (R9) / duomenų atskleidimas (R6) / tapatybės vagystė (R4)
TR104	Išpuolių vykdytojas gali įtikinti naudotoją be priežasties atšaukti naudotojo dėklę.	Neleistinas sandoris (R9) / paslaugos nutraukimas (R13)
TR105	Išpuolių vykdytojas gali įvykdyti komunikacijos perėmimo išpuolį.	Neleistinas sandoris (R9) / duomenų atskleidimas (R6) / sekimas (R14)
TR106	Išpuolių vykdytojas gali pateikti negaliojančius arba atšauktus dėklės, kuri reguliariai neprisijungia prie tinklo, požymius.	Poveikis įvairioms rizikos rūšims
TR107	Išpuolių vykdytojas gali pavogti iš naudotojo gautą informaciją suklastojęs dėklę.	Poveikis įvairioms rizikos rūšims
TR108	Išpuolių vykdytojas gali apsimesti naudotoju, pakartodamas / imituodamas duomenų užklausą (pvz., tapatumo nustatymo), kuri atrodo kaip galiojanti.	Poveikis įvairioms rizikos rūšims
TR109	Išpuolių vykdytojas gali pakartoti naudotojui integruotą informacijos atskleidimo politiką, kad imituotų patvirtintą užklausą.	Poveikis įvairioms rizikos rūšims
TR110	Išpuolių vykdytojas gali pasinaudoti dėklės naudotojų informacijos trūkumu arba nepagrįstu vėlavimu po saugumo pažeidimo ar patikimumo pažeidimo.	Poveikis įvairioms rizikos rūšims
TR111	Išpuolių vykdytojas gali modifikuoti anksčiau įdiegtą teisėtą dėklės egzempliorių, kad įtrauktų kenkimo savybių.	Poveikis įvairioms rizikos rūšims
TR112	Išpuolių vykdytojas gali modifikuoti teisėtą dėklės egzempliorių ir pasiūlyti jį naudotojams kaip teisėtą.	Poveikis įvairioms rizikos rūšims
TR113	Išpuolių vykdytojas gali išderinti patį naudotojo tapatumo nustatymo mechanizmą, kad apeitų dėklės naudotojo tapatumo nustatymą.	Poveikis įvairioms rizikos rūšims
TR114	Išpuolių vykdytojas gali įdiegti kenkėjišką kodą arba užpakalines duris į dėklės kodą, kai jis diegiamas naudotojo įrenginyje.	Poveikis įvairioms rizikos rūšims
TR115	Išpuolių vykdytojas gali įdiegti kenkėjišką kodą arba užpakalines duris į dėklės kodą, kai jis kuriamas.	Poveikis įvairioms rizikos rūšims
TR116	Išpuolių vykdytojas gali suklastoti atsitiktinai generuojamus skaičius, kad pakankamai sumažintų jų entropiją ir galėtų vykdyti išpuolius.	Poveikis įvairioms rizikos rūšims

ID *Identifikatorius*	Grėsmės aprašymas *Nustatytos grėsmės aprašymas* (*)	Rizikos pavadinimas *Susijusi rizika*
TR117	Išpuolių vykdytojas gali suklastoti naudotojo įrenginius tiekimo grandinėje, kad įdiegtų juose kodą arba konfigūraciją, neatitinkančius dėklės naudojimo sąlygų.	Poveikis įvairioms rizikos rūšims
TR118	Išpuolių vykdytojas gali aktyvinti dėklės vienetą naudodamas išpuolių vykdytojų kontroliuojamą suklastotą saugų dėklės šifravimo įrenginį.	Poveikis įvairioms rizikos rūšims
TR119	Išpuolių vykdytojas gali perskaityti į saugią dėklės šifravimo programą ir (arba) saugų dėklės šifravimo įrenginį siunčiamą informaciją.	Poveikis įvairioms rizikos rūšims
TR120	Išpuolių vykdytojas gali išsiųsti savavališką informaciją į saugią dėklės šifravimo programą.	Poveikis įvairioms rizikos rūšims
TR121	Išpuolių vykdytojas gali pavogti informaciją, perimdamas informacijos mainus tarp saugios dėklės šifravimo programos ir (arba) saugaus dėklės šifravimo įrenginio.	Poveikis įvairioms rizikos rūšims
TR122	Išpuolių vykdytojas gali išsiųsti savavališką informaciją į saugų dėklės šifravimo įrenginį.	Poveikis įvairioms rizikos rūšims
TR123	Išpuolių vykdytojas gali išsiųsti informaciją į saugų dėklės šifravimo įrenginį, apeidamas saugią dėklės šifravimo programą.	Poveikis įvairioms rizikos rūšims
TR124	Išpuolių vykdytojas gali pasitelkti duomenų viliojimą, kad paskatintų naudotojus prisijungti prie netikros dėklės ir asmens tapatybės duomenų valdymo internetinės taikomosios programos.	Poveikis įvairioms rizikos rūšims
TR125	Išpuolių vykdytojas gali pakeisti dėklės raktus kitais raktais, kad sukurtų pranešimus, kurie bus naudojami kito išpuolio metu.	Poveikis įvairioms rizikos rūšims
TR126	Išpuolių vykdytojas gali modifikuoti arba sunaikinti piniginės raktus ir dėl to kai kurios dėklės funkcijos tampa nebenaudojamos.	Poveikis įvairioms rizikos rūšims
TR127	Išpuolių vykdytojas gali kontroliuoti kenkimo programinę įrangą, kad gautų prieigą prie dėklėje saugomų duomenų.	Poveikis įvairioms rizikos rūšims
TR128	Išpuolių vykdytojas gali pasiekti dėklėje generuotus įrodymus.	Poveikis įvairioms rizikos rūšims
TR129	Dėklės teikėjai gali pasiekti dėklėje esančius objektus.	Poveikis įvairioms rizikos rūšims
TR130	Dėklės teikėjai gali pasiekti dėklėje generuotus įrodymus.	Poveikis įvairioms rizikos rūšims
TR131	Išpuolių vykdytojas gali pavogti neužrakintą dėklės įrenginį.	Poveikis įvairioms rizikos rūšims
TR132	Išpuolių vykdytojas gali manipuliuoti sistema, kad nebūtų galima užregistruoti tam tikrų įvykių.	Poveikis įvairioms rizikos rūšims
TR133	Išpuolių vykdytojas gali perimti dėklės egzemplioriaus ir saugios dėklės šifravimo programos ryšį arba atkartoti / imituoti naudotoją (pvz., užvaldydamas elektroninio tapatumo nustatymo mechanizmą).	Poveikis įvairioms rizikos rūšims

II PRIEDAS

SAUGUMO UŽTIKRINIMO INFORMACIJOS PRIIMTINUMO VERTINIMO KRITERIJAI

Pavadinimas	Objektas	Į ką atkreipti dėmesį
EKSSS	IRT produktai	Dėl paskelbusios įstaigos: nėra (akredituotos sertifikavimo įstaigos). Dėl taikymo srities: — patikrinti apsaugos profilį ir apsaugos tikslą, — patikrinti vertinimo užtikrinimo lygį ir papildinius. Dėl saugumo užtikrinimo: — patikrinti apribojimus naudotojo dokumentuose, — norint susipažinti su sudėtimi, gali prireikti prieigos prie vertinimo techninės ataskaitos.
ES debesijos saugumo sertifikavimo schema EUCS (jei yra)	Debesijos paslaugos	Dėl paskelbusios įstaigos: nėra (akredituotos sertifikavimo įstaigos). Dėl taikymo srities: — patikrinti debesijos paslaugos aprašymą, — patikrinti vertinimo lygį ir plėtinių profilius. Dėl saugumo užtikrinimo: — patikrinti skaidrumo informaciją ir, jei reikia, informaciją apie sudėtį.
ES veikiančios bendraisiais kriterijais grindžiamos schemos, įskaitant SOG-IS schemas	IRT produktai	Dėl paskelbusios įstaigos: nėra (valstybės narės). Dėl taikymo srities: — patikrinti apsaugos profilį ir apsaugos tikslą, — patikrinti vertinimo užtikrinimo lygį ir papildinius. Dėl saugumo užtikrinimo: — patikrinti apribojimus naudotojo dokumentuose, — norint susipažinti su sudėtimi, gali prireikti prieigos prie vertinimo techninės ataskaitos.
EN 17640:2018 (FITCEM, įskaitant CSPN, BSZ, LINCE, BSZA)	IRT produktai	Dėl paskelbusios įstaigos: — patikrinti sertifikavimo įstaigoms taikomą schemą ir reikalavimus. Dėl taikymo srities: — patikrinti produkto aprašymą, — patikrinti saugumo teiginius, — patikrinti saugumo užtikrinimo lygį. Dėl saugumo užtikrinimo: — patikrinti vykdytą veiklą ir ataskaitoje nurodytus radinius.
Kvalifikuotų parašo kūrimo įtaisų sertifikavimo schemos pagal Reglamento (ES) Nr. 910/2014 30 straipsnį	Kvalifikuotas elektroninio parašo kūrimo įtaisas	Dėl paskelbusios įstaigos: — patikrinti sertifikavimo įstaigoms taikomą schemą ir reikalavimus. Dėl taikymo srities: — patikrinti produkto aprašymą, — patikrinti saugumo teiginius, — patikrinti saugumo užtikrinimo lygį. Dėl saugumo užtikrinimo: — patikrinti vykdytą veiklą.

Pavadinimas	Objektas	Į ką atkreipti dėmesį
EN ISO/IEC 27001:2022	Informacijos saugumo valdymo sistema	Dėl paskelbusios įstaigos: nėra (akredituotos sertifikavimo įstaigos). Dėl taikymo srities: — patikrinti valdymo sistemos aprašymą, — patikrinti taikomumo pareiškimą. Dėl saugumo užtikrinimo: — patikrinti vykdytą veiklą.
SOC2	Organizacijos	Dėl paskelbusios įstaigos: — patikrinti viešojo apskaitininko statusą. Dėl taikymo srities: — patikrinti vadovybės ataskaitą ir kontrolės priemonių aprašymą, — patikrinti taikomumo pareiškimą. Dėl saugumo užtikrinimo: — patikrinti ataskaitoje nurodytus radinius, — prireikus patikrinti tarpinį pranešimą.
Mobiliųjų įrenginių sertifikavimo schema MDSCert (GSMA) (jei yra)	Mobilieji įrenginiai	Dėl paskelbusios įstaigos: — patikrinti sertifikavimo įstaigoms taikomus reikalavimus. Dėl taikymo srities: — patikrinti saugumo užtikrinimo lygį, — patikrinti schemos reikalavimus. Dėl saugumo užtikrinimo: — patikrinti ataskaitoje nurodytus radinius.
Kitos schemos	Bet kuris komponentas	Dėl schemos: — patikrinti schemos aktualumą ir nuostatas. Dėl paskelbusios įstaigos: — patikrinti sertifikavimo įstaigoms taikomus reikalavimus. Dėl taikymo srities: — patikrinti schemos reikalavimus, — patikrinti saugumo tikslą arba panašų dokumentą, kuriame aprašomi saugumo funkciniai ir saugumo užtikrinimo reikalavimai, — patikrinti produkto aprašymą ir pasirinktus saugumo funkcinius reikalavimus. Dėl saugumo užtikrinimo: — patikrinti ataskaitoje nurodytus radinius.

III PRIEDAS

DĖKLĖS SPRENDINIAMS TAIKOMI FUNKCINIAI REIKALAVIMAI

Pagal Reglamento (ES) Nr. 910/2014 5a straipsnio 4, 5, 8 ir 14 dalis, funkciniai kriterijai, kuriuos turi atitikti sertifikuotas dėklės sprendinys ir elektroninės atpažinties schema, pagal kurią jis teikiamas, apima operacijų funkcinius reikalavimus, išvardytus šiuose dokumentuose:

(1) Komisijos įgyvendinimo reglamente (ES) 2024/2979 ([1]), kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 taikymo taisyklės, susijusios su vientisumu ir pagrindinėmis funkcijomis;

(2) Komisijos įgyvendinimo reglamente (ES) 2024/2982 ([2]), kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 nuostatų dėl Europos skaitmeninės tapatybės sistemos palaikytinų protokolų ir sąsajų taikymo taisyklės;

(3) Komisijos įgyvendinimo reglamentas (ES) 2024/2977 ([3]), kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 nuostatų dėl naudojantis europinėmis skaitmeninės tapatybės dėklėmis išduodamų asmens tapatybės duomenų ir elektroninių požymių liudijimų taikymo taisyklės.

([1]) 2024 m. lapkričio 28 d. Komisijos įgyvendinimo reglamentas (ES) 2024/2979, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 taikymo taisyklės, susijusios su europinių skaitmeninės tapatybės dėklių vientisumu ir pagrindinėmis funkcijomis (OL L, 2024/2979, 2024 12 4, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([2]) 2024 m. lapkričio 28 d. Komisijos įgyvendinimo reglamentas (ES) 2024/2982, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 nuostatų dėl Europos skaitmeninės tapatybės sistemos palaikytinų protokolų ir sąsajų taikymo taisyklės (OL L, 2024/2982, 2024 12 4, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([3]) 2024 m. lapkričio 28 d. Komisijos įgyvendinimo reglamentas (ES) 2024/2977, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 nuostatų dėl naudojantis europinėmis skaitmeninės tapatybės dėklėmis išduodamų asmens tapatybės duomenų ir elektroninių požymių liudijimų taikymo taisyklės (OL L, 2024/2977, 2024 12 4, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

IV PRIEDAS

VERTINIMO VEIKLOS METODAI IR PROCEDŪROS

1. **Dėklės sprendinio įgyvendinimo auditas**

Atitikties vertinimo veikla apima konkrečios vertinimo veiklos atranką.

Nacionalinėse sertifikavimo schemose nurodoma vertinimo veikla pateiktai informacijai įvertinti, apimanti bent šiuos dalykus:

a) pateiktos informacijos analizę siekiant patvirtinti, kad ji tinkama vienai iš nacionalinėse sertifikavimo schemose nurodytų architektūrų;

b) analizę, ar aprašytos saugumo kontrolės priemonės aprėpia I priedo rizikos registre nustatytą kibernetinę riziką ir grėsmes.

Atliekant a–b punktuose nurodytą analizę atsižvelgiama į dėklės teikėjo pateiktą loginį pagrindą ir pagrindimą.

2. **Vertinimo veikla, susijusi su saugiu dėklės šifravimo įrenginiu**

1) Nereikalaujama, kad saugiame dėklės šifravimo įrenginyje būtų visiškai įgyvendintos ypatingos svarbos operacijos, įskaitant šifravimo skaičiavimus. Tačiau saugiame dėklės šifravimo įrenginyje įgyvendinta dalis, kuri naudojama kaip dėklės sprendinio dalis, garantuoja ypatingos svarbos operacijų apsaugą nuo išpuolių vykdytojų su dideliu išpuolių vykdymo potencialu pagal Komisijos įgyvendinimo reglamentą (ES) 2015/1502 ([1]).

2) Saugus dėklės šifravimo įrenginys (arba jo dalis) gali būti įtrauktas į sertifikavimo objektą, kai jį pateikia sertifikato turėtojas ar pareiškėjas, arba jis neįtraukiamas į sertifikavimo taikymo sritį, kai yra integruotas į galutinio naudotojo pateiktą įrenginį. Be to, nacionalinėse sertifikavimo schemose nurodoma vertinimo veikla, kuria siekiama patikrinti saugaus dėklės šifravimo įrenginio tinkamumą šiais dviem atvejais:

   a) jei nuo konkretaus saugaus dėklės šifravimo įrenginio priklauso saugi dėklės šifravimo programa (t. y. jei ją reikia vertinti kaip sudėtinį produktą, naudojamą kartu su saugiu dėklės šifravimo įrenginiu), vertinant saugią dėklės šifravimo programą reikia susipažinti su papildoma informacija, susijusia su saugaus dėklės šifravimo įrenginio sertifikavimu, įskaitant visų pirma jo vertinimo techninę ataskaitą;

   b) jeigu schemoje svarstomoje architektūroje naudojami keli saugūs dėklės šifravimo įrenginiai arba kai kurios operacijos, susijusios su ypatingos svarbos turtu, vykdomos ne saugiame dėklės šifravimo įrenginyje, nacionalinės sertifikavimo schemos apima vertinimo veiklą, kuria siekiama užtikrinti, kad bendru sprendiniu būtų užtikrintas tikėtinas saugumo lygis.

3) Būtina sertifikavimo pagal nacionalines sertifikavimo schemas sąlyga yra saugaus dėklės šifravimo įrenginio vertinimas pagal aukšto saugumo užtikrinimo lygio reikalavimus, nustatytus Įgyvendinimo reglamente (ES) 2015/1502.

   Kai tenkinamos 3 straipsnio 3 dalies b punkte nustatytos sąlygos, į saugaus dėklės šifravimo įrenginio arba jos dalies vertinimą įtraukiamas AVA_VAN.5 lygio pažeidžiamumo vertinimas, nustatytas EN ISO/IEC 15408-3:2022 pagal Komisijos įgyvendinimo reglamento (ES) 2024/482 ([2]) I priedo nuostatas, išskyrus atvejus, kai sertifikavimo įstaigai tinkamai pagrindžiama, kad dėl saugios dėklės šifravimo programos saugumo charakteristikų galima taikyti žemesnį vertinimo lygį, išlaikant tokį patį bendrą aukštą saugumo užtikrinimo lygį, koks nustatytas Įgyvendinimo reglamente (ES) 2015/1502.

([1]) 2015 m. rugsėjo 8 d. Komisijos įgyvendinimo reglamentas (ES) 2015/1502, kuriuo pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 8 straipsnio 3 dalį nustatomos minimalios techninės specifikacijos ir procedūros dėl elektroninės atpažinties priemonių saugumo užtikrinimo lygių, (OL L 235, 2015 9 9, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

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

4) Be to, su kiekviena konkrečia architektūra susijusiuose nacionalinių sertifikavimo schemų dokumentuose suformuluojamos saugaus dėklės šifravimo įrenginio vertinimo prielaidos, pagal kurias gali būti užtikrinta apsauga nuo išpuolių vykdytojų su dideliu išpuolių vykdymo potencialu pagal Įgyvendinimo reglamentą (ES) 2015/1502, ir nustatomi vertinimo veiksmai, kuriais patvirtinamos šios prielaidos ir patikinama, kad jos išliks patvirtintos ir išdavus sertifikatą. Nacionalinėse schemose taip pat reikalaujama, kad sertifikavimo kandidatai patikslintų šias prielaidas, atsižvelgdami į jų konkretų įgyvendinimą, ir apibūdintų taikomas priemones, kuriomis užtikrinama, kad prielaidos bus tikrinamos visą sertifikavimo ciklą.

5) Visais atvejais į nacionalines sertifikavimo schemas įtraukiama vertinimo veikla, kuria siekiama patikrinti, ar saugiam dėklės šifravimo įrenginiui priskiriama saugumo užtikrinimo informacija yra tinkama dėklės sprendiniui, analizuojant saugumo užtikrinimo informaciją, pavyzdžiui, EKSSS sertifikatų saugumo tikslą, įskaitant šiuos veiksmus:

   a) patikrinti, ar vertinimo taikymo sritis yra tinkama, o išduodant EKSSS sertifikatus – patikrinti, ar saugumo tikslas atitinka vieną iš EKSSS rekomenduojamų apsaugos profilių;

   b) patikrinti, ar operacinės aplinkos prielaidos yra suderinamos su dėklės sprendiniu, pavyzdžiui, išduodant EKSSS sertifikatus tai reiškia, kad šios prielaidos nurodytos saugumo tiksle;

   c) patikrinti, ar naudotojo gairėse arba dokumentuose pateiktos rekomendacijos atitinka sąlygas, pagal kurias saugus dėklės šifravimo įrenginys turi būti naudojamas dėklės sprendinyje;

   d) patikrinti, ar nacionalinėje sertifikavimo schemoje suformuluotos prielaidos dėl saugaus dėklės šifravimo įrenginio yra patikrintos ir įtrauktos į saugumo užtikrinimo informaciją.

6) Kai po tam tikrų patikrinimų nepateikiami neginčijami įrodymai, nacionalinėse sertifikavimo schemose reikalaujama, kad sertifikavimo įstaigos nustatytų kompensacinius reikalavimus, taikomus kartu su saugiu dėklės šifravimo įrenginiu naudojamai saugiai dėklės šifravimo programai, kurie turi būti įtraukti į saugios dėklės šifravimo programos vertinimą. Jei tai neįmanoma, nacionalinėse sertifikavimo schemose laikoma, kad saugus dėklės šifravimo įrenginys nėra tinkamas. Tai reiškia, kad dėklės sprendiniui nebus išduotas atitikties sertifikatas.

3. **Vertinimo veikla, susijusi su saugia dėklės šifravimo programa**

1) Nacionalinėse sertifikavimo schemose reikalaujama, kad saugi dėklės šifravimo programa, kaip dėklės sprendinio dalis, būtų įvertinta pagal reikalavimus, kuriais užtikrinamas bent aukštas saugumo užtikrinimo lygis, nustatytas Įgyvendinimo reglamente (ES) 2015/1502.

2) Į šį vertinimą įtraukiamas AVA_VAN.5 lygio pažeidžiamumo vertinimas, nustatytas EN ISO/IEC 15408-3:2022 pagal Įgyvendinimo reglamento (ES) 2024/482 I priedo nuostatas, išskyrus atvejus, kai sertifikavimo įstaigai tinkamai pagrindžiama, kad dėl saugios dėklės šifravimo programos saugumo charakteristikų galima taikyti žemesnį vertinimo lygį, išlaikant tokį patį bendrą aukštą saugumo užtikrinimo lygį, koks nustatytas Įgyvendinimo reglamente (ES) 2015/1502.

3) Kai dėklės teikėjas saugios dėklės šifravimo programos nepateikia, nacionalinėse sertifikavimo schemose suformuluojamos saugios dėklės šifravimo programos vertinimo prielaidos, pagal kurias gali būti užtikrinta apsauga nuo išpuolių vykdytojų su dideliu išpuolių vykdymo potencialu pagal Įgyvendinimo reglamentą (ES) 2015/1502, ir nustatomi vertinimo veiksmai, kuriais patvirtinamos šios prielaidos ir patikinama, kad jos išliks patvirtintos ir išdavus sertifikatą. Nacionalinėse schemose taip pat reikalaujama, kad sertifikavimo kandidatai patikslintų šias prielaidas, atsižvelgdami į jų konkretų įgyvendinimą, ir apibūdintų taikomas priemones, kuriomis užtikrinama, kad prielaidos bus tikrinamos visą sertifikavimo ciklą.

4) Visais atvejais į nacionalines sertifikavimo schemas įtraukiama vertinimo veikla, kuria siekiama patikrinti, ar saugiai dėklės šifravimo programai priskiriama saugumo užtikrinimo informacija yra tinkama dėklės sprendiniui, analizuojant saugumo užtikrinimo informaciją, pavyzdžiui, EKSSS sertifikatų saugumo tikslą, įskaitant šiuos veiksmus:

   a) patikrinti, ar vertinimo taikymo sritis yra tinkama, o išduodant EKSSS sertifikatus – patikrinti, ar saugumo tikslas atitinka vieną iš EKSSS rekomenduojamų apsaugos profilių;

   b) patikrinti, ar operacinės aplinkos prielaidos yra suderinamos su dėklės sprendiniu, pavyzdžiui, išduodant EKSSS sertifikatus tai reiškia, kad šios prielaidos nurodytos saugumo tiksle;

c) patikrinti, ar naudotojo gairėse arba dokumentuose pateiktos rekomendacijos atitinka sąlygas, pagal kurias saugi dėklės šifravimo programa turi būti naudojama dėklės sprendinyje;

d) patikrinti, ar nacionalinėje sertifikavimo schemoje suformuluotos prielaidos dėl saugių dėklės šifravimo programų yra patikrintos ir įtrauktos į saugumo užtikrinimo informaciją.

5) Nacionalinėse sertifikavimo schemose reikalaujama, kad saugios dėklės šifravimo programos vertinimas apimtų visas šios saugios dėklės šifravimo programos įgyvendinamas saugumo kontrolės priemones.

4. **Vertinimo veikla, susijusi su galutinio naudotojo įrenginiu**

Kadangi rizikos registre, kuris pateiktas šio reglamento I priede, nustatoma rizika, tiesiogiai susijusi su galutinio naudotojo įrenginio saugumu, nacionalinėse sertifikavimo schemose nustatomi galutinių naudotojų įrenginiams taikomi saugumo reikalavimai. Tačiau, kadangi šiuos įrenginius pateikia galutinis naudotojas, o ne dėklės teikėjas, tokie reikalavimai turi būti įtraukti į prielaidas.

Kiekvienai prielaidai dėklės sprendinyje turi būti mechanizmas, skirtas patikrinti, ar kiekvieno dėklės vieneto pagrindinis galutinio naudotojo įrenginys atitinka prielaidą. Tokie mechanizmai laikomi saugumo kontrolės priemonėmis ir įtraukiami į vertinimo veiklą, siekiant įrodyti jų tinkamumą ir veiksmingumą atitinkamu saugumo užtikrinimo lygiu.

Toliau pateikti du pavyzdžiai:

a) galutinio naudotojo įrenginyje gali būti sertifikuotas saugus dėklės šifravimo įrenginys, kurio buvimą reikia įrodyti. Paprastai tai būtų daroma naudojant šifravimo mechanizmą, skirtą patikrinti, ar sertifikuotame saugiame dėklės šifravimo įrenginyje yra slapta kriptografinė medžiaga, prieinama tik sertifikuotame saugiame dėklės šifravimo įrenginyje. Šiuo atveju tokia kriptografinė paslaptis turėtų būti laikoma ypatingos svarbos turtu ir jai turėtų būti taikoma saugaus dėklės šifravimo įrenginio ir (arba) saugios dėklės šifravimo programos sertifikavimo apimtis;

b) tipinis galutinių naudotojų įrenginiams taikomas reikalavimas – jų saugumo naujiniai. Kadangi šis reikalavimas susijęs su dėklės egzemplioriumi, mechanizmas, naudojamas tikrinant saugumo naujinių prieinamumą, turi būti įtrauktas tik į vertinimo veiklą tokiu saugumo užtikrinimo lygmeniu, kuris yra tinkamas dėklės egzemplioriui, ypač dėl to, kad tikėtina, kad jis bus integruotas į dėklės egzempliorių.

5. **Vertinimo veikla, susijusi su dėklės egzemplioriumi**

1) Vertinant dėklės egzempliorių atsižvelgiama į šiuos du pagrindinius uždavinius:

a) tikėtina, kad egzistuoja keli dėklės egzempliorių variantai, naudojantys tą pačią bazinę taikomąją programą, kai kiekvienas variantas yra skirtas konkrečiai galutinio naudotojo įrenginių kategorijai,

b) tikėtina, kad įvairius dėklės egzempliorių variantus reikės dažnai atnaujinti, kad būtų galima stebėti pagrindinės saugumo platformos kūrimą, pavyzdžiui, kai nustatomi pažeidžiamumai, dėl kurių reikia keisti taikomąsias programas.

2) Vertinant dėklės egzempliorių atsižvelgiama į šiuos konkrečius uždavinius. Viena iš tiesioginių pasekmių yra ta, kad Bendrųjų kriterijų sistema gali būti ne visada tinkama. Todėl prireikus apsvarstomos alternatyvios vertinimo metodikos. Nacionalinėse sertifikavimo schemose atsižvelgiama į EN 17640:2018 metodikos naudojimą:

a) kaip pačią schemos dalį;

b) taikant metodika grindžiamas nacionalines schemas;

c) taikant nacionalines schemas, grindžiamas panašiais principais, bet sukurtas iki EN 17640:2018 metodikos parengimo.

3) Be to, kadangi atliekant išsamų specialų kiekvieno varianto vertinimą pridėtinė vertė gali būti ribota, nacionalinėse sertifikavimo schemose apsvarstoma galimybė nustatyti kriterijus, pagal kuriuos būtų galimas imties sudarymas, siekiant išvengti identiškos vertinimo veiklos kartojimosi ir kad daugiausia dėmesio būtų skiriama konkrečiam variantui būdingai veiklai. Nacionalinėse sertifikavimo schemose reikalaujama, kad visos sertifikavimo įstaigos pagrįstų savo imties sudarymą.

4) Į nacionalines sertifikavimo schemas įtraukiami dėklės egzemplioriaus naujiniai pagal bendrą dėklės sprendinio pakeitimų valdymo procesą. Jose taip pat nustatomos taisyklės dėl procedūrų, kurias turi įgyvendinti dėklės teikėjas atlikdamas kiekvieną naujinimą, (pvz., analizuojant pakeitimų poveikį saugumo kontrolei) ir dėl sertifikavimo įstaigos vykdomos naujinių vertinimo veiklos nurodytomis sąlygomis (pvz., dėl pakeistos saugumo kontrolės veikimo veiksmingumo vertinimo). Pokyčių valdymo procesas yra vienas iš procesų, kurių veiklos efektyvumas turi būti tikrinamas kasmet pagal 18 straipsnio 3 dalį.

6. **Vertinimo veikla, susijusi su dėklės sprendinio teikimui ir naudojimui reikalingomis paslaugomis ir procesais**

1) Vertindama paslaugas ir procesus, kurie yra svarbūs teikiant ir naudojant dėklės sprendinį ir elektroninės atpažinties schemą, pagal kurią jis teikiami, vertinimo grupė renka įrodymus vykdydama vertinimo veiklą, kuri gali apimti audito, kontrolės, patikrinimo ir patvirtinimo veiklą.

2) Sertifikavimo įstaiga patvirtina įrodymų, kuriais pakankamai užtikrinama, kad paslaugos ir procesai atitinka sertifikavimo reikalavimus, pakankamumą ir tinkamumą, patvirtindama:

   a) procesų ir paslaugų aprašyme pateiktos informacijos tikslumą;

   b) procesų ir paslaugų projektavimo ir kontrolės tinkamumą, kad jie atitiktų vertinimo kriterijus,

   c) šios kontrolės priemonių įgyvendinimo veiksmingumą nustatytą laikotarpį iki vertinimo.

3) Kontrolės priemonių aprašymo tikslumas ir veiklos veiksmingumas gali būti laikomi atitinkamų dėklės teikėjo teiginių (t. y. jau įvykusių įvykių arba jau gautų rezultatų sąžiningumo patvirtinimo) patikrinimo tikslais pagal ISO/IEC 17000:2020, o paslaugų ir procesų projekto ir kontrolės priemonių tinkamumas, kad jie atitiktų vertinimo kriterijus, gali būti laikomas atitinkamo dėklės teikėjo teiginio (t. y. tikėtinumo dėl numatomo būsimo naudojimo arba numatomo rezultato patvirtinimo) patvirtinimo tikslu pagal ISO/IEC 17000:2020.

4) Atsižvelgiant į tai, kad dėklės sprendinio negalima naudoti prieš jį sertifikuojant, veiklos veiksmingumo negalima patvirtinti remiantis faktiniu sprendinio veikimu. Todėl jis patvirtinamas atsižvelgiant į testavimo ar bandomojo veikimo metu surinktais įrodymais.

5) Galimai jau esama nacionalinių sertifikavimo schemų, taikomų konkrečioms paslaugoms ir procesams, pavyzdžiui, naudotojų prisijungimui sertifikuoti. Jei taikytina, nacionalinėse sertifikavimo schemose apsvarstoma galimybė pasitelkti tokias esamas schemas.

7. **Vertinimo veikla, susijusi su dėklės sprendinio teikimui ir naudojimui reikalingomis IRT paslaugomis**

1) Kai kurios dėklių architektūros gali būti grindžiamos specialiomis IRT paslaugomis, įskaitant debesijos paslaugas, skirtas dėklės sprendiniui teikti ir naudoti, ir teikiant šias paslaugas gali būti laikomi neskelbtini duomenys ir neskelbtinos operacijos. Tokiu atveju nacionalinėse sertifikavimo schemose nustatomi šių IRT paslaugų saugumo reikalavimai.

2) Jau yra nemažai sertifikavimo schemų, susijusių su IRT paslaugomis, debesijos paslaugomis ir kitais saugumo užtikrinimo informacijos šaltiniais, įskaitant išvardytuosius II priede. Nacionalinės sertifikavimo schemos, kai įmanoma ir taikytina, pasitelkia tokius jau esamus mechanizmus, taikydamos vieną iš šių mechanizmų:

   a) įpareigojimą naudoti konkrečią schemą arba kelių schemų derinį, nurodant sąlygas, kuriomis IRT arba debesijos paslaugos turi būti vertinamos naudojant šias schemas;

   b) leidimą dėklės teikėjui pasirinkti vertinimą ir naudoti priklausomybės analizės veiksmus analizuojant per šiuos vertinimus gautos saugumo užtikrinimo informacijos tinkamumą.

3) Abiem atvejais nacionalinėse sertifikavimo schemose nurodoma papildoma vertinimo veikla, kurios reikia pagal šias esamas schemas gautai informacijai analizuoti arba papildyti.

V PRIEDAS

VIEŠAI PRIEINAMOS INFORMACIJOS APIE DĖKLES SĄRAŠAS

1. Pagal 8 straipsnio 5 dalį viešai skelbiama informacija apima bent:

   a) bet kokius dėklės sprendinio naudojimo apribojimus;

   b) dėklės teikėjo konsultacijas ir rekomendacijas siekiant padėti galutiniams naudotojams dėkles saugiai konfigūruoti, instaliuoti, įtaisyti, naudoti ir prižiūrėti;

   c) laikotarpį, per kurį galutiniams naudotojams bus teikiama saugumo priežiūra, visų pirma, kalbant apie su kibernetiniu saugumu susijusių naujinių teikimą;

   d) gamintojo arba teikėjo kontaktinę informaciją ir priimtinus informacijos apie pažeidžiamumo spragas gavimo iš galutinių naudotojų ir saugumo srities tyrėjų metodus;

   e) nuorodą į internetines duomenų saugyklas, kuriose vardijamos viešai atskleistos pažeidžiamumo spragos, susijusios su dėklėmis, ir atitinkamos kibernetinio saugumo rekomendacijos.

2. 1 dalyje nurodyta informacija viešai prieinamoje erdvėje aiškiai, išsamiai ir suprantamai pateikiama bet kuriam asmeniui, norinčiam naudotis dėklės sprendiniu.

VI PRIEDAS

SAUGUMO UŽTIKRINIMO INFORMACIJOS PRIIMTINUMO VERTINIMO METODIKA

1. **Saugumo užtikrinimo dokumentų prieinamumo vertinimas**

Vertintojai išvardija turimus kiekvieno atitinkamo dėklės sprendinio komponento ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, saugumo užtikrinimo dokumentus. Tada vertintojai įvertina bendrą kiekvieno saugumo užtikrinimo dokumento tinkamumą priklausomybės peržiūrai.

Atliekant analizę atsižvelgiama į šiuos aspektus:

1) informaciją apie pačius saugumo užtikrinimo dokumentus:

   a) saugumo užtikrinimo dokumentų rūšį ir visus reikiamus duomenis,

      (tokių dokumentų pavyzdžiai yra atitikties sertifikatai pagal standartą EN ISO/IEC 27001:2022 arba ISAE ataskaitų 1 arba 2 tipas);

   b) taikymo arba galiojimo laikotarpį

      (šis laikotarpis gali būti papildytas tarpiniu pranešimu (dokumentu, apimančiu laikotarpį nuo dabartinės ISAE ataskaitos ataskaitinio laikotarpio pabaigos iki naujos ISAE ataskaitos paskelbimo) arba panašiu pareiškimu);

   c) taikytiną sistemą (pvz., galiojantį standartą);

   d) informaciją, ar saugumo užtikrinimo dokumentuose pateikta nuoroda į schemos reikalavimus;

2) informaciją apie saugumo užtikrinimo ataskaitą paskelbusios įstaigos profesinę kompetenciją ir nešališkumą:

   a) sertifikavimo įstaigos pavadinimą ir, jei yra, vadovaujančio vertintojo vardą ir pavardę;

   b) sertifikavimo įstaigos ir vertintojo kompetencijos įrodymus (pvz., akreditaciją, asmenims išduotus sertifikatus ir kt.);

   c) sertifikavimo įstaigos ir vertintojo nešališkumo įrodymus (pvz., akreditaciją ir kt.).

2. **Su individualiais reikalavimais susijusio saugumo užtikrinimo vertinimas**

Vertintojai patikrina, ar turimi dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, saugumo užtikrinimo dokumentai yra pakankami, kad būtų galima nustatyti, ar dėklės sprendinys atitinka lūkesčius, susijusius su individualiais sertifikavimo schemos reikalavimais.

Atliekant šį vertinimą vertinamas kiekvienas atitinkamas dėklės sprendinio komponentas ir elektroninės atpažinties schema, pagal kurią jis teikiamas, formuluojant prielaidą dėl dėklės sprendinio saugumo kontrolės priemonių.

Vertindama kiekvieną tokią prielaidą vertinimo grupė nustato, ar turimuose saugumo užtikrinimo dokumentuose nurodytas užtikrinimas yra tinkamas.

Nustatant, ar saugumo užtikrinimas yra pakankamas, remiamasi šiais aspektais:

1) saugumo užtikrinimo dokumentuose pateikta informacija, atsižvelgiant į numatomą saugumo užtikrinimo lygį;

2) saugumo užtikrinimo dokumentuose pateikta informacija neapima visos reikalavimo apimties, tačiau papildomos kontrolės priemonės arba kompensacinės kontrolės priemonės (t. y. vidaus kontrolės priemonės, kuriomis mažinama esamo arba galimo kontrolės priemonės trūkumo rizika), įgyvendinamos dėklės sprendinyje arba elektroninės atpažinties schemoje, pagal kurią jis teikiamas, sudaro sąlygas vertintojams nustatyti, ar informacija yra pakankama;

3) saugumo užtikrinimo dokumentuose pateikta informacija neužtikrina numatyto saugumo užtikrinimo lygio, tačiau kontrolės priemonės, įgyvendintos siekiant įvertinti ir stebėti dėklės teikėją, suteikia sąlygas vertintojams nustatyti, ar informacija yra pakankama;

4) jei saugumo užtikrinimo dokumentuose nurodoma, kad kontrolės priemonių, naudojamų prielaidai įvykdyti, struktūra ar įgyvendinimas neatitinka reikalavimų, dėklės teikėjo pasiūlyti ir įgyvendinti taisomieji veiksmai, kuriuos peržiūrėjo jo vertintojai, turi būti pakankami, kad būtų užtikrinta, jog prielaida iš tiesų yra įvykdyta.

VII PRIEDAS

ATITIKTIES SERTIFIKATO TURINYS

1. Atitikties sertifikatą išduodančios sertifikavimo įstaigos suteiktas unikalus identifikatorius.

2. Informacija, susijusi su sertifikuotu dėklės sprendiniu ir elektroninės atpažinties schemomis, pagal kurias jis teikiamas, taip pat informacija apie atitikties sertifikato turėtoją, įskaitant:
   a) dėklės sprendinio pavadinimą;
   b) elektroninės atpažinties schemų, pagal kurias teikiamas dėklės sprendinys, pavadinimus;
   c) vertinto dėklės sprendinio versiją;
   d) atitikties sertifikato turėtojo vardą, pavardę (pavadinimą), adresą ir kontaktinius duomenis;
   e) nuorodą į atitikties sertifikato turėtojo interneto svetainę, kurioje pateikiama informacija, kurią reikalaujama paskelbti viešai.

3. Informacija, susijusi su dėklės sprendinio ir elektroninės atpažinties schemų, pagal kurias jis teikiamas, vertinimu ir sertifikavimu, įskaitant:
   a) atitikties sertifikatą išdavusios sertifikavimo įstaigos pavadinimą, adresą ir kontaktinius duomenis;
   b) vertinimą atlikusios atitikties vertinimo įstaigos pavadinimą, jei ji skiriasi nuo sertifikavimo įstaigos, kartu su informacija apie jos akreditaciją;
   c) schemos savininko vardą, pavardę (pavadinimą);
   d) nuorodas į Reglamentą (ES) Nr. 910/2014 ir šį reglamentą;
   e) nuorodą į sertifikavimo ataskaitą, susijusią su atitikties sertifikatu;
   f) nuorodą į sertifikavimo vertinimo ataskaitą, susijusią su atitikties sertifikatu;
   g) nuorodą į atliekant vertinimą naudotus standartus, įskaitant jų versijas;
   h) atitikties sertifikato išdavimo datą;
   i) atitikties sertifikato galiojimo laikotarpį.

VIII PRIEDAS

VIEŠAI SKELBIAMOS SERTIFIKAVIMO ATASKAITOS IR SERTIFIKAVIMO VERTINIMO ATASKAITOS TURINYS

1. Viešai skelbiamoje sertifikavimo ataskaitoje pateikiami bent šie duomenys:
   a) santrauka;
   b) dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, identifikavimas;
   c) dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią jis teikiamas, aprašymas;
   d) viešai skelbtina saugumo informacija, aprašyta V priede, arba šios informacijos nuoroda;
   e) preliminaraus audito ir patvirtinimo plano santrauka;
   f) Peržiūros ir sprendimo dėl sertifikavimo santrauka.

2. Sertifikavimo vertinimo ataskaitoje pateikiama bent ši informacija:
   a) dėklės sprendinio projekto, identifikavimo sistemos ir prisijungimo proceso aprašymas, taip pat rizikos vertinimas ir specialus patvirtinimo planas;
   b) paaiškinimas, kaip dėklės sprendinys atitinka aukšto saugumo užtikrinimo lygio reikalavimus ir kaip tokia atitiktis įrodoma pagal šį reglamentą atlikto dėklės sprendinio sertifikavimo vertinimo rezultatais;
   c) dėklės sprendinio ir elektroninės atpažinties schemos, pagal kurią teikiami atitinkami dėklės vienetai, atitikties vertinimo rezultatų aprašymas, visų pirma nurodant atitiktį:
      — Reglamento (ES) Nr. 910/2014 5a straipsnio 4, 5 ir 8 dalyse nustatytiems reikalavimams,
      — Reglamento (ES) Nr. 910/2014 5a straipsnio 14 dalyje nustatytiems loginio atskyrimo reikalavimams,
      — kai taikytina, Reglamento (ES) Nr. 910/2014 5a straipsnio 24 dalyje nurodytiems standartams ir techninėms specifikacijoms, kartu apibūdinant, kaip šie reikalavimai yra susiję su atitinkamais norminiais reikalavimais, nustatytais nacionalinėse sertifikavimo schemose;
   d) patvirtinimo plano vykdymo rezultatų santrauka, įskaitant visas nustatytas neatitiktis.

IX PRIEDAS

PRIVALOMŲ PRIEŽIŪROS VERTINIMŲ TVARKARAŠTIS

1. 18 straipsnyje nustatyti sertifikavimo ciklo reikalavimai, visų pirma reguliarios vertinimo veiklos vykdymo reikalavimai. Ši veikla apima bent:

   a) išsamų atitikties vertinimo objekto įvertinimą atliekant pirminį vertinimą ir kiekvieną pakartotinio sertifikavimo vertinimą, apimantį visas bet kurio produkto komponento naujinimo funkciją;

   b) pažeidžiamumo vertinimą atliekant pirminį vertinimą ir kiekvieną pakartotinio sertifikavimo vertinimą ir bent kas dvejus metus atliekant priežiūros vertinimus, apimančius bent atitikties vertinimo objekto pokyčius ir grėsmės aplinkos pokyčius po paskutinio pažeidžiamumo vertinimo;

   c) papildomą veiklą, pavyzdžiui, skverbties testavimą padidėjus rizikos lygiui arba atsiradus naujoms grėsmėms;

   d) techninės priežiūros procesų veikimo veiksmingumo vertinimą bent kartą per metus atliekant priežiūros ir pakartotinio sertifikavimo vertinimus, apimančius bent versijų kontrolės, atnaujinimo ir pažeidžiamumo valdymo procesus;

   e) atitikties sertifikato išdavimą po pirminio vertinimo ir po kiekvieno pakartotinio sertifikavimo vertinimo, atlikus peržiūrą ir priėmus teigiamą sprendimą dėl sertifikavimo.

2. 1 lentelėje pateiktas 4 metų ciklo pavyzdinis tvarkaraštis, kai:

   a) 1 metai prasideda pirmą kartą išdavus atitikties sertifikatą ir

   b) visa vertinimo veikla turi būti atlikta per 12 mėnesių nuo praėjusių metų vertinimo.

3. 1 lentelėje pateiktas tvarkaraštis yra rekomendacija, kaip užtikrinti pakartotinį sertifikavimą laiku ir išvengti dėklės sprendinio teikimo sutrikimų. Gali būti taikomi ir kitokie tvarkaraščiai, su sąlyga, kad atitikties sertifikatas galioja ne ilgiau kaip penkerius metus pagal Reglamento (ES) Nr. 910/2014 5c straipsnio 4 dalies nuostatas.

4. Be reguliarių vertinimų, sertifikavimo įstaigos arba atitikties sertifikato turėtojo prašymu gali būti pradėtas specialusis vertinimas po to, kai iš esmės pasikeičia sertifikavimo objektas arba grėsmių aplinka.

5. Atlikus bet kokį vertinimą, įskaitant priežiūros vertinimus ir specialiuosius vertinimus, gali būti išduotas naujas atitikties sertifikatas, visų pirma tais atvejais, kai iš esmės pasikeičia sertifikavimo objektas, tačiau jo galiojimo terminas sutampa su pirminio atitikties sertifikato galiojimo pabaigos data.

1 lentelė

Išsamus 4 metų vertinimo ciklas

Laikas	Vert. rūšis	Veikla
0 metai	Pirminis	— Išsamus sertifikavimo objekto vertinimas, įskaitant pažeidžiamumų vertinimą — Apima kiekvieno programinės įrangos komponento naujinimo funkciją — Techninės priežiūros procesų vertinimas, išskyrus jų veikimo veiksmingumą — Atitikties sertifikato išdavimas ir 4 metų ciklo pradžia
1 metai	Priežiūros	— Techninės priežiūros procesų veiksmingumo vertinimas — Bent versijos patikra, naujinimas, pažeidžiamumų valdymas — Pokyčių, darančių poveikį produkto saugumui, vertinimas

Laikas	Vert. rūšis	Veikla
2 metai	Priežiūros	— Viso sprendinio pažeidžiamumų vertinimas — Techninės priežiūros procesų veiksmingumo vertinimas — Bent versijos kontrolės, naujinimas, pažeidžiamumų valdymas — Pokyčių, darančių poveikį produkto saugumui, vertinimas
3 metai	Priežiūros	— Techninės priežiūros procesų veiksmingumo vertinimas — Bent versijos patikra, naujinimas, pažeidžiamumų valdymas — Pokyčių, darančių poveikį produkto saugumui, vertinimas
4 metai	Pakartotinis sertifikavimas	1) Išsamus sertifikavimo objekto vertinimas, įskaitant pažeidžiamumų vertinimą 2) Supaprastintas nepakitusių savybių / procesų vertinimas 3) Apima kiekvieno programinės įrangos komponento naujinimo funkciją 4) Techninės priežiūros procesų, įskaitant jų veikimo veiksmingumą, vertinimas 5) Naujo atitikties sertifikato išdavimas