PATVIRTINTA
Asmens dokumentų išrašymo centro prie Lietuvos Respublikos vidaus reikalų ministerijos
direktoriaus 2020 m. gruodžio 23 d.
įsakymu Nr. 1-59

SERTIFIKAVIMO VEIKLOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Sertifikavimo veiklos nuostatai (toliau – nuostatai) nustato Asmens dokumentų išrašymo centro prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Asmens dokumentų išrašymo centras), kaip kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo (toliau – patikimumo užtikrinimo paslaugų teikėjas), veiklos taisykles, sudarant ir tvarkant sertifikatus pagal Piliečio sertifikato taisyklių, kurių unikalus identifikatorius yra 1.3.6.1.4.1.33621.2.2.2, Valstybės tarnautojo sertifikato taisyklių, kurių unikalus identifikatorius yra 1.3.6.1.4.1.33621.2.3.2, Vidaus tarnybos sistemos pareigūno sertifikato taisyklių, kurių unikalus identifikatorius yra 1.3.6.1.4.1.33621.2.4.2 bei E. rezidento sertifikato taisyklių, kurių unikalus identifikatorius yra 1.3.6.1.4.1.33621.2.5.1, nustatytus reikalavimus.

2. Nuostatų unikalus identifikatorius yra 1.3.6.1.4.1.33621.2.1.2. Identifikatoriaus pirmoji dalis 1.3.6.1.4.1.33621 yra unikalus Asmens dokumentų išrašymo centro numeris IANA įmonių registre, toliau sekanti identifikatoriaus dalis 2.1 žymi konkretų įmonės dokumentą – šiuos nuostatus, paskutinis identifikatoriaus skaičius 2 žymi dokumento versijos pirmąjį skaitmenį. Šio nuostatų dokumento versijos numeris yra 2.4.

3. Vadovaujantis nuostatais, yra sudaromi aštuonių rūšių sertifikatai:

3.1. piliečio sertifikatai:

3.1.1. kvalifikuotas elektroninio parašo sertifikatas;

3.1.2. asmens atpažinimo elektroninėje erdvėje sertifikatas.

3.2. valstybės tarnautojo sertifikatai:

3.2.1. valstybės tarnautojo kvalifikuotas elektroninio parašo sertifikatas;

3.2.2. valstybės tarnautojo atpažinimo elektroninėje erdvėje sertifikatas.

3.3. vidaus tarnybos sistemos pareigūno sertifikatai:

3.3.1. vidaus tarnybos sistemos pareigūno kvalifikuotas elektroninio parašo sertifikatas;

3.3.2. vidaus tarnybos sistemos pareigūno atpažinimo elektroninėje erdvėje sertifikatas.

3.4. e. rezidento sertifikatai:

3.4.1. e. rezidento kvalifikuotas elektroninio parašo sertifikatas;

3.4.2. e. rezidento atpažinimo elektroninėje erdvėje sertifikatas.

4. Nuostatuose vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamente (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (toliau – Reglamentas (ES) Nr. 910/2014), Asmens dokumentų išrašymo centro direktoriaus tvirtinamose Piliečio sertifikato taisyklėse, Valstybės tarnautojo sertifikato taisyklėse, Vidaus tarnybos sistemos pareigūno sertifikato taisyklėse bei E. rezidento sertifikato taisyklėse.

5. Reikalavimus patikimumo užtikrinimo paslaugų teikėjams bei jų teikiamoms paslaugoms nustato Reglamentas (ES) Nr. 910/2014, Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymas ir jų įgyvendinamieji teisės aktai. Sudarant ir tvarkant piliečio, valstybės tarnautojo, vidaus tarnybos sistemos pareigūno ir e. rezidento sertifikatus yra vadovaujamasi Europos telekomunikacijų standartų instituto standartais ETSI EN 319 401, ETSI EN 319 411-1 ir ETSI EN 319 411-2.

II SKYRIUS
PATIKIMUMO UŽTIKRINIMO PASLAUGŲ TEIKĖJO ORGANIZACINĖ STRUKTŪRA

6. Dalis patikimumo užtikrinimo paslaugų teikėjo vykdomos veiklos funkcijų Lietuvos Respublikos vidaus reikalų ministro įsakymų pagrindu yra perduota trečiosioms šalims:

6.1. Informatikos ir ryšių departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos:

6.1.1. vykdyti asmenims sudaromų sertifikatų sudarymui ir tvarkymui naudojamos Sertifikatų valdymo informacinės sistemos techninę priežiūrą, užtikrinant šios sistemos ir joje tvarkomų duomenų saugumą ir nepertraukiamą veiklą;

6.1.2. asmenims, pateikusiems prašymą telefonu, laikinai sustabdyti elektroninių piliečio sertifikatų galiojimą darbo dienomis po darbo valandų bei poilsio ir švenčių dienomis.

6.2. Migracijos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Migracijos departamentas) Alytaus, Kauno, Klaipėdos, Marijampolės, Panevėžio, Šiaulių, Tauragės, Telšių, Utenos ir Vilniaus skyriams išduoti asmens tapatybės korteles su jose įrašytais elektroniniais piliečio sertifikatais ir asmens tapatybės kortelių kontaktinės elektroninės laikmenos aktyvavimo duomenis (slaptažodžius).

6.3. Migracijos departamento direktoriaus nustatytiems Migracijos departamento struktūriniams padaliniams atšaukti ir laikinai sustabdyti elektroninių piliečio sertifikatų galiojimą, panaikinti elektroninių piliečio sertifikatų galiojimo laikiną sustabdymą, asmens prašymu atnaujinti elektroninius piliečio sertifikatus, asmens tapatybės kortelės elektroninio parašo funkcijų blokavimo atveju sukurti naujus kortelės kontaktinės elektroninės laikmenos aktyvavimo duomenis

(slaptažodžius).

6.4. Migracijos departamento direktoriaus nustatytiems Migracijos departamento struktūriniams padaliniams ir Migracijos departamento atrinktiems išorės paslaugų teikėjams išduoti e. rezidento elektroninės atpažinties ir elektroninio parašo priemones su jose įrašytais elektroniniais e. rezidento sertifikatais.

7. Vadovaujantis Valstybės tarnautojo pažymėjimo išdavimo taisyklėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2002 m. liepos 11 d. įsakymu Nr. 338 „Dėl Valstybės tarnautojo pažymėjimo formos ir Valstybės tarnautojo pažymėjimo išdavimo taisyklių patvirtinimo“, valstybės tarnautojų registravimą sertifikatams gauti atlieka institucijų ar įstaigų, kuriose valstybės tarnautojai eina valstybės tarnautojo pareigas, administracijos struktūrinis padalinys arba valstybės tarnautojas, vykdantis personalo administravimo funkcijas.

8. Vadovaujantis Vidaus tarnybos sistemos pareigūno tarnybinio pažymėjimo išdavimo, keitimo, grąžinimo, naikinimo ir paskelbimo negaliojančiu tvarkos aprašu, patvirtintu Lietuvos Respublikos vidaus reikalų ministro 2016 m. kovo 1 d. įsakymu Nr. 1V-155 „Dėl Vidaus tarnybos sistemos pareigūno tarnybinio pažymėjimo blankų privalomųjų formų aprašų ir Vidaus tarnybos sistemos pareigūno tarnybinio pažymėjimo išdavimo, keitimo, grąžinimo, naikinimo ir paskelbimo negaliojančiu tvarkos aprašo patvirtinimo“, vidaus tarnybos sistemos pareigūnų registravimą setifikatams gauti atlieka įstaigos, kurioje vidaus tarnybos sistemos pareigūnas eina pareigas, administracijos struktūrinis padalinys, vykdantis personalo administravimo funkcijas.

9. Už visas teikiamas patikimumo užtikrinimo paslaugas ir vykdomos patikimumo užtikrinimo paslaugų teikimo veiklos atitiktį nuostatų 1 punkte nurodytų taisyklių reikalavimams atsako Asmens dokumentų išrašymo centras.

III SKYRIUS
SERTIFIKAVIMO TARNYBŲ STRUKTŪRA

10. Patikimumo užtikrinimo paslaugoms teikti yra naudojama dviejų lygių sertifikavimo tarnybų struktūra, kurią sudaro:

10.1. pirmojo lygio, hierarchijos viršuje esanti sertifikavimo tarnyba, kurios viešojo rakto sertifikatui pasirašyti naudojamas pačios tarnybos privatusis kriptografinis raktas (toliau – šakninė sertifikavimo tarnyba, angl. *Root CA*). Šios tarnybos privatusis kriptografinis raktas yra naudojamas pasirašyti:

10.1.1. antrojo lygio sertifikavimo tarnybų viešojo rakto sertifikatus;

10.1.2. antrojo lygio sertifikavimo tarnyboms išduotų negaliojančių sertifikatų sąrašus;

10.1.3. užklausų sistemos (OCSP) teikiamiems atsakymams apie antrojo lygio sertifikavimo tarnybų viešojo rakto sertifikatų galiojimo statusą pasirašyti skirtus sertifikatus.

10.2. antrojo lygio, dvi lygiagrečiai naudojamos sertifikavimo tarnybos (toliau – darbinės sertifikavimo tarnybos), kurių privatieji raktai naudojami pasirašyti:

10.2.1. nuostatų 3 punkte nurodytus sertifikatus;

10.2.2. užklausų sistemos teikiamiems atsakymams apie antrojo lygio sertifikavimo tarnybų išduotų sertifikatų (nuostatų 3 punkte nurodytų sertifikatų) galiojimo statusą pasirašyti skirtus sertifikatus;

10.2.3. infrastruktūros sertifikatus (pagalbinius sertifikatus, būtinus užtikrinti patikimumo užtikrinimo paslaugų teikėjo informacinių technologijų infrastruktūros veikimą).

IV SKYRIUS
PATIKIMUMO UŽTIKRINIMO PASLAUGŲ TEIKĖJO IR SERTIFIKATŲ NAUDOTOJŲ PAREIGOS IR ATSAKOMYBĖ

11. Patikimumo užtikrinimo paslaugų teikėjo ir sertifikatų naudotojų pareigos ir atsakomybė yra apibrėžtos kiekvienos nuostatų 3 punkte nurodytos sertifikatų rūšies sertifikatų sudarymo ir tvarkymo sąlygose.

V SKYRIUS
INFORMACIJOS SKELBIMAS

12. Patikimumo užtikrinimo paslaugų teikėjo interneto svetainėje yra skelbiama ir nuolatos viešai prieinama ši informacija:

12.1. sertifikatų taisyklės, nuostatai, sertifikatų sudarymo ir tvarkymo sąlygos;

12.2. vartotojų instrukcijos;

12.3. patikimumo užtikrinimo paslaugų teikėjo sertifikavimo tarnybų viešojo rakto sertifikatai;

12.4. patikimumo užtikrinimo paslaugų teikėjo antrojo lygio sertifikavimo tarnyboms išduotų negaliojančių sertifikatų sąrašai;

12.5. jei buvo atliktas sertifikavimo veiklos atitikties Reglamento (ES) Nr. 910/2014 reikalavimams vertinimas, tai nurodoma atitikties vertinimo įstaiga ir vertinimo išvada.

13. Konfidenciali informacija yra:

13.1. sertifikatų savininkų asmens duomenys, išskyrus tuos, kurie atskleidžiami teikiant sertifikavimo paslaugas;

13.2. patikimumo užtikrinimo paslaugų teikėjo techninė dokumentacija;

13.3. informacija apie sertifikavimo paslaugų teikimui naudojamos techninės ir programinės įrangos apsaugą;

13.4. sertifikavimo paslaugų teikimui naudojamų sistemų techninės priežiūros įrašai bei įrašai apie sertifikavimo paslaugų teikimo sutrikimus;

13.5. bet kokia informacija, kurios atskleidimas galėtų sukelti grėsmę sertifikavimo veiklos saugumui.

14. Konfidenciali informacija saugoma ir tvarkoma patikimumo užtikrinimo paslaugų teikėjo vidaus taisyklių nustatyta tvarka.

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

16. Patikimumo užtikrinimo paslaugų teikėjas asmens duomenis tvarko vadovaudamasis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB.

17. Asmenims sudaromi sertifikatai viešai neskelbiami ir jų paieška negalima.

VI SKYRIUS
PRAŠYMUS TEIKIANČIŲ ASMENŲ TAPATYBĖS NUSTATYMAS

Asmens tapatybės tikrinimas, prašant sudaryti sertifikatą, kai asmens tapatybės kortelė, valstybės tarnautojo pažymėjimas ar vidaus tarnybos sistemos pareigūno tarnybinis pažymėjimas nekeičiami

18. Prašymą sudaryti sertifikatą pagal nuostatų 46 punktą asmens tapatybės kortelėje įrašyto sertifikato savininkas gali pateikti tik asmeniškai atvykęs į registravimo tarnybą ir pateikęs asmens tapatybės kortelę. Prašymą sudaryti sertifikatą pagal nuostatų 47 punktą valstybės tarnautojas gali pateikti tik asmeniškai atvykęs į personalo administravimo tarnybą ir pateikęs valstybės tarnautojo pažymėjimą ir Lietuvos Respublikos piliečio pasą ar asmens tapatybės kortelę. Prašymą sudaryti sertifikatą pagal nuostatų 48 punktą vidaus tarnybos sistemos pareigūnas gali pateikti tik asmeniškai atvykęs į personalo administravimo tarnybą ir pateikęs vidaus tarnybos sistemos pareigūno tarnybinį pažymėjimą ir Lietuvos Respublikos piliečio pasą ar asmens tapatybės kortelę.

19. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

19.1. patikrinamas prašymą teikiančio asmens veido ir pateiktame asmens tapatybę patvirtinančiame dokumente esančio veido atvaizdo vizualinis atitikimas;

19.2. patikrinamas pateikto asmens tapatybę patvirtinančio dokumento tikrumas, įvertinant pateikto asmens tapatybę patvirtinančio dokumento būklę, ir galiojimas;

19.3. patikrinama, ar prašyme nurodyti duomenys ir asmens tapatybės kortelės (valstybės tarnautojo pažymėjimo, vidaus tarnybos sistemos pareigūno tarnybinio pažymėjimo) duomenys sutampa;

19.4. atnaujinant asmens tapatybės kortelėse įrašytus sertifikatus, prašyme pateikta informacija palyginama su Lietuvos Respublikos gyventojų registro duomenų centrinės bazės informacija.

Atšaukti sertifikato galiojimą prašančio asmens tapatybės tikrinimas

20. Prašymą atšaukti sertifikato galiojimą asmens tapatybės kortelėje įrašyto sertifikato savininkas gali pateikti tik asmeniškai atvykęs į registravimo tarnybą ir pateikęs Lietuvos Respublikos piliečio pasą ar asmens tapatybės kortelę. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

20.1. patikrinamas prašymą teikiančio asmens veido ir pateiktame asmens tapatybę patvirtinančiame dokumente esančio veido atvaizdo vizualinis atitikimas;

20.2. patikrinamas pateikto asmens tapatybę patvirtinančio dokumento tikrumas, įvertinant pateikto asmens tapatybę patvirtinančio dokumento būklę, ir galiojimas;

20.3. patikrinama, ar prašyme nurodyti duomenys ir pateikto asmens tapatybę patvirtinančio dokumento duomenys sutampa.

21. Prašymą atšaukti valstybės tarnautojo arba vidaus tarnybos sistemos pareigūno tarnybiniame pažymėjime įrašyto sertifikato galiojimą sertifikato savininkas teikia personalo administravimo tarnybai. Sertifikato savininkas savo asmens tapatybę turi patvirtinti, pateikdamas Lietuvos Respublikos piliečio pasą arba asmens tapatybės kortelę. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

21.1. patikrinamas prašymą teikiančio asmens veido ir pateiktame asmens tapatybę patvirtinančiame dokumente esančio veido atvaizdo vizualinis atitikimas;

21.2. patikrinamas pateikto asmens tapatybę patvirtinančio dokumento tikrumas, įvertinant pateikto asmens tapatybę patvirtinančio dokumento būklę, ir galiojimas.

Laikinai sustabdyti sertifikato galiojimą prašančio asmens tapatybės tikrinimas

22. Prašymą laikinai sustabdyti sertifikato galiojimą asmens tapatybės kortelėje įrašyto sertifikato savininkas gali pateikti registravimo tarnybai raštu arba paskambinęs telefonu į Asmens dokumentų išrašymo centro Sertifikatų skyrių.

23. Kai prašymą laikinai sustabdyti asmens tapatybės kortelėje įrašyto sertifikato galiojimą sertifikato savininkas teikia raštu, jis turi pateikti Lietuvos Respublikos piliečio pasą ar asmens tapatybės kortelę. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

23.1. patikrinamas prašymą teikiančio asmens veido ir pateiktame asmens tapatybę patvirtinančiame dokumente esančio veido atvaizdo vizualinis atitikimas;

23.2. patikrinamas pateikto asmens tapatybę patvirtinančio dokumento tikrumas, įvertinant pateikto asmens tapatybę patvirtinančio dokumento būklę, ir galiojimas;

23.3. patikrinama, ar prašyme nurodyti duomenys ir pateikto asmens tapatybę patvirtinančio dokumento duomenys sutampa.

24. Kai prašymą laikinai sustabdyti asmens tapatybės kortelėje įrašyto sertifikato galiojimą

sertifikato savininkas pateikia Asmens dokumentų išrašymo centro Sertifikatų skyriui telefonu, jis turi nurodyti savo vardą, pavardę, gimimo datą, gyvenamąją vietą ir kitus, Lietuvos Respublikos gyventojų registro įstatymo 9 straipsnio 1 dalyje nurodytus duomenis.

25. Prašymą laikinai sustabdyti valstybės tarnautojo arba vidaus tarnybos sistemos pareigūno tarnybiniame pažymėjime įrašyto sertifikato galiojimą sertifikato savininkas turi pateikti Asmens dokumentų išrašymo centrui raštu. Sertifikato savininkas savo asmens tapatybę turi patvirtinti, pateikdamas Lietuvos Respublikos piliečio pasą arba asmens tapatybės kortelę. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

25.1. patikrinamas prašymą teikiančio asmens veido ir pateiktame asmens tapatybę patvirtinančiame dokumente esančio veido atvaizdo vizualinis atitikimas;

25.2. patikrinamas pateikto asmens tapatybę patvirtinančio dokumento tikrumas, įvertinant pateikto asmens tapatybę patvirtinančio dokumento būklę, ir galiojimas.

26. Kai sertifikato galiojimą laikinai sustabdyti reikalauja teisėsaugos institucija, ji turi pateikti prašymą, kuriame turi būti nurodyti sertifikato, kurio galiojimas sustabdomas, savininko duomenys ir galiojimo sustabdymo priežastys.

Panaikinti sertifikato galiojimo laikiną sustabdymą prašančio asmens tapatybės tikrinimas

27. Prašymą panaikinti sertifikato galiojimo laikiną sustabdymą asmens tapatybės kortelėje įrašyto sertifikato savininkas gali pateikti tik asmeniškai atvykęs į registravimo tarnybą ir pateikęs Lietuvos Respublikos piliečio pasą ar asmens tapatybės kortelę. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

27.1. patikrinamas prašymą teikiančio asmens veido ir pateiktame asmens tapatybę patvirtinančiame dokumente esančio veido atvaizdo vizualinis atitikimas;

27.2. patikrinamas pateikto asmens tapatybę patvirtinančio dokumento tikrumas, įvertinant pateikto asmens tapatybę patvirtinančio dokumento būklę, ir galiojimas;

27.3. patikrinama, ar prašyme nurodyti duomenys ir pateikto asmens tapatybę patvirtinančio dokumento duomenys sutampa.

28. Prašymą panaikinti sertifikato galiojimo laikiną sustabdymą valstybės tarnautojo arba vidaus tarnybos sistemos pareigūno tarnybiniame pažymėjime įrašyto sertifikato savininkas gali pateikti tik asmeniškai atvykęs į personalo administravimo tarnybą ir pateikęs Lietuvos Respublikos piliečio pasą ar asmens tapatybės kortelę. Asmens tapatybės tikrinimo procedūros metu atliekami šie veiksmai:

28.1. patikrinamas prašymą teikiančio asmens veido ir pateiktame asmens tapatybę patvirtinančiame dokumente esančio veido atvaizdo vizualinis atitikimas;

28.2. patikrinamas pateikto asmens tapatybę patvirtinančio dokumento tikrumas, įvertinant

pateikto asmens tapatybę patvirtinančio dokumento būklę, ir galiojimas.

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

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

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

29.2. patikrinamas asmens tapatybės kortelės tikrumas, įvertinant pateiktos asmens tapatybės kortelės būklę, ir galiojimas;

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

Užsieniečių, siekiančių gauti e. rezidento statusą, ir užsieniečių, kuriems šis statusas jau yra suteiktas, tapatybės tikrinimas

30. Užsieniečio, teikiančio prašymą suteikti e. rezidento statusą ir atitinkamai išduoti e. rezidento elektroninės atpažinties ir elektroninio parašo priemonę, tapatybės tikrinimas yra atliekamas Lietuvos Respublikos elektroninio rezidento statuso suteikimo tvarkos aprašo, tvirtinamo Lietuvos Respublikos vidaus reikalų ministro įsakymu, nustatyta tvarka. Užsieniečio, siekiančio gauti e. rezidento statusą ir užsieniečio, kuriam e. rezidento statusas jau yra suteiktas, tapatybės nustatymas asmeniui jungiantis prie Lietuvos migracijos informacinės sistemos (toliau – MIGRIS) atliekamas naudojant dviejų faktorių autentifikaciją, trimis žingsniais, paeiliui vedant elektroninio pašto adresą, slaptažodį ir MIGRIS automatiškai sugeneruotą bei į asmens elektroninio pašto adresą išsiųstą vienkartinį kodą.

VII SKYRIUS
ASMENIMS SUDAROMŲ SERTIFIKATŲ SUDARYMO IR TVARKYMO REIKALAVIMAI

Sertifikatų sudarymas

31. Asmenims sudaromų sertifikatų sandara atitinka standarto ETSI EN 319 412-2 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons“ nustatytus reikalavimus.

32. Patikimumo užtikrinimo paslaugų teikėjas užtikrina, kad:

32.1. kriptografinių raktų poros yra generuojamos saugiai ir privačiųjų kriptografinių raktų

slaptumas yra išlaikomas iki jų įteikimo sertifikatų savininkui;

32.2. sertifikato sudarymo procedūra yra saugiai susieta su asmenų registravimo sertifikatams gauti procedūra;

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

32.4. kvalifikuoti elektroninio parašo kūrimo įtaisai sertifikatų savininkams yra perduodami saugiai;

32.5. asmenims sudarytuose sertifikatuose nurodyti asmens identifikavimo duomenys yra unikalūs ir nepriskirtini kitam asmeniui.

33. Piliečio unikalus identifikatorius piliečio sertifikatuose yra asmens kodas. Valstybės tarnautojo unikalus identifikatorius valstybės tarnautojo sertifikatuose yra valstybės tarnautojo kodas. Vidaus tarnybos sistemos pareigūno unikalus identifikatorius vidaus tarnybos sistemos pareigūno sertifikatuose yra vidaus tarnybos sistemos pareigūno kodas. E. rezidento unikalus identifikatorius e. rezidento sertifikatuose yra interesų Lietuvoje turinčio užsieniečio kodas.

34. Asmenims sudaromuose sertifikatuose įrašomi tik tokie parašo patvirtinimo duomenys, kurie kartu su juos atitinkančiais parašo kūrimo duomenimis yra generuoti asmens tapatybės kortelės, valstybės tarnautojo pažymėjimo, vidaus tarnybos sistemos pareigūno tarnybinio pažymėjimo ar e. rezidento elektroninės atpažinties ir elektroninio parašo priemonės kontaktinėje elektroninėje laikmenoje, kuri yra kvalifikuotas elektroninio parašo kūrimo įtaisas, atitinkantis Lietuvos standarto LST ISO/IEC 15408-3 „Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai. 3 dalis. Saugumo užtikrinimo komponentai“ nustatytą informacinių technologijų saugumo įvertinimo užtikrinimo lygį EAL4+ atitinkančio apsaugos profilio BSI-CC-PP-0059-2009 arba apsaugos profilio BSI-CC-PP-0072-2012-MA-01 reikalavimus.

Sertifikatų išdavimas

35. Į asmens tapatybės korteles įrašomi sertifikatai pirmą kartą išduodami Asmens tapatybės kortelės ir paso išdavimo tvarkos aprašo, patvirtinto Lietuvos Respublikos vidaus reikalų ministro ir Lietuvos Respublikos užsienio reikalų ministro 2015 m. kovo 19 d. įsakymu Nr. 1V-200/V-62, nustatyta tvarka. Sertifikatai atnaujinami, vadovaujantis Piliečių registravimo sertifikatams gauti taisyklių, tvirtinamų Asmens dokumentų išrašymo centro direktoriaus įsakymu, nustatyta tvarka.

36. Į valstybės tarnautojo pažymėjimus įrašomi sertifikatai pirmą kartą išduodami Valstybės tarnautojo pažymėjimo išdavimo taisyklių, tvirtinamų Lietuvos Respublikos vidaus reikalų ministro įsakymu, nustatyta tvarka. Sertifikatai atnaujinami, vadovaujantis Valstybės tarnautojų registravimo

sertifikatams gauti taisyklių, tvirtinamų Asmens dokumentų išrašymo centro direktoriaus įsakymu, nustatyta tvarka.

37. Į vidaus tarnybos sistemos pareigūno tarnybinius pažymėjimus įrašomi sertifikatai pirmą kartą išduodami Lietuvos Respublikos vidaus reikalų ministro valdymo srities vidaus tarnybos sistemos pareigūno tarnybinio pažymėjimo išdavimo, keitimo, grąžinimo, naikinimo ir paskelbimo negaliojančiu tvarkos aprašo, tvirtinamo Lietuvos Respublikos vidaus reikalų ministro įsakymu, nustatyta tvarka. Sertifikatai atnaujinami, vadovaujantis Vidaus tarnybos sistemos pareigūnų registravimo sertifikatams gauti taisyklių, tvirtinamų Asmens dokumentų išrašymo centro direktoriaus įsakymu, nustatyta tvarka.

38. Į e. rezidentų elektroninės atpažinties ir elektroninio parašo priemones sertifikatai įrašomi tik šių priemonių gamybos metu Lietuvos Respublikos elektroninio rezidento statuso suteikimo tvarkos aprašo, tvirtinamo Lietuvos Respublikos vidaus reikalų ministro įsakymu, nustatyta tvarka.

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

40. 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 asmuo pasirašo atitinkamo prašymo formoje.

41. 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 prašyme atnaujinti valstybės tarnautojo pažymėjime įrašomus sertifikatus, 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).

42. Atsiimdamas vidaus tarnybos sistemos pareigūno tarnybinį pažymėjimą, pareigūnas pasirašo prašymo išduoti vidaus tarnybos sistemos pareigūno tarnybinį pažymėjimą formoje, kad susipažino ir sutinka su vidaus tarnybos sistemos pareigūno sertifikatų sudarymo ir tvarkymo sąlygomis, gavo vidaus tarnybos sistemos pareigūno tarnybinį pažymėjimą bei šio pažymėjimo kontaktinės elektroninės laikmenos aktyvavimo duomenis (slaptažodį). Atnaujinant vidaus tarnybos sistemos pareigūno tarnybiniame pažymėjime įrašytus sertifikatus pareigūnas pasirašo prašyme atnaujinti vidaus tarnybos sistemos pareigūno tarnybiniame pažymėjime įrašomus sertifikatus, kad

susipažino ir sutinka su vidaus tarnybos sistemos pareigūno sertifikatų sudarymo ir tvarkymo sąlygomis bei gavo šio pažymėjimo kontaktinės elektroninės laikmenos aktyvavimo duomenis (slaptažodį).

43. E. rezidentas sutikimą su E. rezidento sertifikatų sudarymo ir tvarkymo sąlygomis patvirtina prisijungęs prie asmeninės paskyros MIGRIS, uždėdamas tam skirtą žymą prašymo Lietuvos Respublikos elektroninio rezidento statusui gauti elektroninėje formoje.

44. Atsiimant piliečio, valstybės tarnautojo ir vidaus tarnybos sistemos pareigūno sertifikatus, jų savininkui yra sudaroma galimybė susipažinti su sudarytuose sertifikatuose įrašytais asmens duomenimis. E. rezidentas pasitikrinti jam sudarytuose sertifikatuose įrašytus asmens duomenis turi pats.

Parašo kūrimo ir patvirtinimo duomenų bei juos atitinkančių sertifikatų naudojimas

45. Parašo kūrimo ir patvirtinimo duomenų bei juos atitinkančių sertifikatų naudojimui yra taikomi atitinkamose nuostatų 1 punkte nurodytose sertifikato taisyklėse nustatyti reikalavimai.

Sertifikatų atnaujinimas

46. Nauji sertifikatai nekeičiant asmens tapatybės kortelės, asmens prašymo pagrindu išduodami šiais atvejais:

46.1. artėjant sertifikatų galiojimo terminui į pabaigą arba jam pasibaigus, kai asmens tapatybės kortelės galiojimas dar nėra pasibaigęs. Jei senų sertifikatų galiojimo terminas dar nėra pasibaigęs, prieš sudarant naujus sertifikatus asmens prašymo pagrindu senųjų sertifikatų galiojimas yra atšaukiamas;

46.2. kai anksčiau išduotų sertifikatų galiojimas atšaukiamas dėl asmens tapatybės kortelės kontaktinės elektroninės laikmenos aktyvavimo duomenų (slaptažodžio) atskleidimo ir asmens tapatybės kortelė nėra prarasta ar pamesta ir tebėra galiojanti.

47. Nauji sertifikatai nekeičiant valstybės tarnautojo pažymėjimo išduodami:

47.1. kai pasikeičia valstybės tarnautojo pareigos;

47.2. valstybės tarnautojo prašymo pagrindu, artėjant sertifikatų galiojimo terminui į pabaigą arba jam pasibaigus, kai valstybės tarnautojo pažymėjimo galiojimas dar nėra pasibaigęs. Jei senų sertifikatų galiojimo terminas dar nėra pasibaigęs, prieš sudarant naujus sertifikatus valstybės tarnautojo prašymo pagrindu senųjų sertifikatų galiojimas yra atšaukiamas;

47.3. kai anksčiau išduotų sertifikatų galiojimas atšaukiamas dėl valstybės tarnautojo pažymėjimo kontaktinės elektroninės laikmenos aktyvavimo duomenų (slaptažodžio) atskleidimo ir valstybės tarnautojo pažymėjimas nėra prarastas ar pamestas ir tebėra galiojantis;

47.4. kai valstybės tarnautojas tris kartus iš eilės įveda neteisingus valstybės tarnautojo

pažymėjimo kontaktinės elektroninės laikmenos aktyvavimo duomenis (slaptažodį) ir dėl to yra blokuojamas parašo kūrimo duomenų naudojimas.

48. Nauji sertifikatai nekeičiant vidaus tarnybos sistemos pareigūno tarnybinio pažymėjimo išduodami:

48.1. kai pasikeičia vidaus tarnybos sistemos pareigūno pareigos;

48.2. vidaus tarnybos sistemos pareigūno prašymo pagrindu, artėjant sertifikatų galiojimo terminui į pabaigą arba jam pasibaigus, kai vidaus tarnybos sistemos pareigūno tarnybinio pažymėjimo galiojimas dar nėra pasibaigęs. Jei senų sertifikatų galiojimo terminas dar nėra pasibaigęs, prieš sudarant naujus sertifikatus vidaus tarnybos sistemos pareigūno prašymo pagrindu senųjų sertifikatų galiojimas yra atšaukiamas;

48.3. kai anksčiau išduotų sertifikatų galiojimas atšaukiamas dėl vidaus tarnybos sistemos pareigūno tarnybinio pažymėjimo kontaktinės elektroninės laikmenos aktyvavimo duomenų (slaptažodžio) atskleidimo ir vidaus tarnybos sistemos pareigūno tarnybinis pažymėjimas nėra prarastas ar pamestas ir tebėra galiojantis;

48.4. kai vidaus tarnybos sistemos pareigūnas tris kartus iš eilės įveda neteisingus vidaus tarnybos sistemos pareigūno tarnybinio pažymėjimo kontaktinės elektroninės laikmenos aktyvavimo duomenis (slaptažodį) ir dėl to yra blokuojamas parašo kūrimo duomenų naudojimas.

49. E. rezidentams sudaromi sertifikatai yra atnaujinami (sudaromi nauji sertifikatai) tik išduodant naują e. rezidento elektroninės atpažinties ir elektroninio parašo priemonę.

50. Išduodant naują sertifikatą visada yra sukuriami nauji elektroninio parašo kūrimo ir patvirtinimo duomenys.

Sertifikatų galiojimo atšaukimas

51. Sertifikato galiojimas atšaukiamas šiais atvejais:

51.1. sertifikato savininko prašymu;

51.2. sertifikato savininkui praradus sertifikatą atitinkančių parašo kūrimo duomenų kontrolę;

51.3. išaiškėjus, kad patikimumo užtikrinimo paslaugų teikėjui buvo pateikti klaidingi duomenys sertifikatui sudaryti arba jie pasikeitė;

51.4. gavus pranešimą, kad sertifikato savininkas yra pripažintas neveiksniu ar mirė;

51.5. patikimumo užtikrinimo paslaugų teikėjo sprendimu, paaiškėjus, kad sertifikato savininkas nesilaiko sertifikato sudarymo ir tvarkymo sąlygų;

51.6. kai patikimumo užtikrinimo paslaugų teikėjas nutraukia savo veiklą ir joks kitas patikimumo užtikrinimo paslaugų teikėjas neperima sertifikavimo veiklos;

51.7. kai pažeidžiamas patikimumo užtikrinimo paslaugų teikėjo sistemų saugumas, keliantis pavojų sudarytų sertifikatų patikimumui, arba dėl nuo patikimumo užtikrinimo paslaugų teikėjo

nepriklausomų priežasčių pasikeičia sertifikatų patikimumui užtikrinti keliami saugumo reikalavimai;

51.8. kitais įstatymų numatytais atvejais.

52. Prašymai atšaukti sertifikato galiojimą teikiami nuostatų 20-21 punktuose nustatyta tvarka. Patikimumo užtikrinimo paslaugų teikėjas atšaukia sertifikato galiojimą iškart po prašymo patikrinimo.

53. Jeigu sertifikato galiojimas yra atšaukiamas 51.2, 51.3 arba 51.5-51.8 papunkčiuose nurodytais atvejais, sertifikato savininkas yra apie tai informuojamas nurodant atšaukimo priežastį.

54. Sertifikatų galiojimas yra automatiškai atšaukiamas visais atvejais, nustojus galioti asmens tapatybės kortelei (valstybės tarnautojo pažymėjimui, vidaus tarnybos sistemos pareigūno tarnybiniam pažymėjimui), kurioje šie sertifikatai yra įrašyti, e. rezidento sertifikatų atveju – pasibaigus e. rezidento statuso galiojimui.

Sertifikatų galiojimo laikinas sustabdymas

55. Sertifikato galiojimas visais atvejais yra automatiškai laikinai sustabdomas iškart po sertifikato sudarymo. Sertifikato galiojimo laikinas sustabdymas yra panaikinamas, kai sertifikato savininkas atsiima asmens tapatybės kortelę, valstybės tarnautojo pažymėjimą ar vidaus tarnybos sistemos pareigūno tarnybinį pažymėjimą ir pasirašo, kad susipažino ir sutinka su atitinkamų sertifikatų sudarymo ir tvarkymo sąlygomis, taip pat kai e. rezidentas atsiima e. rezidento elektroninės atpažinties ir elektroninio parašo priemonę ir per asmeninę paskyrą MIGRIS patvirtina e. rezidento elektroninės atpažinties ir elektroninio parašo priemonės gavimą.

56. Vėliau sertifikato galiojimo laikotarpiu sertifikato galiojimas laikinai sustabdomas šiais atvejais:

56.1. sertifikato savininko prašymu – jo nurodytam terminui;

56.2. teisėsaugos institucijų motyvuotu reikalavimu, siekiant užkirsti kelią nusikalstamoms veikoms, – jų nurodytam terminui;

56.3. gavus informacijos, kad sertifikato duomenys yra galimai neteisingi;

56.4. gavus informacijos, kad sertifikato savininkas galimai prarado sertifikatą atitinkančių parašo kūrimo duomenų kontrolę.

57. Prašymai laikinai sustabdyti sertifikato galiojimą teikiami nuostatų 22-26 punktuose nustatyta tvarka. Sertifikato galiojimas laikinai sustabdomas iškart po prašymo patikrinimo. E. rezidentas prašymą laikinai sustabdyti jam sudarytų sertifikatų galiojimą teikia per asmeninę paskyrą MIGRIS.

58. Jeigu sertifikato galiojimas yra laikinai sustabdomas 56.2-56.4 papunkčiuose nurodytais atvejais, sertifikato savininkas yra apie tai informuojamas nurodant sustabdymo priežastį.

59. Jei sertifikato galiojimas buvo laikinai sustabdytas dėl nuostatų 56.1-56.2 papunkčiuose nurodytų priežasčių, sertifikato galiojimo laikinas sustabdymas panaikinamas pasibaigus nurodytam terminui arba gavus sertifikato savininko arba teisėsaugos institucijos, kurios prašymu sertifikato galiojimas buvo sustabdytas, prašymą.

60. Jei sertifikato galiojimas buvo laikinai sustabdytas dėl nuostatų 56.3-56.4 papunkčiuose nurodytų priežasčių, sertifikato galiojimo laikinas sustabdymas panaikinamas gavus sertifikato savininko prašymą ir paaiškinimą, paneigiantį informaciją, kurios pagrindu sertifikato galiojimas buvo laikinai sustabdytas. Nepanaikinus sertifikato galiojimo laikino sustabdymo per 30 dienų, sertifikato galiojimas atšaukiamas.

61. Prašymai panaikinti sertifikato galiojimo laikiną sustabdymą teikiami nuostatų 27-28 punktuose nustatyta tvarka. Sertifikato galiojimo laikinas sustabdymas panaikinamas iškart po prašymo patikrinimo. E. rezidentas prašymą panaikinti sertifikato galiojimo laikiną sustabdymą teikia per asmeninę paskyrą MIGRIS.

Informacijos apie sertifikatų galiojimo statusą teikimas

62. Šakninės sertifikavimo tarnybos darbinėms sertifikavimo tarnyboms išduotų sertifikatų galiojimo statusas tikrinamas pagal negaliojančių sertifikatų sąrašus arba naudojant užklausų sistemą.

63. Negaliojančių darbinėms sertifikavimo tarnyboms išduotų sertifikatų sąrašai yra atnaujinami kas 6 mėnesius. Atnaujintas negaliojančių sertifikatų sąrašas yra generuojamas ir publikuojamas likus 3 savaitėms iki ankstesniojo sąrašo galiojimo pabaigos.

64. Asmenims sudaromų sertifikatų galiojimo statusas tikrinamas tik naudojant užklausų sistemą. Sertifikatų galiojimo statuso tikrinimo paslauga teikiama laikantis siūlomo interneto standarto RFC 6960 reikalavimų.

65. Informacija apie sertifikato galiojimo statusą teikiama 7 dienas per savaitę, 24 valandas per parą. Jei dėl tiesiogiai nuo patikimumo užtikrinimo paslaugų teikėjo nepriklausančių priežasčių sutrinka informacijos apie sertifikato galiojimo statusą teikimas, patikimumo užtikrinimo paslaugų teikėjas turi imtis visų įmanomų priemonių jam atstatyti ne ilgiau kaip per 4 valandas.

66. Informacijos apie sertifikato galiojimo statusą vientisumas ir autentiškumas yra užtikrinamas naudojant patikimumo užtikrinimo paslaugų teikėjo elektroninį parašą. Ši informacija yra vieša ir prieinama tarptautiniu mastu. Informacija apie sertifikato galiojimo statusą teikiama taip pat ir pasibaigus sertifikato galiojimo laikotarpiui.

Parašo kūrimo duomenų apsauga

67. Siekiant apsaugoti asmens tapatybės kortelių, valstybės tarnautojo pažymėjimų, vidaus

tarnybos sistemos pareigūnų tarnybinių pažymėjimų ir e. rezidento elektroninės atpažinties ir elektroninio parašo priemonių kontaktinėse elektroninėse laikmenose esančius elektroninio parašo kūrimo duomenis, yra naudojami kontaktinės elektroninės laikmenos aktyvavimo duomenys (slaptažodis) bei ribojamas nesėkmingų bandymų įvesti teisingą slaptažodį skaičius – tris kartus iš eilės įvedus neteisingą slaptažodį, parašo kūrimo duomenų naudojimas yra blokuojamas. Išduodant naują sertifikatą, visais atvejais yra sudaromi ir nauji kontaktinės elektroninės laikmenos aktyvavimo duomenys (slaptažodis).

68. Prašymai sudaryti naujus asmens tapatybės kortelės kontaktinės elektroninės laikmenos aktyvavimo duomenis (slaptažodį) parašo kūrimo duomenų naudojimo blokavimo atveju teikiami nuostatų 29 punkte nustatyta tvarka. Nauji asmens tapatybės kortelės kontaktinės elektroninės laikmenos aktyvavimo duomenys (slaptažodis) sudaromi iškart, tik gavus prašymą.

69. Valstybės tarnautojo pažymėjimo arba vidaus tarnybos sistemos pareigūno tarnybinio pažymėjimo kontaktinės elektroninės laikmenos aktyvavimo duomenys (slaptažodis) parašo kūrimo duomenų naudojimo blokavimo atveju yra keičiami tik atnaujinant sertifikatus valstybės tarnautojo pažymėjime arba vidaus tarnybos sistemos pareigūno tarnybiniame pažymėjime. Parašo kūrimo duomenų naudojimo blokavimą nekeičiant paskutinių teisingų kontaktinės elektroninės laikmenos aktyvavimo duomenų (paskutinio teisingo slaptažodžio) valstybės tarnautojai, vidaus tarnybos sistemos pareigūnai ir e. rezidentai gali panaikinti patys, naudodami tam skirtą programinę įrangą ir kontaktinės elektroninės laikmenos blokavimo panaikinimo duomenis (PUK kodą).

VIII SKYRIUS
ĮRANGOS, VALDYMO IR PROCEDŪRŲ KONTROLĖ

Bendrosios nuostatos

70. Patikimumo užtikrinimo paslaugų teikėjas:

70.1. yra apibrėžęs ir įgyvendina informacijos saugos politiką, kuri yra dokumentuota, patvirtinta vadovybės, reguliariai peržiūrima ir pagal poreikį atnaujinama;

70.2. skleidžia informacijos saugos politiką savo ir kitų sertifikavimo paslaugų teikimo procese dalyvaujančių institucijų darbuotojams;

70.3. kai tai yra taikytina, informuoja apie informacijos saugos politikos pasikeitimus trečiąsias šalis – sertifikatų naudotojus, atitikties vertinimo įstaigą, priežiūros įstaigą ar kitas priežiūros institucijas;

70.4. užtikrina, kad būtų apibrėžtos, įgyvendinamos, prižiūrimos ir dokumentuojamos visos su patikimumo užtikrinimo paslaugų teikėjo įrenginiais, sistemomis ir informaciniu turtu susijusios saugumo valdymo priemonės ir procedūros;

70.5. periodiškai atlieka saugumo ir veiklos procedūrų reikalavimams nustatyti būtiną rizikos

analizę;

70.6. inventorizuoja sertifikavimo paslaugų teikimui naudojamą ir paslaugų teikimo procese sukauptą informacinį turtą ir pagal rizikos analizės rezultatus klasifikuoja šio turto saugos reikalavimus;

70.7. užtikrina, kad visi įtakos informacijos saugai turintys pakeitimai būtų patvirtinti patikimumo užtikrinimo paslaugų teikėjo vadovybės;

70.8. užtikrina, kad sertifikavimo paslaugoms teikti naudojamų sistemų konfigūracija būtų reguliariai tikrinama, siekiant nustatyti galimas neatitiktis informacijos saugos politikos reikalavimams;

70.9. užtikrina, kad informacijos kaupikliai ir laikmenos, kuriose saugoma jautri informacija, būtų sunaikinti iš karto po to, kai jie tampa nereikalingi sertifikavimo veiklai vykdyti.

Fizinio saugumo kontrolė

71. Sertifikavimo paslaugų teikimui naudojama įranga yra dubliuota ir laikoma dviejose saugyklose, esančiose skirtingais adresais.

72. Testavimui skirta įranga yra fiziškai ir logiškai atskirta nuo paslaugų teikimui naudojamos įrangos.

73. Sertifikavimo paslaugų teikimui naudojamos įrangos fizinis saugumas yra užtikrinamas šiomis priemonėmis:

73.1. saugyklų patalpos yra sugriežtintos apsaugos zonoje, kurią visą parą saugo budėtojas;

73.2. saugyklų patalpose įrengta vaizdo stebėjimo sistema;

73.3. saugyklų patalpose įrengta įsilaužimo signalizavimo sistema;

73.4. saugyklų patalpose įdiegta įėjimo kontrolės sistema – asmenims identifikuoti naudojamos elektroninės identifikavimo kortelės ir biometriniai duomenys;

73.5. teisę patekti į saugyklas turi tik sertifikatų valdymo informacinės sistemos administratoriai. Kiti asmenys į saugyklas gali patekti tik lydimi sertifikatų valdymo informacinės sistemos administratoriaus. Kiekvienas patekimas į saugyklą registruojamas techninėmis priemonėmis. Taip pat yra vedamas elektroninis žurnalas.

73.6. 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.

73.7. saugyklose yra įdiegta inertines dujas naudojanti priešgaisrinės apsaugos sistema, atitinkanti priešgaisrinės saugos reikalavimus.

73.8. saugyklos yra apsaugotos nuo užpylimo vandeniu.

Procedūrų saugumo kontrolė

74. Patikimumo užtikrinimo paslaugų teikėjas užtikrina, kad loginė prieiga prie paslaugų teikimui naudojamų sistemų yra suteikta tik tinkamai autorizuotam personalui:

74.1. sertifikavimo paslaugų teikimui naudojamų sistemų administratorių, auditorių ir operatorių prieigos teisės yra valdomos;

74.2. sertifikavimo paslaugų teikimui naudojamose sistemose aukštos atsakomybės pareigybių teisės yra atskirtos. Pagalbinių programų naudojimas yra ribojamas ir kontroliuojamas;

74.3. sertifikatų sudarymo ir tvarkymo kritines operacijas atliekantys darbuotojai yra identifikuojami ir autentifikuojami;

74.4. patikimumo užtikrinimo paslaugų teikėjo darbuotojų veiksmai yra kontroliuojami, fiksuojant ir išsaugant informaciją apie sistemų naudojimą.

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

76. Atliekant kritines sertifikavimo veiklos operacijas (visas su sertifikavimo paslaugų teikėjo sertifikatų ir kriptografinių raktų gyvavimo ciklo valdymu susijusias operacijas) dalyvauja mažiausiai trys asmenys, tarp kurių visada turi būti sertifikavimo tarnybos pareigūnas.

Personalo patikimumo kontrolė

77. Patikimumo užtikrinimo paslaugų teikėjo darbuotojai turi aukštąjį išsilavinimą bei žinių, patirties ir kvalifikaciją, kurių reikia sertifikavimo paslaugoms teikti, yra dalyvavę asmens duomenų ir elektroninės informacijos apsaugos mokymuose.

78. Darbuotojams, pažeidusiems patikimumo užtikrinimo paslaugų teikėjo informacijos saugos politikos ir procedūrų reikalavimus, yra taikomos tinkamos drausminės nuobaudos.

79. Už sertifikatų valdymo informacinės sistemos elektroninės informacijos saugą, priežiūrą ir veikimą atsakingi darbuotojai eina aukštos atsakomybės pareigas. Aukštos atsakomybės pareigos, kurias gali eiti vienas ar keli asmenys, yra šios:

79.1. sertifikatų valdymo informacinės sistemos saugos įgaliotinis, atsakingas už sistemos elektroninės informacijos saugos politikos įgyvendinimo koordinavimą ir priežiūrą;

79.2. sertifikavimo tarnybos pareigūnas, atsakingas už sertifikavimo paslaugų teikimui reikalingų infrastruktūros sertifikatų išdavimą, dalyvauja visose kritinėse sertifikavimo veiklos operacijose;

79.3. sertifikavimo tarnybos administratorius, atsakingas už patikimumo užtikrinimo paslaugų teikėjo sertifikatų sudarymui ir tvarkymui naudojamų sertifikavimo tarnybų diegimą, konfigūravimą ir veikimą;

79.4. sertifikavimo tarnybos operatorius, atsakingas už sertifikatų sudarymo ir tvarkymo sistemų nenutrūkstamą veikimą, įgaliotas daryti atsargines kopijas ir vykdyti informacijos iš jų atstatymo procedūras;

79.5. sertifikavimo tarnybos auditorius, atsakingas už sertifikavimo tarnybų bei kitų sertifikatų valdymo informacinę sistemą sudarančių tarnybinių stočių operacinių sistemų audito įrašų peržiūrą, perkėlimą į archyvus ir nereikalingų įrašų išvalymą.

80. Vadovaujančias pareigas einantys patikimumo užtikrinimo paslaugų teikėjo darbuotojai išmano elektroninio parašo technologijas ir turi informacijos saugos ir rizikos valdymo patirties.

81. Aukštos atsakomybės pareigas einantys patikimumo užtikrinimo paslaugų teikėjo darbuotojai negali turėti jokių interesų, kurie galėtų turėti įtakos patikimumo užtikrinimo paslaugų teikėjo veiklos nešališkumui.

82. Patikimumo užtikrinimo paslaugų teikėjo darbuotojai pasirašytinai patvirtina, kad susipažino ir sutinka su jiems keliamais reikalavimais ir nustatytomis pareigomis.

83. Patikimumo užtikrinimo paslaugų teikėjo darbuotojų biografija tikrinama laikantis Lietuvos Respublikos įstatymų. Patikimumo užtikrinimo paslaugų teikėjo darbuotojai negali būti teisti.

Įrašų kaupimas ir archyvavimas

84. Patikimumo užtikrinimo paslaugų teikėjas veda sertifikatų valdymo informacinės sistemos techninės priežiūros žurnalą, kuriame yra fiksuojami visi:

84.1. patikimumo užtikrinimo paslaugų teikėjo naudojamos kriptografinės įrangos gyvavimo ciklo įvykiai;

84.2. patikimumo užtikrinimo paslaugų teikėjo kriptografinių raktų gyvavimo ciklo įvykiai;

84.3. patikimumo užtikrinimo paslaugų teikėjo sertifikavimo tarnybų sertifikatų gyvavimo ciklo įvykiai;

84.4. sertifikatų valdymo informacinės sistemos konfigūracijos pakeitimai;

84.5. sertifikatų valdymo informacinės sistemos darbo sutrikimai ir sutrikimų šalinimo aprašymai.

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

85.1. asmenims sudarytų sertifikatų gyvavimo ciklo įvykiai;

85.2. negaliojančių sertifikatų sąrašų generavimo ir publikavimo įvykiai.

86. Sistemos audito žurnalas nuo pakeitimų yra apsaugomas patikimumo užtikrinimo paslaugų teikėjo elektroniniu parašu.

87. Patikimumo užtikrinimo paslaugų teikėjas kaupia bei saugo šiuos veiklos duomenis:

87.1. prašymus laikinai sustabdyti arba atšaukti sertifikato galiojimą, panaikinti sertifikato galiojimo laikiną sustabdymą, keisti asmens tapatybės kortelės kontaktinės elektroninės laikmenos aktyvavimo duomenis (slaptažodį), išduoti ir atnaujinti asmens tapatybės kortelėje (valstybės tarnautojo pažymėjime, vidaus tarnybos sistemos pareigūno tarnybiniame pažymėjime) įrašomus sertifikatus ir šių prašymų registravimo duomenis;

87.2. sistemos audito, sistemos saugumo diagnostikos ir sertifikatų valdymo informacinės sistemos techninės priežiūros žurnalus;

87.3. sudarytus sertifikatus ir šių sertifikatų tvarkymo duomenis;

87.4. negaliojančių sertifikatų sąrašus.

88. Nuostatų 87 punkte nurodyti duomenys yra saugomi 10 metų (7 metus nuo išduotų sertifikatų galiojimo pabaigos). Pasibaigus saugojimo terminui duomenys yra sunaikinami.

Veiklos atkūrimas didelių incidentų ir paslaugų patikimumo praradimo atveju

89. Sertifikatų valdymo informacinėje sistemoje yra automatiškai pildomas elektroninis sistemos saugumo diagnostikos žurnalas, kuriame yra fiksuojami visi su sistemos sauga susiję įvykiai.

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

91. Peržiūrėti sistemos saugumo diagnostikos ir kitus elektroninius žurnalus gali tik sistemos administratoriai ir auditorius.

92. Sertifikavimo veiklos grėsmių prevencijai užtikrinti ir jų įtakai sumažinti, patikimumo užtikrinimo paslaugų teikėjas taiko šias priemones:

93. Sistemos darbui po sutrikimų atstatyti yra daromos šios programinės įrangos, duomenų bazių ir kitų svarbių duomenų atsarginės kopijos:

93.1. operacinių sistemų konfigūracijos duomenų kopijos;

93.2. pilnos operacinių sistemų kopijos;

93.3. sertifikatų duomenų bazės kopijos;

93.4. negaliojančių sertifikatų sąrašų kopijos;

93.5. sistemos audito žurnalo kopijos.

94. Aparatinės įrangos gedimo atveju paslaugų teikimo sutrikimo padarinių išvengti ar juos sumažinti leidžia įrangos dubliavimas ir dviejų fiziškai atskirtų aparatinės įrangos saugyklų naudojimas.

95. Patikimumo užtikrinimo paslaugų teikėjo privačiojo kriptografinio rakto kontrolės praradimo atveju, patikimumo užtikrinimo paslaugų teikėjas nedelsdamas atlieka šiuos veiksmus:

95.1. sertifikatų naudotojai ir kiti su patikimumo užtikrinimo paslaugų teikėjo veikla susiję

asmenys yra nedelsiant informuojami apie patikimumo užtikrinimo paslaugų teikėjo privačiojo kriptografinio rakto kontrolės praradimą žiniasklaidos ir kitomis priemonėmis;

95.2. nurodoma, kad nebekontroliuojamu privačiuoju kriptografiniu raktu pasirašyti sertifikatai, per užklausų sistemą išsiųsti pranešimai apie sertifikatų galiojimo statusą ir negaliojančių sertifikatų sąrašai negali būti laikomi patikimais;

95.3. atšaukiamas patikimumo užtikrinimo paslaugų teikėjo nebekontroliuojamą privatųjį raktą atitinkančio sertifikato bei visų dar galiojančių nebekontroliuojamu privačiuoju kriptografiniu raktu pasirašytų sertifikatų galiojimas.

96. Paaiškėjus, kad kuris nors iš patikimumo užtikrinimo paslaugų teikėjo sertifikavimo paslaugų teikimui naudojamų kriptografinių algoritmų tapo nepatikimu, patikimumo užtikrinimo paslaugų teikėjas privalo nedelsiant apie tai informuoti visus sertifikatų naudotojus ir kitus su patikimumo užtikrinimo paslaugų teikėjo veikla susijusius asmenis bei sudaryti sertifikatų, kuriems sudaryti buvo naudojamas nepatikimu tapęs algoritmas, galiojimo nutraukimo planą.

Sertifikavimo paslaugų teikimo nutraukimas

97. Patikimumo užtikrinimo paslaugų teikėjas sertifikavimo veiklos nutraukimo atvejui yra parengęs ir su priežiūros institucija suderinęs veiklos nutraukimo planą.

IX SKYRIUS
TECHNINĖS SAUGUMO PRIEMONĖS

Patikimumo užtikrinimo paslaugų teikėjo kriptografinių raktų sudarymo ir tvarkymo reikalavimai

98. Patikimumo užtikrinimo paslaugų teikėjo kriptografiniai raktai generuojami naudojant kriptografinius modulius, kurie atitinka JAV Nacionalinio standartų ir technologijų instituto standarto FIPS PUB 140-2 „Saugos reikalavimai kriptografiniams moduliams“ trečiojo saugumo lygmens reikalavimus.

99. Patikimumo užtikrinimo paslaugų teikėjo kriptografinių raktų ilgis ir generavimo algoritmas atitinka standarto ETSI TS 119 312 reikalavimus.

100. Patikimumo užtikrinimo paslaugų teikėjas generuoja tokio ilgio raktus:

100.1. šakninės sertifikavimo tarnybos raktų – RSA 4096 bitų;

100.2. darbinių sertifikavimo tarnybų raktų – RSA 2048 bitų;

100.3. asmenims generuojamų raktų – RSA 2048 bitų arba ECDSA 256 bitų.

101. Patikimumo užtikrinimo paslaugų teikėjo kriptografinių raktų generavimo procedūros metu atliekami veiksmai yra fiksuojami protokole, kurį pasirašo visi procedūros dalyviai. Šakninės sertifikavimo tarnybos raktų generavimo atveju protokolą pasirašo patikimas nepriklausomas

asmuo.

102. Patikimumo užtikrinimo paslaugų teikėjo viešuosius kriptografinius raktus atitinkantys sertifikatai skelbiami patikimumo užtikrinimo paslaugų teikėjo interneto svetainėje.

103. Šakninė sertifikavimo tarnyba ir su ja susietas kriptografininis modulis, kuriame saugomi šios tarnybos privatieji kriptografiniai raktai, yra visada atjungti nuo kompiuterių tinklo. Šakninė sertifikavimo tarnyba ir su ja susietas kriptografininis modulis yra laikomi išjungti ir įjungiami tik atliekant kritines operacijas arba diegiant operacinės sistemos atnaujinimus.

104. Patikimumo užtikrinimo paslaugų teikėjo privatieji kriptografiniai raktai nearchyvuojami. Pasibaigus galiojimo terminui, šie raktai sunaikinami.

105. Patikimumo užtikrinimo paslaugų teikėjo kriptografinių raktų kopijos yra šifruojamos, šifravimo raktas yra padalinamas į dalis ir saugomas specialiose, su kriptografine įranga susietose lustinėse kortelėse.

106. Patikimumo užtikrinimo paslaugų teikėjas nedaro asmenų privačiųjų kriptografinių raktų kopijų.

107. Patikimumo užtikrinimo paslaugų teikėjo generuojamų kriptografinių raktų naudojimo terminai yra šie:

107.1. šakninės sertifikavimo tarnybos raktų – 12 metų.

107.2. darbinių sertifikavimo tarnybų raktų – 6 metai.

107.3. asmenims generuojamų raktų – 3 metai.

108. Patikimumo užtikrinimo paslaugų teikėjas užtikrina tinkamą jo privačiųjų kriptografinių raktų naudojimą, įskaitant bet neapsiribojant tuo, kad:

108.1. privatieji kriptografiniai raktai yra naudojami tik pagal jų paskirtį;

108.2. privatieji kriptografiniai raktai yra naudojami tik fiziškai saugioje aplinkoje;

108.3. visos privačiųjų kriptografinių raktų kopijos pasibaigus atitinkamų raktų numatytam naudojimo terminui yra sunaikinamos.

109. Patikimumo užtikrinimo paslaugų teikėjas užtikrina kriptografinių modulių saugumą viso jų gyvavimo ciklo metu, t.y. užtikrina, kad:

109.1. kriptografiniai moduliai nebuvo pažeisti iki jų pateikimo patikimumo užtikrinimo paslaugų teikėjui;

109.2. kriptografiniai moduliai nebuvo pažeisti sandėliuojant;

109.3. kriptografiniai moduliai veikia tinkamai.

Prieigos valdymas

110. Patikimumo užtikrinimo paslaugų teikėjas užtikrina, kad prieiga prie paslaugų teikimui naudojamose sistemose tvarkomos informacijos yra suteikta tik tinkamai autorizuotam personalui:

110.1. paslaugų teikimui naudojamos sistemos yra apsaugotos ugniasienėmis;

110.2. vietinio tinklo įranga yra laikoma saugioje aplinkoje;

110.3. sertifikatų sudarymo, jų galiojimo atšaukimo ir laikino sustabdymo sistemose yra naudojama nuolatinio stebėjimo ir signalizavimo sistema, skirta nustatyti ir registruoti neteisėtus bandymus prieiti prie sistemos išteklių bei juos užkirsti;

110.4. konfidencialūs duomenys yra apsaugoti nuo jų atskleidimo dėl antrinio laikmenų panaudojimo.

Sistemų veikimo užtikrinimas

111. Patikimumo užtikrinimo paslaugų teikėjas užtikrina, kad paslaugų teikimui naudojamos sistemos veiktų saugiai ir patikimai, paslaugų teikimui naudojamų sistemų prieinamumas, atsižvelgiant į Techninius valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimus, patvirtintus Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 “Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo”, per metus būtų ne mažesnis kaip 96 procentai laiko visą parą, o pokyčių sukeltų sutrikimų rizika būtų minimali:

111.1. įgyvendinant bet kokį sistemų plėtros projektą, projektavimo ir poreikių nustatymo etape yra atliekama saugumo reikalavimų analizė;

111.2. programinės įrangos atnaujinimas, modifikavimas ar skubus taisymas yra valdomas, dokumentuojant atliktus pakeitimus;

111.3. patikimumo užtikrinimo paslaugų teikėjo įrangos ir jo valdomos informacijos vientisumas yra apsaugotas nuo pažeidimų, kuriuos gali sukelti kompiuteriniai virusai, kenkėjiška programinė įranga ar neleistinas programinės įrangos naudojimas;

111.4. patikimumo užtikrinimo paslaugų teikėjo sistemose naudojami informacijos kaupikliai ir laikmenos yra tvarkomi saugiai, užtikrinant jų apsaugą nuo sugadinimo, vagystės, neteisėto panaudojimo ar susidėvėjimo;

111.5. patikimumo užtikrinimo paslaugų teikėjo sistemose naudojami informacijos kaupikliai ir laikmenos yra apsaugoti nuo susidėvėjimo visą juose esančių įrašų privalomojo saugojimo laikotarpį;

111.6. visų aukštos atsakomybės pareigas einančių darbuotojų vykdomos veiklos procedūros yra tiksliai apibrėžtos ir jų turi būti laikomasi;

111.7. saugumo spragoms užtaisyti skirti programinės įrangos atnaujinimai yra diegiami laiku, nebent jų diegimas galėtų pakenkti sistemų darbui;

111.8. ateityje reikalingų išteklių poreikis yra planuojamas.

Tinklo saugumo valdymas

112. Patikimumo užtikrinimo paslaugų teikėjas užtikrina sertifikavimo paslaugų teikimui naudojamų sistemų apsaugą nuo tinklo atakų:

112.1. patikimumo užtikrinimo paslaugų teikėjo vidinis kompiuterių tinklas yra padalintas į atskiras zonas, atsižvelgiant į jose esančių įrangos komponentų saugos ir atliekamų funkcijų reikalavimus;

112.2. prieiga prie zonų ir tarpusavio ryšiai yra ribojami taip, kad zonos būtų pasiekiamos tik su sertifikavimo paslaugų teikimu susijusioms funkcijoms vykdyti;

112.3. sertifikavimo paslaugų teikimui naudojamos sistemos yra administruojamos iš atskiro, tam skirto potinklio;

112.4. ryšių tarp atskirų sertifikavimo paslaugų teikimui naudojamų sistemų saugumui užtikrinti yra naudojamas šifravimas ir patikimas ryšio mazgų identifikavimas;

112.5. viešieji ir privatūs sertifikavimo paslaugų teikimui naudojamo tinklo adresai yra periodiškai skenuojami, siekiant nustatyti galimus pažeidžiamumus. Skenavimą turi atlikti kompetetingas ir nepriklausomas asmuo ar įstaiga;

112.6. sertifikavimo paslaugų teikimui naudojamoms sistemoms turi būti atliktas etiško įsilaužimo testas, kurį turi atlikti kompetetingas ir nepriklausomas asmuo ar įstaiga. Testas turi būti atliekamas pradedant sistemų naudojimą, taip pat atlikus ženklius sistemų pakeitimus.

X SKYRIUS
SERTIFIKATŲ IR NEGALIOJANČIŲ SERTIFIKATŲ SĄRAŠŲ PROFILIAI

113. Sertifikatų ir negaliojančių sertifikatų sąrašų profiliai nustatyti nuostatų 2–14 prieduose.

XI SKYRIUS
SERTIFIKAVIMO VEIKLOS ATITIKTIES SERTIFIKAVIMO VEIKLOS NUOSTATAMS UŽTIKRINIMAS

114. Patikimumo užtikrinimo paslaugų teikėjo vykdomos sertifikavimo veiklos atitiktis nuostatų ir nuostatų 1 punkte nurodytų sertifikato taisyklių reikalavimams yra tikrinama ne rečiau kaip kartą per metus.

115. Vidinį sertifikavimo veiklos tikrinimą atlieka patikimumo užtikrinimo paslaugų teikėjo vadovo skiriamas vidaus auditorius. Išorinis veiklos tikrinimas vykdomas reglamento (ES) Nr. 910/2014 ir kitų teisės aktų nustatyta tvarka.

116. Išorinių veiklos tikrinimų išvados skelbiamos patikimumo užtikrinimo paslaugų teikėjo interneto svetainėje.

117. Patikimumo užtikrinimo paslaugų teikėjas apie bet kokius kvalifikuotų patikimumo užtikrinimo paslaugų teikimo pakeitimus, nedelsdamas, bet ne vėliau kaip per 3 darbo dienas nuo

šių pakeitimų dienos, informuoja priežiūros įstaigą.

XII SKYRIUS
KITOS NUOSTATOS

118. Patikimumo užtikrinimo paslaugų teikėjo paslaugos yra teikiamos nemokamai.

119. Patikimumo užtikrinimo paslaugų teikėjas pasilieka teisę imti mokesčius už tam tikras paslaugas, išskyrus mokestį už informacijos, reikalingos jo sudarytų sertifikatų patikimumui nustatyti, bei informacijos apie jo sudarytų sertifikatų galiojimo statusą teikimą. Nustačius mokesčius, paslaugų įkainiai turi būti skelbiami patikimumo užtikrinimo paslaugų teikėjo interneto svetainėje.

120. Patikimumo užtikrinimo paslaugų teikėjo įsipareigojimams užtikrinti Patikimumo užtikrinimo paslaugų teikėjas draudžia savo civilinę atsakomybę, vadovaudamasis Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo 10 straipsnyje nustatyta tvarka.

121. Visiems su patikimumo užtikrinimo paslaugų teikimu susijusiems santykiams taikoma Lietuvos Respublikos teisė. Visi ginčai, susiję su sertifikatų sudarymu ir tvarkymu, sprendžiami vadovaujantis Lietuvos Respublikos įstatymais.

122. Sertifikavimo paslaugos yra teikiamos vadovaujantis Lietuvos Respublikos įstatymais ir kitais teisės aktais, sudarant paslaugų vartotojams galimybes įsitikinti vykdomos veiklos legalumu.

XIII SKYRIUS
SERTIFIKAVIMO VEIKLOS NUOSTATŲ ADMINISTRAVIMAS

123. Sertifikatų naudotojai turi vadovautis aktualia nuostatų redakcija. Naujai patvirtinta ir paskelbta nuostatų redakcija panaikina ankstesnės nuostatų redakcijos galiojimą. Patvirtinus naują nuostatų redakciją, ji nedelsiant skelbiama patikimumo užtikrinimo paslaugų teikėjo tinklalapyje. Ankstesnė nuostatų redakcija perkeliama į tinklalapio skyrių, paženklintą kaip taisyklių ir nuostatų archyvas.

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

125. Nuostatų pakeitimai gali būti:

125.1. esminiai, apie kuriuos turi būti pranešama sertifikatų naudotojams;

125.2. neesminiai, apie kuriuos sertifikatų naudotojams pranešti nėra privaloma.

126. Neesminiais pakeitimais laikomi rekomendacinio, paaiškinamojo, tikslinamojo pobūdžio informacijos arba už nuostatų tvarkymą atsakingų asmenų kontaktinių duomenų pakeitimai.

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

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

128. Atlikus esminius pakeitimus, keičiamas unikalus nuostatų identifikatorius (nuostatų dokumento versiją atitinkantis identifikatoriaus elementas – paskutinis identifikatoriaus skaitmuo) bei naujos nuostatų redakcijos dokumento versijos pirmas skaitmuo. Atlikus neesminius pakeitimus, nuostatų unikalus identifikatorius nėra keičiamas, o keičiamas tik naujos nuostatų redakcijos dokumento versijos antras skaitmuo.

129. Nuostatų peržiūra, keitimas ir tvirtinimas vykdomi tokia tvarka:

129.1. nuostatų pakeitimus gali inicijuoti patikimumo užtikrinimo paslaugų teikėjas arba sertifikatų naudotojai;

129.2. už saugumo politiką atsakingi patikimumo užtikrinimo paslaugų teikėjo darbuotojai:

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

129.2.2. peržiūros metu nustačius poreikį keisti nuostatus, inicijuoja nuostatų keitimą ir rengia naują nuostatų redakciją;

129.2.3. priima sprendimą teikti tvirtinti naują nuostatų redakciją;

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

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

129.5. parengus naują nuostatų redakciją, visada yra patikrinamas jos atitikimas nuostatų 1 punkte nurodytų sertifikato taisyklių aktualioms redakcijoms;

129.6. nuostatų naują redakciją tvirtina patikimumo užtikrinimo paslaugų teikėjo vadovas.

130. Apie naują nuostatų redakciją nedelsiant informuojama priežiūros įstaiga.

Sertifikavimo veiklos nuostatų
1 priedas

SERTIFIKAVIMO PASLAUGAS TEIKIANČIŲ ĮSTAIGŲ KONTAKTINIAI DUOMENYS

Patikimumo užtikrinimo paslaugų teikėjas

Organizacija	Asmens dokumentų išrašymo centras prie Lietuvos Respublikos vidaus reikalų ministerijos
Adresas	Žirmūnų g. 1D, LT-09239 Vilnius
Tel.	(8 5) 271 8000
URL:	https://www.nsc.vrm.lt
El. paštas:	adic@adic.gov.lt

Asmens dokumentų išrašymo centro Sertifikatų skyrius, tel.: (8 5) 271 6062

Darbo laikas:	I-IV	7.30–11.30, 12.15–16.30
	V	7.30–11.30, 12.15–15.15

Registravimo tarnybos

Organizacija	Asmens dokumentų išrašymo centras prie Lietuvos Respublikos vidaus reikalų ministerijos
Adresas	Žirmūnų g. 1D, LT-09239 Vilnius
Tel.	(8 5) 271 8000
URL:	https://www.nsc.vrm.lt
El. paštas:	adic@adic.gov.lt

Organizacija	Migracijos departamento Alytaus, Kauno, Klaipėdos, Marijampolės, Panevėžio, Šiaulių, Tauragės, Telšių, Utenos ir Vilniaus skyriai. Kontaktai pateikiami tinklalapyje http://migracija.lrv.lt/lt/asmenu-aptarnavimas

Už nuostatų administravimą atsakingo asmens kontaktiniai duomenys

Organizacija	Asmens dokumentų išrašymo centras prie Lietuvos Respublikos vidaus reikalų ministerijos
Asmuo	Nerijus Rudaitis
Adresas	Žirmūnų g. 1D, LT-09239 Vilnius
Tel.	(8 5) 271 8000
URL:	https://www.nsc.vrm.lt
El. paštas:	nerijus.rudaitis@adic.gov.lt

_____

Sertifikavimo veiklos nuostatų
2 priedas

ŠAKNINĖS SERTIFIKAVIMO TARNYBOS SERTIFIKATO PROFILIS

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			V3(2)
Serial number			automatiškai generuojamas numeris
Signature algorithm			sha256RSA
Issuer			CN=ADIC Root CA O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
Validity		notBefore	sertifikato galiojimo pradžios data UTC laiku
		notAfter	sertifikato galiojimo pabaigos data UTC laiku
Subject			CN=ADIC Root CA O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
Public key			viešojo (4096 bitų) rakto reikšmė ir parašo kūrimo algoritmo identifikatorius (RSA)
Papildomi laukai			
Subject Key Identifier	Ne		160 bitų ilgio ADIC Root CA viešojo rakto identifikatorius
CA Version	Ne		sudaroma sukuriant sertifikatą
Key Usage	Taip		Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constraints	Taip		Subject Type=CA Path Length Constraint=None

_____

Sertifikavimo veiklos nuostatų
3 priedas

DARBINĖS SERTIFIKAVIMO TARNYBOS SERTIFIKATO PROFILIS

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			V3(2)
Serial number			automatiškai generuojamas numeris
Signature algorithm			sha256RSA
Issuer			CN=ADIC Root CA O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
Validity		notBefore	sertifikato galiojimo pradžios data UTC laiku
		notAfter	sertifikato galiojimo pabaigos data UTC laiku
Subject			CN=ADIC CA-A arba CN=ADIC CA-B O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
Public key			viešojo (2048 bitų) rakto reikšmė ir parašo kūrimo algoritmo identifikatorius (RSA)
Papildomi laukai			
Subject Key Identifier	Ne	keyIdentifier	160 bitų ilgio ADIC CA-A arba ADIC CA-B viešojo rakto identifikatorius
Authority Key Identifier	Ne	keyIdentifier	160 bitų ilgio ADIC Root CA viešojo rakto identifikatorius
CA Version	Ne		sudaroma sukuriant sertifikatą
Certificate Policies	Ne	policyIdentifier	2.5.29.32.0
		policyQualifier-Info	policyQualifierId=CPS qualifier=http://nsc.vrm.lt/repository
CRL Distribution Points	Ne	distributionPoint	distributionPointName fullName: URL=http://nsc.vrm.lt/cdp/ADIC_Root_CA.crl
Authority Information Access	Ne	accessDescription	accessMethod=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation= http://nsc.vrm.lt/OCSP/ocspresponder.nsc
		accessDescription	accessMethod=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) accessLocation= http://nsc.vrm.lt/aia/ADIC_Root_CA.crt
Key Usage	Taip		Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constraints	Taip		Subject Type=CA Path Length Constraint=None

_____

Sertifikavimo veiklos nuostatų
4 priedas

ŠAKNINĖS SERTIFIKAVIMO TARNYBOS OCSP PRANEŠIMŲ TVIRTINIMO SERTIFIKATO PROFILIS

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			V3(2)
Serial number			automatiškai generuojamas numeris
Signature algorithm			sha256RSA
Issuer			CN=ADIC Root CA O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
Validity		notBefore	sertifikato galiojimo pradžios data UTC laiku
		notAfter	sertifikato galiojimo pabaigos data UTC laiku
Subject			CN=OCSP for ADIC Root CA O=Asmens dokumentu israsymo centras prie LR VRM C=LT
Public key			viešojo (2048 bitų) rakto reikšmė ir parašo kūrimo algoritmo identifikatorius (RSA)
Papildomi laukai			
Subject Key Identifier	Ne	keyIdentifier	160 bitų ilgio OCSP for ADIC Root CA viešojo rakto identifikatorius
Authority Key Identifier	Ne	keyIdentifier	160 bitų ilgio ADIC Root CA viešojo rakto identifikatorius
Certificate Policies	Ne	policyIdentifier	1.3.6.1.4.1.33621.2.1.1
		policyQualifier-Info	policyQualifierId=CPS qualifier=http://nsc.vrm.lt/repository
Authority Information Access		accessDescription	accessMethod=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) accessLocation= http://nsc.vrm.lt/aia/ADIC_Root_CA.crt
Key Usage	Taip		Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage	Ne		OCSP Signing (1.3.6.1.5.5.7.3.9)

_____

Sertifikavimo veiklos nuostatų
5 priedas

DARBINĖS SERTIFIKAVIMO TARNYBOS OCSP PRANEŠIMŲ TVIRTINIMO SERTIFIKATO PROFILIS

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			V3(2)
Serial number			automatiškai generuojamas numeris
Signature algorithm			sha256RSA
Issuer			CN=ADIC CA-A arba CN=ADIC CA-B O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
Validity		notBefore	sertifikato galiojimo pradžios data UTC laiku
		notAfter	sertifikato galiojimo pabaigos data UTC laiku
Subject			CN= OCSP for ADIC CA-A arba CN= OCSP for ADIC CA-B O=Asmens dokumentu israsymo centras prie LR VRM C=LT
Public key			viešojo (2048 bitų) rakto reikšmė ir parašo kūrimo algoritmo identifikatorius (RSA)
Papildomi laukai			
Subject Key Identifier	Ne	keyIdentifier	160 bitų ilgio OCSP for ADIC CA-A arba OCSP for ADIC CA-B viešojo rakto identifikatorius
Authority Key Identifier	Ne	keyIdentifier	160 bitų ilgio ADIC CA-A arba ADIC CA-B viešojo rakto identifikatorius
Certificate Policies	Ne	policyIdentifier	1.3.6.1.4.1.33621.2.1.1
		policyQualifier-Info	policyQualifierId=CPS qualifier=http://nsc.vrm.lt/repository
Authority Information Access		accessDescription	accessMethod=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) accessLocation= http://nsc.vrm.lt/aia/ADIC_CA-A.crt arba http://nsc.vrm.lt/aia/ADIC_CA-B.crt
Application policies	Ne	Application Certificate Policy	Policy Identifier=OCSP Signing
Key Usage	Taip		Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage	Ne		OCSP Signing (1.3.6.1.5.5.7.3.9)

_____

Sertifikavimo veiklos nuostatų
6 priedas

KVALIFIKUOTO ELEKTRONINIO PARAŠO SERTIFIKATO PROFILIS

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			V3(2)
Serial number			automatiškai generuojamas numeris
Signature algorithm			sha256RSA
Issuer			CN=ADIC CA-A arba CN=ADIC CA-B O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
Validity		notBefore	sertifikato galiojimo pradžios data UTC laiku
		notAfter	sertifikato galiojimo pabaigos data UTC laiku
Subject		commonName	CN=vardas pavardė
		givenName	G=vardas
		surname	SN=pavardė
		serialNumber	SERIALNUMBER=asmens kodas
		countryName	C=LT
Public key			viešojo (2048 bitų) rakto reikšmė ir parašo kūrimo algoritmo identifikatorius (RSA)
Papildomi laukai			
Subject Directory Attributes	Ne	gender	M arba F
		dateOfBirth	gimimo data
		countryOf-Citizenship	LT
Subject Key Identifier	Ne	keyIdentifier	160 bitų ilgio asmens viešojo rakto identifikatorius
Authority Key Identifier	Ne	keyIdentifier	160 bitų ilgio ADIC CA-A arba ADIC CA-B viešojo rakto identifikatorius
Certificate Policies	Ne	policyIdentifier	1.3.6.1.4.1.33621.2.2.2
		policyQualifier-Info	policyQualifierId=CPS qualifier=http://nsc.vrm.lt/repository
Authority Information Access	Ne	accessDescription	accessMethod=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation= http://nsc.vrm.lt/OCSP/ocspresponder.nsc
		accessDescription	accessMethod=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) accessLocation= http://nsc.vrm.lt/aia/ADIC_CA-A.crt arba http://nsc.vrm.lt/aia/ADIC_CA-B.crt
Qualified Certificate Statement	Ne	EU Qualified Certificate statement	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		SSCD statement	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		PDS statement	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) PdsLocation: URL= http://nsc.vrm.lt/pds language=en
Application policies	Ne	Application Certificate Policy	Policy Identifier=Document Signing
Key Usage	Taip		Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage	Ne		Document Signing (1.3.6.1.4.1.311.10.3.12)

_____

Sertifikavimo veiklos nuostatų
7 priedas

ASMENS ATPAŽINIMO ELEKTRONINĖJE ERDVĖJE SERTIFIKATO PROFILIS

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			V3(2)
Serial number			automatiškai generuojamas numeris
Signature algorithm			sha256RSA
Issuer			CN=ADIC CA-A arba CN=ADIC CA-B O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
Validity		notBefore	sertifikato galiojimo pradžios data UTC laiku
		notAfter	sertifikato galiojimo pabaigos data UTC laiku
Subject		commonName	CN=vardas pavardė
		givenName	G=vardas
		surname	SN=pavardė
		serialNumber	SERIALNUMBER=asmens kodas
		countryName	C=LT
Public key			viešojo (2048 bitų) rakto reikšmė ir parašo kūrimo algoritmo identifikatorius (RSA)
Papildomi laukai			
Subject Directory Attributes	Ne	gender	M arba F
		dateOfBirth	gimimo data
		countryOf-Citizenship	LT
Subject Key Identifier	Ne	keyIdentifier	160 bitų ilgio asmens viešojo rakto identifikatorius
Authority Key Identifier	Ne	keyIdentifier	160 bitų ilgio ADIC CA-A arba ADIC CA-B viešojo rakto identifikatorius
Certificate Policies	Ne	policyIdentifier	1.3.6.1.4.1.33621.2.2.2
		policyQualifier-Info	policyQualifierId=CPS qualifier=http://nsc.vrm.lt/repository
Authority Information Access	Ne	accessDescription	accessMethod=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation= http://nsc.vrm.lt/OCSP/ocspresponder.nsc
		accessDescription	accessMethod=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) accessLocation= http://nsc.vrm.lt/aia/ADIC_CA-A.crt arba http://nsc.vrm.lt/aia/ADIC_CA-B.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
8 priedas

VALSTYBĖS TARNAUTOJO KVALIFIKUOTO ELEKTRONINIO PARAŠO SERTIFIKATO PROFILIS

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			V3(2)
Serial number			automatiškai generuojamas numeris
Signature algorithm			sha256RSA
Issuer			CN=ADIC CA-A arba CN=ADIC CA-B O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
Validity		notBefore	sertifikato galiojimo pradžios data UTC laiku
		notAfter	sertifikato galiojimo pabaigos data UTC laiku
Subject		commonName	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 (2048 bitų) rakto reikšmė ir parašo kūrimo algoritmo identifikatorius (RSA)
Papildomi laukai			
Subject Key Identifier	Ne	keyIdentifier	160 bitų ilgio asmens viešojo rakto identifikatorius
Subject Alternative Name	Ne	RFC822 Name	RFC822 Name=valstybės tarnautojo elektroninio pašto adresas
Authority Key Identifier	Ne	keyIdentifier	160 bitų ilgio ADIC CA-A arba ADIC CA-B viešojo rakto identifikatorius
Certificate Policies	Ne	policyIdentifier	1.3.6.1.4.1.33621.2.3.2
		policyQualifier-Info	policyQualifierId=CPS qualifier=http://nsc.vrm.lt/repository
Authority Information Access	Ne	accessDescription	accessMethod=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation= http://nsc.vrm.lt/OCSP/ocspresponder.nsc
		accessDescription	accessMethod=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) accessLocation= http://nsc.vrm.lt/aia/ADIC_CA-A.crt arba http://nsc.vrm.lt/aia/ADIC_CA-B.crt

Papildomi laukai			
Qualified Certificate Statements	Ne	qualified certificate statement ID	Id-etsi-pcs-QcCompliance (0.4.0.1862.1.1)
		SSCD statement ID	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		PDS statement	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) PdsLocation: URL= http://nsc.vrm.lt/pds language=en
Application policies	Ne	Application Certificate Policy	Policy Identifier=Secure Email Policy Identifier=Document Signing
Key Usage	Taip		Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage	Ne		Secure Email (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12)

_____

Sertifikavimo veiklos nuostatų
9 priedas

VALSTYBĖS TARNAUTOJO ATPAŽINIMO ELEKTRONINĖJE ERDVĖJE SERTIFIKATO PROFILIS

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			V3(2)
Serial number			automatiškai generuojamas numeris
Signature algorithm			sha256RSA
Issuer			CN=ADIC CA-A arba CN=ADIC CA-B O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
Validity		notBefore	sertifikato galiojimo pradžios data UTC laiku
		notAfter	sertifikato galiojimo pabaigos data UTC laiku
Subject		commonName	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 (2048 bitų) rakto reikšmė ir parašo kūrimo algoritmo identifikatorius (RSA)
Papildomi laukai			
Subject Key Identifier	Ne	keyIdentifier	160 bitų ilgio asmens viešojo rakto identifikatorius
Subject Alternative Name	Ne	RFC822 Name	RFC822 Name=valstybės tarnautojo elektroninio pašto adresas
Authority Key Identifier	Ne	keyIdentifier	160 bitų ilgio ADIC CA-A arba ADIC CA-B viešojo rakto identifikatorius
Certificate Policies	Ne	policyIdentifier	1.3.6.1.4.1.33621.2.3.2
		policyQualifier-Info	policyQualifierId=CPS qualifier=http://nsc.vrm.lt/repository
Authority Information Access	Ne	accessDescription	accessMethod=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation= http://nsc.vrm.lt/OCSP/ocspresponder.nsc
		accessDescription	accessMethod=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) accessLocation= http://nsc.vrm.lt/aia/ADIC_CA-A.crt arba http://nsc.vrm.lt/aia/ADIC_CA-B.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
10 priedas

VIDAUS TARNYBOS SISTEMOS PAREIGŪNO KVALIFIKUOTO ELEKTRONINIO PARAŠO SERTIFIKATO PROFILIS

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			V3(2)
Serial number			automatiškai generuojamas numeris
Signature algorithm			sha256RSA
Issuer			CN=ADIC CA-A arba CN=ADIC CA-B O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
Validity		notBefore	sertifikato galiojimo pradžios data UTC laiku
		notAfter	sertifikato galiojimo pabaigos data UTC laiku
Subject		commonName	CN=pareigūno vardas ir pavardė
		givenName	G=pareigūno vardas
		surname	SN=pareigūno pavardė
		serialNumber	SERIALNUMBER=pareigūno kodas vidaus reikalų pareigūnų registre
		countryName	C=LT
		email	E=pareigūno elektroninio pašto adresas
		title	T=pareigūno pareigų pavadinimas
		organization	O=įstaigos, kurioje pareigūnas eina pareigas, pavadinimas
Public key			viešojo (2048 bitų) rakto reikšmė ir parašo kūrimo algoritmo identifikatorius (RSA)
Papildomi laukai			
Subject Key Identifier	Ne	keyIdentifier	160 bitų ilgio asmens viešojo rakto identifikatorius
Subject Alternative Name	Ne	RFC822 Name	RFC822 Name=pareigūno elektroninio pašto adresas
Authority Key Identifier	Ne	keyIdentifier	160 bitų ilgio ADIC CA-A arba ADIC CA-B viešojo rakto identifikatorius
Certificate Policies	Ne	policyIdentifier	1.3.6.1.4.1.33621.2.4.2
		policyQualifier-Info	policyQualifierId=CPS qualifier=http://nsc.vrm.lt/repository
Authority Information Access	Ne	accessDescription	accessMethod=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation= http://nsc.vrm.lt/OCSP/ocspresponder.nsc
		accessDescription	accessMethod=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) accessLocation= http://nsc.vrm.lt/aia/ADIC_CA-A.crt arba http://nsc.vrm.lt/aia/ADIC_CA-B.crt
Qualified Certificate Statements	Ne	qualified certificate statement ID	Id-etsi-pcs-QcCompliance (0.4.0.1862.1.1)
		SSCD statement ID	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		PDS statement	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) PdsLocation: URL= http://nsc.vrm.lt/pds language=en

Papildomi laukai			
Application policies	Ne	Application Certificate Policy	Policy Identifier=Secure Email Policy Identifier=Document Signing
Key Usage	Taip		Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage	Ne		Secure Email (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12)

_____

Sertifikavimo veiklos nuostatų
11 priedas

VIDAUS TARNYBOS SISTEMOS PAREIGŪNO ATPAŽINIMO ELEKTRONINĖJE ERDVĖJE SERTIFIKATO PROFILIS

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			V3(2)
Serial number			automatiškai generuojamas numeris
Signature algorithm			sha256RSA
Issuer			CN=ADIC CA-A arba CN=ADIC CA-B O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
Validity		notBefore	sertifikato galiojimo pradžios data UTC laiku
		notAfter	sertifikato galiojimo pabaigos data UTC laiku
Subject		commonName	CN=pareigūno vardas ir pavardė
		givenName	G=pareigūno vardas
		surname	SN=pareigūno pavardė
		serialNumber	SERIALNUMBER=pareigūno kodas vidaus reikalų pareigūnų registre
		countryName	C=LT
		email	E=pareigūno elektroninio pašto adresas
		title	T=pareigūno pareigų pavadinimas
		organization	O=įstaigos, kurioje pareigūnas eina pareigas, pavadinimas
Public key			viešojo (2048 bitų) rakto reikšmė ir parašo kūrimo algoritmo identifikatorius (RSA)
Papildomi laukai			
Subject Key Identifier	Ne	keyIdentifier	160 bitų ilgio asmens viešojo rakto identifikatorius
Subject Alternative Name	Ne	RFC822 Name	RFC822 Name=pareigūno elektroninio pašto adresas
Authority Key Identifier	Ne	keyIdentifier	160 bitų ilgio ADIC CA-A arba ADIC CA-B viešojo rakto identifikatorius
Certificate Policies	Ne	policyIdentifier	1.3.6.1.4.1.33621.2.4.2
		policyQualifier-Info	policyQualifierId=CPS qualifier=http://nsc.vrm.lt/repository
Authority Information Access	Ne	accessDescription	accessMethod=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation= http://nsc.vrm.lt/OCSP/ocspresponder.nsc
		accessDescription	accessMethod=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) accessLocation= http://nsc.vrm.lt/aia/ADIC_CA-A.crt arba http://nsc.vrm.lt/aia/ADIC_CA-B.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)

_____

E. REZIDENTO KVALIFIKUOTO ELEKTRONINIO PARAŠO SERTIFIKATO PROFILIS

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			V3(2)
Serial number			automatiškai generuojamas numeris
Signature algorithm			sha256RSA
Issuer			CN=ADIC CA-A arba CN=ADIC CA-B O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
Validity		notBefore	sertifikato galiojimo pradžios data UTC laiku
		notAfter	sertifikato galiojimo pabaigos data UTC laiku
Subject		commonName	CN=vardas pavardė
		givenName	G=vardas
		surname	SN=pavardė
		serialNumber	SERIALNUMBER=identifikavimo kodas
Public key			viešojo rakto reikšmė ir parašo kūrimo algoritmo identifikatorius (ECDSA)
Papildomi laukai			
Subject Key Identifier	Ne	keyIdentifier	160 bitų ilgio asmens viešojo rakto identifikatorius
Authority Key Identifier	Ne	keyIdentifier	160 bitų ilgio ADIC CA-A arba ADIC CA-B viešojo rakto identifikatorius
Certificate Policies	Ne	policyIdentifier	1.3.6.1.4.1.33621.2.5.1
		policyQualifier-Info	policyQualifierId=CPS qualifier=http://nsc.vrm.lt/repository
Authority Information Access	Ne	accessDescription	accessMethod=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation= http://nsc.vrm.lt/OCSP/ocspresponder.nsc
		accessDescription	accessMethod=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) accessLocation= http://nsc.vrm.lt/aia/ADIC_CA-A.crt arba http://nsc.vrm.lt/aia/ADIC_CA-B.crt
Qualified Certificate Statement	Ne	EU Qualified Certificate statement	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		SSCD statement	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		PDS statement	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) PdsLocation: URL= http://nsc.vrm.lt/pds language=en
Application policies	Ne	Application Certificate Policy	Policy Identifier=Document Signing
Key Usage	Taip		Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage	Ne		Document Signing (1.3.6.1.4.1.311.10.3.12)

_____

E. REZIDENTO ATPAŽINIMO ELEKTRONINĖJE ERDVĖJE SERTIFIKATO PROFILIS

Pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			V3(2)
Serial number			automatiškai generuojamas numeris
Signature algorithm			sha256RSA
Issuer			CN=ADIC CA-A arba CN=ADIC CA-B O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
Validity		notBefore	sertifikato galiojimo pradžios data UTC laiku
		notAfter	sertifikato galiojimo pabaigos data UTC laiku
Subject		commonName	CN=vardas pavardė
		givenName	G=vardas
		surname	SN=pavardė
		serialNumber	SERIALNUMBER= identifikavimo kodas
Public key			viešojo rakto reikšmė ir parašo kūrimo algoritmo identifikatorius (ECDSA)
Papildomi laukai			
Subject Key Identifier	Ne	keyIdentifier	160 bitų ilgio asmens viešojo rakto identifikatorius
Authority Key Identifier	Ne	keyIdentifier	160 bitų ilgio ADIC CA-A arba ADIC CA-B viešojo rakto identifikatorius
Certificate Policies	Ne	policyIdentifier	1.3.6.1.4.1.33621.2.5.1
		policyQualifier-Info	policyQualifierId=CPS qualifier=http://nsc.vrm.lt/repository
Authority Information Access	Ne	accessDescription	accessMethod=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation= http://nsc.vrm.lt/OCSP/ocspresponder.nsc
		accessDescription	accessMethod=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) accessLocation= http://nsc.vrm.lt/aia/ADIC_CA-A.crt arba http://nsc.vrm.lt/aia/ADIC_CA-B.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
14 priedas

NEGALIOJANČIŲ DARBINĖMS SERTIFIKAVIMO TARNYBOMS IŠDUOTŲ SERTIFIKATŲ SĄRAŠO PROFILIS

CRL pagrindiniai laukai	Atributas	Reikšmė
Version		V2(1)
Signature algorithm		sha256RSA
Issuer		CN=ADIC Root CA O=Asmens dokumentu israsymo centras prie LR VRM 2.5.4.97=188778315 C=LT
This update		išleidimo (galiojimo pradžios) data ir laikas
Next update		galiojimo pabaigos data ir laikas
Negaliojančių sertifikatų sąrašas		
userCertificate		negaliojančio sertifikato serijinis numeris
revocationDate		galiojimo atšaukimo ar laikino sustabdymo data ir laikas
reasonCode		galiojimo atšaukimo ar laikino sustabdymo priežastis
CRL plėtiniai		
Authority Key Identifier	Key Identifier	160 bitų ilgio ADIC Root CA viešojo rakto identifikatorius
CA Version		V0.0
CRL Number		automatiškai ADIC Root CA sudaromas numeris
Next CRL Publish		planuojama atnaujinto sąrašo išleidimo data ir laikas

_____

SERTIFIKAVIMO VEIKLOS NUOSTATŲ PRIEDAS, DETALIZUOJANTIS KAI KURIUOS PATIKIMUMO UŽTIKRINIMO PASLAUGŲ TEIKĖJO VEIKLOS ASPEKTUS

1. [6] Pagrindinis dokumentas, nustatantis kitų asmenims sudaromų sertifikatų sudarymo ir tvarkymo procese dalyvaujančių institucijų vaidmenį yra Sertifikatų valdymo informacinės sistemos nuostatai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2011 m. rugsėjo 19 d. įsakymu Nr. 1V-697 „Dėl Sertifikatų valdymo informacinės sistemos nuostatų patvirtinimo“: https://www.e-tar.lt/portal/lt/legalAct/TAR.7A23B2DD576F/vsLvwkmeel

2. [8^1] Registravimo tarnybų darbuotojai, turintys teisę laikinai sustabdyti arba atšaukti sertifikato galiojimą, panaikinti sertifikato galiojimo laikiną sustabdymą, neturi tiesioginės prieigos prie patikimumo užtikrinimo paslaugų teikėjo sertifikavimo tarnybų infrastruktūros. Šių darbuotojų tapatybė nustatoma per išorines sistemas (Gyventojų registrą, Valstybės tarnautojų registrą, Vidaus reikalų pareigūnų registrą). Užklausos sustabdyti arba atšaukti sertifikato galiojimą, panaikinti sertifikato galiojimo laikiną sustabdymą yra kuriamos šiose išorinėse sistemose ir į patikimumo užtikrinimo paslaugų teikėjo sertifikavimo tarnybas persiunčiamos anonimiškai. Patikimumo užtikrinimo paslaugų teikėjo organizacijoje nėra specifinio vaidmens, atsakingo už asmenims sudaromų sertifikatų galiojimo statuso valdymą. Visos registravimo tarnybų (piliečio sertifikatų atveju – migracijos skyrių, valstybės tarnautojų ir vidaus tarnybos sistemos pareigūnų sertifikatų atveju – valstybės ir savivaldybių įstaigų ir institucijų personalo tarnybų) patikimumo užtikrinimo paslaugų teikėjui siunčiamos užklausos sustabdyti arba atšaukti sertifikato galiojimą, panaikinti sertifikato galiojimo laikiną sustabdymą yra apdorojamos automatiškai.

3. [8^2] Asmens tapatybės kortelių užsakymai yra perduodami ryšio kanalu Gyventojų registras <> Asmens dokumentų išrašymo centras, o užklausos sustabdyti arba atšaukti piliečio sertifikatų galiojimą, panaikinti sertifikatų galiojimo laikiną sustabdymą yra perduodamos ryšio kanalu Gyventojų registras <> Sertifikatų valdymo informacinė sistema. Gyventojų registras ir Asmens dokumentų išrašymo centro sistemos, taip pat Sertifikatų valdymo informacinė sistema veikia dedikuotame vidaus reikalų telekomunikacijų tinkle. Popieriniai dokumentai, pvz., piliečių prašymai, yra saugomi tuose migracijos skyriuose, kuriuose jie yra pateikti. Popieriniai dokumentai yra tvarkomi vadovaujantis bendromis visame valstybiniame sektoriuje galiojančiomis taisyklėmis.

4. [8^3] Valstybės tarnautojo pažymėjimų užsakymai yra perduodami ryšio kanalu Valstybės tarnautojų registras <> Asmens dokumentų išrašymo centras, o užklausos sustabdyti arba atšaukti valstybės tarnautojo sertifikatų galiojimą, panaikinti sertifikatų galiojimo laikiną sustabdymą yra perduodamos ryšio kanalu Valstybės tarnautojų registras <> Sertifikatų valdymo informacinė sistema. Valstybės tarnautojų registras ir Asmens dokumentų išrašymo centro sistemos, taip pat Sertifikatų valdymo informacinė sistema veikia dedikuotame vidaus reikalų telekomunikacijų tinkle. Popieriniai dokumentai, pvz., valstybės tarnautojų prašymai, yra saugomi toje valstybės ar

savivaldybės įstaigos ar institucijos personalo tarnyboje, kurioje jie yra pateikti. Kiekviena valstybės ir savivaldybių įstaigų ir institucijų personalo tarnyba veikia kaip registravimo tarnyba tik toje įstaigoje ar institucijoje dirbantiems valstybės tarnautojams.

5. [8^4] Vidaus tarnybos sistemos pareigūnų tarnybinių pažymėjimų užsakymai yra perduodami ryšio kanalu Vidaus reikalų pareigūnų registras <> Asmens dokumentų išrašymo centras, o užklausos sustabdyti arba atšaukti vidaus tarnybos sistemos pareigūno sertifikatų galiojimą, panaikinti sertifikatų galiojimo laikiną sustabdymą yra perduodamos ryšio kanalu Vidaus reikalų pareigūnų registras <> Sertifikatų valdymo informacinė sistema. Vidaus reikalų pareigūnų registras ir Asmens dokumentų išrašymo centro sistemos, taip pat Sertifikatų valdymo informacinė sistema veikia dedikuotame vidaus reikalų telekomunikacijų tinkle. Popieriniai dokumentai, pvz., vidaus tarnybos sistemos pareigūnų prašymai, yra saugomi toje vidaus tarnybos sistemos įstaigos personalo tarnyboje, kurioje jie yra pateikti. Kiekviena vidaus tarnybos sistemos įstaigos personalo tarnyba veikia kaip registravimo tarnyba tik toje įstaigoje dirbantiems vidaus tarnybos sistemos pareigūnams.

6. [8^5] Informatikos ir ryšių departamento darbuotojai, turintys teisę laikinai sustabdyti piliečio sertifikatų galiojimą, turi tiesioginę prieigą (naudotojo paskyras) prie Gyventojų registro. Sertifikatų galiojimo sustabdymas vykdomas iškart po prašančiojo asmens tapatybės nustatymo. Tarp Informatikos ir ryšių departamento ir Asmens dokumentų išrašymo centro nėra jokio papildomo su sertifikatų galiojimo sustabdymu susijusio popierinių dokumentų apsikeitimo.

7. [22] Ne darbo metu visi skabučiai į telefono numerį (8 5) 271 6062 yra automatiškai peradresuojami į Informatikos ir ryšių departamento techninės pagalbos tarnybą, kuri veikia 7 dienas per savaitę, 24 valandas per parą.

8. [25] Kadangi valstybės tarnautojo ir vidaus tarnybos sistemos pareigūno kvalifikuoti elektroninio parašo sertifikatai gali būti naudojami tik oficialiųjų elektroninių dokumentų pasirašymui, patikimumo užtikrinimo paslaugų teikėjas nėra nustatęs reikalavimo, pagal kurį sertifikatų galiojimą būtų galima sustabdyti 7 dienas per savaitę, 24 valandas per parą. Patikimumo užtikrinimo paslaugų teikėjas tokią nuostatą laiko adekvačia galimai rizikai, todėl šių sertifikatų galiojimo sustabdymas įmanomas tik darbo metu.

9. [32.4] Kvalifikuotus elektroninio parašo kūrimo įtaisus ir PIN kodo vokus gaunančios institucijos (piliečio sertifikatų atveju – migracijos skyriai), taip pat juos vežantys kurjeriai siuntas su elektroninio parašo kūrimo įtaisais ir PIN kodo vokais gauna pasirašytinai. Sekti siuntų pristatymą galima dviem būdais – kurjerių tarnybos siuntų paieškos sistemoje ir Gyventojų registro dedikuotame siuntų paskirstymo modulyje. Rašytinis siuntos įteikimo patvirtinimas nėra grąžinamas Asmens dokumentų išrašymo centrui. Užsakymų tvarkymo procesas yra detaliai aprašytas https://www.e-tar.lt/portal/lt/legalAct/TAR.61D39ED06C43/lYBQHhvivM

10. [32^1] Kvalifikuotų elektroninio parašo kūrimo įtaisų personalizavimo Asmens dokumentų

išrašymo centre metu šiuose įtaisuose yra generuojamos kriptografinių raktų poros (privatusis ir viešasis raktai), viešajam raktui yra kuriama sertifikato užklausa, kuri siunčiama į sertifikavimo tarnybų infrastruktūrą, vienoje iš sertifikavimo tarnybų yra išduodamas sertifikatas ir sertifikato kopija siunčiama atgal į Asmens dokumentų išrašymo centrą jos įrašymui į kvalifikuotą elektroninio parašo kūrimo įtaisą.

11. [44^1] Vienintelis veiksmas, kurį registravimo tarnybos atlieka po kvalifikuoto elektroninio parašo kūrimo įtaiso ir PIN kodo voko įteikimo, yra sertifikatų galiojimo laikino sustabdymo panaikinimas. Pats patikimumo užtikrinimo paslaugų teikėjas jokių papildomų veiksmų neatlieka bei neturi būti privalomai informuotas apie asmens tapatybės kortelės, valstybės tarnautojo pažymėjimo, vidaus tarnybos sistemos pareigūno tarnybinio pažymėjimo ar e. rezidento elektroninės atpažinties ir elektroninio parašo priemonės įteikimą ir tai, kad sertifikatų savininkas raštu patvirtino, kad yra susipažinęs su sertifikatų sudarymo ir tvarkymo sąlygomis ir jomis sutinka.

12. [50^1] Patikimumo užtikrinimo paslaugų teikėjas į sertifikatus neįrašo jokių specifinių požymių, kuriuos skiria specifinius požymius suteikiančios įstaigos (pvz., „daktaras“, „notaras“ ir pan.) ir dėl kurių įrašymo galėtų atsirasti poreikis atšaukti sertifikatą tiems požymiams pasikeitus.

13. [52^1] Patikimumo užtikrinimo paslaugų teikėjas naudoja tokį sertifikavimo tarnybų techninį sprendimą, kuris neleidžia atstatyti atšauktų sertifikatų galiojimo.

14. [63] Kadangi sertifikatų galiojimo statuso teikimui naudojama užklausų sistema naudoja sertifikatų duomenų bazės duomenis tiesiogiai, naują sertifikato galiojimo statusą užklausų sistema teikia be jokio vėlavimo.

15. [70] Naudojama dubliuota katalogo tarnyba – yra du domeno valdikliai – vienas pagrindiniame duomenų centre, kitas – rezerviniame duomenų centre. Skirstymas į pagrindinį ir rezervinį duomenų centrus yra tik sąlyginis, nes abu duomenų centrai veikia lygiagrečiai ir juose veikia identiška įranga. Duomenų bazių sinchronizavimas, įskaitant sertifikatų ir jų galiojimo statuso duomenis, tarp duomenų centrų yra realizuotas naudojant duomenų saugojimo tinklo replikavimo technologijas.

16. [72^1] Asmens dokumentų išrašymo centro Sertifikatų skyrius, kuris teikia pagalbos telefonu paslaugas, operatorių, archyvų patalpos bei kitos patalpos, kuriose vyksta atskiri kvalifikuotų sertifikatų sudarymo procesai, fiziškai randasi sustiprintos apsaugos zonoje. Norėdami patekti į patalpas, darbuotojai naudoja nekontaktines RFID korteles ir biometrinę įrangą. Teisę patekti į atskiras patalpas turinčių patikimumo užtikrinimo paslaugų teikėjo darbuotojų sąrašai yra tvirtinami Asmens dokumentų išrašymo centro direktoriaus įsakymais ir atitinkamai diegiami prieigos valdymo sistemoje. Patikimumo užtikrinimo paslaugų teikėjo darbuotojai neturi prieigos teisių, leidžiančių patekti į Informatikos ir ryšių departamento patalpas, susijusias su kvalifikuotų patikimumo užtikrinimo paslaugų teikimu (visų pirma į abiejuose duomenų centruose esančias įrangos saugyklas).

17. [78] Patikimumo užtikrinimo paslaugų teikėjas taiko originalią kompanijos Microsoft rolių atskyrimo sistemą (https://technet.microsoft.com/library/cc732590.aspx):

Veiklos nuostatai	Windows Server implementacija
Sertifikatų valdymo informacinės sistemos saugos įgaliotinis	Saugos įgaliotinis: Sertifikatų valdymo informacinėje sistemoje paskyros neturi.
Sertifikatų valdymo informacinės sistemos administratorius	Domeno administratorius, Lokalus administratorius: Diegti sertifikavimo tarnybas, atnaujinti sertifikavimo tarnybų raktus, įjungti/išjungti rolių atskyrimą.
Sertifikavimo tarnybos administratorius	Sertifikavimo tarnybos administratorius: Konfigūruoti policy ir exit modulius, stabdyti ir paleisti Certificate Services paslaugą, konfigūruoti plėtinius, konfigūruoti roles, nustatyti Sertifikavimo tarnybos pareigūno teisių ribojimus, duomenų bazėje trinti pavienius įrašus ar įrašų blokus.
Sertifikavimo tarnybos pareigūnas	Certificate Manager (Sertifikavimo tarnybos pareigūnas): Duomenų bazėje trinti įrašų blokus, išduoti ir patvirtiniti sertifikatus, atmesti sertifikatų užklausas, atšaukti sertifikatus, panaikinti sertifikatų galiojimo sustabdymą, atnaujinti sertifikatus.
Sertifikavimo tarnybos operatorius	Atsarginių kopijų operatorius: Daryti failų ir katalogų atsargines kopijas, atstatyti failus ir katalogus iš jų atsarginių kopijų
Sertifikavimo tarnybos auditorius	Auditorius: Tvarkyti audito ir saugos žurnalus

18. [78] Patikimumo užtikrinimo paslaugų teikėjas taiko šią rolių atskyrimo matricą, apibrėžiančią atskirų rolių suderinamumą, paremtą atsakomybių atskyrimo principu:

Rolės	Sertifikatų valdymo informacinės sistemos saugos įgaliotinis	Sertifikatų valdymo informacinės sistemos administratorius	Sertifikavimo tarnybos administratorius	Sertifikavimo tarnybos pareigūnas	Sertifikavimo tarnybos operatorius	Sertifikavimo tarnybos auditorius
Sertifikatų valdymo informacinės sistemos saugos įgaliotinis		X	X	X	X	X
Sertifikatų valdymo informacinės sistemos administratorius	X		X	X		X
Sertifikavimo tarnybos administratorius	X	X		X	X	X
Sertifikavimo tarnybos pareigūnas	X	X	X		X	X
Sertifikavimo tarnybos operatorius	X		X	X		X
Sertifikavimo tarnybos auditorius	X	X	X	X	X	

19. [87[1]] Patikimumo užtikrinimo paslaugų teikėjas nesinaudoja jokių išorės archyvų paslaugomis.

20. [97] Patikimumo užtikrinimo paslaugų teikėjo darbinės sertifikavimo tarnybos naudoja du kompanijos Thales e-Security modelio nShield F3 Connect 1500+ tinklo kriptografinius modulius. Patikimumo užtikrinimo paslaugų teikėjo šakninė sertifikavimo tarnyba naudoja kompanijos Thales e-Security modelio nShield F3 Solo 500+ (PCI Express) kriptografinį modulį. Abu kriptografinių modulių modeliai yra įtraukti į sertifikuotų pagal FIPS 140-2 kriptografinių modulių sąrašą http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#2148

21. [111.4] Duomenų sinchronizavimui tarp pagrindinio ir rezervinio duomenų centrų, kuriuos valdo Informatikos ir ryšių departamentas, yra naudojamas dedikuotas optinis kabelis, saugiam ryšiui tarp duomenų centrų ir patikimumo užtikrinimo paslaugų teikėjo nuosavų sistemų, tarp patikimumo užtikrinimo paslaugų teikėjo nuosavų sistemų ir registravimo tarnybų naudojamų sistemų, taip pat tarp duomenų centrų ir registravimo tarnybų naudojamų sistemų yra naudojamas TLS. Kiekvienos sąsajos atveju abu jos galiniai taškai (serveris ir klientas) TLS rankų paspaudimo metu yra autentifikuojami naudojant autentifikavimo sertifikatus (serverio ir kliento).

22. [114] Vidaus auditorius yra skiriamas konkrečiam auditui pasirengimo auditui metu. Skiriant vidaus auditorių yra vadovaujamasi standarto ISO 19011:2011 4 paragrafo e) punktu.
