

PATVIRTINTA
Gyventojų registro tarnybos prie
Lietuvos Respublikos vidaus reikalų
ministerijos direktoriaus 2009 m. sausio 27 d.
įsakymu Nr. (29)4R-9

SERTIFIKATO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Sertifikato taisyklės (toliau – taisyklės) nustato kvalifikuoto sertifikato ir asmens atpažinimo elektroninėje erdvėje sertifikato sudarymo ir tvarkymo reikalavimus ir sertifikavimo paslaugų teikėjo bei sertifikatų naudotojų teises, pareigas ir atsakomybę.

2. Pagal šias taisykles sudaromi sertifikatai naudojami šiais tikslais:

2.1. kvalifikuotas sertifikatas naudojamas kvalifikuotam elektroniniam parašui patvirtinti;

2.2. asmens atpažinimo elektroninėje erdvėje sertifikatas naudojamas asmens tapatybei elektroninėje erdvėje nustatyti.

3. Šiose taisyklėse vartojamos sąvokos:

Aktyvavimo duomenys – duomenys, kuriuos būtina įvesti, norint pasinaudoti parašo formavimo duomenimis. Pagal šias taisykles sudaromiems sertifikatams – asmens tapatybės kortelėse esančių kontaktinių elektroninių laikmenų aktyvavimo duomenys (slaptažodžiai).

Asmenims sudaromi sertifikatai – kvalifikuoti sertifikatai ir asmens atpažinimo elektroninėje erdvėje sertifikatai.

Kompromitacija – privačiojo kriptografinio rakto atskleidimas, pavogimas, modifikavimas, neteisėtas panaudojimas arba kitoks privačiojo kriptografinio rakto saugos pažeidimas.

Kriptografinis saugumo modulis – elektroninio parašo formavimo ir tikrinimo duomenims generuoti ir saugoti bei elektroniniam parašui kurti naudojama techninė ir programinė įranga.

Kriptografinių raktų pora – matematiškai susijusių privačiojo ir viešojo kriptografinių raktų pora.

Kvalifikuotas elektroninis parašas – saugus elektroninis parašas, sukurtas saugia parašo formavimo įranga ir patvirtintas kvalifikuotu sertifikatu.

Negaliojančių sertifikatų sąrašas – sertifikavimo paslaugų teikėjo periodiškai leidžiamas sertifikatų, kurių galiojimas nutrauktas ar sustabdytas, sąrašas.

Privatusis kriptografinis raktas – unikalūs elektroninio parašo formavimo duomenys.

Sertifikatais pasitikinčios šalys – fiziniai ir juridiniai asmenys, gaunantys sertifikavimo paslaugų teikėjo sudarytus sertifikatus ir jais patvirtintus elektrinius parašus bei siekiantys

įsitikinti sertifikatų galiojimu, sertifikatų savininkų tapatybe ir kita sertifikatuose nurodyta informacija.

Sertifikato savininkas – fizinis asmuo, kurio vardu sudaromas sertifikatas.

Sertifikatų naudotojai – sertifikatų savininkai ir sertifikatais pasitikinčios šalys.

Sertifikavimo paslaugų teikėjo sertifikatas – sertifikavimo paslaugų teikėjo viešojo kriptografinio rakto sertifikatas.

Viešasis kriptografinis raktas – į sertifikatą įrašomi unikalūs elektroninio parašo tikrinimo duomenys.

Kitos šiose taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos elektroninio parašo įstatyme (Žin., 2000, Nr. 61-1827, Žin., 2002, Nr. 64-2572, toliau – Elektroninio parašo įstatymas), Lietuvos Respublikos asmens tapatybės kortelės įstatyme (Žin., 2001, Nr.97-3417; 2008, Nr.76-3007, toliau – Asmens tapatybės kortelės įstatymas), Reikalavimuose kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, Reikalavimuose elektroninio parašo įrangai, Kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkoje ir Elektroninio parašo priežiūros reglamente, patvirtintuose Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimu Nr. 2108 (Žin., 2003, Nr. 2-47).

4. Elektroninio parašo kūrimą, tikrinimą, galiojimą, parašo naudotojų teises ir atsakomybę, sertifikavimo paslaugas, įskaitant kvalifikuotų sertifikatų sudarymo ir tvarkymo paslaugas ir reikalavimus jų teikėjams, bei atsakomybę nustato Elektroninio parašo įstatymas.

Į sertifikatus įrašomus asmens duomenis nustato Asmens tapatybės kortelės įstatymas.

Elektroninius parašus tvirtinant sertifikatais, sudaromais ir tvarkomais pagal šias taisykles, turi būti naudojama sertifikavimo paslaugų teikėjo teikiama saugi parašo formavimo įranga (elektroninė laikmena, kurioje saugomi kriptografiniai raktai).

5. Šių taisyklių unikalus identifikatorius yra 1.3.6.1.4.1.31912.1.1.1 (1 priedas). Sertifikavimo paslaugų teikėjas, sudarytuose sertifikatuose įrašydamas šių taisyklių unikalų identifikatorių, pažymi, kad jo sudaromi sertifikatai atitinka šių taisyklių reikalavimus, ir patvirtina, kad prisiima visus šiose taisyklėse nustatytus įsipareigojimus ir atsakomybę.

6. Šias taisykles administruojančio darbuotojo kontaktinė informacija pateikta šių taisyklių 2 priede.

II. SERTIFIKAVIMO PASLAUGŲ TEIKĖJO TEIKIAMOS PASLAUGOS, TEISĖS, PAREIGOS IR ATSAKOMYBĖ

7. Sertifikavimo paslaugų teikėjo veikla turi būti organizuojama vadovaujantis sertifikavimo paslaugų teikėjo tvirtinamais sertifikavimo veiklos nuostatais, kuriuose turi būti

nustatyta sertifikatų sudarymo ir tvarkymo paslaugų teikimo tvarka, atitinkanti šių taisyklių reikalavimus.

8. Sertifikavimo paslaugų teikėjo vadovas ar kitas teisės aktų suteiktus įgaliojimus turintis asmuo (toliau – vadovas):

8.1. tvirtina sertifikavimo veiklos nuostatus;

8.2. atsako už sertifikavimo veiklos nuostatų tinkamą įgyvendinimą;

8.3. paskiria už sertifikavimo veiklos administravimą ir priežiūrą atsakingus darbuotojus.

9. Sertifikavimo paslaugų teikėjas teikia šias sertifikavimo paslaugas:

9.1. asmenų registravimas – priima asmenų prašymus išduoti sertifikatus, tikrina juose pateiktus duomenis, būtinus sertifikatams sudaryti, įsitikina prašymus teikiančių asmenų tapatybę;

9.2. sertifikatų sudarymas – iš gautų asmens duomenų ir viešojo kriptografinio rakto sudaro sertifikatus;

9.3. sertifikatų išdavimas – sudarytą sertifikatą perduoda sertifikato savininkui;

9.4. saugios parašo formavimo įrangos parengimas ir teikimas – rengia ir teikia saugią parašo formavimo įrangą asmenims;

9.5. sertifikatų statuso valdymas – sustabdo sertifikato galiojimą, atšaukia sertifikato galiojimo sustabdymą ar nutraukia sertifikato galiojimą;

9.6. informacijos apie sertifikatų statusą teikimas – kaupia informaciją apie negaliojančius sertifikatus specialioje duomenų bazėje, iš kurios duomenų formuojami negaliojančių sertifikatų sąrašai bei kurios duomenys pagal užklausas teikiami tikrinant sertifikato statusą.

9.7. sertifikatų naudotojų konsultavimas – konsultuoja sertifikatų naudotojus ir teikia informaciją apie sertifikatų naudojimo paskirties apribojimus ir sąlygas.

10. Sertifikavimo paslaugų teikėjas dalį ar visas sertifikavimo paslaugas gali perduoti trečiosioms šalims. Atsakomybė už visas teikiamas sertifikavimo paslaugas ir vykdomą sertifikavimo veiklą tenka sertifikavimo paslaugų teikėjui.

11. Sertifikavimo paslaugų teikėjo pareigos:

11.1. bet kuriuo paros metu teikti sertifikatų statusui tikrinti reikalingą informaciją;

11.2. vykdyti prašymus sustabdyti arba nutraukti sertifikato galiojimą; sertifikato galiojimas sustabdomas ar nutraukiamas iškart gavus tinkamos formos prašymą;

11.3. informuoti sertifikato savininką apie jo sertifikato galiojimo sustabdymą ar nutraukimą;

11.4. nedelsiant atšaukti sertifikato galiojimo sustabdymą, gavus sertifikato savininko arba Vyriausybės nustatytos teisėsaugos institucijos, kurios prašymu sertifikato galiojimas buvo sustabdytas, prašymą.

11.5. rinkti Vyriausybės ar jos įgaliotos institucijos nustatytą informaciją, susijusią su sertifikatų tvarkymu ir atsakymais į sertifikatų naudotojų užklausas, nustatytą laiką ją saugoti.

12. Sertifikavimo paslaugų teikėjas atsako už:

12.1. sudaryto sertifikato duomenų tikslumą;

12.2. privačiojo ir viešojo kriptografinių raktų atitikimą;

12.3. tai, kad sudarytame sertifikate nurodytas asmuo yra privataus rakto, atitinkančio sertifikate nurodytą viešąjį raktą, turėtojas;

12.4. sertifikato galiojimo nutraukimą ar sustabdymą laiku.

13. Sertifikavimo paslaugų teikėjo finansinės atsakomybės įsipareigojimams užtikrinti sertifikavimo veiklos civilinės atsakomybės draudimo suma nustatoma vadovaujantis Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2003 m. kovo 31 d. įsakymu Nr. T-31 „Dėl minimalios draudiminės sumos kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams nustatymo“ (Žin., 2003, Nr. 32-1355).

III. SERTIFIKATŲ NAUDOTOJŲ TEISĖS IR PAREIGOS

14. Sertifikato savininkas turi:

14.1. teikti sertifikavimo paslaugų teikėjui tikslią ir išsamią informaciją šių taisyklių ir sertifikavimo veiklos nuostatų nustatyta tvarka;

14.2. naudoti savo viešojo ir privačiojo kriptografinių raktų poras tik elektroniniams parašams sudaryti ir asmens atpažinimo elektroninėje erdvėje procedūrai vykdyti pagal konkrečiame sertifikate nurodytus sertifikato naudojimo paskirties apribojimus;

14.3. užtikrinti tinkamą privačiojo kriptografinio rakto ir jo aktyvavimo duomenų apsaugą nuo neteisėto panaudojimo;

14.4. nedelsiant informuoti sertifikavimo paslaugų teikėją, jei dar nepasibaigus sertifikato galiojimo terminui įvyko bent vienas iš šių įvykių:

14.4.1. privatusis kriptografinis raktas buvo pamestas, pavogtas ar kitaip sukompromituotas;

14.4.2. atskleisti aktyvavimo duomenys ar dėl kitų priežasčių sertifikato savininkas prarado privačiojo kriptografinio rakto kontrolę;

14.4.3. buvo nustatyti sertifikate įrašytos informacijos netikslumai arba pasikeitė sertifikate įrašyti duomenys.

14.5. privačiojo kriptografinio rakto sukompromitavimo atveju nedelsiant visam laikui nutraukti jo naudojimą;

14.6. leisti sertifikavimo paslaugų teikėjui naudoti ir saugoti asmens duomenis taisyklėse ir nuostatuose nustatyta tvarka.

15. Sertifikatais pasitikinčios šalys turi:

15.1. įsitikinti sertifikato galiojimu;

15.2. įsitikinti, kad sertifikatas naudojamas pagal paskirtį, nurodytą sertifikate;

15.3. patikrinti sertifikatą patvirtinančią sertifikatų seką sudarančių sertifikatų galiojimą.

IV. MOKESČIAI

16. Sertifikavimo paslaugų teikėjas gali nustatyti mokesčius už sertifikavimo paslaugas, išskyrus šiuos atvejus:

16.1. už sertifikato taisyklių ir sertifikavimo veiklos nuostatų skelbimą bei negaliojančių sertifikatų sąrašo teikimą;

16.2. už užklausų sistemos, teikiančios informaciją apie sertifikato statusą jo tikrinimo metu, paslaugas;

16.3. už sertifikato galiojimo nutraukimą ar sustabdymą.

V. INFORMACIJOS SKELBIMAS IR SAUGOJIMAS

17. Sertifikavimo paslaugų teikėjas turi viešai publikuoti ir prieš sudarydamas sertifikatą, pateikti sertifikatų sudarymo ir tvarkymo sąlygų dokumentą, kuris skirtas geriau susipažinti su pagrindiniais sertifikavimo veiklos aspektais, tačiau nekeičia ir nepavadoja sertifikato taisyklių ar sertifikavimo veiklos nuostatų.

18. Sertifikatų sudarymo ir tvarkymo sąlygų dokumente turi būti nurodyta:

18.1. sertifikavimo paslaugų teikėjo pavadinimas ir kontaktai;

18.2. sertifikatų naudojimo paskirties apribojimai;

18.3. sertifikato galiojimo tikrinimo, nutraukimo ir sustabdymo procedūros;

18.4. sertifikavimo paslaugų teikėjo pareigos ir atsakomybė;

18.5. sertifikato savininko pareigos ir atsakomybė;

18.6. pasitikinčių šalių pareigos ir atsakomybė;

18.7. rinkliavos už teikiamas sertifikavimo paslaugas;

18.8. informacija apie sertifikavimo paslaugų teikėjo garantinius įsipareigojimus bei draudimo programas;

18.9. taikomų sutarčių, sertifikavimo veiklos nuostatų, sertifikatų taisyklių ir kitų susijusių dokumentų identifikacija ir nuorodos;

18.10. taikomų piniginių lėšų sugražinimo taisyklių aprašas ir nuorodos;

18.11. taikomos teisės nustatymas, skundų procedūra, ginčų sprendimo mechanizmai;

18.12. taikomų asmens duomenų apsaugos taisyklių aprašas ir nuorodos;

18.13. informacija apie sertifikavimo paslaugų teikėjo statusą: kvalifikuotas sertifikavimo paslaugų teikėjas ir/arba akredituotas sertifikavimo paslaugų teikėjas;

18.14. jei buvo atliktas auditas, tai pateikiama audito ataskaita ir nurodomas audito atlikėjas;

18.15. kita, patikimą sertifikavimo veiklą įrodanti informacija.

19. Sertifikavimo paslaugų teikėjas sertifikatų savininkų asmens duomenis privalo tvarkyti ir saugoti Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (Žin., 1996, Nr. 63-1479; 2008, Nr. 22-804, toliau – Asmens duomenų teisinės apsaugos įstatymas) nustatyta tvarka. Sudaryti sertifikatai ir juose esantys asmens duomenys viešai neskelbiami.

20. Sertifikavimo paslaugų teikėjas savo interneto svetainėje turi skelbti šią informaciją:

20.1. sertifikato taisykles ir sertifikavimo veiklos nuostatus;

20.2. sertifikatų sudarymo ir tvarkymo sąlygas;

20.3. negaliojančių sertifikatų sąrašus.

VI. SERTIFIKAVIMO VEIKLOS REIKALAVIMAI

21. Sertifikavimo veiklos procedūros, saugumo, techniniai ir personalo reikalavimai turi būti detalizuoti sertifikavimo veiklos nuostatuose (toliau – nuostatai), kurie turi užtikrinti sertifikavimo paslaugų teikėjo veiklos patikimumą ir atitikimą šių taisyklių reikalavimams.

22. Nuostatuose sertifikavimo paslaugų teikėjas privalo:

22.1. detalizuoti sertifikavimo veiklos taisykles ir procedūras, kurios turi atitikti šių taisyklių reikalavimus;

22.2. detalizuoti trečiųjų asmenų, kuriems yra perduotos sertifikavimo paslaugos, pareigas ir atsakomybę;

I. SERTIFIKAVIMO PASLAUGŲ TEIKĖJO SERTIFIKATŲ SUDARYMO IR TVARKYMO REIKALAVIMAI

23. Sertifikavimo paslaugų teikėjo kriptografiniai raktai turi būti sudaromi fiziškai saugioje aplinkoje.

24. Sertifikavimo paslaugų teikėjo kriptografiniams raktams sudaryti ir saugoti turi būti naudojama įranga, atitinkanti vieno iš šių dokumentų reikalavimus:

24.1. JAV Nacionalinio standartų ir technologijų instituto standarto FIPS PUB 140-2 „Saugos reikalavimai kriptografiniams moduliams“, pagal kurio vertinimo kriterijus turi būti naudojama ne žemesnio kaip trečiojo saugumo lygmens (Level 3) įranga;

24.2. Lietuvos standarto LST CWA 14167-2:2005 „Sertifikavimo paslaugų teikėjų pasirašymo operacijų kriptografinis modulis su atkūrimo galimybe. Apsaugos profilis“;

24.3. Lietuvos standarto LST ISO/IEC 15408 „Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai“, pagal kurio vertinimo kriterijus turi būti naudojama ne žemesnio kaip ketvirtojo saugumo įvertinimo lygmens įranga (EAL 4).

25. Sertifikavimo paslaugų teikėjo sudaromų kriptografinių raktų ilgis ir elektroninio parašo kūrimo algoritmas turi būti tinkami kvalifikuotiems sertifikatams tvirtinti.

26. Sertifikavimo paslaugų teikėjo privačiųjų kriptografinių raktų saugumui užtikrinti turi būti naudojamos tokios techninės priemonės ir procedūros, kurios užtikrintų tinkamą privačiojo kriptografinio rakto apsaugą nuo neteisėto atskleidimo ar naudojimo, garantuotų privataus kriptografinio rakto konfidencialumą ir vientisumą.

27. Sertifikavimo paslaugų teikėjas turi užtikrinti, kad privatus kriptografinis raktas būtų laikomas ir naudojamas tik kartu su įranga, kuri atitinka šių taisyklių 24 punkto reikalavimus.

28. Jei sertifikavimo paslaugų teikėjo privatieji kriptografiniai raktai ar jų kopijos saugomi ar laikomi ne kriptografiniame saugumo modulyje, jie turi būti šifruojami. Šifravimui turi būti naudojamas toks privačiojo kriptografinio rakto ilgis ir algoritmas, kurie užtikrintų sertifikavimo paslaugų teikėjo privačiųjų kriptografinių raktų saugumą ir atsparumą kriptografinėms atakoms visą privačiųjų kriptografinių raktų galiojimo laikotarpį.

29. Sertifikavimo paslaugų teikėjo privačiųjų kriptografinių raktų atsarginės kopijos turi būti daromos ir saugomos bei privatieji kriptografiniai raktai iš jų atstatomi tik saugioje aplinkoje.

30. Sertifikavimo paslaugų teikėjo privačiųjų kriptografinių raktų atsarginių kopijų saugumo lygis turi būti lygiavertis kriptografinių raktų saugumo lygmeniui ar už jį aukštesnis.

31. Sertifikavimo paslaugų teikėjas turi savo interneto svetainėje skelbti savo viešuosius kriptografinius raktus, užtikrindamas juos sudarančių duomenų vientisumą ir autentiškumą.

32. Sertifikavimo paslaugų teikėjas savo privačiuosius kriptografinius raktus ir jų atsargines kopijas turi saugoti ir laikyti taip, kad autorizuotoms trečiosioms šalims nebūtų sudarytos sąlygos juos dešifruoti.

33. Sertifikavimo paslaugų teikėjas turi garantuoti tinkamą jo privačiųjų kriptografinių raktų naudojimą. Jis turi užtikrinti, kad:

33.1. asmenims sudaromiems sertifikatams ir negaliojančių sertifikatų sąrašams tvirtinti naudojami sertifikavimo paslaugų teikėjo privatieji kriptografiniai raktai nebūtų naudojami jokiais kitais tikslais;

33.2. sertifikavimo paslaugų teikėjo sertifikatų tvirtinimo privatieji kriptografiniai raktai būtų naudojami tik fiziškai saugioje aplinkoje.

34. Pasibaigus sertifikavimo paslaugų teikėjo kriptografinių raktų galiojimo terminui, jie turi būti sunaikinti be galimybės juos atstatyti. Tolesniam naudojimui sudaroma nauja kriptografinių raktų pora.

II. SERTIFIKATAMS TVIRTINTI NAUDOJAMOS KRIPTOGRAFINĖS ĮRANGOS SUDARYMO IR TVARKYMO REIKALAVIMAI

35. Sertifikavimo paslaugų teikėjas atsako už kriptografinių saugumo modulių saugumą ir tinkamą naudojimą viso jų gyvavimo ciklo metu:

35.1. sertifikavimo paslaugų teikėjas turi užtikrinti, kad kriptografiniai saugumo moduliai, naudojami sertifikatams, užklausų sistemos teikiamiems pranešimams apie sertifikato būseną ir negaliojančių sertifikatų sąrašams tvirtinti, nebuvo pažeisti iki jų pateikimo sertifikavimo paslaugų teikėjui, taip pat jų sandėliavimo metu ir veikia tinkamai;

35.2. sertifikavimo paslaugų teikėjas turi užtikrinti jo privačiųjų kriptografinių raktų diegimo, aktyvavimo, kopijų darymo ir atstatymo procedūrų vykdymo dviejų lygmenų kontrolę, procedūrų vykdymą pavedant darbuotojams, einantiems aukštos atsakomybės pareigas;

35.3. sertifikavimo paslaugų teikėjas turi užtikrinti, kad pasibaigus kriptografinių saugumo modulių naudojimo laikotarpiui, juose esantys kriptografiniai raktai būtų sunaikinti be galimybės juos atstatyti.

III. ASMENIMS SUDAROMŲ SERTIFIKATŲ SUDARYMO IR TVARKYMO REIKALAVIMAI

Asmenų registravimas

36. Sertifikavimo paslaugų teikėjas, vykdydamas registravimo funkcijas, privalo:

36.1. pasirašytinai supažindinti asmenį su sertifikatų sudarymo ir tvarkymo sąlygų dokumentu;

36.2. įstatymų ir kitų teisės aktų nustatyta tvarka nustatyti asmens tapatybę;

36.2.1. asmens tapatybę įrodantys duomenys turi būti sulyginti su asmens duomenimis (veido atvaizdu ar kitais biometriniais duomenimis), tiesiogiai arba netiesiogiai naudojant priemones, lygiavertes fizinio asmens buvimui patikros vietoje;

36.2.2. asmens tapatybės įrodymai gali būti pateikiami rašytine arba jai prilyginta elektronine forma;

36.3. užtikrinti, kad asmeniui sudarytame sertifikate, atsižvelgiant į sertifikato rūšį, būtų nurodyti visi reikiami asmens duomenys;

36.4. nustatyti surinktų duomenų saugojimo terminą, adekvatų laikotarpiui, per kurį šie duomenys gali būti reikalingi įrodymams teisiniuose procesuose pateikti;

36.5. užtikrinti registracijos duomenų konfidencialumą ir integralumą;

36.6. užtikrinti asmenų registracijos funkcijas vykdančių tarnybų, su kuriomis registravimo procedūros metu keičiamasi duomenimis, identifikavimą.

37. Sertifikavimo paslaugų teikėjas privalo saugoti šią informaciją:

37.1. visą asmens tapatybei nustatyti naudotą informaciją, taip pat naudotų dokumentų registracijos numerius bei šių dokumentų galiojimo apribojimus, jei tokie nustatyti;

37.2. rašytinę sutartį, kurioje turi būti sertifikato savininko parašu patvirtinta, kad jis susipažino ir sutinka su sertifikatų sudarymo ir tvarkymo sąlygomis.

Sertifikatų sudarymas

38. Sertifikavimo paslaugų teikėjas turi užtikrinti, kad asmeniui sudaromo sertifikato kriptografinių raktų pora būtų generuojama saugiai, taip pat garantuoti privačiojo kriptografinio rakto slaptumą. Sertifikavimo paslaugų teikėjas turi užtikrinti, kad:

38.1. kriptografinių raktų poros būtų sudaromos naudojant algoritmus, atitinkančius kvalifikuoto elektroninio parašo reikalavimus;

38.2. būtų naudojami tik kvalifikuotam elektroniniam parašui sudaryti tinkami kriptografinių raktų ilgiai ir elektroninių parašų kūrimo algoritmai;

38.3. sudaryti privatieji kriptografiniai raktai jų savininkams būtų perduoti saugiai, o jų slaptumas būtų išlaikytas iki privačiojo kriptografinio rakto įteikimo jo savininkui.

39. Kriptografinių raktų poroms generuoti ir saugoti turi būti naudojama trečiojo tipo saugi elektroninio parašo formavimo įranga (SSCD type 3), kurios saugumas pagal Lietuvos standarto LST ISO/IEC 15408 „Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai“ vertinimo kriterijus turi būti ne žemesnio kaip ketvirtojo saugumo įvertinimo lygmens (EAL 4).

40. Sertifikavimo paslaugų teikėjas turi užtikrinti elektroninio parašo formavimo įrangos parengimo, laikymo ir perdavimo sertifikatų savininkams saugumą ir šių procedūrų kontrolę.

41. Pasikeitus sertifikato duomenims (pvz., sertifikate įrašytiems asmens duomenims), pastebėjus klaidų sertifikate įrašytuose duomenyse ar keičiant sertifikatą atitinkančių kriptografinių raktų ilgį turi būti sudaromas naujas sertifikatas. Tokie sertifikatų atnaujinimo būdai, kaip naujų duomenų įrašymas į asmeniui sudarytą sertifikatą ar kriptografinių raktų pakeitimas nekeičiant asmeniui išduoto sertifikato, pagal šias taisykles sudaromiems sertifikatams netaikomi.

42. Sertifikatų sudarymo procesas ir sudaryti sertifikatai turi atitikti šiuos reikalavimus:

42.1. sudaromi kvalifikuoti sertifikatai turi atitikti Europos Parlamento ir Tarybos 1999 m. gruodžio 13 d. direktyvos Nr. 1999/93/EB „Dėl Bendrijos elektroninių parašų reguliavimo

sistemos“ I ir II priedeliuose ir Elektroninio parašo įstatyme kvalifikuotiems sertifikatams nustatytus reikalavimus;

42.2. sertifikato sudarymo procedūra turi būti saugiai susieta su kitomis sertifikatų sudarymo ir tvarkymo procedūromis;

42.3. sertifikato sudarymo procedūra turi būti saugiai susieta su kriptografinių raktų poros sudarymo procedūra;

42.4. privatusis kriptografinis raktas turi būti saugiai perduotas sertifikato savininkui;

42.5. konkrečiame sudarytame sertifikate nurodyti asmens identifikavimo duomenys turi būti unikalūs tarp visų sertifikavimo paslaugų teikėjo sudarytų sertifikatų ir negali būti priskirti kitam asmeniui.

Sertifikatų išdavimo reikalavimai

43. Sudarytą sertifikatą jo savininkas turi atsiimti asmeniškai ir raštu patvirtinti sertifikato, saugios parašo formavimo įrangos ir aktyvavimo duomenų priėmimo faktą.

44. Sertifikavimo paslaugų teikėjas negali viešai skelbti asmenims sudarytų sertifikatų.

Sertifikatų galiojimo nutraukimas ir sustabdymas

45. Sertifikavimo paslaugų teikėjas turi užtikrinti, kad sertifikatų galiojimo nutraukimas ir sustabdymas būtų vykdomi tinkamai ir laiku, pagal gautus įgaliotų asmenų patvirtintus prašymus.

46. Sertifikavimo paslaugų teikėjo nuostatuose turi būti nustatytos sertifikatų galiojimo nutraukimo ir sustabdymo procedūros, kuriose turi būti nurodyta:

46.1. asmenys, kurie gali pateikti prašymą nutraukti ar sustabdyti sertifikato galiojimą;

46.2. prašymo pateikimo tvarka;

46.3. sertifikato galiojimo sustabdymo ir galiojimo nutraukimo atvejai ir priežastys;

46.4. informacijos apie sertifikatų statusą teikimo būdai.

47. Sertifikavimo paslaugų teikėjas turi užtikrinti, kad:

47.1. gauti prašymai nutraukti ar sustabdyti sertifikato galiojimą būtų išnagrinėti nedelsiant;

47.2. prašymai nutraukti ar sustabdyti sertifikato galiojimą yra autentiški ir teisėti pagal nuostatų reikalavimus;

47.3. maksimalus laikotarpis nuo sertifikato galiojimo nutraukimo ar sustabdymo prašymo gavimo iki informacijos apie sertifikato statuso pasikeitimą pateikimo būtų ne ilgesnis nei 1 diena;

47.4. sertifikato galiojimo nutraukimas negalėtų būti atšauktas.

48. Sertifikato galiojimo nutraukimas ir sustabdymas negali būti vykdomi atgaline data ar laiku.

49. Sertifikavimo paslaugų teikėjas, išduodamas sertifikatą, privalo informuoti sertifikato savininką apie sertifikato galiojimo nutraukimo ir sustabdymo būdus.

50. Informaciją apie sertifikato statusą sertifikavimo paslaugų teikėjas turi skelbti:

50.1. negaliojančių sertifikatų sąrašė, kuris turi būti atnaujinamas ne rečiau kaip kartą per 24 valandas. Kiekviename negaliojančių sertifikatų sąrašė turi būti nurodytas kito negaliojančių sertifikatų sąrašo paskelbimo laikas;

50.2. per užklausų sistemą teikiamuose pranešimuose apie sertifikato būseną sertifikato tikrinimo metu.

51. Informacija apie sertifikato statusą turi būti teikiama 7 dienas per savaitę, 24 valandas per parą. Jei dėl priežasčių, tiesiogiai nepriklausančių nuo sertifikavimo paslaugų teikėjo veiklos, sutrinka prieiga prie šios tarnybos, sertifikavimo paslaugų teikėjas turi imtis visų įmanomų priemonių jai atstatyti per laikotarpį, nustatytą šias taisykles įgyvendinančiuose nuostatuose.

52. Sertifikavimo paslaugų teikėjas turi užtikrinti jo teikiamos informacijos apie sertifikatų statusą vientisumą ir autentiškumą. Ši informacija turi būti vieša ir prieinama tarptautiniu mastu.

IV. SERTIFIKAVIMO PASLAUGŲ TEIKĖJO VEIKLOS REIKALAVIMAI

Saugumo valdymas

53. Sertifikavimo paslaugų teikėjas turi užtikrinti, kad jo vykdoma sertifikavimo veikla atitiktų įstatymų ir kitų teisės aktų reikalavimus.

54. Sertifikavimo paslaugų teikėjas privalo:

54.1. suformuoti saugumo valdymo grupę ir jos darbuotojams pavesti:

54.1.1. formuoti saugumo politiką;

54.1.2. skleisti saugumo politiką kitiems sertifikavimo paslaugų teikėjo darbuotojams;

54.2. užtikrinti nuolatinę sertifikavimo paslaugų teikėjo valdomos informacijos apsaugą ir infrastruktūros priežiūrą;

54.3. užtikrinti, kad visi informacijos saugumui įtakos turintys pakeitimai būtų patvirtinti sertifikavimo paslaugų teikėjo saugumo valdymo grupės;

54.4. užtikrinti, kad būtų apibrėžtos, įgyvendinamos, prižiūrimos ir dokumentuojamos visos su sertifikavimo paslaugų teikėjo įrenginiais, sistemomis ir informacija susijusios saugumo valdymo priemonės ir procedūros;

54.5. užtikrinti tinkamą valdomos informacijos ir kito materialaus ir nematerialaus turto apsaugą;

54.6. periodiškai atlikti saugumo ir veiklos procedūrų reikalavimams nustatyti būtiną rizikos analizę ir jos vertinimą;

54.7. inventorizuoti turimą turtą ir pagal rizikos analizės rezultatus suklasifikuoti turto saugos reikalavimus.

Personalo patikimumo kontrolė

55. Sertifikavimo paslaugų teikėjo darbuotojai turi turėti aukštąjį išsilavinimą bei žinių, patirties ir kvalifikaciją, kurių reikia siūlomoms paslaugoms teikti.

56. Sertifikavimo paslaugų teikėjo saugumo politikoje nustatytos saugumo užtikrinimo pareigos ir atsakomybės turi būti nurodytos pareigybių aprašymuose. Aukštos atsakomybės pareigybės, nuo kurių tiesiogiai priklauso sertifikavimo paslaugų teikėjo veikla ir saugumas, turi būti tiksliai ir aiškiai apibrėžtos.

57. Visoms sertifikavimo paslaugų teikėjo pareigybėms turi būti parengti ir patvirtinti pareigybių aprašymai.

58. Pareigybių aprašymai turi būti parengti atsižvelgiant į konkrečios pareigybės paskirtį, veiklos sritį ir funkcijas. Pareigybei turi būti priskirtas atitinkamas jautrumo lygis, kuris nustatomas atsižvelgiant į konkrečiai pareigybei nustatytas pareigas ir jai priskirtą prieigos lygį.

59. Atsižvelgiant į pareigybės paskirtį ir funkcijas, nustatomi pareigybei užimti reikalingi įgūdžių ir patirties reikalavimai.

60. Sertifikatų sudarymo ir tvarkymo funkcijas vykdančioms pareigybėms turi būti nustatyti šie reikalavimai:

60.1. į vadybines pareigas priimami darbuotojai turi išmanyti elektroninio parašo technologijas ir turėti informacijos saugumo ir rizikos valdymo patirties;

60.2. aukštos atsakomybės pareigas užimantys sertifikavimo paslaugų teikėjo darbuotojai turi vengti bet kokių interesų konfliktų, kurie gali turėti įtakos sertifikavimo paslaugų teikėjo operacijų objektyvumui.

61. Asmenis į aukštos atsakomybės pareigas skiria sertifikavimo paslaugų teikėjo vadovas. Sertifikavimo paslaugų teikėjas turi nustatyti šias aukštos atsakomybės pareigas ir joms priskirti tokią atsakomybę:

61.1. saugumo pareigūnas – atsakingas už saugumo politikos vykdymą, sertifikavimo paslaugų teikėjo valdomų sertifikatų sudarymo ir tvarkymo procedūrų tvirtinimą;

61.2. sistemos administratorius – atsakingas už sertifikavimo paslaugų teikėjo sertifikatų valdymui naudojamų sistemų diegimą, konfigūravimą ir priežiūrą;

61.3. sistemos operatorius – atsakingas už sertifikavimo paslaugų teikėjo sertifikatų valdymo sistemų naudojimą;

61.4. sistemos auditorius – atsakingas už sertifikavimo paslaugų teikėjo patikimų sistemų archyvų ir audito įrašų peržiūrą.

62. Sertifikavimo paslaugų teikėjas negali priimti dirbti asmens, kuris įstatymų nustatyta tvarka pripažintas kaltu dėl nusikalstamos veikos vykdymo ir turi neišnykusį ar nepanaikintą teistumą.

Fizinio saugumo kontrolė

63. Sertifikavimo paslaugų teikėjas turi užtikrinti prieigos prie kritinių sertifikavimo paslaugų teikėjo sistemų fizinę apsaugą ir minimizuoti fizinio pažeidimo riziką.

64. Sertifikavimo paslaugų teikėjas turi užtikrinti, kad:

64.1. fizinė prieiga prie sertifikatų sudarymo, saugios parašo formavimo įrangos rengimo ir sertifikatų galiojimo nutraukimo ar sustabdymo įrangos būtų suteikta tik autorizuotam personalui;

64.2. būtų įgyvendintos turto apsaugos priemonės, skirtos užtikrinti turto apsaugą nuo praradimo, sugadinimo, kompromitacijos ar veiklos sustabdymo;

64.3. būtų įgyvendintos informacijos apsaugos priemonės, skirtos užtikrinti informacijos ir informacijos apdorojimo priemonių apsaugą nuo kompromitacijos ar vagystės.

65. Fizinei apsaugai užtikrinti sertifikavimo paslaugų teikėjas turi nustatyti specialią patalpų zoną, kurioje turi būti vykdomos sertifikatų sudarymo ir saugios parašo formavimo įrangos rengimo procedūros. Bet kokios bendrai su kitomis organizacijomis naudojamos patalpos turi būti už šios zonos ribų.

66. Sertifikavimo paslaugų teikėjas turi įgyvendinti šias patalpų, kuriose laikoma jo įranga, fizinės ir aplinkos poveikio apsaugos priemones:

66.1. fizinės prieigos kontrolę;

66.2. priešgaisrinę apsaugą;

66.3. komunalinių paslaugų (pvz., elektros energijos, telekomunikacijų) teikimo apsaugą nuo sutrikimų;

66.4. santechnikos įrenginių apsaugą;

66.5. apsaugą nuo vagysčių;

66.6. apsaugą nuo galimų stichinių nelaimių.

Procedūrų saugumo kontrolė

67. Sertifikavimo paslaugų teikėjas turi užtikrinti, kad sertifikavimo veiklai naudojamos sistemos veiktų saugiai ir tinkamai, o sutrikimų rizika būtų minimali.

68. Sertifikavimo paslaugų teikėjas turi užtikrinti, kad:

68.1. sertifikavimo paslaugų teikėjo įrangos ir jo valdomos informacijos vientisumas būtų apsaugotas nuo kompiuterinių virusų ir kitų programinių pažeidimų;

68.2. veikimo sutrikimų padariniai turi būti minimizuoti naudojant pranešimų apie incidentus ir reagavimo į juos procedūras;

68.3. sertifikavimo paslaugų teikėjo sistemose naudojami informacijos kaupikliai ir laikmenos būtų apsaugoti nuo gedimų, vagysčių, nesankcionuotos prieigos ar susidėvėjimo;

68.4. būtų nustatyta atitinkamo saugumo lygmens informacijos kaupiklių ir laikmenų apsauga;

68.5. informacijos kaupikliai ir laikmenos, kuriose saugoma jautri informacija, būtų sunaikinti iš karto po to, kai jie tampa nereikalingi veiklai vykdyti;

68.6. visų aukštos atsakomybės pareigybių vykdomos veiklos procedūros būtų tiksliai apibrėžtos ir įgyvendintos;

68.7. būtų planuojamas ateityje numatomų išteklių poreikis.

69. Sertifikavimo paslaugų teikėjo saugumo užtikrinimo procedūros turi būti atskirtos nuo kitų veiklos procedūrų. Saugumo užtikrinimo procedūros apima:

69.1. veiklos procedūrų ir atsakomybių nustatymą;

69.2. saugių sistemų planavimą;

69.3. sistemų apsaugą nuo žalingų programų;

69.4. sertifikavimo paslaugų teikėjo patalpų priežiūrą;

69.5. kompiuterinio tinklo valdymą, aktyvią audito žurnalų stebėseną;

69.6. užfiksuotų įvykių analizę;

69.7. informacijos laikmenų valdymą ir apsaugą;

69.8. apsikeitimą duomenimis ir programine įranga.

70. Sertifikavimo paslaugų teikėjo saugumo užtikrinimo procedūrų valdymo funkcijas atlieka aukštos atsakomybės pareigas užimantys darbuotojai. Šias funkcijas žemesnės kvalifikacijos specialistai gali vykdyti tik lydimi aukštos atsakomybės pareigas užimančių darbuotojų.

Prieigos prie sistemų valdymas

71. Sertifikavimo paslaugų teikėjas turi užtikrinti, kad prieiga prie sertifikavimo paslaugų teikėjo sistemų būtų suteikta tik tinkamai autorizuotam personalui.

72. Sertifikavimo paslaugų teikėjas turi užtikrinti:

72.1. sertifikavimo paslaugų teikėjo vidinio kompiuterių tinklo apsaugą nuo pasiekiamumo išoriniais tinklais;

72.2. svarbių duomenų apsaugą perdavimo išoriniais tinklais metu;

72.3. sistemos naudotojų, tarp jų ir sistemos operatorių, administratorių bei kitų naudotojų, kuriems suteikta tiesioginės prieigos teisė, administravimą;

72.4. sistemos naudotojų registracijos duomenų valdymą, sistemoje atliekamų svarbių veiksmų fiksavimą;

72.5. prieigos kontrolės nuostatas atitinkančius prieigos prie sistemos duomenų ir funkcijų apribojimus;

72.6. užtikrinti aukštos atsakomybės pareigų atskyrimą, atskiriant sistemos administravimo ir operacines funkcijas;

72.7. sertifikatų sudarymo ir tvarkymo kritines operacijas atliekančio personalo identifikavimą ir autentifikavimą;

72.8. sertifikavimo paslaugų teikėjo sistemose atliktų veiksmų apskaitą užfiksuojant ir išsaugant duomenų apie sistemų naudojimą išrašus;

73. Sertifikavimo paslaugų teikėjas, siekdamas laiku reaguoti į galimus neteisėtus veiksmus, turi:

73.1. sertifikatų sudarymo, jų galiojimo nutraukimo ir sustabdymo sistemose naudoti nuolatinio stebėjimo ir signalizavimo sistemą, skirtą nustatyti ir registruoti bandymus prieiti prie sistemos išteklių;

73.2. užtikrinti sertifikatų išdavimo ir informacijos apie sertifikatų statusą teikimo sistemų kontrolę tais atvejais, kai bandoma pridėti, pašalinti ar pakeisti sertifikatus ir kitą susijusią informaciją;

74. Sertifikavimo paslaugų teikėjas privalo naudoti patikimas, nuo modifikacijos apsaugotas sistemas. Įgyvendinant bet kokį sistemos plėtros projektą, saugumo reikalavimų analizė turi būti atliekama projektavimo ir poreikių nustatymo etape.

75. Sertifikavimo paslaugų teikėjas turi užtikrinti, kad saugumo valdymo priemonės būtų įgyvendintos visose tiesiogiai ar netiesiogiai su sertifikavimo veikla susijusiose informacinėse sistemose.

76. Sertifikavimo paslaugų teikėjas turi nustatyti dėl programinės įrangos modifikavimo ar tobulinimo atsirandančių pokyčių valdymo procedūras.

Veiklos sutrikimų ir tęstinumo valdymas

77. Sertifikavimo paslaugų teikėjas turi užtikrinti, kad bet kokių gedimų atveju, tarp jų ir sertifikavimo paslaugų teikėjo privačiųjų kriptografinių raktų kompromitacijos atveju, nedelsiant būtų imtasi visų galimų priemonių sertifikavimo paslaugų teikėjo veiklai atstatyti kaip galima greičiau..

78. Sertifikavimo paslaugų teikėjas turi sudaryti veiklos tęstinumo, esant sutrikimams arba įtariant privačiojo kriptografinio rakto kompromitaciją, planą.

79. Kompromitacijos atveju, sertifikavimo paslaugų teikėjas turi nedelsiant imtis šių minimalių veiksmų:

79.1. informuoti visus sertifikatų naudotojus, pasitikinčias puses ir kitus su sertifikavimo paslaugų teikėjo veikla susijusius asmenis;

79.2. nurodyti, kad sukompromituotu privačiuoju kriptografiniu raktu patvirtinti sudaryti sertifikatai, per užklausų sistemą siunčiami pranešimai apie sertifikatų būseną ir negaliojančių sertifikatų sąrašai gali tapti negaliojančiais.

79.3. nutraukti asmenims sudarytų sertifikatų galiojimą.

Sertifikavimo paslaugų teikimo nutraukimas arba perdavimas

80. Nutraukdamas sertifikavimo paslaugų teikimą, sertifikavimo paslaugų teikėjas turi:

80.1. ne vėliau nei prieš vieną mėnesį apie tai informuoti visus sertifikatų naudotojus ir elektroninio parašo priežiūros instituciją;

80.2. nutraukti visų trečiųjų šalių įgaliojimus veikti sertifikavimo paslaugų teikėjo vardu teikiant sertifikavimo paslaugas;

80.3. per vieną mėnesį po paskelbimo apie numatomą sertifikavimo paslaugų teikimo nutraukimą visus sudarytus sertifikatus ir elektroninio parašo priežiūros institucijos nustatytą informaciją, susijusią su sertifikatų sudarymu ir tvarkymu privalo, perduoti veiklos perėmėjui arba elektroninio parašo priežiūros institucijai. Veiklos perėmėjas turi užtikrinti informacijos apie sertifikatų statusą teikimo paslaugos teikimą.

81. Sertifikavimo paslaugų teikėjo nuostatuose turi būti nustatyta:

81.1. sertifikatų naudotojų informavimo būdai;

81.2. įsipareigojimų perdavimo tvarka;

81.3. informacijos apie sertifikatų statusą teikimo paslaugų perdavimo tvarka.

Įrašų kaupimas ir archyvavimas

82. Sertifikavimo paslaugų teikėjas, siekdamas pateikti teisingos sertifikavimo veiklos įrodymus teisiniuose procesuose, privalo kaupti įrašus apie visas sertifikatų sudarymo ir tvarkymo operacijas.

83. Incidentų bei specifinių veiklos įvykių faktai ir jų aplinkybės turi būti dokumentuojamos ir archyvuojamos. Sertifikavimo paslaugų teikėjas privalo saugoti asmenų registracijos informaciją

ir informaciją apie esminius sertifikavimo paslaugų teikėjo aplinkos, kriptografinių raktų ir sertifikatų valdymo įvykius.

84. Sertifikavimo paslaugų teikėjas privalo fiksuoti:

84.1. visus sertifikavimo paslaugų teikėjo valdomų kriptografinių raktų gyvavimo ciklo įvykius;

84.2. visus sudaromų sertifikatų gyvavimo ciklo įvykius;

84.3. visus asmenims generuojamų kriptografinių raktų porų gyvavimo ciklo įvykius;

84.4. visus įvykius, susijusius su saugios parašo formavimo įrangos parengimu ir išdavimu;

84.5. visus įvykius, susijusius su sertifikatų statuso keitimu, įskaitant prašymus, ataskaitas ir su jais susijusius įvykius.

85. Užtikrinti, kad dokumentuose būtų fiksuojama ši registracijos metu gauta informacija:

85.1. prašymuose sudaryti sertifikatą pateiktų dokumentų rūšys;

85.1.1. prašymą priėmusio darbuotojo identifikavimo duomenys;

85.1.2. registracijos tarnybos pavadinimas.

86. Duomenys turi būti saugomi nuostatuose nustatytą laiką. Visą saugojimo laiką duomenys turi būti pasiekiami ir apsaugoti nuo praradimo bei sugadinimo. Sertifikavimo paslaugų teikėjas privalo:

86.1. užtikrinti einamųjų ir archyvinių įrašų apie sertifikatus konfidencialumą ir vientisumą;

86.2. užtikrinti, kad įrašai būtų saugomi Lietuvos Respublikos dokumentų ir archyvų įstatymo (Žin., 1995, Nr. 107-2389; 2004, Nr.57-1982) nustatyta tvarka;

86.3. užtikrinti, kad būtų fiksuojamas tikslus su sertifikavimo paslaugų teikėjo veikla, sertifikatų ar kriptografinių raktų gyvavimo ciklu susijusių svarbių įvykių laikas;

86.4. su sertifikatais susijusių įrašų saugojimo terminas turi būti nustatytas atsižvelgiant į laikotarpį, per kurį sertifikavimo paslaugų teikėjas turi teikti sertifikavimo veiklos teisinius įrodymus kvalifikuotų elektroninių parašų tikrumui įrodyti;

86.5. fiksuojamus įvykių duomenis apsaugoti nuo pakeitimo ar sunaikinimo visą jų saugojimo laikotarpį.

VII. SERTIFIKAVIMO PASLAUGŲ TEIKĖJO VEIKLOS ORGANIZAVIMO BENDRIEJI REIKALAVIMAI

87. Sertifikavimo paslaugų teikėjas turi užtikrinti jo vykdomos veiklos patikimumą šiomis priemonėmis:

87.1. įgyvendinama politika ir vykdomos procedūros turi būti nešališki;

87.2. veikla turi būti vykdoma vadovaujantis Lietuvos Respublikos įstatymais ir kitais teisės aktais;

- 87.3. turi būti sudarytos galimybės įsitikinti vykdomos veiklos legalumu;
- 87.4. turi būti taikomos tinkamos kokybės ir informacijos valdymo sistemos;
- 87.5. turi būti numatyti dėl priimtoms atsakomybės atsiradusių įsipareigojimų įvykdymo būdai;
- 87.6. turi būti užtikrintas finansinis stabilumas ir numatyti kiti ištekliai, reikalingi tinkamai įgyvendinti taisykles;
- 87.7. turi būti nustatytos su sertifikavimo veikla susijusių ginčų sprendimo procedūros;
- 87.8. subrangos, samdos ir kitos veiklos funkcijų perdavimo sutartys turi būti tinkamai įformintos ir teisiškai galiojančios.
88. Sertifikavimo paslaugų teikėjo vykdoma sertifikatų sudarymo, jų galiojimo nutraukimo ir sustabdymo veikla turi būti nepriklausoma.
89. Veiklos nešališkumui, objektyvumui ir skaidrumui užtikrinti, visa sertifikavimo paslaugų teikėjo vykdoma sertifikatų sudarymo, jų galiojimo nutraukimo ir sustabdymo veikla turi būti griežtai dokumentuota.

VIII. TAISYKLIŲ ADMINISTRAVIMAS

90. Sertifikatų naudotojai turi vadovautis taisyklių, kurių unikalus identifikatorius įrašytas sertifikate, redakcija. Naujai patvirtinta ir paskelbta taisyklių redakcija panaikina ankstesnės taisyklių redakcijos galiojimą. Naujausia aktuali taisyklių redakcija turi būti skelbiama internete.
91. Taisyklės gali būti keičiamos pastebėjus jose klaidas ar atsiradus poreikiui jas atnaujinti.
92. Taisyklių pakeitimai gali būti:
- 92.1. esminiai, kuriuos atlikus keičiamas ir taisyklių unikalus identifikatorius; apie šiuos pakeitimus turi būti pranešama sertifikatų naudotojams;
- 92.2. neesminiai, apie kuriuos sertifikavimo paslaugų teikėjas neprivalo pranešti kitoms šalims; šiuo atveju taisyklių unikalus identifikatorius nėra keičiamas.
93. Neesminiais pakeitimais laikomi rekomendacinio, paaiškinamojo, tikslinamojo pobūdžio informacijos arba už taisyklių tvarkymą atsakingų asmenų kontaktinių duomenų, jei tokie duomenys yra nurodyti, pakeitimai.
- Kitais atvejais pakeitimai yra esminiai. Visais atvejais, kai taisyklių pakeitimai yra susiję su sertifikavimo paslaugų saugumo lygio keitimu, taisyklių pakeitimai yra esminiai.
94. Atlikus esminius pakeitimus, keičiamas naujos taisyklių redakcijos versijos pirmas skaitmuo (1 priedas) bei atitinkamas unikalus taisyklių identifikatoriaus dokumento versijos elementas (paskutinis skaitmuo). Atlikus neesminius pakeitimus keičiami naujos taisyklių redakcijos versijos antrasis skaitmuo.

95. Taisyklių priežiūros, keitimo ir tvirtinimo procedūros vykdomos tokia tvarka:

95.1. taisyklių pakeitimus gali inicijuoti sertifikavimo paslaugų teikėjas arba sertifikatų naudotojai;

95.2. už saugumo politiką atsakingi sertifikavimo paslaugų teikėjo darbuotojai:

95.2.1. per vienerius metus nuo vėliausios taisyklių redakcijos paskelbimo peržiūri ir įsitikinta taisyklių aktualumu;

95.2.2. peržiūros metu nustatčius poreikį keisti taisykles, inicijuoja taisyklių keitimą ir rengia naują taisyklių redakciją;

95.2.3. priima sprendimą teikti tvirtinti naują taisyklių redakciją;

95.3. esminių pakeitimų atveju, parengtas naujos taisyklių redakcijos projektas turi būti teikiamas suinteresuotoms šalims pastaboms ir pasiūlymams, paskelbiant projektą internete ne trumpesiam kaip 30 kalendorinių dienų laikotarpiui; atsižvelgus į per 30 dienų gautas pastabas arba per šį laikotarpį negavus pastabų, taisyklių nauja redakcija teikiama tvirtinti;

95.4. neesminių pakeitimų atveju nauja taisyklių redakcija teikiama tvirtinti iš karto ją parengus;

95.5. naują taisyklių redakciją tvirtina sertifikavimo paslaugų teikėjo vadovas.

96. Apie parengtą naują taisyklių pataisymo projektą turi būti informuota elektroninio parašo priežiūros institucija.

Sertifikato taisyklių
1 priedas**SERTIFIKATO TAISYKLIŲ UNIKALAUŠ IDENTIFIKATORIAUS REIKŠMĖS IR
TAISYKLIŲ VERSIJA****Taisyklių unikalus identifikatorius**

<u>Pavadinimas</u>	<u>Reikšmė</u>
ISO	1
ISO pripažinta organizacija	3
JAV Gynybos departamentas	6
Internetas	1
Privati įmonė	4
IANA registruota privati įmonė	1
Gyventojų registro tarnyba	31912
Sertifikatų sudarymo skyrius	1
Dokumento tipas (Sertifikato taisyklės)	1
Dokumento versijos pirmasis skaitmuo	1

Taisyklių versija 1.0

**TAISYKLES ADMINISTRUOJANČIO DARBUOTOJO KONTAKTINĖ
INFORMACIJA**

Įstaiga	Gyventojų registro tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos
Asmuo	Marija Norkevičienė
Pareigos	Gyventojų registro tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos direktorius
Adresas	A. Vivulskio g. 4 A, LT-03220 Vilnius
Tel.	(8 5) 271 6069
Faks.	(8 5) 271 6250
URL:	http://www.nsc.vrm.lt/
El.paštas:	marija.norkeviciene@vrm.lt
