

PATVIRTINTA
Gyventojų registro tarnybos prie
Lietuvos Respublikos vidaus reikalų
ministerijos direktoriaus 2011 m. sausio 31 d.
įsakymu Nr. (29)4R-10

SERTIFIKAVIMO VEIKLOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Sertifikavimo veiklos nuostatai (toliau – nuostatai) nustato Gyventojų registro tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Gyventojų registro tarnyba), kaip sertifikavimo paslaugų teikėjo, veiklos taisykles, sertifikatų sudarymo ir tvarkymo techninius, procedūrų ir saugumo reikalavimus.

2. Nuostatai įgyvendina Sertifikato taisykles, kurių unikalus identifikatorius yra 1.3.6.1.4.1.31912.1.1.1 bei Valstybės tarnautojo sertifikato taisykles, kurių unikalus identifikatorius yra 1.3.6.1.4.1.31912.1.3.1.

3. Šių nuostatų unikalus identifikatorius yra 1.3.6.1.4.1.31912.1.2.2 (1 priedas).

4. Šiuose nuostatuose vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos elektroninio parašo įstatyme (Žin., 2000, Nr. 61-1827, 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 direktoriaus tvirtinamose Sertifikato taisyklėse bei Valstybės tarnautojo sertifikato taisyklėse.

5. Vadovaujantis šiais nuostatais, yra sudaromi keturių rūšių sertifikatai:

5.1. į asmens tapatybės korteles įrašomi:

5.1.1. kvalifikuotas sertifikatas;

5.1.2. asmens atpažinimo elektroninėje erdvėje sertifikatas.

5.2. į valstybės tarnautojo pažymėjimus įrašomi:

5.2.1. valstybės tarnautojo elektroninio parašo kvalifikuotas sertifikatas;

5.2.2. valstybės tarnautojo atpažinimo elektroninėje erdvėje sertifikatas.

6. Sudaromų sertifikatų sandarą ir paskirtį, elektroninio parašo kūrimą, tikrinimą, galiojimą, parašo naudotojų teises ir atsakomybę, sertifikavimo paslaugas, reikalavimus jų teikėjams bei atsakomybę nustato:

- 6.1. Elektroninio parašo įstatymas;
 - 6.2. Asmens tapatybės kortelės įstatymas;
 - 6.3. 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).
 - 6.4. 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);
 - 6.5. 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).
7. Visiems su sertifikavimo paslaugų teikimu susijusiems santykiams taikoma Lietuvos Respublikos teisė. Visi ginčai, susiję su sertifikatų sudarymu ir tvarkymu, sprendžiami vadovaujantis Lietuvos Respublikos įstatymais.

II. SERTIFIKAVIMO PASLAUGŲ TEIKĖJO ORGANIZACINĖ STRUKTŪRA

8. Vadovaujantis Lietuvos Respublikos vidaus reikalų ministro 2008 m. gruodžio 1 d. įsakymu Nr. 1V-427 „Dėl įgaliojimų suteikimo“, trečiosioms šalims yra perduodamos šios sertifikavimo veiklos funkcijos:
- 8.1. Asmens dokumentų išrašymo centrui prie 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 kontaktinių elektroninių laikmenų aktyvavimo duomenis;
 - 8.2. Informatikos ir ryšių departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas) – sertifikatų sudarymui ir tvarkymui naudojamos techninės įrangos priežiūra;
 - 8.3. 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 kontaktinių elektroninių laikmenų aktyvavimo duomenis. Vilniaus apskrities vyriausiojo policijos komisariato Migracijos valdybą, Alytaus, Kauno, Klaipėdos, Marijampolės, Panevėžio,

Šiaulių, Tauragės, Telšių ir Utenos apskričių vyriausiųjų policijos komisariatų migracijos skyrius sustabdyti ir nutraukti sertifikatų galiojimą, atšaukti jų galiojimo sustabdymą, asmens prašymu atnaujinti sertifikatus, įrašytus asmens tapatybės kortelėse, keisti asmens tapatybės kortelės kontaktinės elektroninės laikmenos aktyvavimo duomenis (slaptažodžius).

9. Vadovaujantis Valstybės tarnautojo pažymėjimo išdavimo taisyklėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2002 m. liepos 11 d. įsakymu Nr. 338 (Žin., 2002, Nr. 77-3309; 2009, Nr. 139-6133), valstybės tarnautojų registravimą sertifikatams gauti atlieka institucijų ar įstaigų, kuriose valstybės tarnautojai eina valstybės tarnautojo pareigas, administracijos struktūrinis padalinys arba valstybės tarnautojas, vykdamas personalo administravimo funkcijas.

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

III. SERTIFIKATŲ SEKOS SUDARYMAS

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

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

11.1.1. nuostatų sertifikavimo tarnybinės stoties sertifikatus;

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

11.1.3. sertifikatus, skirtus tvirtinti iki šakninės sertifikavimo tarnybinės stoties sertifikato atnaujinimo galiojusį šakninės sertifikavimo tarnybinės stoties sertifikatą.

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

11.2.1. darbinės sertifikavimo tarnybinės stoties sertifikatus;

11.2.2. užklausų sistemos teikiamiems pranešimams apie nuostatų sertifikavimo tarnybos stoties išduotų sertifikatų būseną tvirtinti skirtus sertifikatus.

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

11.3.1. šių nuostatų 5 punkte išvardintus sertifikatus;

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

11.3.3. infrastruktūros sertifikatus.

IV. SERTIFIKAVIMO PASLAUGŲ TEIKĖJO IR SERTIFIKATŲ NAUDOTOJŲ PAREIGOS IR ATSAKOMYBĖ

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

V. MOKESČIAI

13. Nemokamai teikiamos šios sertifikavimo paslaugos:

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

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

13.3. sertifikato galiojimo sustabdymas ir nutraukimas.

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

VI. INFORMACIJOS TVARKYMO REIKALAVIMAI

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

15.1. Sertifikatų taisyklės, šie nuostatai, sertifikatų sudarymo ir tvarkymo sąlygos, elektroninio parašo taisyklės;

15.2. už sertifikavimo paslaugas mokamų mokesčių kainininkai;

15.3. vartotojų instrukcijos;

15.4. sertifikavimo paslaugų teikėjui priklausantys sertifikatai;

15.5. negaliojančių sertifikatų sąrašai;

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

16. Konfidenciali informacija yra ši:

16.1. asmens duomenys, išskyrus tuos, kurie atskleidžiami teikiant sertifikavimo paslaugas;

16.2. sertifikavimo paslaugų teikėjo atliktų operacijų įrašai;

16.3. įrašai apie sertifikavimo paslaugų sutrikimus;

16.4. informacija apie veiklos patikrinimus, jei jos paskelbimas kelia grėsmę sertifikavimo veiklos saugumui;

16.5. veiksmų, įvykus avarijai, planai;

16.6. informacija apie techninės ir programinės įrangos apsaugą ir sertifikavimo paslaugų

operacijų atlikimą.

17. Konfidenciali informacija saugoma ir tvarkoma sertifikavimo paslaugų teikėjo vidaus taisyklių nustatyta tvarka.

18. Konfidenciali informacija teisėsaugos institucijoms teikiama Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatyta tvarka.

19. 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) nustatyta tvarka.

20. Sertifikatų savininkai susipažįsta su sertifikate nurodoma informacija ir patvirtina, kad sutinka su jos naudojimu atitinkamose sertifikato taisyklėse ir šiuose nuostatuose nustatyta tvarka.

21. Sertifikatų savininkams sudaromi sertifikatai viešai neskelbiami ir jų paieška negalima.

22. Sertifikavimo paslaugų teikėjo teikiama informacija turi būti atnaujinama:

22.1. nuostatai keičiami, tvirtinami ir skelbiami šių nuostatų XII skyriuje nustatyta tvarka;

22.2. negaliojančių sertifikatų sąrašas atnaujinamas periodiškai, šių nuostatų 66-67 punktuose nustatytais terminais;

22.3. kita informacija skelbiama ją patvirtinus.

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

23. Ne rečiau kaip kartą per vienerius metus turi būti tikrinama, ar sertifikavimo paslaugų teikėjo vykdoma veikla atitinka Sertifikato taisyklių ir Sertifikavimo veiklos nuostatų reikalavimus.

24. Vidinį sertifikavimo veiklos tikrinimą atlieka sertifikavimo paslaugų teikėjo auditorius ir saugumo pareigūnas. Išorinis patikrinimas vykdomas teisės aktų nustatyta tvarka.

25. Sertifikavimo paslaugų teikėjo veiklai įvertinti yra tikrinama:

25.1. fizinis saugumas;

25.2. programinės įrangos ir sertifikatų valdymo sistemos kompiuterių tinklo saugumas;

25.3. sertifikavimo paslaugos ir jų teikimo procedūros;

25.4. registracijos žurnalų ir sertifikatų valdymo sistemos priežiūros procedūros;

25.5. informacijos atsarginių kopijų darymas;

25.6. archyvų tvarkymo procedūros;

25.7. įrašai apie techninės ir programinės įrangos tikrinimą ir priežiūrą.

26. Per 30 kalendorinių dienų nuo sertifikavimo paslaugų teikėjo veiklos patikrinimo saugumo pareigūnas turi:

26.1. raštu pareikšti savo nuomonę dėl patikrinimo protokole išdėstytų trūkumų;

- 26.2. numatyti trūkumų pašalinimo veiksmus ir terminus;
- 26.3. informaciją apie trūkumų pašalinimą pateikti sertifikavimo paslaugų teikėjo veiklą tikrinusiai organizacijai.
27. Tikrinimų išvados skelbiamos sertifikavimo paslaugų teikėjo interneto svetainėje.

VIII. SERTIFIKATŲ SAVININKAMS SUDAROMŲ SERTIFIKATŲ GYVAVIMO CIKLO VALDYMAS

I. SERTIFIKATŲ SUDARYMAS IR IŠDAVIMAS

28. Sertifikatų savininkams sertifikatai išduodami ir naudojami tik kartu su asmens tapatybės kortele arba valstybės tarnautojo pažymėjimu, kurie atitinka technologinius saugios elektroninio parašo formavimo įrangos reikalavimus. Asmens tapatybės kortelės arba valstybės tarnautojo pažymėjimo kontaktinėje elektroninėje laikmenoje generuojami parašo formavimo ir tikrinimo duomenys bei saugomi sertifikatai.

29. Į asmens tapatybės kortelės įrašomi sertifikatai pirmą kartą išduodami 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. Sertifikatai atnaujinami, vadovaujantis Asmenų registravimo sertifikatams gauti ir asmenų konsultavimo taisyklių, tvirtinamų Gyventojų registro tarnybos direktoriaus įsakymu, nustatyta tvarka.

30. Į valstybės tarnautojo pažymėjimus sertifikatai įrašomi, vadovaujantis Valstybės tarnautojo pažymėjimo išdavimo taisyklėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2002 m. liepos 11 d. įsakymu Nr. 338 (Žin., 2002, Nr. 77-3309; 2009, Nr. 139-6133). Sertifikatai atnaujinami, vadovaujantis Valstybės tarnautojų registravimo sertifikatams gauti ir konsultavimo taisyklių, tvirtinamų Gyventojų registro tarnybos direktoriaus įsakymu, nustatyta tvarka.

31. Prieš sudarant ir išduodant sertifikatus, būsimam sertifikatų savininkui pateikiamos sertifikatų sudarymo ir tvarkymo sąlygos.

32. Atsiimdamas asmens tapatybės kortelę, asmuo pasirašo prašymo asmens tapatybės kortelei gauti formoje, patvirtindamas, kad susipažino ir sutinka su sertifikatų sudarymo ir tvarkymo sąlygomis bei prisiima visus jose nustatytus įsipareigojimus ir atsakomybę. Atnaujinant asmens tapatybės kortelėje įrašytus sertifikatus su asmeniu yra sudaroma sutartis dėl sertifikavimo paslaugų teikimo (naujų sertifikatų sudarymo).

33. Atsiimdamas valstybės tarnautojo pažymėjimą, valstybės tarnautojas pasirašo prašymo išduoti valstybės tarnautojo pažymėjimą formoje, kad susipažino ir sutinka su valstybės tarnautojo sertifikatų sudarymo ir tvarkymo sąlygomis, gavo valstybės tarnautojo pažymėjimą bei šio

pažymėjimo kontaktinės elektroninės laikmenos aktyvavimo duomenis (slaptažodį). Atnaujinant valstybės tarnautojo pažymėjime įrašytus sertifikatus valstybės tarnautojas pasirašo prašymo atnaujinti sertifikatus valstybės tarnautojo pažymėjimą formoje, kad susipažino ir sutinka su valstybės tarnautojo sertifikatų sudarymo ir tvarkymo sąlygomis, gavo valstybės tarnautojo pažymėjimą bei šio pažymėjimo kontaktinės elektroninės laikmenos aktyvavimo duomenis (slaptažodį).

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

35. Visi asmenims sudarytuose sertifikatuose nurodyti vardai yra unikalūs. Asmens unikalus identifikatorius asmens tapatybės kortelėje įrašomuose sertifikatuose yra asmens kodas. Valstybės tarnautojo unikalus identifikatorius valstybės tarnautojo pažymėjime įrašomuose sertifikatuose yra valstybės tarnautojo kodas.

36. Sertifikatų savininkams sudaromuose sertifikatuose nurodyti vardai sudaromi laikantis X.500 standarto rekomendacijų.

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

II. SERTIFIKATŲ SUDARYMAS IR ASMENS TAPATYBĖS KORTELĖS (VALSTYBĖS TARNAUTOJO PAŽYMĖJIMO) KEITIMAS

37. Asmens tapatybės kortelė keičiama ir nauji sertifikatai sudaromi:

37.1. kai išduodant asmens tapatybės kortelę nustatoma, kad sertifikatuose įrašyti asmens duomenys yra neteisingi;

37.2. Asmens tapatybės kortelės įstatymo 5 straipsnio 5 punkte minimais atvejais.

38. Asmens tapatybės kortelės keitimo procedūra atliekama Asmens tapatybės kortelės išdavimo, keitimo, paskelbimo negaliojančia ir naikinimo tvarkos aprašo nustatyta tvarka. Kartu su nauja asmens tapatybės kortele išduodami ir nauji sertifikatai.

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

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

39.2. 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 nustatytos formos prašymą. Jei senų sertifikatų galiojimas dar nėra pasibaigęs, sertifikato savininkas pirma turi pateikti prašymą nutraukti senų sertifikatų galiojimą.

40. Nauji sertifikatai nekeičiant valstybės tarnautojo pažymėjimo sudaromi:

40.1. kai sudarant sertifikatus dėl Sertifikavimo paslaugų teikėjo kaltės buvo padaryta klaidų;

40.2. kai pasikeičia valstybės tarnautojo pareigos;

40.3. kai baigiasi sertifikatų galiojimo terminas ir valstybės tarnautojo pažymėjimas dar yra galiojantis;

40.4. kai sertifikatų galiojimas nutraukiamas dėl parašo formavimo duomenų arba valstybės tarnautojo pažymėjimo elektroninės laikmenos aktyvavimo duomenų atskleidimo ir valstybės tarnautojo pažymėjimas nėra prarastas ar pamestas.

41. Tokie sertifikatų atnaujinimo būdai, kaip naujų duomenų įrašymas į asmeniui išduotą sertifikatą ar naujo sertifikato išdavimas nekeičiant sertifikatą atitinkančių parašo formavimo ir tikrinimo duomenų, pagal šiuos nuostatus sudaromiems sertifikatams netaikomi. Visais atvejais sudaromas naujas sertifikatas.

III. SERTIFIKATO GALIOJIMO NUTRAUKIMAS

42. Sertifikato galiojimas nutraukiamas šiais atvejais:

42.1. gavus sertifikato savininko prašymą;

42.2. sertifikato duomenims tapus neteisingais ar paaiškėjus, kad sudarant sertifikatą buvo

panaudoti neteisingi duomenys;

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

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

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

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

42.7. sertifikato savininkui tapus neveiksniam;

42.8. sertifikato savininkui mirus;

42.9. sertifikato savininkui pažeidus elektroninio parašo naudojimą reglamentuojančius teisės aktus arba sutarties su sertifikavimo paslaugų teikėju sąlygas;

42.10. kitais įstatymų numatytais atvejais.

43. Prašymai nutraukti sertifikato galiojimą teikiami šių nuostatų 55-56 punktuose nustatyta tvarka. Sertifikavimo paslaugų teikėjas nutraukia sertifikato galiojimą iškart po prašymo patikrinimo. Atlikus sertifikato galiojimo nutraukimo operaciją, sertifikato savininkas informuojamas apie pasikeitusį sertifikato statusą.

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

45. Sertifikatų galiojimas yra automatiškai nutraukiamas visais atvejais, nustojus galioti asmens tapatybės kortelei (valstybės tarnautojo pažymėjimui), kurioje sertifikatai įrašyti.

IV. SERTIFIKATO GALIOJIMO SUSTABDYMAS

46. Sertifikato galiojimas sustabdomas šiais atvejais:

46.1. gavus sertifikato savininko prašymą;

46.2. teisėsaugos institucijų reikalavimu, siekiant užkirsti kelią nusikaltimams;

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

47. Prašymus sustabdyti sertifikato galiojimą gali teikti:

47.1. sertifikato savininkas;

47.2. teisėsaugos institucijos.

48. Prašymai sustabdyti sertifikato galiojimą teikiami šių nuostatų 57-60 punktuose nustatyta tvarka. Sertifikato galiojimas sustabdomas iškart po prašymo patikrinimo. Atlikus sertifikato galiojimo sustabdymo operaciją, sertifikato savininkas informuojamas apie pasikeitusį

sertifikato statusą.

49. 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.

50. 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 61 punkte nustatyta tvarka. Sertifikato galiojimo sustabdymas atšaukiamas iškart po prašymo patikrinimo. Atlikus sertifikato galiojimo sustabdymo atšaukimo operaciją, sertifikato savininkas informuojamas apie pasikeitusį sertifikato statusą.

51. Jei sertifikato galiojimas buvo sustabdytas sertifikato savininko prašymu, prašyme atšaukti sertifikato galiojimo sustabdymą sertifikato savininkas privalo raštu patvirtinti, kad sertifikato galiojimo sustabdymo laikotarpiu jis nebuvo praradęs nei privačiojo kriptografinio rakto, nei privačiojo kriptografinio rakto aktyvavimo duomenų kontrolės.

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

IX. SERTIFIKAVIMO VEIKLOS REIKALAVIMAI

I. PRAŠYMUS TEIKIANČIŲ ASMENŲ IDENTIFIKAVIMAS

Asmens tapatybės tikrinimas, prašant sudaryti sertifikatą, kai asmens tapatybės kortelė (valstybės tarnautojo pažymėjimas) nekeičiama

53. Prašymą sudaryti sertifikatą pagal šių nuostatų 39 punktą asmens tapatybės kortelėje įrašyto sertifikato savininkas gali pateikti tik asmeniškai atvykęs į registravimo tarnybą ir pateikęs asmens tapatybės kortelę. Prašymą sudaryti sertifikatą pagal šių nuostatų 40 punktą valstybės tarnautojas gali pateikti tik asmeniškai atvykęs į personalo administravimo tarnybą ir pateikęs valstybės tarnautojo pažymėjimą.

54. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

54.1. patikrinamas prašymą teikiančio asmens veido ir asmens tapatybės kortelėje (valstybės tarnautojo pažymėjime) esančio veido atvaizdo vizualinis atitikimas;

54.2. patikrinamas asmens tapatybės kortelės (valstybės tarnautojo pažymėjimo) tikrumas ir galiojimas;

54.3. patikrinama, ar prašyme nurodyti duomenys ir asmens tapatybės kortelės (valstybės tarnautojo pažymėjimo) duomenys sutampa;

54.4. atnaujinant asmens tapatybės kortelėse įrašytus sertifikatus, prašyme pateikta

informacija palyginama su Lietuvos Respublikos gyventojų registro duomenų centrinės bazės (toliau – Gyventojų registras) informacija.

Sertifikato galiojimą nutraukti prašančio asmens tapatybės tikrinimas

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

55.1. patikrinamas prašymą teikiančio asmens veido ir asmens tapatybę įrodančiame dokumente esančio veido atvaizdo vizualinis atitikimas;

55.2. patikrinamas pateiktų dokumentų tikrumas ir galiojimas;

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

55.4. nutraukiant asmens tapatybės kortelėse įrašytų sertifikatų galiojimą, prašyme pateikta informacija palyginama su Gyventojų registro informacija.

56. Prašymą nutraukti valstybės tarnautojo pažymėjime įrašyto sertifikato galiojimą sertifikato savininkas gali pateikti Gyventojų registro tarnybos Sertifikatų tvarkymo skyriui telefonu. Šiuo atveju jis turi nurodyti 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 1 dalyje minimus duomenis.

Sertifikato galiojimą sustabdyti prašančio asmens tapatybės tikrinimas

57. Prašymą sustabdyti sertifikato galiojimą asmens tapatybės kortelėje įrašyto sertifikato savininkas gali pateikti registravimo tarnybai raštu arba paskambinęs telefonu į Gyventojų registro tarnybos Sertifikatų tvarkymo skyrių. Valstybės tarnautojams sudaromų sertifikatų galiojimo laikinas sustabdymas nėra atliekamas.

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

59. Kai prašymą sustabdyti asmens tapatybės kortelėje įrašyto sertifikato galiojimą sertifikato savininkas pateikia Gyventojų registro tarnybos Sertifikatų tvarkymo skyriui telefonu, jis turi nurodyti 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 1 dalyje minimus duomenis.

60. Kai sertifikato galiojimą sustabdyti reikalauja teisėsaugos institucija, ji turi pateikti prašymą, kuriame turi būti nurodyta sertifikato, kurio galiojimas sustabdomas, savininko duomenys

ir galiojimo sustabdymo priežastys.

Sertifikato galiojimo sustabdymą atšaukiančio asmens tapatybės tikrinimas

61. Prašymą atšaukti sertifikato galiojimo sustabdymą asmens tapatybės kortelėje įrašyto sertifikato savininkas gali pateikti tik asmeniškai atvykęs į registravimo tarnybą ir pateikęs asmens tapatybę įrodantį dokumentą. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

61.1. patikrinamas prašymą teikiančio asmens veido ir asmens tapatybę įrodančiame dokumente esančio veido atvaizdo vizualinis atitikimas;

61.2. patikrinamas asmens tapatybę įrodančio dokumento tikrumas ir galiojimas;

61.3. patikrinama, ar prašyme nurodyti duomenys ir asmens tapatybę įrodančio dokumento duomenys sutampa;

61.4. atšaukiant asmens tapatybės kortelėse įrašytų sertifikatų galiojimo sustabdymą, prašyme pateikta informacija palyginama su Gyventojų registro informacija.

Asmens tapatybės tikrinimas, kai išduodami nauji asmens tapatybės kortelės kontaktinės elektroninės laikmenos aktyvavimo duomenys

62. Prašymą keisti asmens tapatybės kortelės kontaktinės elektroninės laikmenos aktyvavimo duomenis sertifikato savininkas gali pateikti tik asmeniškai atvykęs į registravimo tarnybą ir pateikęs asmens tapatybės kortelę. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

62.1. patikrinamas prašymą teikiančio asmens veido ir asmens tapatybės kortelėje esančio veido atvaizdo vizualinis atitikimas;

62.2. patikrinamas asmens tapatybės kortelės tikrumas ir galiojimas;

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

62.4. kai keičiami asmens tapatybės kortelės kontaktinės elektroninės laikmenos aktyvavimo duomenys, prašyme pateikta informacija palyginama su Gyventojų registro informacija.

II. SERTIFIKATO SUDARYMAS

63. Sertifikavimo paslaugų teikėjas užtikrina, kad:

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

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

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

63.4. 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;

63.5. saugi parašo formavimo įranga sertifikato savininkui perduodama saugiai;

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

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

III. SERTIFIKATŲ STATUSO TIKRINIMAS IR NEGALIOJANČIŲ SERTIFIKATŲ SĄRAŠŲ SKELBIMAS

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

65. 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.

66. 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 nuo paskutinio darbinės sertifikavimo tarnybinės stoties negaliojančių sertifikatų sąrašo atnaujinimo įvykę sertifikatų statuso pokyčiai.

67. Šakninės ir nuostatų sertifikavimo tarnybinių stočių negaliojančių sertifikatų sąrašas atnaujinamas kas 3 mėnesius, negaliojančių sertifikatų sąrašų persidengimo periodas – 3 savaitės.

68. Skelbiamoje aktualioje negaliojančių sertifikatų sąrašo versijoje nurodomas kitos versijos paskelbimo laikas. Negaliojančių sertifikatų sąrašai yra tvirtinami sąrašą sudariusios sertifikavimo tarnybinės stoties elektroniniu parašu.

IV. PRIVAČIOJO KRIPTOGRAFINIO RAKTO AKTYVAVIMO DUOMENŲ VALDYMAS

69. Privačiojo kriptografinio rakto aktyvavimo duomenys pateikiami išduodant sertifikatą.

Išduodant naują sertifikatą, visais atvejais sudaromi ir nauji privačiojo kriptografinio rakto aktyvavimo duomenys.

70. Prašymai sudaryti naujus asmens tapatybės kortelėje esančių privačiųjų kriptografinių raktų aktyvavimo duomenis teikiami šių nuostatų 62 punkte nustatyta tvarka. Nauji privačiųjų kriptografinių raktų aktyvavimo duomenys sudaromi iškart, tik gavus prašymą. Valstybės tarnautojo pažymėjime esančių privačiųjų kriptografinių raktų aktyvavimo duomenys yra keičiami tik atnaujinant sertifikatus valstybės tarnautojo pažymėjime.

V. DUOMENŲ APIE SERTIFIKAVIMO VEIKLĄ KAUPIMAS

71. Sertifikavimo paslaugų teikėjas, priimdamas ir tenkindamas asmenų prašymus, kaupia šiuos dokumentus:

71.1. prašymus sustabdyti arba nutraukti sertifikato galiojimą, atšaukti sertifikato galiojimo sustabdymą, keisti asmens tapatybės kortelės kontaktinės elektroninės laikmenos aktyvavimo duomenis (slaptažodį), atnaujinti asmens tapatybės kortelėje (valstybės tarnautojo pažymėjime) įrašytus sertifikatus;

71.2. sertifikavimo paslaugų teikimo sutartis.

72. Sertifikavimo paslaugų teikėjas veda sertifikatų valdymo sistemos techninės priežiūros žurnalą, kuriame yra fiksuojami:

72.1. visi sertifikavimo paslaugų teikėjo naudojamos kriptografinės įrangos gyvavimo ciklo įvykiai;

72.2. visi sertifikavimo paslaugų teikėjo kriptografinių raktų gyvavimo ciklo įvykiai;

72.3. visi sertifikavimo paslaugų teikėjo sertifikatų gyvavimo ciklo įvykiai;

72.4. visi sertifikatų valdymo sistemos konfigūracijos pakeitimai;

72.5. visi sertifikatų valdymo sistemos darbo sutrikimai ir sutrikimų šalinimo aprašymai.

73. Sertifikatų valdymo sistemoje yra automatiškai pildomas elektroninis sistemos audito žurnalas, kuriame fiksuojami:

73.1. asmenims sudarytų sertifikatų gyvavimo ciklo įvykiai;

73.2. negaliojančių sertifikatų sąrašų generavimo ir publikavimo įvykiai.

74. Sistemos audito žurnalas nuo pakeitimų yra apsaugomas infrastruktūriniu sertifikavimo paslaugų teikėjo elektroniniu parašu.

75. Sertifikatų valdymo sistemoje yra automatiškai pildomas elektroninis sistemos saugumo diagnostikos žurnalas, kuriame yra fiksuojami visi su sistemos saugumu susiję įvykiai.

76. Elektroninių žurnalų įrašai peržiūrimi ne rečiau kaip kartą per savaitę. Kiekvienas didesnės reikšmės įvykis turi būti papildomai aprašytas sistemos techninės priežiūros žurnale.

77. Sistemos audito, sistemos saugumo diagnostikos ir kitus elektroninius žurnalus

peržiūrėti gali tik sistemos administratorius, saugumo pareigūnas ir auditorius.

VI. DUOMENŲ ATSARGINIŲ KOPIJŲ DARYMAS IR DUOMENŲ ARCHYVAVIMAS

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

- 78.1. operacinių sistemų konfigūracijos duomenų kopijos;
- 78.2. pilnos operacinių sistemų kopijos;
- 78.3. sertifikatų duomenų bazės kopijos;
- 78.4. negaliojančių sertifikatų sąrašų kopijos;
- 78.5. sistemos audito žurnalo kopijos.

79. Sertifikavimo paslaugų teikėjas Lietuvos Respublikos dokumentų ir archyvų įstatymo (Žin., 1995, Nr. 107-2389; 2004, Nr. 57-1982, toliau – Dokumentų ir archyvų įstatymas) nustatyta tvarka saugo šiuos duomenis:

- 79.1. asmenų prašymų registravimo duomenis;
- 79.2. sistemos audito, sistemos saugumo diagnostikos ir sertifikatų valdymo sistemos techninės priežiūros žurnalus;
- 79.3. pasibaigusio galiojimo sertifikatų duomenis;
- 79.4. negaliojančių sertifikatų sąrašus;

80. Šių nuostatų 79 punkte nustatyti duomenys sertifikavimo paslaugų teikėjo archyve saugomi 10 metų, tolesnis jų saugojimas užtikrinamas Dokumentų ir archyvų įstatymo nustatyta tvarka.

VII. SERTIFIKAVIMO VEIKLOS GRĖSMIŲ VALDYMAS

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

- 81.1. fiziniai sistemų pažeidimai;
- 81.2. programinės įrangos veiklos sutrikimai;
- 81.3. išorinių telekomunikacijų ir elektros tinklų funkcionavimo sutrikimai;
- 81.4. vidinių kompiuterių tinklų sutrikimai.

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

- 82.1. Veiklos atkūrimas:
 - 82.1.1. turi būti periodiškai daromos sistemų duomenų bazių, programinės įrangos ir kitų duomenų atsarginės kopijos;
 - 82.1.2. 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.

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

82.3. Elektros tiekimo užtikrinimas. Naudojami atsarginiai elektros energijos šaltiniai (nenutrūkstamo maitinimo šaltinis (UPS) ir dyzelinis elektros generatorius), kurie elektros energiją sistemai gali tiekti 24 valandas.

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

83.1. iš naujo suteikti prieigos prie sistemos teises;

83.2. informuoti sistemos naudotojus apie sistemos atstatymą.

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

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

84.2. kompromituotą privatųjį raktą atitinkantis sertifikavimo paslaugų teikėjo sertifikatas įrašomas į negaliojančių sertifikatų sąrašą.

VIII. SERTIFIKAVIMO PASLAUGŲ TEIKĖJO VEIKLOS NUTRAUKIMAS

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

85.1. ne vėliau kaip prieš vieną mėnesį iki sertifikavimo veiklos nutraukimo apie tai informuos visus sertifikatų savininkus ir elektroninio parašo priežiūros instituciją;

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

X. SAUGUMO PRIEMONĖS

I. FIZINIO SAUGUMO PRIEMONĖS

86. Sertifikatų valdymo sistemos pagrindinė įranga saugoma Informatikos ir ryšių

departamento tarnybinių stočių saugykloje, esančioje Asmens dokumentų išrašymo centre adresu Žirmūnų g.1 D, LT-09229 Vilnius.

87. Sertifikatų valdymo sistemos atsarginė ir testavimo sistemos įranga saugomos Informatikos ir ryšių departamento tarnybinių stočių saugykloje adresu Šventaragio g. 2, LT-01510 Vilnius.

88. Sertifikatų valdymo sistemos pagrindinės įrangos saugumas yra užtikrinamas šiomis priemonėmis:

88.1. saugyklos patalpos yra sugriežtintos apsaugos zona, jas visą parą saugo budėtojas;

88.2. saugyklos patalpose įrengta vaizdo stebėjimo sistema;

88.3. saugyklos patalpose įdiegta biometrinė įėjimo kontrolės sistema: asmeniui identifikuoti naudojami asmens biometriniai duomenys;

88.4. Į saugyklą teisę patekti turi tik sertifikatų valdymo sistemos saugumo pareigūnas, sertifikatų valdymo sistemos auditorius ir sertifikatų valdymo sistemos administratorius. Kiti asmenys į saugyklą gali patekti tik lydimi minėtas pareigas einančių darbuotojų. Kiekvienas patekimas į saugyklą registruojamas techninėmis priemonėmis. Taip pat yra vedamas elektroninis žurnalas.

89. Sertifikatų valdymo sistemos atsarginės įrangos saugumas yra užtikrinamas šiomis priemonėmis:

89.1. saugyklos patalpos yra sugriežtintos apsaugos zona, jas visą parą saugo budėtojas;

89.2. saugyklos patalpose įrengta vaizdo stebėjimo sistema;

89.3. saugyklos patalpose įdiegta įėjimo kontrolės sistema: asmeniui identifikuoti naudojamos elektroninės identifikavimo kortelės;

89.4. Į saugyklą teisę patekti turi tik sertifikatų valdymo sistemos saugumo pareigūnas, sertifikatų valdymo sistemos auditorius ir sertifikatų valdymo sistemos administratorius. Kiti asmenys į šią zoną patekti gali tik lydimi minėtas pareigas einančių darbuotojų. Kiekvienas patekimas į saugyklą registruojamas techninėmis priemonėmis. Taip pat yra vedamas elektroninis žurnalas.

90. Sertifikatų valdymo sistemos saugyklose yra įrengta oro kondicionavimo sistema, palaikanti reikiamą vienodą temperatūrą. Sutrikus elektros energijos tiekimui, nenutrūkstamo maitinimo šaltinis (UPS) ir dyzelinis elektros generatorius iki 24 valandų užtikrina nepertraukiamą sistemos darbą.

91. Sertifikatų valdymo sistemos pagrindinės įrangos saugykla yra apsaugota nuo potvynio ar užpylimo vandeniu.

92. Sertifikatų valdymo sistemos pagrindinės ir atsarginės įrangos saugyklų patalpose įdiegta inertines dujas naudojanti priešgaisrinės apsaugos sistema, atitinkanti priešgaisrinės saugos

reikalavimus.

93. Laikmenos su archyvų duomenimis ir atsarginėmis kopijomis saugomos atsarginės įrangos saugyklos patalpose.

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

II. PERSONALO SAUGUMO PRIEMONĖS

95. Už sertifikatų valdymo sistemos techninę priežiūrą atsakingi darbuotojai eina aukštos atsakomybės pareigas. 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:

95.1. 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;

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

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

95.4. sistemos auditorius, įgaliotas peržiūrėti sertifikavimo paslaugų teikėjo sistemų archyvus ir audito įrašus.

96. Sertifikavimo paslaugų teikėjo naudojamos kriptografinės įrangos instaliavimas, valdymas, diagnostika, remontas bei deinstaliavimas atliekami dalyvaujant mažiausiai dviem už sertifikatų valdymo sistemos techninę priežiūrą atsakingiems asmenims.

97. Atliekant sertifikavimo paslaugų teikimo veiklos kritines operacijas dalyvauja mažiausiai 3 asmenys, tarp kurių visada turi būti saugumo pareigūnas.

98. Kritinės operacijos apima visas su sertifikavimo paslaugų teikėjo sertifikatų ir kriptografinių raktų gyvavimo ciklo valdymu susijusias operacijas.

99. Sertifikavimo paslaugų teikėjas taiko šias aukštos atsakomybės darbuotojų teisių administravimo priemones:

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

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

99.3. užtikrina teisių valdymą sertifikavimo paslaugų teikėjo informacinėse sistemose;

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

100. Sertifikavimo paslaugų teikėjas užtikrina, kad jo darbuotojai:

100.1. turi aukštąjį išsilavinimą;

100.2. yra išklause su jų pareigų vykdymu susijusius kvalifikacijos kursus;

100.3. yra išklause asmens duomenų ir informacijos apsaugos mokymus;

100.4. nebuvo teisti.

101. Sertifikavimo paslaugų teikėjo darbuotojų biografija tikrinama laikantis Lietuvos Respublikos įstatymų.

102. Sertifikavimo paslaugų teikėjo ir registravimo tarnybų darbuotojai turi būti išklause mokymus ir susipažinę su šia informacija:

102.1. taisyklėmis, nuostatais, sertifikatų sudarymo ir tvarkymo sąlygomis, asmenų registravimo ir konsultavimo taisyklėmis;

102.2. sistemos veikimo sutrikimo atvejais atliekamų veiksmų aprašais.

103. Darbuotojai pasirašytinai patvirtina, kad susipažino su šių nuostatų 102 punkte nurodyta informacija ir sutinka su jiems keliamais reikalavimais ir nustatytais pareigomis.

104. Papildomi sertifikavimo paslaugų teikėjo darbuotojų mokymai vykdomi, kai yra įgyvendinti svarbesni veiklos pakeitimai.

105. Užduotims sertifikatų valdymo sistemos patalpose atlikti samdomus asmenis turi lydėti sertifikavimo paslaugų teikėjo darbuotojas.

III. TECHNINIO SAUGUMO PRIEMONĖS

106. Sertifikavimo paslaugų teikėjo 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 sistemos techninės priežiūros žurnale, pasirašant visiems procedūroje dalyvavusiems asmenims.

107. Sertifikatų savininkams sudaromus sertifikatus atitinkančias kriptografinių raktų poras 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.

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

109. Saugioje parašo formavimo įrangoje generuotas asmens viešasis kriptografinis raktas

saugiomis ryšio priemonėmis perduodamas darbinei sertifikavimo tarnybinei stočiai, kuri sudaro sertifikatą.

110. Sertifikavimo paslaugų teikėjo viešieji kriptografiniai raktai yra įrašyti į sertifikavimo paslaugų teikėjui priklausančius sertifikatus, kurie skelbiami sertifikavimo paslaugų teikėjo interneto svetainėje.

111. Sertifikavimo paslaugų teikėjas generuoja tokio ilgio raktus:

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

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

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

111.4. Asmenims generuojamų raktų ilgis – 2048 bitai.

112. Šakninė sertifikavimo tarnybinė stotis ir nuostatų sertifikavimo tarnybinė stotis bei su jomis susieti kriptografiniai saugumo moduliai, kuriuose saugomi šių stočių privatieji kriptografiniai raktai, yra visada atjungti nuo kompiuterių tinklo. Šakninė sertifikavimo tarnybinė stotis ir nuostatų sertifikavimo tarnybinė stotis bei su jomis susieti kriptografiniai saugumo moduliai yra laikomi išjungti ir įjungiami tik atliekant kritines operacijas arba diegiant operacinių sistemų atnaujinimus.

113. Sertifikavimo paslaugų teikėjo privatieji kriptografiniai raktai nearchyvuojami. Pasibaigus galiojimo terminui, šie raktai sunaikinami.

114. Sertifikavimo paslaugų teikėjo kriptografinių raktų kopijos yra šifruojamos, šifravimo raktas yra padalinamas į dalis ir saugomas specialiose, su kriptografinė įranga susietose lustinėse kortelėse.

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

116. Kriptografinių raktų galiojimo terminai yra šie:

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

116.2. Nuostatų sertifikavimo tarnybinės stoties rakto galiojimo – 12 metų.

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

116.4. Sertifikatų savininkams sudaromų raktų galiojimo – 3 metai.

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

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

117.2. priemonės, įgalinančios atskirti sistemoje leistinas pareigas;

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

117.4. kriptografinės informacijos apsaugos priemonės, kai ši informacija perduodama

tinklu;

117.5. nesankcionuotos priegos prie kompiuterinių išteklių valdymo ir informavimo priemonės.

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

119. Kuriant papildomas sertifikavimo paslaugų teikėjo sistemas laikomasi visų sertifikato taisyklių ir pokyčių valdymo reikalavimų. Kiekvienas naujas programinės įrangos modulis ar techninė įranga išbandoma testavimo aplinkoje ir sertifikavimo paslaugoms teikti pradami naudoti tik gavus saugumo pareigūno patvirtinimą.

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

121. Sertifikavimo paslaugų teikėjo kompiuterių tinklas padalintas į kelis lygmenis, kiekvienam iš jų taikomi atskiri priegos ir saugumo reikalavimai. Kiekvienas tinklo lygmuo apsaugotas ugniasiene.

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

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

122.2. kriptografinis saugumo modulis nebuvo pažeistas sandėliuojant;

122.3. kriptografinis saugumo modulis veikia tinkamai.

XI. SERTIFIKATŲ IR NEGALIOJANČIŲ SERTIFIKATŲ SĄRAŠŲ PROFILIAI

123. Sertifikatų ir negaliojančių sertifikatų sąrašų profiliai nustatyti šių nuostatų 4–16 prieduose.

XII. SERTIFIKAVIMO VEIKLOS NUOSTATŲ ADMINISTRAVIMAS

124. 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.

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

126. Nuostatų pakeitimai gali būti:

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

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

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

128. Kitais atvejais pakeitimai yra esminiai. Visais atvejais, kai nuostatų pakeitimai yra susiję su sertifikavimo paslaugų saugumo lygio keitimu, nuostatų pakeitimai yra esminiai.

129. 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 tolesni skaitmenys.

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

130.1. nuostatų pakeitimus gali inicijuoti sertifikavimo paslaugų teikėjas arba sertifikatu naudotojai;

130.2. už saugumo politiką atsakingi sertifikavimo paslaugų teikėjo darbuotojai:

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

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

130.2.3. priima sprendimą teikti tvirtinti naują nuostatų redakciją;

130.3. 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;

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

130.5. parengus naują nuostatų redakciją, visada yra patikrinamas jos atitikimas šių nuostatų 2 punkte išvardintų sertifikato taisyklių aktualioms redakcijoms;

130.6. nuostatų naują redakciją tvirtina sertifikavimo paslaugų teikėjo vadovas.

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

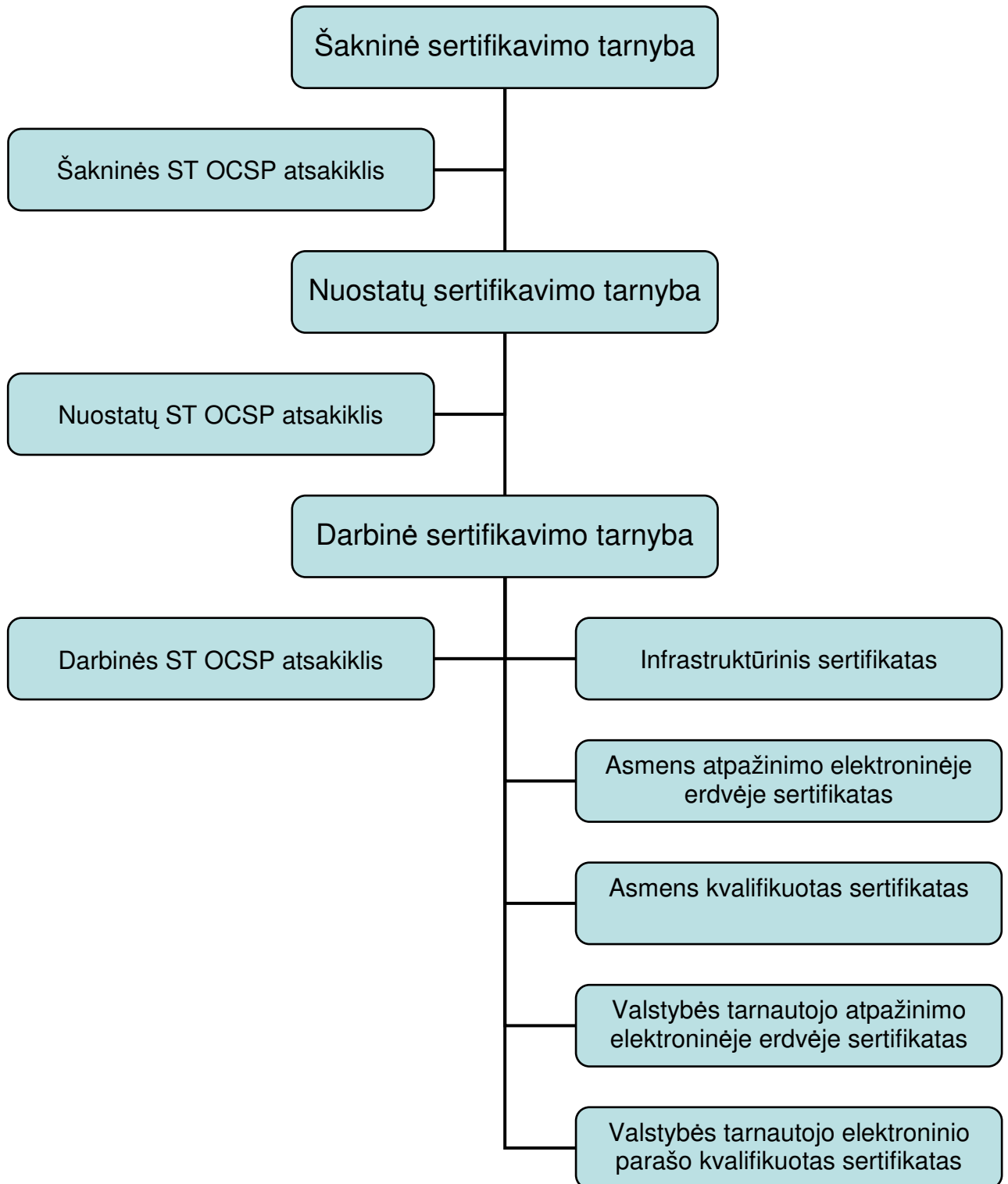
**SERTIFIKAVIMO VEIKLOS NUOSTATŲ UNIKALAUŠ IDENTIFIKATORIAUS
REIŠMĖS IR NUOSTATŲ VERSIJA**

Nuostatų unikalūs identifikatoriai

<u>Pavadinimas</u>	<u>Reiškė</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 tvarkymo skyrius	1
Dokumento tipas (Sertifikavimo veiklos nuostatai)	2
Dokumento versijos pirmasis skaitmuo	2

Nuostatų versija 2.1

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: <http://www.nsc.vrm.lt/>
El. paštas: grt@vrm.lt

Gyventojų registro tarnybos Sertifikatų tvarkymo skyrius, 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.

Registravimo tarnybos

Organizacija Gyventojų registro tarnybos Sertifikatų tvarkymo skyrius
Adresas A. Vivulskio g. 4 A, LT-03220 Vilnius
Tel. (8 5) 271 6352
Faks. (8 5) 271 6250
URL: <http://www.nsc.vrm.lt/>
El. paštas: grt@vrm.lt

Organizacija Vilniaus apskrities vyriausiojo policijos komisariato Migracijos valdyba,
Alytaus, Kauno, Klaipėdos, Marijampolės, Panevėžio, Šiaulių, Tauragės, Telšių
ir Utenos apskričių vyriausiųjų policijos komisariatų migracijos skyriai

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: <http://www.nsc.vrm.lt/>
El. paštas: marija.norkeviciene@vrm.lt

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	http://nsc.vrm.lt/repository
Previous CA Certificate Hash			Ankstesniojo Root CA viešojo rakto 160 bitų SHA-1 hash reikšmė.
Key Usage	Taip		Certificate Signing, Off-line CRL Signing, CRL Signing (06)
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	http://nsc.vrm.lt/repository
CRL Distribution Points	Ne	Distribution Point Name	URL= http://nsc.vrm.lt/cdp/RootCA.crl
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	http://nsc.vrm.lt/OCSP/ocspresponder.nsc
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	http://nsc.vrm.lt/aia/RootCA.crt
Key Usage	Taip		Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constraints	Taip		Subject Type=CA Path Length Constraint=None

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 sertifikata
Certificate Policies	Ne	Policy Identifier	1.3.6.1.4.1.31912.1.1.1
		Policy Qualifier Id=CPS	http://nsc.vrm.lt/repository
CRL Distribution Points	Ne	Distribution Point Name	URL=http://nsc.vrm.lt/cdp/PolicyCA.crl
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	http://nsc.vrm.lt/OCSP/ocspresponder.nsc
		Access Method=Certificati on Authority Issuer (1.3.6.1.5.5.7.48.2)	http://nsc.vrm.lt/aia/PolicyCA.crt
Key Usage	Taip		Certificate Signing, Off-line CRL Signing, CRL Signing (06)

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
Certificate Policies	Ne	Policy Identifier	1.3.6.1.4.1.31912.1.1.1
		Policy Qualifier Id=CPS	http://nsc.vrm.lt/repository
Key Usage	Ne		Digital Signature, Non-Repudiation (c0)
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 = 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 (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
Certificate Policies	Ne	Policy Identifier	1.3.6.1.4.1.31912.1.1.1
		Policy Qualifier Id=CPS	http://nsc.vrm.lt/repository
CRL Distribution Points	Ne	Distribution Point Name	URL= http://nsc.vrm.lt/cdp/RootCA(1).crl
Authority Information Access	Ne	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	URL= http://nsc.vrm.lt/aia/RootCA(1).crt
Key Usage	Taip		Digital Signature, Non-Repudiation (c0)

**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
Certificate Policies	Ne	Policy Identifier	1.3.6.1.4.1.31912.1.1.1
		Policy Qualifier Id=CPS	http://nsc.vrm.lt/repository
CRL Distribution Points	Ne	Distribution Point Name	URL=http://nsc.vrm.lt/cdp/PolicyCA(1).crl
Authority Information Access		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	URL=http://nsc.vrm.lt/aia/PolicyCA(1).crt
Key Usage	Taip		Digital Signature, Non-Repudiation (c0)

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 pavardė
		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)
Papildomi laukai (extensions)			
Subject Directory Attributes	Ne	gender	Lytis, Value=M or F
		dateOfBirth	Gimimo data
		countryOfCitizenship	Pilietybė, Value=LT
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 priedus ir Lietuvos elektroninio parašo įstatymą.
		Policy Qualifier Id=CPS	http://nsc.vrm.lt/repository

Papildomi laukai	Kritinis	Atributas	Reikšmė [paaiškinimas]
CRL Distribution Points	Ne	Distribution Point Name	<i>URL= http://nsc.vrm.lt/cdp/IssuingCA(1).crl</i>
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	<i>http://nsc.vrm.lt/OCSP/ocspresponder.nsc</i>
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	<i>http://nsc.vrm.lt/aia/IssuingCA(1).crt</i>
Qualified Certificate Statement	Ne	qualified certificate statement ID	<i>id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)</i>
	Ne	SSCD statement ID	<i>id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)</i>
Application policies	Ne	Application Certificate Policy	<i>[1]Policy Identifier=Document Signing</i>
Key Usage	Taip		<i>Digital Signature, Non-Repudiation (c0)</i>
Enhanced Key Usage	Ne		<i>Document Signing (1.3.6.1.4.1.311.10.3.12)</i>

**Sertifikavimo veiklos nuostatų
11 priedas**

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 pavardė
		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)
Papildomi laukai (extensions)			
Subject Directory Attributes	Ne	gender	Lytis, Value=M or F
		dateOfBirth	Gimimo data
		countryOfCitizenship	Pilietybė, Value=LT
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	http://nsc.vrm.lt/repository
CRL Distribution Points	Ne	Distribution Point Name	URL= http://nsc.vrm.lt/cdp/IssuingCA(1).crl
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	http://nsc.vrm.lt/OCSP/ocspreponder.nsc
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	http://nsc.vrm.lt/aia/IssuingCA(1).crt
Application Policies	Ne	Application Certificate Policy	Policy Identifier=Client Authentication
Key Usage	Taip		Digital Signature (80)
Enhanced Key Usage	Ne		Client Authentication (1.3.6.1.5.5.7.3.2)

**Sertifikavimo veiklos nuostatų
12 priedas**

VALSTYBĖS TARNAUTOJO 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 = valstybės tarnautojo vardas ir pavardė
		GivenName	G = valstybės tarnautojo vardas
		Surname	SN = valstybės tarnautojo pavardė
		SerialNumber	SERIALNUMBER = valstybės tarnautojo kodas valstybės tarnautojų registre
		CountryName	C = LT
		Email	E = valstybės tarnautojo elektroninio pašto adresas
		Title	T = valstybės tarnautojo pareigų pavadinimas
		Organization	O = valstybės ar savivaldybės institucijos ar įstaigos, kurioje valstybės tarnautojas eina pareigas, pavadinimas
Public key			Viešojo rakto reikšmė (2048 bit) ir parašo formavimo algoritmo identifikatorius (RSA)
Papildomi laukai (extensions)			
Subject Key Identifier	Ne	Key Identifier	Asmens viešojo rakto 160 bitų SHA-1 hash reikšmė
Subject Alternative Name	Ne	RFC822 Name	RFC822 Name = valstybės tarnautojo elektroninio pašto adresas
Authority Key Identifier	Ne	Key Identifier	Issuing CA viešojo rakto 160 bitų SHA-1 hash reikšmė
Certificate Policies	Ne	Policy Identifier	1.3.6.1.4.1.31912.1.3.1
		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 priedus ir Lietuvos elektroninio parašo įstatymą.
		Policy Qualifier Id=CPS	http://nsc.vrm.lt/repository

Papildomi laukai	Kritinis	Atributas	Reikšmė [paaiškinimas]
CRL Distribution Points	Ne	Distribution Point Name	URL= <i>http://nsc.vrm.lt/cdp/IssuingCA(1).crl</i>
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	<i>http://nsc.vrm.lt/OCSP/ocspresponder.nsc</i>
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	<i>http://nsc.vrm.lt/aia/IssuingCA(1).crt</i>
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>
Application policies	Ne	Application Certificate Policy	<i>[1]Policy Identifier=Secure Email</i> <i>[2]Policy Identifier=Document Signing</i>
Key Usage	Taip		<i>Digital Signature, Non-Repudiation (c0)</i>
Enhanced Key Usage	Ne		<i>Secure Email (1.3.6.1.5.5.7.3.4)</i> <i>Document Signing (1.3.6.1.4.1.311.10.3.12)</i>

VALSTYBĖS TARNAUTOJO 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 = Gyventojų 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 pavardė
		GivenName	G = vardas
		Surname	SN = pavardė
		SerialNumber	SERIALNUMBER = valstybės tarnautojo kodas valstybės tarnautojų registre
		CountryName	C = LT
		Email	E = valstybės tarnautojo elektroninio pašto adresas
		Title	T = valstybės tarnautojo pareigų pavadinimas
Organization			O = valstybės ar savivaldybės institucijos ar įstaigos, kurioje valstybės tarnautojas eina pareigas, pavadinimas
Public key			Viešojo rakto reikšmė (2048 bit) ir parašo formavimo algoritmo identifikatorius (RSA)
Papildomi laukai (extensions)			
Subject Key Identifier	Ne	Key Identifier	Asmens viešojo rakto 160 bitų SHA-1 hash reikšmė
Subject Alternative Name	Ne	RFC822 Name	RFC822 Name = valstybės tarnautojo elektroninio pašto adresas
Authority Key Identifier	Ne	Key Identifier	Issuing CA viešojo rakto 160 bitų SHA-1 hash reikšmė
Certificate Policies	Ne	Policy Identifier	1.3.6.1.4.1.31912.1.3.1
		Policy Qualifier Id=CPS	http://nsc.vrm.lt/repository
CRL Distribution Points	Ne	Distribution Point Name	URL= http://nsc.vrm.lt/cdp/IssuingCA(1).crl
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	http://nsc.vrm.lt/OCSP/ocspresponder.nsc
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	http://nsc.vrm.lt/aia/IssuingCA(1).crt

Papildomi laukai (extensions)	Kritinis	Atributas	Reikšmė [paaiškinimas]
Application Policies	Ne	Application Certificate Policy	<i>Policy Identifier=Client Authentication</i>
Key Usage	Taip		<i>Digital Signature (80)</i>
Enhanced Key Usage	Ne		<i>Client Authentication (1.3.6.1.5.5.7.3.2)</i>

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

**DARBINĖS 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 (Issuing CA) OU = Nacionalinis sertifikavimo centras (NSC) O = Gyventojų registro tarnyba prie LR VRM - i.k. 188756767 C = LT</i>
This update		<i>Išleidimo data ir laikas</i>
Next update		<i>Atnaujinimo data ir laikas</i>
Signature		<i>sha1RSA</i>
Negaliojančių sertifikatų sąrašas		
userCertificate		<i>Negaliojančio sertifikato serijinis numeris</i>
revocationDate		<i>Galiojimo nutraukimo ar sustabdymo data ir laikas</i>
Reason Code		<i>Galiojimo nutraukimo ar sustabdymo priežastis</i>
CRL Plėtiniai		
Authority Key Identifier	Key Identifier	<i>Issuing CA viešojo rakto hash reikšmė SHA1 algoritmu</i>
CA Version		<i>V0.0</i>
CRL Number		<i>Sudaromas Issuing CA</i>
Next CRL Publish		<i>Kitos versijos publikavimo data</i>