

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

## SERTIFIKAVIMO VEIKLOS NUOSTATAI

### I. BENDROSIOS NUOSTATOS

1. Sertifikavimo veiklos nuostatai (toliau – nuostatai) nustato sertifikavimo paslaugų teikėjo veiklos taisykles, sertifikatų sudarymo ir tvarkymo techninius, procedūrų ir saugumo reikalavimus.

2. Nuostatai įgyvendina Sertifikavimo taisykles, kurių unikalus identifikatorius yra 1.3.6.1.4.1.31912.1.2.1.

3. Nuostatose sertifikavimo paslaugų teikėjas nurodo, kaip jis įgyvendina pasirinktą sertifikavimo veiklos politiką, apibrėžtą taisyklėse.

4. Šiuose nuostatuose 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), Gyventojų registro tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Gyventojų registro tarnyba) direktoriaus tvirtinamose Sertifikato taisyklėse.

5. Šių nuostatų unikalus identifikatorius yra 1.3.6.1.4.1.31912.1.2.1 (1 priedas).

6. Asmenims sudaromi dviejų rūšių sertifikatai:

6.1. kvalifikuotas sertifikatas;

6.2. asmens atpažinimo elektroninėje erdvėje sertifikatas.

7. Sertifikatų paskirties apibrėžimai turi būti apibrėžti sertifikatų laukuose *key usage* ir *enhanced key usage*.

8. Visiems su sertifikavimo paslaugų teikimu susijusiems santykiams taikoma Lietuvos Respublikos teisė.

9. Elektroninio parašo kūrimą, tikrinimą, galiojimą, sertifikavimo paslaugas, reikalavimus jų teikėjams bei atsakomybę, sudaromų sertifikatų sandarą ir paskirtį nustato:

9.1. Elektroninio parašo įstatymas;  
9.2. Asmens tapatybės kortelės įstatymas;  
9.3. Reikalavimai kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, Reikalavimai elektroninio parašo įrangai, Kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarka ir Elektroninio parašo priežiūros reglamentas, patvirtinti Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimu Nr. 2108 (Žin., 2003, Nr. 2-47).

9.4. Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2003 m. sausio 29 d. įsakymas Nr. T-7 „Dėl asmenų registravimo sertifikatams gauti ir asmenų konsultavimo paslaugų teikimo tvarkos patvirtinimo“ (Žin., 2003, Nr. 11-431);

9.5. Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2003 m. kovo 31 d. įsakymas Nr. T-31 „Dėl minimalios draudiminės sumos kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams nustatymo“ (Žin., 2003, Nr. 32-1355).

10. Visi ginčai, susiję su sertifikatų sudarymu ir tvarkymu, sprendžiami vadovaujantis Lietuvos Respublikos įstatymais.

## **II. SERTIFIKAVIMO PASLAUGŲ TEIKĖJO ORGANIZACINĖ STRUKTŪRA**

11. Sertifikavimo paslaugų teikėjas yra Gyventojų registro tarnyba.

12. Lietuvos Respublikos vidaus reikalų ministro 2008 m. gruodžio 1 d. įsakymu Nr. 1V-427 „Dėl įgaliojimo suteikimo“ atitinkamoms įstaigoms deleguotos šios sertifikavimo paslaugos ir veiklos funkcijos:

12.1. Asmens dokumentų išrašymo centrui prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Asmens dokumentų išrašymo centras) – įrašyti į asmens tapatybės korteles Gyventojų registro tarnybos sudarytus sertifikatus, sukurti parašo formavimo ir tikrinimo duomenis (kriptografinių raktų poras) ir asmens tapatybės kortelių elektroninių laikmenų aktyvavimo duomenis;

12.2. Informatikos ir ryšių departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas) – sertifikatų sudarymui ir tvarkymui naudojamos techninės įrangos priežiūra;

12.3. Vilniaus apskrities vyriausiojo policijos komisariato Migracijos valdybą, Alytaus, Kauno, Klaipėdos, Marijampolės, Panevėžio, Šiaulių, Tauragės, Telšių ir Utenos apskričių vyriausiųjų policijos komisariatų migracijos skyrius, policijos komisariatų migracijos poskyrius, grupes – išduoti ir keisti asmens tapatybės korteles su įrašytais sertifikatais ir asmens tapatybės kortelių aktyvavimo duomenis.

13. Skiriamos sertifikavimo paslaugų teikėjo ir registravimo tarnybų funkcijos:

13.1. Sertifikavimo paslaugų teikėjo funkcijos:

13.1.1. sertifikatų sudarymas;

13.1.2. saugios parašo formavimo įrangos parengimas ir teikimas;

13.1.3. sertifikatų galiojimo nutraukimas, sustabdymas ir sustabdymo atšaukimas;

13.1.4. informacijos apie sertifikatų statusą teikimas;

13.1.5. kitos, teisės aktų nustatyta tvarka priskirtos, funkcijos.

13.2. Registravimo tarnybų funkcijos:

13.2.1. prašymų išduoti sertifikatą, nutraukti ar sustabdyti sertifikato galiojimą, atšaukti sertifikato galiojimo stabdymą priėmimas ir asmenų tapatybės nustatymas;

13.2.2. sertifikatų ir asmens tapatybės kortelių elektroninių laikmenų aktyvavimo duomenų įteikimas asmenims;

13.2.3. informacijos apie sertifikavimo veiklą teikimas ir asmenų konsultavimas;

13.2.4. kitos, Asmenų registravimo sertifikatams gauti ir konsultavimo paslaugų teikimo tvarkos, patvirtintos Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2003 m. sausio 29 d. įsakymu Nr. T-7 (Žin., 2003, Nr. 11-431), priskirtos funkcijos.

14. Sertifikavimo paslaugų teikėjas yra įsteigęs informacijos teikimo ir sertifikavimo veiklos palaikymo tarnybą (toliau – sertifikavimo veiklos palaikymo tarnyba), kuri telefonu priima prašymus sustabdyti sertifikato galiojimą ir teikia su sertifikavimo veikla susijusią informaciją.

15. Už visas teikiamas sertifikavimo paslaugas ir vykdomą sertifikavimo veiklą atsako Gyventojų registro tarnyba.

### **III. SERTIFIKATŲ SEKOS SUDARYMAS**

16. Sertifikatų seką suformuoja trijų lygmenų sertifikatus sudarančios tarnybinės stotys (2 priedas):

16.1. Pirmojo lygmens – šakninė sertifikavimo tarnybinė stotis, kuri pati pasirašo savo sertifikatą (angl. *self-signed certificate*). Ji sudaro šiuos sertifikatus:

16.1.1. nuostatų sertifikavimo tarnybinės stoties sertifikatus;

16.1.2. užklausų sistemos teikiamiems pranešimams apie šakninės sertifikavimo tarnybinės stoties išduotų sertifikatų būseną tvirtinti skirtus sertifikatus.

16.2. Antrojo lygmens – nuostatų sertifikavimo tarnybinė stotis, kuri sudaro šiuos sertifikatus:

16.2.1. darbinės sertifikavimo tarnybinės stoties sertifikatus;

16.2.2. užklausų sistemos teikiamiems pranešimams apie nuostatų sertifikavimo tarnybos

stoties išduotų sertifikatų būseną tvirtinti skirtus sertifikatus.

16.3. Trečiojo lygmens – darbinė sertifikavimo tarnybinė stotis, kuri sudaro šiuos sertifikatus:

16.3.1. asmenims išduodamus sertifikatus;

16.3.2. užklausų sistemos teikiamiems pranešimams apie darbinės sertifikavimo tarnybinės stoties išduotų sertifikatų būseną tvirtinti skirtus sertifikatus;

16.3.3. infrastruktūros sertifikatus.

17. Šakninė ir nuostatų sertifikavimo tarnybinės stotys saugomos izoliuotoje aplinkoje, jos neturi būti prijungtos prie tinklo.

#### **IV. SERTIFIKAVIMO PASLAUGŲ TEIKĖJO IR SERTIFIKATŲ NAUDOTOJŲ PAREIGOS IR ATSAKOMYBĖ**

18. Sertifikavimo paslaugų teikėjo ir sertifikatų naudotojų pareigos ir atsakomybė apibrėžtos šių sertifikavimo veiklos nuostatų įgyvendinamose taisyklėse.

#### **V. MOKESČIAI**

19. Nemokamai teikiamos šios sertifikavimo paslaugos:

19.1. taisyklių, nuostatų, sertifikatų sudarymo ir tvarkymo sąlygų, elektroninio parašo taisyklių ir kitos informacijos skelbimas sertifikavimo paslaugų teikėjo interneto svetainėje;

19.2. informacijos apie sertifikatų statusą teikimas naudojant negaliojančių sertifikatų sąrašus ir užklausų sistemą;

19.3. sertifikato galiojimo sustabdymas ir nutraukimas.

20. Sertifikavimo paslaugų teikėjas turi teisę imti mokesčius už kitas sertifikavimo paslaugas. Paslaugų įkainiai skelbiami sertifikavimo paslaugų teikėjo interneto svetainėje.

#### **VI. INFORMACIJOS SKELBIMO, SAUGOJIMO IR INFORMACIJOS KONFIDENCIALUMO REIKALAVIMAI**

21. Sertifikavimo paslaugų teikėjo interneto svetainėje viešai skelbiama ši informacija:

21.1. taisyklės, nuostatai, sertifikatų sudarymo ir tvarkymo sąlygos, elektroninio parašo taisyklės;

21.2. už sertifikavimo paslaugas mokamų mokesčių kainininkai;

21.3. vartotojų instrukcijos;

21.4. sertifikavimo paslaugų teikėjui priklausantys sertifikatai;

21.5. negaliojančių sertifikatų sąrašai;

21.6. veiklos tikrinimo ataskaitos ir kiti patikimą sertifikavimo veiklą įrodantys dokumentai.

22. Konfidenciali informacija yra ši:

- 22.1. asmens duomenys, išskyrus tuos, kurie atskleidžiami teikiant sertifikavimo paslaugas;
  - 22.2. sertifikavimo paslaugų teikėjo atliktų operacijų įrašai;
  - 22.3. įrašai apie sertifikavimo paslaugų sutrikimus;
  - 22.4. informacija apie veiklos patikrinimus, jei jos paskelbimas kelia grėsmę sertifikavimo veiklos saugumui;
  - 22.5. veiksmų, įvykus avarijai, planai;
  - 22.6. informacija apie techninės ir programinės įrangos apsaugą ir sertifikavimo paslaugų operacijų atlikimą.
23. Konfidenciali informacija saugoma ir tvarkoma sertifikavimo paslaugų teikėjo vidaus taisyklių nustatyta tvarka.
24. Konfidenciali informacija teisėsaugos institucijoms teikiama Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatyta tvarka.
25. Sertifikavimo paslaugų teikėjas privalo tvarkyti ir saugoti asmens duomenis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (Žin., 1996, Nr. 63-1479; 2008, Nr. 22-804, toliau – Asmens duomenų teisinės apsaugos įstatymas) nustatyta tvarka.
26. Sertifikatų savininkai susipažįsta su sertifikate nurodoma informacija ir patvirtina, kad sutinka su jos naudojimu taisyklėse ir nuostatuose nustatyta tvarka.
27. Asmenims išduoti sertifikatai viešai neskelbiami ir jų paieška negalima.
28. Sertifikavimo paslaugų teikėjo teikiama informacija turi būti atnaujinama:
- 28.1. nuostatai keičiami, tvirtinami ir skelbiami šių nuostatų 151–158 punktuose nustatyta tvarka;
  - 28.2. negaliojančių sertifikatų sąrašas atnaujinamas periodiškai, šių nuostatų 76–77 punktuose nustatytais terminais;
  - 28.3. kita informacija skelbiama ją patvirtinus.

## **VII. SERTIFIKAVIMO VEIKLOS ATITIKIMO SERTIFIKATO TAISYKLĖMS IR SERTIFIKAVIMO VEIKLOS NUOSTATAMS UŽTIKRINIMAS**

29. Ne rečiau kaip kartą per vienerius metus turi būti tikrinama, ar sertifikavimo paslaugų teikėjo vykdoma veikla atitinka taisyklių ir nuostatų reikalavimus.
30. Vidinį sertifikavimo veiklos tikrinimą atlieka sertifikavimo paslaugų teikėjo auditorius ir saugumo pareigūnas. Išorinis patikrinimas vykdomas teisės aktų nustatyta tvarka.
31. Sertifikavimo paslaugų teikėjo veiklai įvertinti yra tikrinama:
- 31.1. fizinis saugumas;
  - 31.2. programinės įrangos ir sistemos kompiuterių tinklų saugumas;
  - 31.3. personalo patikimumas;

- 31.4. sertifikavimo paslaugos ir jų teikimo procedūros;
  - 31.5. registracijos žurnalų ir sistemos tvarkymo procedūros;
  - 31.6. informacijos atsarginių kopijų darymas;
  - 31.7. archyvų tvarkymo procedūros;
  - 31.8. įrašai apie techninės ir programinės įrangos tikrinimą ir priežiūrą.
32. Per 30 kalendorinių dienų nuo sertifikavimo paslaugų teikėjo veiklos patikrinimo saugumo pareigūnas turi:
- 32.1. raštu pareikšti savo nuomonę dėl patikrinimo protokole išdėstytų trūkumų;
  - 32.2. numatyti trūkumų pašalinimo veiksmus ir terminus;
  - 32.3. informaciją apie trūkumų pašalinimą pateikti sertifikavimo paslaugų teikėjo veiklą tikrinusiai organizacijai.
33. Tikrinimų išvados skelbiamos sertifikavimo paslaugų teikėjo internetinėje svetainėje.

## **VIII. ASMENŲ IDENTIFIKAVIMAS**

### **I. SERTIFIKATŲ IŠDAVIMAS**

34. Asmenims sertifikatai išduodami ir naudojami tik kartu su asmens tapatybės kortele, atitinkančia saugios elektroninio parašo formavimo įrangos reikalavimus. Šios kortelės elektroninėje laikmenoje generuojami parašo formavimo ir tikrinimo duomenys bei saugomi sertifikatai. Asmens tapatybės kortelei tapus negaliojančia, automatiškai nutraukiamas ir joje įrašytų sertifikatų galiojimas.

35. Pirmą kartą sertifikatas išduodamas kartu su asmens tapatybės kortele. Asmens tapatybės kortelės išdavimo procedūra atliekama Lietuvos Respublikos asmens tapatybės įstatymo 5 straipsnio nustatyta ir Asmens tapatybės kortelės išdavimo, keitimo, paskelbimo negaliojančia ir naikinimo tvarkos aprašo, patvirtinto Lietuvos Respublikos vidaus reikalų ministro 2008 m. gruodžio 24 d. įsakymu Nr. 1V-473, nustatyta tvarka. Papildomos asmens tapatybės tikrinimo procedūros ar prašymo teikimas neatliekami.

36. Atsiimant sertifikatą, sertifikato savininkui pateikiamos sertifikatų sudarymo ir tvarkymo sąlygos.

37. Asmuo, registracijos tapatybės kortelei gauti formoje patvirtindamas, kad susipažino su šių nuostatų 36 punkte nurodytomis sąlygomis, taip pat patvirtina, kad sutinka su jomis ir prisiima visus jose nustatytus įsipareigojimus ir atsakomybę.

38. Atsiimant sertifikatą, jo savininkui pateikiami sudarytame sertifikate įrašyti asmens duomenys.

39. Išdavus tapatybės kortelę neveiksniam asmeniui, joje esantys sertifikatai neaktyvuojami, sertifikatų sudarymo ir tvarkymo sąlygos nėra pateikiamos, privataus kriptografinio

rakto aktyvavimo duomenys neįteikiami.

## II. ASMENS IDENTIFIKAVIMO SERTIFIKATE DUOMENYS

40. Visi asmenims sudarytuose sertifikatuose nurodyti vardai yra unikalūs. Unikalus asmens identifikatorius yra asmens kodas.

41. Asmens identifikavimo vardas sudaromas laikantis X.509 standarto rekomendacijų.

DN vardo lauko žymėjimas ir jo paskirtis	Nurodoma reikšmė
Sertifikavimo paslaugų teikėjo DN	
C (angl. <i>Country</i> ), šalis	LT
O (angl. <i>Organization</i> ), organizacija	Gyventojų registro tarnyba prie LR VRM - i.k. 188756767
OU (angl. <i>Organization Unit</i> ), organizacijos padalinys	Nacionalinis sertifikavimo centras (NSC)
CN (angl. <i>Common Name</i> )	Nacionalinis sertifikavimo centras (RootCA)
Fizinio asmens sertifikato savininko DN	
G (angl. <i>Given Name</i> )	Vardas
SN (angl. <i>SurnName</i> )	Pavardė
CN (angl. <i>Common Name</i> )	Asmens vardas, pavardė
Serijinis numeris	Asmens kodas
C (angl. <i>Country</i> ), šalis	LT

## III. SERTIFIKATŲ SUDARYMAS IR ASMENS TAPATYBĖS KORTELĖS KEITIMAS

42. Tokie sertifikatų atnaujinimo būdai, kaip naujų duomenų įrašymas į asmeniui išduotą sertifikatą ar kriptografinių raktų pakeitimas nekeičiant asmeniui išduoto sertifikato, pagal šiuos nuostatus sudaromiems sertifikatams netaikomi. Visais atvejais sudaromas naujas sertifikatas.

43. Asmens tapatybės kortelė keičiama ir nauji sertifikatai sudaromi, kai:

43.1. sudarant sertifikatus dėl sertifikavimo paslaugų teikėjo kaltės buvo padaryta klaidų;

43.2. Asmens tapatybės kortelės išdavimo, keitimo, paskelbimo negaliojančia ir naikinimo tvarkos aprašo 27 punkte minimais atvejais.

44. Tapatybės kortelės keitimo procedūra atliekama Asmens tapatybės kortelės įstatymo 5 straipsnio ir Asmens tapatybės kortelės išdavimo, keitimo, paskelbimo negaliojančia ir naikinimo tvarkos aprašo nustatyta tvarka. Kartu su nauja asmens tapatybės kortele išduodami ir nauji sertifikatai. Papildomos asmens tapatybės nustatymo procedūros ar prašymo teikimas neatliekami.

45. Naujas sertifikatas, nekeičiant asmens tapatybės kortelės, išduodamas šiais atvejais:

45.1. kai pasibaigia sertifikato galiojimo terminas, tačiau dar galioja asmens tapatybės kortelė;

45.2. sertifikato savininko prašymu, kada asmens tapatybės kortelė nėra prarasta ar pamesta ir tebėra galiojanti. Šiuo atveju sertifikato savininkas turi asmeniškai atvykti į registravimo tarnybą ir pateikti asmens tapatybės kortelę bei užpildyti prašymą. Jei sertifikatai yra galiojantys, sertifikato savininkas pirmiausia turi pateikti prašymą nutraukti sertifikatų galiojimą.

#### **IV. PRAŠYMUS TEIKIANČIŲ ASMENŲ IDENTIFIKAVIMAS**

##### **Asmens tapatybės tikrinimas, prašant sudaryti sertifikatą, kai asmens tapatybės kortelė nekeičiama**

46. Prašymą sudaryti sertifikatą pagal šių nuostatų 45 punktą sertifikato savininkas gali pateikti tik asmeniškai atvykęs į registravimo tarnybą ir pateikęs asmens tapatybės kortelę.

47. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

47.1. tapatybės kortelėje esanti informacija palyginama su prašymą pateikusių asmeniu tiesiogiai arba kitais būdais, lygiaverčiais fizinio asmens buvimui patikros vietoje (pvz., biometrinių duomenų nuskaitymas ar veido atvaizdo palyginimas);

47.2. patikrinamas tapatybės kortelės tikrumas ir galiojimas;

47.3. patikrinama, ar prašyme nurodyti duomenys ir asmens tapatybės kortelės duomenys sutampa;

47.4. prašyme pateikta informacija palyginama su Lietuvos Respublikos gyventojų registro (toliau – gyventojų registras) informacija.

##### **Sertifikato galiojimą nutraukti prašančio asmens tapatybės tikrinimas**

48. Prašymą nutraukti sertifikato galiojimą sertifikato savininkas gali pateikti tik asmeniškai atvykęs į registravimo tarnybą ir pateikęs asmens tapatybę įrodantį dokumentą. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

48.1. pateiktų dokumentų informacija palyginama su prašymą pateikusių asmeniu tiesiogiai arba kitais būdais, lygiaverčiais fizinio asmens buvimui patikros vietoje (pvz., biometrinių duomenų nuskaitymas ar veido atvaizdo palyginimas);

48.2. patikrinamas pateiktų dokumentų tikrumas ir galiojimas;

48.3. patikrinama, ar prašyme nurodyti duomenys ir pateiktų asmens tapatybę įrodančių dokumentų duomenys sutampa;

48.4. prašyme pateikta informacija palyginama su gyventojų registro informacija.

##### **Sertifikato galiojimą sustabdyti prašančio asmens tapatybės tikrinimas**

49. Prašymą sustabdyti sertifikato galiojimą sertifikato savininkas gali pateikti:

49.1. raštu – registravimo tarnybai;

49.2. telefonu – sertifikavimo veiklos palaikymo tarnybai.

50. Kai prašymą sustabdyti sertifikato galiojimą sertifikato savininkas pateikia registravimo tarnybai, jis turi pateikti asmens tapatybę įrodantį dokumentą. Tikrinamas tik sertifikato savininko pateiktų dokumentų galiojimas ir tikrumas.

51. Kai prašymą sustabdyti sertifikato galiojimą sertifikato savininkas pateikia sertifikavimo veiklos palaikymo tarnybai telefonu, jis turi nurodyti šią informaciją: savo vardą, pavardę, gimimo datą, gyvenamąją vietą ir kitus, Lietuvos Respublikos gyventojų registro įstatymo (Žin., 1992, Nr. 5-78; 2008, Nr. 87-3467) 9 straipsnio pirmoje dalyje minimus, duomenis.

52. Kai sertifikato galiojimą sustabdyti reikalauja tam suteiktus įgaliojimus turinti institucija, ji turi pateikti prašymą, kuriame turi būti nurodyta sertifikato, kurio galiojimas sustabdomas, duomenys ir galiojimo sustabdymo priežastys.

#### **Sertifikato galiojimo sustabdymą atšaukiančio asmens tapatybės tikrinimas**

53. Prašymą atšaukti sertifikato galiojimo sustabdymą sertifikato savininkas gali pateikti tik asmeniškai atvykęs į registravimo tarnybą ir pateikęs asmens tapatybės kortelę. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

53.1. tapatybės kortelėje esanti informacija palyginama su prašymą pateikusių asmeniu tiesiogiai arba kitais būdais, lygiaverčiais fizinio asmens buvimui patikros vietoje (pvz., biometrinių duomenų nuskaitymas ar veido atvaizdo palyginimas);

53.2. patikrinamas tapatybės kortelės tikrumas ir galiojimas;

53.3. patikrinama, ar prašyme nurodyti duomenys ir asmens tapatybės kortelės duomenys sutampa;

53.4. prašyme pateikta informacija palyginama su gyventojų registro informacija.

#### **Sertifikatą aktyvuoti prašančio asmens tapatybės tikrinimas**

54. Prašymą aktyvuoti sertifikatus sertifikato savininkas gali pateikti tik asmeniškai atvykęs į registravimo tarnybą ir pateikęs asmens tapatybės kortelę. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

54.1. tapatybės kortelėje esanti informacija palyginama su prašymą pateikusių asmeniu tiesiogiai arba kitais būdais, lygiaverčiais fizinio asmens buvimui patikros vietoje (pvz., biometrinių duomenų nuskaitymas ar veido atvaizdo palyginimas);

54.2. patikrinamas tapatybės kortelės tikrumas ir galiojimas;

54.3. patikrinama, ar prašyme nurodyti duomenys ir asmens tapatybės kortelės duomenys sutampa;

54.4. prašyme pateikta informacija palyginama su gyventojų registro informacija.

### **Asmens tapatybės tikrinimas, kai išduodami nauji privačiojo rakto aktyvavimo duomenys**

55. Prašymą išduoti naujus privačiojo rakto aktyvavimo duomenis sertifikato savininkas gali pateikti tik asmeniškai atvykęs į registravimo tarnybą. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

55.1. tapatybės kortelėje esanti informacija palyginama su prašymą pateikusių asmeniu tiesiogiai arba kitais būdais, lygiaverčiais fizinio asmens buvimui patikros vietoje (pvz., biometrinių duomenų nuskaitymas ar veido atvaizdo palyginimas);

55.2. patikrinamas tapatybės kortelės tikrumas ir galiojimas;

55.3. patikrinama, ar prašyme nurodyti duomenys ir asmens tapatybės kortelės duomenys sutampa;

55.4. prašyme pateikta informacija palyginama su gyventojų registro informacija.

## **IX. SERTIFIKAVIMO VEIKLOS REIKALAVIMAI**

### **I. SERTIFIKATO SUDARYMAS**

56. Sertifikavimo paslaugų teikėjas užtikrina, kad:

56.1. sudaromi kvalifikuoti sertifikatai atitinka Elektroninio parašo įstatyme kvalifikuotiems sertifikatams nustatytus reikalavimus;

56.2. asmenims sudaromi sertifikatai atitinka Asmens tapatybės kortelės įstatyme kvalifikuotiems ir asmens atpažinimo elektroninėje erdvėje sertifikatams nustatytus reikalavimus;

56.3. sertifikatai atitinka Lietuvos standarto LST ETSI TS 101 862 „Kvalifikuoto sertifikato profilis“ sertifikatų sandarai nustatytus reikalavimus;

56.4. kriptografinių raktų poros generavimo procedūra yra saugiai susieta su sertifikato sudarymo procedūra;

56.5. privačiam raktui generuoti naudojama Lietuvos standarto LST ISO/IEC 15408 „Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai“ trečiojo saugumo lygmens (*SSCD Type 3*) reikalavimus atitinkanti saugi parašo formavimo įranga;

56.6. saugi parašo formavimo įranga sertifikato savininkui perduodama saugiai;

56.7. sudarytame sertifikate nurodyti asmens identifikavimo duomenys yra unikalūs ir nepriskirtini kitam asmeniui;

56.8. sertifikatams sudaryti naudotų duomenų konfidencialumas ir integralumas užtikrinamas viso sertifikato gyvavimo ciklo metu.

57. pirmą kartą sertifikatas išduodamas kartu su asmens tapatybės kortele, kuri vadovaujantis Asmens tapatybės kortelės įstatymo 5 straipsnio 13 dalimi, turi būti išduota ne vėliau kaip per vieną mėnesį nuo dokumentų gavimo dienos.

58. Kai sertifikatas sudaromas nekeičiant asmens tapatybės kortelės, naujas sertifikatas sudaromas iškart po prašymo patikrinimo.

59. Sertifikatą asmeniškai atsiima sertifikato savininkas. Įteikiant sertifikatą, sertifikato savininkui pateikiamas sudaryto sertifikato turinys. Pastebėjus klaidų, sertifikato galiojimas nutraukiamas.

60. Kartu su sertifikatu įteikiami privačiojo rakto aktyvavimo duomenys.

61. Sertifikato savininkas patvirtina sertifikato ir privačiojo rakto aktyvavimo duomenų gavimo faktą.

## **II. SERTIFIKATO AKTYVAVIMAS**

62. Sertifikatas aktyvuojamas išduodant sertifikatą, sertifikato savininkui patvirtinus sertifikato priėmimo faktą.

63. Teikiant prašymą aktyvuoti sertifikatą, išduodami nauji privačiojo rakto aktyvavimo duomenys, kurių gavimo faktą sertifikato savininkas patvirtina teikiamame prašyme.

## **III. SERTIFIKATO GALIOJIMO NUTRAUKIMAS**

64. Sertifikato galiojimas nutraukiamas šiais atvejais:

64.1. gavus sertifikato savininko prašymą;

64.2. sertifikato duomenims tapus neteisingais ar paaiškėjus, kad sudarant sertifikatą buvo panaudoti neteisingi duomenys;

64.3. sertifikato savininkui praradus sertifikatą atitinkančių parašo formavimo duomenų kontrolę;

64.4. sertifikavimo paslaugų teikėjo sprendimu, kai paaiškėja, kad sertifikato savininkas nesilaiko sertifikato naudojimo sąlygų ir sertifikato galiojimo apribojimų;

64.5. sertifikavimo paslaugų teikėjas nutraukia savo veiklą ir joks kitas sertifikavimo paslaugų teikėjas neperima sertifikavimo veiklos;

64.6. kai pažeidžiamas sertifikavimo paslaugų teikėjo privačiojo rakto ar sistemų saugumas ir dėl to atsiranda pavojus sudarytų sertifikatų patikimumui;

64.7. sertifikato savininkui tapus neveiksniam;

64.8. sertifikato savininkui mirus;

64.9. sertifikato savininkui pažeidus elektroninio parašo naudojimą reglamentuojančius teisės aktus;

64.10. įstatymų numatytais atvejais.

65. Prašymai nutraukti sertifikato galiojimą teikiami šių nuostatų 48 punkte nustatyta tvarka. Sertifikavimo paslaugų teikėjas nutraukia sertifikato galiojimą iškart po prašymo patikrinimo. Atlikus sertifikato galiojimo nutraukimo operaciją, sertifikato savininkas informuojamas apie pasikeitusį sertifikato statusą.

66. Jei sertifikato galiojimas nutraukiamas ne sertifikato savininko prašymu, sertifikavimo paslaugų teikėjas turi informuoti sertifikato savininką apie sertifikato galiojimo nutraukimą raštu.

67. Sertifikatų galiojimas yra automatiškai nutraukiamas visais atvejais, nustojus galioti asmens tapatybės kortelei, kurioje sertifikatai įrašyti.

#### **IV. SERTIFIKATO GALIOJIMO SUSTABDYMAS**

68. Sertifikato galiojimas sustabdomas šiais atvejais:

68.1. gavus sertifikato savininko prašymą;

68.2. teisėsaugos institucijų reikalavimu, siekiant užkirsti kelią nusikaltimams;

68.3. gavus informacijos ar kilus įtarimui, kad sertifikato duomenys yra neteisingi arba sertifikato savininkas prarado sertifikatą atitinkančių parašo formavimo duomenų kontrolę.

69. Prašymus sustabdyti sertifikato galiojimą gali teikti:

69.1. sertifikato savininkas;

69.2. teisėsaugos institucijos.

70. Prašymai sustabdyti sertifikato galiojimą teikiami šių nuostatų 49-52 punktų nustatyta tvarka. Sertifikato galiojimas sustabdomas iškart po prašymo patikrinimo. Atlikus sertifikato galiojimo sustabdymo operaciją, sertifikato savininkas informuojamas apie pasikeitusį sertifikato statusą.

71. Kai sertifikato galiojimą sustabdo sertifikavimo paslaugų teikėjas ar sertifikato galiojimas yra sustabdomas teisėsaugos institucijos prašymu, sertifikavimo paslaugų teikėjas turi informuoti sertifikato savininką apie sertifikato galiojimo sustabdymą raštu.

72. Sertifikato galiojimo sustabdymas atšaukiamas gavus sertifikato savininko arba teisėsaugos institucijos, kurios prašymu sertifikato galiojimas buvo sustabdytas, prašymą. Prašymai atšaukti sertifikato galiojimo sustabdymą teikiami šių nuostatų 53 punkte nustatyta tvarka. Sertifikato galiojimo sustabdymas atšaukiamas iškart po prašymo patikrinimo. Atlikus sertifikato galiojimo sustabdymo atšaukimo operaciją, sertifikato savininkas informuojamas apie pasikeitusį sertifikato statusą.

73. Jei per 1 mėnesį nuo sertifikato galiojimo sustabdymo negaunamas prašymas atšaukti sertifikato galiojimo sustabdymą, sertifikato galiojimas nutraukiamas.

## **V. SERTIFIKATŲ STATUSO TIKRINIMAS IR NEGALIOJANČIŲ SERTIFIKATŲ SĄRAŠŲ SKELBIMAS**

74. Sertifikato statusas tikrinamas pagal negaliojančių sertifikatų sąrašą arba naudojant užklausų sistemą. Sertifikato galiojimo tikrinimo detali procedūra nustatoma elektroninio parašo taisyklėse.

75. Parašui tikrinti naudojant negaliojančių sertifikatų sąrašą, pasitikinčios šalys turi atsisiųsti sertifikavimo paslaugų teikėjo interneto svetainėje skelbiamą aktualią negaliojančių sertifikatų sąrašo versiją. Sertifikato statusas pagal negaliojančių sertifikatų sąrašą tikrinamas, jei šio sąrašo atnaujinimo periodiškumas yra tinkamas parašo tikrintojui.

76. Darbinės sertifikavimo tarnybinės stoties negaliojančių sertifikatų sąrašas atnaujinamas kas 7 dienas, negaliojančių sertifikatų sąrašų persidengimo periodas – 3 dienos. Kas 24 valandas skelbiamas darbinės sertifikavimo tarnybinės stoties *delta* negaliojančių sertifikatų sąrašas, kuriame nurodomi per paskutiniąsias 24 valandas negaliojančiais tapę sertifikatai.

77. Šakninės ir nuostatų sertifikavimo tarnybinių stočių, kurios nėra prijungtos prie tinklo, negaliojančių sertifikatų sąrašas atnaujinamas kas 3 mėnesius, negaliojančių sertifikatų sąrašų persidengimo periodas – 3 savaitės.

78. Skelbiamoje periodinėje negaliojančių sertifikatų sąrašo versijoje nurodomas kitos versijos paskelbimo laikas.

## **VI. PRIVAČIOJO KRIPTOGRAFINIO RAKTO AKTYVAVIMO DUOMENŲ VALDYMAS**

79. Privačiojo kriptografinio rakto aktyvavimo duomenys pateikiami išduodant sertifikatą. Išduodant naują sertifikatą, visais atvejais sudaromi ir nauji privačiojo kriptografinio rakto aktyvavimo duomenys.

80. Prašymai sudaryti naujus privačiojo kriptografinio rakto aktyvavimo duomenis teikiami šių nuostatų 55 punkte nustatyta tvarka. Nauji privačiojo kriptografinio rakto aktyvavimo duomenys sudaromi iškart, tik gavus prašymą.

## **VII. ĮRAŠŲ APIE SERTIFIKAVIMO VEIKLĄ KAUPIMAS**

81. Sertifikavimo paslaugų teikėjo sistemų vykdomos sertifikatų sudarymo ir tvarkymo operacijos turi būti fiksuojamos operacijų žurnale, kuriame fiksuojama ši informacija:

- 81.1. užklausos sertifikatams gauti;
- 81.2. sertifikatų ir raktų generavimo faktai;
- 81.3. sertifikato statuso keitimo operacijos;
- 81.4. sertifikatų būsenos tikrinimo užklausos ir atsakymai į jas;

- 81.5. negaliojančių sertifikatų sąrašų generavimo ir publikavimo faktai.
82. Operacijų žurnalas pasirašomas infrastruktūriniu sertifikavimo paslaugų teikėjo elektroniniu parašu.
83. Sistemų veiklai stebėti ir gedimams diagnozuoti sudaromas sistemų funkcionavimo diagnostikos ir klaidų žurnalas (toliau – sistemų funkcionavimo žurnalas), kurio įrašai naudojami sistemų veiklos analizei ir diagnostikai atlikti bei sutrikimams šalinti.
84. Diagnostikos žurnale fiksuojama ši informacija:
- 84.1. ugniasienių ir apsaugos sistemų perspėjimai;
  - 84.2. duomenys apie techninės ir programinės įrangos pakeitimus;
  - 84.3. duomenys apie kompiuterių tinklo pakeitimus;
  - 84.4. fizinio patekimo į saugias zonas duomenys;
  - 84.5. duomenys apie slaptažodžių ir darbuotojų pareigų pakeitimus;
  - 84.6. atsarginių kopijų, archyvinių duomenų kaupimo duomenys.
85. Klaidų žurnale fiksuojama informacija apie sistemos sutrikimus ir klaidas.
86. Žurnalų įrašai peržiūrimi ne rečiau kaip kartą per mėnesį. Kiekvienas didesnės reikšmės įvykis turi būti papildomai aprašytas.
87. Sertifikavimo paslaugų teikėjas operacijų ir sistemų funkcionavimo žurnalus turi saugoti 10 metų po jų užbaigimo. Tolesnis jų saugojimas užtikrinamas Lietuvos Respublikos dokumentų ir archyvų įstatymo (Žin., 1995, Nr. 107-2389; 2004, Nr. 57-1982, toliau – Dokumentų ir archyvų įstatymas) nustatyta tvarka.
88. Operacijų, sistemų funkcionavimo diagnostikos ir klaidų žurnalų atsarginės kopijos daromos kiekvieną savaitę. Šiuos žurnalus peržiūrėti gali tik saugumo pareigūnas, sistemos administratorius ir auditorius. Niekas neturi teisės pakeisti žurnalo turinį.

## **VIII. DUOMENŲ ARCHYVAVIMAS IR ATSARGINIŲ KOPIJŲ DARYMAS**

89. Sertifikavimo paslaugų teikėjas Dokumentų ir archyvų įstatymo nustatyta tvarka saugo šiuos duomenis:
- 89.1. operacijų ir sistemų funkcionavimo žurnalus;
  - 89.2. sudarytų sertifikatų duomenų bazę;
  - 89.3. negaliojančių sertifikatų sąrašus;
  - 89.4. sertifikavimo paslaugų teikėjui priklausančių kriptografinių raktų gyvavimo ciklo valdymo istoriją;
  - 89.5. asmenims priklausančių kriptografinių raktų ir sertifikatų gyvavimo ciklo valdymo istoriją.
90. Šių nuostatų 89 punkte nustatyti duomenys sertifikavimo paslaugų teikėjo archyve

saugomi 10 metų, tolesnis jų saugojimas užtikrinamas Dokumentų ir archyvų įstatymo nustatyta tvarka.

91. Atsarginės kopijos skirtos sistemos darbui po sutrikimų atstatyti. Daromos šios programinės įrangos, duomenų bazių ir kitų duomenų atsarginės kopijos:

91.1. sertifikavimo paslaugų teikėjo sistemų programinės įrangos diegimo rinkmenų;

91.2. taikomųjų programų diegimo rinkmenų;

91.3. sertifikavimo paslaugų teikėjo interneto svetainėje teikiamų duomenų;

91.4. sertifikatų duomenų bazės;

91.5. negaliojančių sertifikatų sąrašų;

91.6. operacijų, sistemų funkcionavimo diagnostikos ir klaidų žurnalų.

92. Duomenų bazių atsarginės kopijos daromos kas 24 valandas, kitos informacijos atsarginės kopijos daromos kas savaitę. Saugomos kiekvienos programinės įrangos versijos atsarginės kopijos.

93. Įvykus veiklos sutrikimams, sertifikavimo paslaugų teikėjo darbas atstatomas ne vėliau kaip per 72 valandas.

## **IX. SERTIFIKAVIMO VEIKLOS GRĖSMIŲ VALDYMAS**

94. Sertifikavimo paslaugų teikėjas turi atsižvelgti į šias sertifikavimo veiklos grėsmes:

94.1. fiziniai sistemų pažeidimai;

94.2. programinės įrangos veiklos sutrikimai;

94.3. išorinių telekomunikacijų ir elektros tinklų funkcionavimo sutrikimai;

94.4. vidinių kompiuterių tinklų sutrikimai.

95. Sertifikavimo veiklos grėsmių prevencijai užtikrinti ar jų įtaikai sumažinti, sertifikavimo paslaugų teikėjas turi taikyti šias priemones:

95.1. Veiklos atkūrimas:

95.1.1. turi būti periodiškai daromos sistemų duomenų bazių, programinės įrangos ir kitų duomenų atsarginės kopijos;

95.1.2. turi būti parengta atsarginė sertifikavimo paslaugų teikėjo veiklai ir sertifikato būsenos tikrinimo funkcijoms atkurti skirta įranga, kurią naudojant sertifikavimo paslaugų teikėjo veikla būtų atnaujinta ne vėliau kaip per 72 valandas, sertifikatų statuso tikrinimo paslauga – per 4 valandas.

95.2. Sertifikavimo paslaugų teikėjo sistemų pakeitimų valdymas. Sertifikavimo paslaugų teikėjo naudojamų sistemų programinė įranga turi būti atnaujinama tik išbandžius naują programinę įrangą testavimo aplinkoje.

95.3. Elektros tinklų funkcionavimo užtikrinimas. Naudojami atsarginiai energijos šaltiniai

(nenutrūkstamo maitinimo šaltinis (UPS) ir dyzelinis elektros generatorius), kurie elektros energiją sistemai gali tiekti 24 valandas.

96. Po gedimo atkūrus sistemos veikimą, sertifikavimo paslaugų teikėjo saugumo pareigūnas privalo:

96.1. pakeisti fizinio patekimo į sertifikavimo paslaugų teikėjo patalpas slaptažodžius ir kodus;

96.2. iš naujo suteikti prieigos prie sistemos teises;

96.3. informuoti sistemos naudotojus apie sistemos atstatymą.

97. Sertifikavimo paslaugų teikėjo privačiojo rakto sukompromitavimo atveju, sertifikavimo paslaugų teikėjas nedelsdamas atlieka šiuos veiksmus:

97.1. sertifikatų naudotojai nedelsiant informuojami apie sertifikavimo paslaugų teikėjo privačiojo rakto kompromitaciją masinėmis informacijos platinimo ir kitomis priemonėmis;

97.2. sukompromituotą privatųjį raktą atitinkantis sertifikavimo paslaugų teikėjo sertifikatas įrašomas į negaliojančių sertifikatų sąrašą;

97.3. nutraukiamas visų sertifikavimo paslaugų teikėjo asmenims sudarytų sertifikatų galiojimas.

## **X. SERTIFIKAVIMO PASLAUGŲ TEIKĖJO VEIKLOS NUTRAUKIMAS**

98. Sertifikavimo paslaugų teikėjas įsipareigoja, kad prieš nutraukdamas sertifikavimo veiklą įsipareigoja:

98.1. ne vėliau, kaip prieš 1 mėnesį iki sertifikavimo veiklos nutraukimo apie tai informuoti visus sertifikatų savininkus ir elektroninio parašo priežiūros instituciją;

98.2. per vieną mėnesį po paskelbimo apie veiklos nutraukimą, sukauptus veiklos duomenis perduos veiklos perėmėjui ar elektroninio parašo priežiūros institucijai, kurie užtikrina duomenų, reikalingų sertifikato statusui tikrinti, teikimą pasitikinčioms šalims.

## **X. SAUGUMO PRIEMONĖS**

### **I. FIZINIO SAUGUMO PRIEMONĖS**

99. Už sertifikavimo veiklą atsakingos Gyventojų registro tarnybos buveinės adresas:  
A. Vivulskio g. 4 A, LT-03220 Vilnius.

100. Sertifikavimo paslaugų teikėjo sistemų įranga saugoma Informatikos ir ryšių departamento tarnybinių stočių saugykloje, esančioje Asmens dokumentų išrašymo centre adresu Žirmūnų g.1 D, LT-09229 Vilnius.

101. Sertifikavimo paslaugų teikėjo rezervinė ir testavimo sistemos įranga saugomos Informatikos ir ryšių departamento tarnybinių stočių saugykloje adresu Šventaragio g. 2, LT-

01510 Vilnius.

102. Išskirtos dvi sertifikavimo paslaugų teikėjo patalpų saugumo zonos:

102.1. sertifikavimo paslaugų teikėjo kritinių sistemų zona;

102.2. sertifikavimo paslaugų teikėjo operacijų zona.

103. Sertifikavimo paslaugų teikėjo kritinių sistemų zonoje saugoma pagrindinė sertifikavimo paslaugų teikėjo techninė įranga ir kriptografiniai saugumo moduliai, kuriuose saugomi sertifikavimo paslaugų teikėjo viešieji raktai.

104. Sertifikavimo paslaugų teikėjo kritinių sistemų zona yra įrengta Asmens dokumentų išrašymo centro tarnybinių stočių saugykloje, kurios saugumas užtikrintas šiomis priemonėmis:

104.1. Asmens dokumentų išrašymo centro patalpos yra sugriežtintos apsaugos zona, jas visą parą saugo budėtojas;

104.2. Asmens dokumentų išrašymo centro patalpose įgyvendinta dviejų lygių įėjimo kontrolės sistema:

104.2.1. įeinant į padidinto saugumo (kritinių sistemų) zoną, asmeniui identifikuoti naudojamos identifikavimo kortelės ir nuskaitomas piršto antspaudas;

104.2.2. įeinant į kitas zonas (operacijų zonas) asmeniui identifikuoti naudojamos tik identifikavimo kortelės.

104.3. Asmens dokumentų išrašymo centro patalpose įrengta vaizdo stebėjimo sistema.

104.4. Į kritinių sistemų zoną patekti teisę turi tik sertifikavimo paslaugų teikėjo saugumo pareigūnas, sistemos auditorius ir sistemos administratorius. Kiti asmenys į šią zoną patekti gali tik lydimi minėtas pareigas užimančių darbuotojų. Kiekvienas patekimas į šią zoną registruojamas.

105. Sertifikavimo paslaugų teikėjo operacijų zoną sudaro:

105.1. Informacijos ir ryšių departamento patalpos;

105.2. Asmens dokumentų išrašymo centro patalpos;

105.3. Gyventojų registro tarnybos patalpos.

106. Sertifikavimo paslaugų teikėjo operacijų zonos patalpose atliekamos su sertifikavimo veikla susijusios operacijos ir saugoma su sertifikavimo veikla susijusi informacija bei techninė įranga. Į šią zoną gali patekti tik aukštos atsakomybės pareigas užimantys darbuotojai. Kiti asmenys į šią zoną patekti gali tik lydimi minėtas pareigas užimančių darbuotojų.

107. Asmens dokumentų išrašymo centro tarnybinių stočių saugykloje yra įrengta oro kondicionavimo sistema, palaikanti reikiamą vienodą temperatūrą. Sutrikus elektros energijos tiekimui, nenutrūkstamo maitinimo šaltinis (UPS) ir dyzelinis elektros generatorius užtikrina nepertraukiamą sistemos darbą iki 24 valandų.

108. Asmens dokumentų išrašymo centro tarnybinių stočių saugykla yra apsaugota nuo potvynio ar užpylimo vandeniu.

109. Sertifikavimo paslaugų teikėjo įrangos pagrindinės ir rezervinės saugyklų patalpose įdiegta priešgaisrinės apsaugos sistema, atitinkanti priešgaisrinės apsaugos tarnybos nustatytus reikalavimus, kurioje yra naudojama gesinimo inertinėmis dujomis sistema.

110. Laikmenos su archyvų duomenimis ir atsarginėmis kopijomis saugomos operacijų zonoje.

111. Popierius ir elektroninės laikmenos, kuriose yra svarbi informacija, pasibaigus jų saugojimo terminui, sunaikinamos specialiais plėšymo ar smulkinimo įrenginiais.

## **II. PERSONALO SAUGUMO PRIEMONĖS**

112. Aukštos atsakomybės pareigas einantys darbuotojai vykdo kritines ir itin svarbias sertifikavimo veiklos operacijas. Aukštos atsakomybės pareigos, kurias gali eiti vienas ar keli asmenys, yra šios:

112.1. saugumo pareigūnas, atsakingas už saugumo politikos kūrimą, skleidimą bei įgyvendinimą; dalyvauja visose kritinėse sertifikavimo veiklos operacijose; atsako už slaptažodžių generavimą, teisių skyrimą, papildomai tvirtina sertifikavimo paslaugų teikėjo valdomų sertifikatų gyvavimo ciklo operacijas;

112.2. sistemos administratorius, atsakingas už sertifikavimo paslaugų teikėjo sistemų, naudojamų sertifikatų sudarymui ir tvarkymui, diegimą, konfigūravimą ir palaikymą;

112.3. sistemos operatorius, atsakingas už sertifikatų sudarymo ir tvarkymo sistemų naudojimą; įgaliotas daryti atsargines kopijas ir vykdyti informacijos iš jų atstatymo procedūras;

112.4. sistemos auditorius, atsakingas už sertifikavimo paslaugų teikėjo vidaus audito vykdymą, veiklos atitikimo taisyklėms ir nuostatams tikrinimą, ataskaitų apie sertifikavimo veiklos saugumą ir patikimumą formavimą; įgaliotas peržiūrėti sertifikavimo paslaugų teikėjo sistemų archyvus ir audito įrašus;

112.5. sertifikavimo paslaugų teikėjo sistemų prižiūrėtojas, atsakingas už kasdienį sertifikavimo paslaugų teikėjo sistemų funkcionavimo palaikymą, pavaldus administratoriui.

113. Sertifikavimo paslaugų teikėjas savo darbuotojų pareigybėms atskirti ir identifikuoti naudoja šias priemones:

113.1. sudaro asmenų, kuriems leidžiama patekti į sertifikavimo paslaugų teikėjo patalpas, sąrašą;

113.2. sudaro asmenų, kuriems suteikiama fizinė prieiga prie sertifikavimo paslaugų teikėjo sistemų, sąrašą;

113.3. užtikrina teisių valdymą sertifikavimo paslaugų teikėjo informacinėse sistemose;

113.4. aiškiai išskiria ir apibrėžia aukštos atsakomybės pareigas einančių darbuotojų vykdomas funkcijas.

114. Sertifikavimo paslaugų teikėjas užtikrina, kad jo darbuotojai:
- 114.1. turi aukštąjį išsilavinimą;
  - 114.2. yra išklause su jų pareigų vykdymu susijusius kvalifikacijos kursus;
  - 114.3. yra išklause asmens duomenų ir informacijos apsaugos mokymus;
  - 114.4. nebuvo teisti.
115. Sertifikavimo paslaugų teikėjo darbuotojų biografija tikrinama laikantis Lietuvos Respublikos vidaus reikalų ministerijos darbuotojams taikomos tvarkos.
116. Sertifikavimo paslaugų teikėjo ir registravimo tarnybų darbuotojai turi būti išklause mokymus ir susipažinę su šia informacija:
- 116.1. taisyklėmis, nuostatais, sertifikatų sudarymo ir tvarkymo sąlygomis, asmenų registravimo ir konsultavimo taisyklėmis, elektroninio parašo taisyklėmis;
  - 116.2. sertifikavimo paslaugų teikėjo ir registravimo tarnybų saugumo reikalavimais;
  - 116.3. sistemos veikimo sutrikimo atvejais atliekamų veiksmų aprašais.
117. Darbuotojai pasirašytinai patvirtina, kad susipažino su šių nuostatų 116 punkte nurodyta informacija ir sutinka su jiems keliamais reikalavimais ir nustatytais pareigomis.
118. Papildomi sertifikavimo paslaugų teikėjo darbuotojų mokymai vykdomi, kai yra įgyvendinti svarbesni veiklos pakeitimai.
119. Atliekant sertifikavimo paslaugų teikimo veiklos kritines operacijas dalyvauja mažiausiai 3 asmenys, tarp kurių visada turi būti saugumo pareigūnas. Šie asmenys turi turėti specialias, su kriptografiniu įranga susietas, identifikavimo korteles. Kiekvienai operacijai atlikti reikia 3 iš 6 kortelių.
120. Kritinės operacijos apima visas su sertifikavimo paslaugų teikėjo sertifikatų ir kriptografinių raktų gyvavimo ciklo valdymu susijusias operacijas.
121. Užduotims sertifikavimo paslaugų teikėjo patalpose atlikti samdomas asmenis turi lydėti sertifikavimo paslaugų teikėjo darbuotojas.

### **III. TECHNINIO SAUGUMO PRIEMONĖS**

122. Sertifikavimo paslaugų teikėjo sertifikatų kriptografinių raktų poros generuojamos naudojant kriptografinius saugumo modulius, kurie atitinka JAV Nacionalinio standartų ir technologijų instituto standarto FIPS PUB 140-2 „Saugos reikalavimai kriptografiniams moduliams“ trečiojo saugumo lygmens reikalavimus. Generavimo procedūros veiksmai yra fiksuojami dokumentuose, kurie pasirašomi visų procedūroje dalyvavusių asmenų.
123. Asmenims išduodamų sertifikatų kriptografinių raktų porą generuoja techninės priemonės, naudojančios saugią parašo formavimo įrangą, kuri atitinka Lietuvos standarto LST ISO/IEC 15408 „Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo

įvertinimo kriterijai“ trečiojo saugumo lygmens (SSCD Type 3) reikalavimus.

124. Privatieji kriptografiniai raktai saugomi saugioje parašo formavimo įrangoje, kuri įteikiama asmeniškai sertifikato savininkui.

125. Saugioje parašo formavimo įrangoje sugeneruotas asmens viešasis kriptografinis raktas saugiomis ryšio priemonėmis perduodamas darbinei sertifikavimo tarnybinei stočiai, kuri sudaro sertifikatą.

126. Sertifikavimo paslaugų teikėjo viešieji kriptografiniai raktai yra įrašyti į sertifikavimo paslaugų teikėjui priklausančius sertifikatus, skelbiami sertifikavimo paslaugų teikėjo interneto svetainėje ir perduodami naudotojams tvirtinant jiems išduodamus sertifikatus.

127. Sertifikavimo paslaugų teikėjas generuoja tokio dydžio raktus:

127.1. Šakninės sertifikavimo tarnybinės stoties rakto ilgis – 4096 bitai;

127.2. Nuostatų sertifikavimo tarnybinės stoties rakto ilgis – 2048 bitai;

127.3. Darbinės sertifikavimo tarnybinės stoties rakto ilgis – 2048 bitai;

127.4. Asmenims generuojamo rakto ilgis – 2048 bitai.

128. Sertifikavimo paslaugų teikėjo kriptografinius raktus generuoja techninės priemonės, naudojančios kriptografinius saugumo modulius, atitinkančius FIPS PUB 140-2 standarto trečiojo saugumo lygmens (Level3) reikalavimus.

129. Asmenims išduodamų sertifikatų kriptografinių raktų poras generuoja aparatinėmis priemonėmis, naudojant saugią parašo formavimo įrangą, kuri atitinka Lietuvos standarto LST ISO/IEC 15408 „Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai“ trečiojo saugumo lygmens (SSCD Type 3) reikalavimus..

130. Sertifikavimo paslaugų teikėjo kriptografiniams raktams generuoti naudojami kriptografiniai saugumo moduliai, atitinkantys FIPS PUB 140-2 standarto trečiojo saugumo lygmens reikalavimus.

131. Šakninės sertifikavimo tarnybinės stoties ir nuostatų sertifikavimo tarnybinės stoties privatieji kriptografiniai raktai saugomi kriptografiniuose saugumo moduluose, kurie turi būti atjungti nuo tinklo.

132. Visi kriptografiniai saugumo moduliai saugomi Asmens dokumentų išrašymo centro tarnybinių stočių saugyklos patalpose. Kiekviena procedūra ar operacija, susijusi su sertifikavimo paslaugų teikėjo kriptografinių raktų gyvavimo ciklo valdymu fiksuojama dokumentuose.

133. Sertifikavimo paslaugų teikėjo kriptografinių raktų kopijos yra šifruojamos, šifravimo raktas yra padalinamas į dalis ir saugomas specialiose, su kriptografine įranga susietose identifikavimo kortelėse. Šiam raktui atkurti reikia 3 iš 6 kortelių.

134. Sertifikavimo paslaugų teikėjas nedaro asmenų privačiųjų kriptografinių raktų kopijų.

135. sertifikavimo paslaugų teikėjo privatieji kriptografiniai raktai nearchyvuojami.

Pasibaigus galiojimo terminui, šie raktai sunaikinami.

136. Kiekviena sertifikavimo paslaugų teikėjo sertifikavimo tarnybinė stotis naudoja tik jai skirtą atskirą kriptografinį saugumo modulį, todėl kriptografinio rakto įvedimo ir išvedimo procedūra atliekama tik atkuriant privatųjį kriptografinį raktą ir darant jo kopijas.

137. Sertifikavimo paslaugų teikėjo privatusis kriptografinis raktas aktyvuojamas į kriptografinį modulį įvedus 3 iš 6 identifikavimo kortelių.

138. Asmens privatusis kriptografinis raktas, kuris laikomas sertifikavimo paslaugų teikėjo jam parengtoje saugioje parašo formavimo įrangoje, aktyvuojamas įvedus aktyvavimo duomenis.

139. Sertifikavimo paslaugų teikėjo privačiojo rakto deaktyvavimas atliekamas iš kriptografinio saugumo modulio ištraukus bent vieną identifikavimo kortelę.

140. Sertifikato savininko privatusis kriptografinis raktas deaktyvuojamas išjungus saugią parašo formavimo įrangą.

141. Sertifikavimo paslaugų teikėjo privačiojo rakto sunaikinimas reiškia rakto ištrynimą arba laikmenų, kuriose buvo saugomas raktas, sunaikinimą.

142. Sertifikavimo paslaugų teikėjas išsaugo ir archyvuoja visus sudarytus sertifikatus. Sertifikatuose įrašyti viešieji kriptografiniai raktai turi būti išsaugomi taip, kad parašą patikrinti būtų galima ir pasibaigus sertifikato galiojimo terminui.

143. Kriptografinių raktų galiojimo terminai yra šie:

143.1. Šakninės sertifikavimo tarnybinės stoties rakto galiojimo – 18 metų.

143.2. Nuostatų sertifikavimo tarnybinės stoties rakto galiojimo – 12 metai.

143.3. Darbinės sertifikavimo tarnybinės stoties rakto galiojimo – 6 metai.

143.4. Asmenims sudaromų raktų galiojimo – 3 metai.

144. Sertifikavimo paslaugų teikėjo kompiuteriai turi atitikti šiuos saugos reikalavimus ir juose turi būti įgyvendintos šios saugumo priemonės:

144.1. operacinės sistemos ir taikomųjų programų lygmeniu numatytos privalomos registravimo priemonės;

144.2. priemonės, įgalinančios atskirti sistemoje leistinas pareigas;

144.3. prie sistemos prisijungiančių asmenų pareigų identifikavimo ir autentifikavimo priemonės;

144.4. kriptografinės informacijos apsaugos priemonės, kai ši informacija perduodama tinklu;

144.5. nesankcionuotos prieigos prie kompiuterinių išteklių valdymo ir informavimo priemonės.

145. Kompiuterių saugą įvertina auditorius, kuris teikia išvadas saugumo pareigūnui.

146. Kuriant papildomas sertifikavimo paslaugų teikėjo sistemas laikomasi visų sertifikato

taisyklių ir pokyčių valdymo reikalavimų. Kiekvienas kuriamas programinės įrangos modulis ar techninė įrangą išbandoma testavimo aplinkoje ir sertifikavimo paslaugoms teikti pradedama naudoti tik gavus saugumo pareigūno patvirtinimą.

147. Sistemos konfigūracijos keitimai fiksuojami ir kontroliuojami laikantis sertifikavimo paslaugų teikėjo nustatytų saugumo taisyklių.

148. Šakninė ir nuostatų sertifikavimo tarnybinės stotys veikia atjungtos nuo tinklo. Sertifikavimo paslaugų teikėjo kompiuterių tinklas padalintas į kelis lygmenis, kiekvienam iš jų taikomi atskiri prieigos ir saugumo reikalavimai. Kiekvienas tinklo lygmuo apsaugotas ugniasiene.

149. Sertifikavimo paslaugų teikėjas turi užtikrinti kriptografinių saugumo modulių saugumą viso jų gyvavimo ciklo metu. Sertifikavimo paslaugų teikėjas turi užtikrinti, kad:

149.1. kriptografinis saugumo modulis nebuvo pažeistas iki jo pateikimo sertifikavimo paslaugų teikėjui;

149.2. kriptografinis saugumo modulis nebuvo pažeistas sandėliuojant;

149.3. kriptografinis saugumo modulis veikia tinkamai.

## **XI. SERTIFIKATŲ IR NEGALIOJANČIŲ SERTIFIKATŲ SĄRAŠŲ PROFILIAI**

150. Sertifikatų sandara atitinka Lietuvos standarto LST ETSI TS 101 862 „Kvalifikuoto sertifikato profilis“ reikalavimus. Sertifikatų ir negaliojančių sertifikatų sąrašų profiliai nustatyti šių nuostatų 4–14 prieduose.

## **XII. SERTIFIKAVIMO VEIKLOS NUOSTATŲ ADMINISTRAVIMAS**

151. Sertifikatų naudotojai turi vadovautis aktualia nuostatų redakcija. Naujai patvirtinta ir paskelbta nuostatų redakcija panaikina ankstesnės nuostatų redakcijos galiojimą. Naujausia aktuali nuostatų redakcija turi būti skelbiama internete.

152. Nuostatai gali būti keičiami pastebėjus juose klaidas ar atsiradus poreikiui juos atnaujinti.

153. Nuostatų pakeitimai gali būti:

153.1. esminiai, kuriuos atlikus keičiamas ir nuostatų unikalus identifikatorius; apie šiuos pakeitimus turi būti pranešama sertifikatų naudotojams;

153.2. neesminiai, apie kuriuos sertifikavimo paslaugų teikėjas neprivalo pranešti kitoms šalims; šiuo atveju nuostatų unikalus identifikatorius nėra keičiamas.

154. Neesminiais pakeitimais laikomi rekomendacinio, paaiškinamojo, tikslinamojo pobūdžio informacijos arba už nuostatų tvarkymą atsakingų asmenų kontaktinių duomenų, jei tokie duomenys yra nurodyti, pakeitimai.

155. Kitais atvejais pakeitimai yra esminiai. Visais atvejais, kai nuostatų pakeitimai yra

susiję su sertifikavimo paslaugų saugumo lygio keitimu, nuostatų pakeitimai yra esminiai.

156. Atlikus esminius pakeitimus, keičiamas naujos nuostatų redakcijos versijos pirmas skaitmuo (1 priedas) bei atitinkamas unikalaus nuostatų identifikatoriaus dokumento versijos elementas (paskutinis skaitmuo). Atlikus neesminius pakeitimus keičiami naujos nuostatų redakcijos versijos antras ir tolimesni skaitmenys.

157. Nuostatų priežiūros, keitimo ir tvirtinimo procedūros vykdomos tokia tvarka:

157.1. nuostatų pakeitimus gali inicijuoti sertifikavimo paslaugų teikėjas arba sertifikatų naudotojai;

157.2. už saugumo politiką atsakingi sertifikavimo paslaugų teikėjo darbuotojai:

157.2.1. per vienerius metus nuo vėliausios nuostatų redakcijos paskelbimo peržiūri ir įsitikinta nuostatų aktualumu;

157.2.2. peržiūros metu nustatčius poreikį keisti nuostatus, inicijuoja nuostatų keitimą ir rengia naują nuostatų redakciją;

157.2.3. priima sprendimą teikti tvirtinti naują nuostatų redakciją;

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

157.4. neesminių pakeitimų atveju nauja nuostatų redakcija teikiama tvirtinti iš karto ją parengus;

157.5. nuostatų naują redakciją tvirtina sertifikavimo paslaugų teikėjo vadovas.

158. Apie rengiamą naują nuostatų projektą turi būti informuota elektroninio parašo priežiūros institucija.

---

**SERTIFIKAVIMO VEIKLOS NUOSTATŲ UNIKALAUŠ  
IDENTIFIKATORIAUS REIKŠMĖS IR NUOSTATŲ VERSIJA**

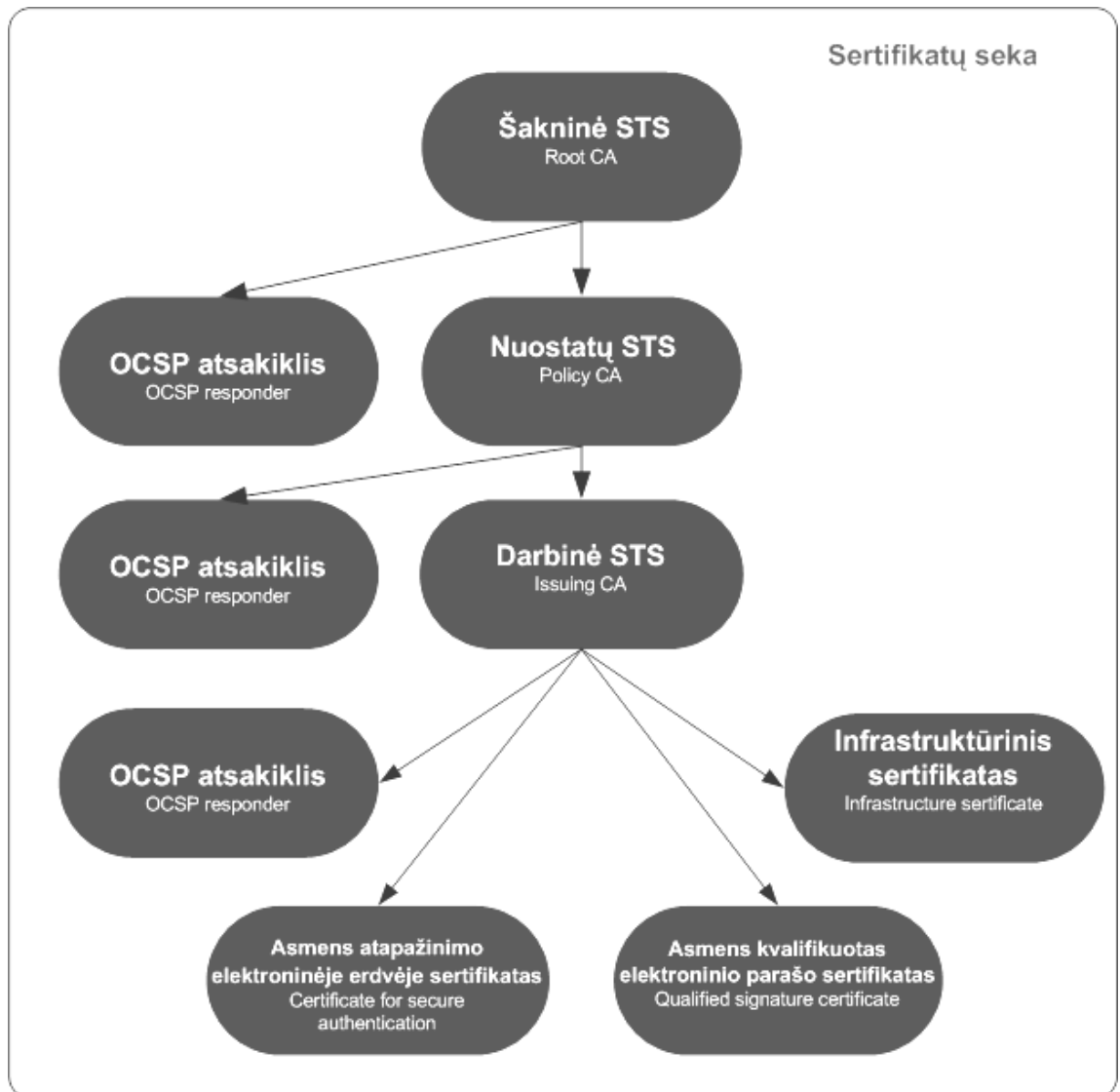
**Nuostatų unikalūs identifikatoriai**

<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 ir tvarkymo skyrius	1
Dokumento tipas (Sertifikavimo veiklos nuostatai)	2
Dokumento versijos pirmasis skaitmuo	1

**Nuostatų versija 1.0**

---

## SERTIFIKAVIMO TARNYBŲ HIERARCHIJOS SCHEMA



## SERTIFIKAVIMO PASLAUGAS TEIKIANČIŲ ĮSTAIGŲ KONTAKTINIAI DUOMENYS

### Sertifikavimo paslaugų teikėjas

Organizacija	Gyventojų registro tarnyba prie Lietuvos respublikos vidaus reikalų ministerijos
Adresas	A. Vivulskio g. 4 A, LT-03220 Vilnius;
Tel.	(8 5) 271 6352
Faks.	(8 5) 271 6250
URL:	<a href="http://www.nsc.vrm.lt/">http://www.nsc.vrm.lt/</a>
El.paštas:	<b>grt@vrm.lt</b>

### Registravimo tarnyba

Organizacija	Gyventojų registro tarnybos padaliniai
Adresas	A. Vivulskio g. 4 A, LT-03220 Vilnius; Lvovo g. 7/Slucko g. 6, LT-09313 Vilnius.
Tel.	(8 5) 271 6352
Faks.	(8 5) 271 6250
URL:	<a href="http://www.nsc.vrm.lt/">http://www.nsc.vrm.lt/</a>
El.paštas:	<b>grt@vrm.lt</b>
Organizacija	Migracijos tarnybos*
Adresas	Sertifikato savininkas turi kreiptis į tą migracijos tarnybą, kurioje yra deklaravęs savo gyvenamąją vietą, jei sertifikato savininkas gyvenamosios vietos nėra deklaravęs – į asmens tapatybės kortelę išdavusią migracijos tarnybą.

\* migracijos tarnybos paslaugas pradės teikti nuo 2009 m. liepos 1 d.

**Sertifikavimo veiklos palaikymo tarnyba:** tel.: 8 5 271 6062

Darbo laikas

I-IV	7.30-11.30 val., 12.15-16.30 val.
V	7.30-11.30 val., 12.15-15.15 val.
VI-VII	9.00-10.00 val.

**Už nuostatų atitikimą taisyklėms ir nuostatų administravimą atsakingo asmens  
kontaktiniai duomenys**

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

---

**ŠAKNINĖS SERTIFIKAVIMO TARNYBINĖS STOTIES SERTIFIKATO PROFILIS**

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė [paaiškinimas]
Version			2 [V3 trečia versija]
Serial number			sudaromas Root CA
Signature algorithm			sha1RSA
Issuer			CN = Nacionalinis sertifikavimo centras (RootCA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventojų registro tarnyba prie LR VRM - i.k. 188756767 C = LT
Validity			Galiojimo pradžios ir pabaigos datos (notBefore, notAfter) UTC laiku
Subject			CN = Nacionalinis sertifikavimo centras (RootCA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventojų registro tarnyba prie LR VRM - i.k. 188756767 C = LT
Public key			Viešojo rakto reikšmė (4096 bit) ir parašo formavimo algoritmo identifikatorius (RSA)
Papildomi laukai (extensions)			
Subject Key Identifier	Ne		Šakninio CA viešojo rakto 160 bitų SHA-1 hash reikšmė
CA Version	Ne		Sudaromas sukuriant sertifikatą
Certificate Policies	Ne	Policy Identifier	1.3.6.1.4.1.31912.1.1.1
		Policy Qualifier Id=CPS	<a href="http://nsc.vrm.lt/repository">http://nsc.vrm.lt/repository</a>
Key Usage	Taip		keyCertSign (5), cRLSign (6)
Basic Constraints	Taip		Subject Type=CA Path Length Constraint=None

## NUOSTATŲ SERTIFIKAVIMO TARNYBINĖS STOTIES SERTIFIKATO PROFILIS

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė [paaiškinimas]
Version			2 [V3 trečia versija]
Serial number			sudaromas Root CA
Signature algorithm			sha1RSA
Issuer			CN = Nacionalinis sertifikavimo centras (RootCA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventoju registro tarnyba prie LR VRM - i.k. 188756767 C = LT
Validity			Galiojimo pradžios ir pabaigos datos (notBefore, notAfter) UTC laiku
Subject			CN = Nacionalinis sertifikavimo centras (PolicyCA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventoju registro tarnyba prie LR VRM - i.k. 188756767 C = LT
Public key			Viešojo rakto reikšmė (2048 bit) ir parašo formavimo algoritmo identifikatorius (RSA)
Papildomi laukai (extensions)			
Subject Key Identifier	Ne	Key Identifier	Policy CA viešojo rakto 160 bitų SHA-1 hash reikšmė
Authority Key Identifier	Ne		Root CA viešojo rakto 160 bitų SHA-1 hash reikšmė
CA Version	Ne		Sudaromas sukuriant sertifikatą
Certificate Policies	Ne	Policy Identifier	1.3.6.1.4.1.31912.1.1.1
		Policy Qualifier Id=CPS	<a href="http://nsc.vrm.lt/repository">http://nsc.vrm.lt/repository</a>
CRL Distribution Points	Ne	Distribution Point Name	URL= <a href="http://nsc.vrm.lt/cdp/RootCA.crl">http://nsc.vrm.lt/cdp/RootCA.crl</a>
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	<a href="http://nsc.vrm.lt/OCSP/ocspresponder.nsc">http://nsc.vrm.lt/OCSP/ocspresponder.nsc</a>
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	<a href="http://nsc.vrm.lt/aia/RootCA.crt">http://nsc.vrm.lt/aia/RootCA.crt</a>
Basic Constraints	Taip		Subject Type=CA Path Length Constraint=None
Key Usage	Taip		keyCertSign (5), cRLSign (6)

**DARBINĖS SERTIFIKAVIMO TARNYBINĖS STOTIES SERTIFIKATO PROFILIS**

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė [paaiškinimas]
Version			2 [V3 trečia versija]
Serial number			sudaromas Policy CA
Signature algorithm			sha1RSA
Issuer			CN = Nacionalinis sertifikavimo centras (PolicyCA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventoju registro tarnyba prie LR VRM - i.k. 188756767 C = LT
Validity			Galiojimo pradžios ir pabaigos datos (notBefore, notAfter) UTC laiku
Subject			CN = Nacionalinis sertifikavimo centras (IssuingCA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventoju registro tarnyba prie LR VRM - i.k. 188756767 C = LT
Public key			Viešojo rakto reikšmė (2048 bit) ir parašo formavimo algoritmo identifikatorius (RSA)
Papildomi laukai (extensions)			
Subject Key Identifier	Ne	Key Identifier	Issuing CA viešojo rakto 160 bitų SHA-1 hash reikšmė
Authority Key Identifier	Ne		Policy CA viešojo rakto 160 bitų SHA-1 hash reikšmė
CA Version	Ne		Sudaromas sukuriant sertifikatą
Certificate Policies	Ne	Policy Identifier	1.3.6.1.4.1.31912.1.1.1
		Policy Qualifier Id=CPS	<a href="http://nsc.vrm.lt/repository">http://nsc.vrm.lt/repository</a>
CRL Distribution Points	Ne	Distribution Point Name	URL= <a href="http://nsc.vrm.lt/cdp/PolicyCA.crl">http://nsc.vrm.lt/cdp/PolicyCA.crl</a>
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	<a href="http://nsc.vrm.lt/OCSP/ocspresponder.nsc">http://nsc.vrm.lt/OCSP/ocspresponder.nsc</a>
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	<a href="http://nsc.vrm.lt/aia/PolicyCA.crt">http://nsc.vrm.lt/aia/PolicyCA.crt</a>
Basic Constraints	Taip		Subject Type=CA Path Length Constraint=None
Key Usage	Taip		keyCertSign (5), cRLSign (6)

**ŠAKNINĖS SERTIFIKAVIMO TARNYBINĖS STOTIES OCSP PRANEŠIMŲ  
TVIRTINIMO SERTIFIKATO PROFILIS**

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė [paaiškinimas]
Version			2 [V3 trečia versija]
Serial number			sudaromas Root CA
Signature algorithm			sha1RSA
Issuer			CN = Nacionalinis sertifikavimo centras (RootCA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventojų registro tarnyba prie LR VRM - i.k. 188756767 C = LT
Validity			Galiojimo pradžios ir pabaigos datos (notBefore, notAfter) UTC laiku
Subject			CN = NSC OCSP (RootCA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventojų registro tarnyba prie LR VRM - i.k. 188756767 C = LT
Public key			Viešojo rakto reikšmė (4096 bit) ir parašo formavimo algoritmo identifikatorius (RSA)
Papildomi laukai (extensions)			
Subject Key Identifier	Ne	Key Identifier	Šakninio CA viešojo rakto 160 bitų SHA-1 hash reikšmė
CA Version	Ne		Sudaromas sukuriant sertifikatą
Certificate Policies	Ne	Policy Identifier	1.3.6.1.4.1.31912.1.1.1
		Policy Qualifier Id=CPS	<a href="http://nsc.vrm.lt/repository">http://nsc.vrm.lt/repository</a>
Key Usage	Ne		Digital Signature (0), Non-Repudiation (1)
Basic Constraints	Taip		Subject Type=CA Path Length Constraint=None

**NUOSTATŲ SERTIFIKAVIMO TARNYBINĖS STOTIES OCSP PRANEŠIMŲ  
TVIRTINIMO SERTIFIKATO PROFILIS**

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė [paaiškinimas]
Version			2 [V3 trečia versija]
Serial number			sudaromas Root CA
Signature algorithm			sha1RSA
Issuer			CN = Nacionalinis sertifikavimo centras (RooCA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventojų registro tarnyba prie LR VRM - i.k. 188756767 C = LT
Validity			Galiojimo pradžios ir pabaigos datos (notBefore, notAfter) UTC laiku
Subject			CN = NSC OCSP (PolicyCA)) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventojų registro tarnyba prie LR VRM - i.k. 188756767 C = LT
Public key			Viešojo rakto reikšmė (2048 bit) ir parašo formavimo algoritmo identifikatorius (RSA)
Papildomi laukai (extensions)			
Subject Key Identifier	Ne	Key Identifier	Policy CA viešojo rakto 160 bitų SHA-1 hash reikšmė
Authority Key Identifier	Ne		Root CA viešojo rakto 160 bitų SHA-1 hash reikšmė
CA Version	Ne		Sudaromas sukuriant sertifikata
Certificate Policies	Ne	Policy Identifier	1.3.6.1.4.1.31912.1.1.1
		Policy Qualifier Id=CPS	<a href="http://nsc.vrm.lt/repository">http://nsc.vrm.lt/repository</a>
CRL Distribution Points	Ne	Distribution Point Name	URL= <a href="http://nsc.vrm.lt/cdp/RootCA.crl">http://nsc.vrm.lt/cdp/RootCA.crl</a>
Authority Information Access	Ne	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	<a href="http://nsc.vrm.lt/aia/RootCA.crt">http://nsc.vrm.lt/aia/RootCA.crt</a>
Basic Constraints	Taip		Subject Type=CA Path Length Constraint=None
Key Usage	Taip		Digital Signature (0), Non-Repudiation (1)

**DARBINĖS SERTIFIKAVIMO TARNYBINĖS STOTIES OCSP PRANEŠIMŲ  
TVIRTINIMO SERTIFIKATO PROFILIS**

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė [paaiškinimas]
Version			2 [V3 trečia versija]
Serial number			sudaromas Policy CA
Signature algorithm			sha1RSA
Issuer			CN = Nacionalinis sertifikavimo centras (PolicyCA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventoju registro tarnyba prie LR VRM - i.k. 188756767 C = LT
Validity			Galiojimo pradžios ir pabaigos datos (notBefore, notAfter) UTC laiku
Subject			CN = NSC OCSP (IssuingCA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventoju registro tarnyba prie LR VRM - i.k. 188756767 C = LT
Public key			Viešojo rakto reikšmė (2048 bit) ir parašo formavimo algoritmo identifikatorius (RSA)
Papildomi laukai (extensions)			
Subject Key Identifier	Ne	Key Identifier	Issuing CA viešojo rakto 160 bitų SHA-1 hash reikšmė
Authority Key Identifier	Ne		Policy CA viešojo rakto 160 bitų SHA-1 hash reikšmė
CA Version	Ne		Sudaromas sukuriant sertifikatą
Certificate Policies	Ne	Policy Identifier	1.3.6.1.4.1.31912.1.1.1
		Policy Qualifier Id=CPS	<a href="http://nsc.vrm.lt/repository">http://nsc.vrm.lt/repository</a>
CRL Distribution Points	Ne	Distribution Point Name	URL= <a href="http://nsc.vrm.lt/cdp/PolicyCA.crl">http://nsc.vrm.lt/cdp/PolicyCA.crl</a>
Authority Information Access	Ne	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	<a href="http://nsc.vrm.lt/aia/PolicyCA.crt">http://nsc.vrm.lt/aia/PolicyCA.crt</a>
Basic Constraints	Taip		Subject Type=CA Path Length Constraint=None
Key Usage	Taip		Digital Signature (0), Non-Repudiation (1)

### KVALIFIKUOTO SERTIFIKATO PROFILIS

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė [paaiškinimas]
Version			2 [V3 trečia versija]
Serial number			sudaromas Issuing CA
Signature algorithm			sha1RSA
Issuer			CN = Nacionalinis sertifikavimo centras (IssuingCA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventoju registro tarnyba prie LR VRM - i.k. 188756767 C = LT
Validity			Galiojimo pradžios ir pabaigos datos (notBefore, notAfter) UTC laiku
Subject		Common Name	CN = vardas pavarde
		GivenName	G=vardas
		surname	SN=pavardė
		SerialNumber	SERIALNUMBER=asmens kodas
		CountryName	C=LT
Public key			Viešojo rakto reikšmė (2048 bit) ir parašo formavimo algoritmo identifikatorius (RSA)
<b>Papildomi laukai (extensions)</b>			
Subject Directory Attributes	Ne	gender	Lytis, Value=M or F
		dateOfBirth	Gimimo data
		countryOfCitizenship	Pilietybė, Value=LT arba kitos šalies kodas
Subject Key Identifier	Ne	Key Identifier	Asmens viešojo rakto 160 bitų SHA-1 hash reikšmė
Authority Key Identifier	Ne	Key Identifier	Issuing CA viešojo rakto 160 bitų SHA-1 hash reikšmė
Certificate Policies	Ne	Policy Identifier	1.3.6.1.4.1.31912.1.1.1
		Policy Qualifier Id=User Notice	This statement is a statement by the issuer that this certificate is issued as a Qualified certificate according Annex I and II of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, as implemented in the law of the country specified in the issuer field of this certificate. Šis sertifikatas yra kvalifikuotas sertifikatas pagal ES direktyvos 1999/93/EC dėl Bendrijos elektroninio parašo pagrindinių nuostatų I ir II priedėlius ir Elektroninio parašo įstatymą.
		Policy Qualifier Id=CPS	<a href="http://nsc.vrm.lt/repository">http://nsc.vrm.lt/repository</a>

Papildomi laukai	Kritinis	Atributas	Reikšmė [paaiškinimas]
CRL Distribution Points	Ne	Distribution Point Name	URL= <a href="http://nsc.vrm.lt/cdp/IssuingCA.crl">http://nsc.vrm.lt/cdp/IssuingCA.crl</a>
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	<a href="http://nsc.vrm.lt/OCSP/ocspresponder.nsc">http://nsc.vrm.lt/OCSP/ocspresponder.nsc</a>
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	<a href="http://nsc.vrm.lt/aia/IssuingCA.crt">http://nsc.vrm.lt/aia/IssuingCA.crt</a>
Qualified Certificate Statement	Ne	qualified certificate statement ID	<i>Id-etsi-pcs-QcCompliance (0.4.0.1862.1.1)</i>
	Ne	SSCD statement ID	<i>id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)</i>
Key Usage	Taip		<i>Digital Signature (0), Non-Repudiation (1)</i>
Enhanced Key Usage	Ne		<i>Document Signing (1.3.6.1.4.1.311.10.3.12) Secure Email (1.3.6.1.5.5.7.3.4)</i>
Basic Constraints	Taip		<i>Subject Type=End Entity Path Length Constraint=None</i>

**ASMENS ATPAŽINIMO ELEKTRONINĖJE ERDVĖJE SERTIFIKATO PROFILIS**

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė [paaiškinimas]
Version			2 [V3 trečia versija]
Serial number			sudaromas Issuing CA
Signature algorithm			sha1RSA
Issuer			CN = Nacionalinis sertifikavimo centras (IssuingCA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventoju registro tarnyba prie LR VRM - i.k. 188756767 C = LT
Validity			Galiojimo pradžios ir pabaigos datos (notBefore, notAfter) UTC laiku
Subject		Common Name	CN = vardas pavarde
		GivenName	G=vardas
		surname	SN=pavardė
		SerialNumber	SERIALNUMBER=asmens kodas
		CountryName	C=LT
Public key			Viešojo rakto reikšmė (2048 bit) ir parašo formavimo algoritmo identifikatorius (RSA)
<b>Papildomi laukai (extensions)</b>			
Subject Directory Attributes	Ne	gender	Lytis, Value=M or F
		dateOfBirth	Gimimo data
		countryOfCitizenship	Pilietybė, Value=LT arba kitos šalies kodas
		hip	
Subject Key Identifier	Ne	Key Identifier	Asmens viešojo rakto 160 bitų SHA-1 hash reikšmė
Authority Key Identifier	Ne	Key Identifier	Issuing CA viešojo rakto 160 bitų SHA-1 hash reikšmė
Certificate Policies	Ne	Policy Identifier	1.3.6.1.4.1.31912.1.1.1
		Policy Qualifier Id=CPS	<a href="http://nsc.vrm.lt/repository">http://nsc.vrm.lt/repository</a>
CRL Distribution Points	Ne	Distribution Point Name	URL= <a href="http://nsc.vrm.lt/cdp/IssuingCA.crl">http://nsc.vrm.lt/cdp/IssuingCA.crl</a>
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	<a href="http://nsc.vrm.lt/OCSP/ocspreponder.nsc">http://nsc.vrm.lt/OCSP/ocspreponder.nsc</a>
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	<a href="http://nsc.vrm.lt/aia/IssuingCA.crt">http://nsc.vrm.lt/aia/IssuingCA.crt</a>
Application Policies	Ne	Application Certificate Policy	Policy Identifier=Client Authentication
Key Usage	Taip		Digital Signature (0)
Basic Constraints	Taip		Subject Type=End Entity Path Length Constraint=None

**ŠAKNINĖS SERTIFIKAVIMO TARNYBINĖS STOTIES NEGALIOJANČIŲ  
SERTIFIKATŲ SĄRAŠO PROFILIS**

CRL pagrindiniai laukai	Atributas	Reikšmė [paaiškinimas]
Version		1 [V2 antra versija]
Issuer		CN = Nacionalinis sertifikavimo centras (RootCA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventojų registro tarnyba prie LR VRM - i.k. 188756767 C = LT
This update		Išleidimo data ir laikas
Next update		Atnaujinimo data ir laikas
Signature		sha1RSA
Negaliojantys sertifikatai		
userCertificate		Negaliojančio sertifikato serijinis numeris
revocationDate		Galiojimo nutraukimo ar sustabdymo data ir laikas
CRL Plėtiniai		
Authority Key Identifier	Key Identifier	Root CA viešojo rakto hash reikšmė SHA1 algoritmu
CA Version		V0.0
CRL Number		sudaromas Root CA
Next CRL Publish		Kitos versijos publikavimo data

---

**NUOSTATŲ SERTIFIKAVIMO TARNYBINĖS STOTIES NEGALIOJANČIŲ  
SERTIFIKATŲ SĄRAŠO PROFILIS**

CRL pagrindiniai laukai	Atributas	Reikšmė [paaiškinimas]
Version		<i>1 [V2 antra versija]</i>
Issuer		<i>CN = Nacionalinis sertifikavimo centras (Policy CA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventojų registro tarnyba prie LR VRM - i.k. 188756767 C = LT</i>
Effective date		<i>Išleidimo data ir laikas</i>
This update		<i>Atnaujinimo data ir laikas</i>
Signature		<i>sha1RSA</i>
<b>Negaliojantys sertifikatai</b>		
userCertificate		<i>Negaliojančio sertifikato serijinis numeris</i>
revocationDate		<i>Galiojimo nutraukimo ar sustabdymo data ir laikas</i>
<b>CRL Plėtiniai</b>		
Authority Key Identifier	Key Identifier	<i>Policy CA viešojo rakto hash reikšmė SHA1 algoritmu</i>
CA Version		<i>V0.0</i>
CRL Number		<i>sudaromas Policy CA</i>
Next CRL Publish		<i>Kitos versijos publikavimo data</i>

---

**DARBINĖS SERTIFIKAVIMO TARNYBINĖS STOTIES NEGALIOJANČIŲ  
SERTIFIKATŲ SĄRAŠO PROFILIS**

CRL pagrindiniai laukai	Atributas	Reikšmė [paaiškinimas]
Version		1 [V2 antra versija]
Issuer		CN = Nacionalinis sertifikavimo centras (Issuing CA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventojų registro tarnyba prie LR VRM - i.k. 188756767 C = LT
This update		Išleidimo data ir laikas
Next update		Atnaujinimo data ir laikas
Signature		sha1RSA
<b>Negaliojantys sertifikatai</b>		
userCertificate		Negaliojančio sertifikato serijinis numeris
revocationDate		Galiojimo nutraukimo ar sustabdymo data ir laikas
Reason Code		Galiojimo nutraukimo ar sustabdymo priežastis
<b>CRL Plėtiniai</b>		
Authority Key Identifier	Key Identifier	Issuing CA viešojo rakto hash reikšmė SHA1 algoritmu
CA Version		V0.0
CRL Number		sudaromas Issuing CA
Next CRL Publish		Kitos versijos publikavimo data