Sertifikato taisyklės

SSC GDL CA

Versija 4.4

2013

Pakeitimų istorija

Versija	Data	Paaiškinimai
4.4	2013.05.29	Suderinta su CPS redakcija anglų kalba

TURINYS

1 ĮŽANGA

Esminę dalį elektroninių paslaugų saugumo užtikrina Sertifikavimo tarnybos (angl. *Certification Authority* – CA), kurių procedūros ir prevencinės priemonės minimizuoja potencialių grėsmių ir rizikos galimybes, susijusias su Viešojo rakto infrastruktūros (angl. *Public Key Infrastructure* - PKI) procesais ir saugos valdymu.

Sertifikato Taisyklės (angl. *Certificate Policy* – CP arba Taisyklės) yra aukštesnio lygio dokumentas, kuris taikomas visoms sertifikavimo tarnyboms, valdomoms pagal bendras taisykles. Kitas dokumentas – sertifikavimo veiklos nuostatai (angl. *Certificate Practice Statement* – CPS arba Nuostatai) aprašo, kaip konkreti tarnyba užtikrina šiame dokumente pateiktų techninių, organizacinių ir procedūrinių reikalavimų laikymąsi. Žemesnio lygio dokumentacija, remiantis jos specifika, laikoma privati, gali būti naudojama kasdieninėje veikloje, numatant procedūras, kurios yra būtinos siekiant užtikrinti šiame dokumente nurodytus reikalavimus.

Taisyklės nurodo sąlygas, asmenis ir taikomąsias sistemas, kuriems skirtas šis dokumentas, parengtas remiantis [ETSI TS 101 042], [ETSI101456] ir [ETSITS102023] reikalavimais.

CP struktūra atitinka [RFC3647], todėl kai kurios dalys paliktos dėl suderinamumo, nors tiesiogiai ir nėra susijusios su pagal šias Taisykles teikiamomis paslaugomis.

Raktiniai žodžiai „PRIVALO“, „NEPRIVALO“, „BŪTINA“, „TURI“, „NETURI“, „TURĖTŲ“, „NETURĖTŲ“, „REKOMENDUOJAMA“, „GALI“ ir „PASIRINKTINAI“ šiame dokumente turi būti aiškinami taip, kaip tai aprašyta [RFC2119].

Frazė “Sąlygų nėra*”* šiame dokumente priklausomai nuo konteksto reiški*a* “*netaikoma*” arba “*taikomi aukštesnio lygio normatyvinio dokumento reikalavimai*”.

1.1 Apžvalga

Kiekviena CA PRIVALO išleisti savo veiklos Nuostatus, pateikiant potencialiems klientams

informaciją apie pagrindines technines, procedūrines ir juridines paslaugų teikimo sąlygas. Minėta informacija PRIVALO būti pateikta kaip nuoroda arba su atitinkamu OID (*angl. Object Identifier* – OID)[1] kodu.

Sertifikatai, išduodami pagal šias Taisykles, PRIVALO turėti taikomo sertifikato Taisyklių OID kodą, kuris naudojamas siekiant vertinti, ar sertifikatas gali būti tinkamas konkrečiam naudojimui. Šios Taisyklės taikomos visiems sertifikatams nepriklausomai nuo jų naudojimo, jeigu nėra nurodyta priešingai.

Užsakovai ir *Pasitikinčios šalys,* prieš pradedant naudotis šios sertifikavimo tarnybos išduodamais sertifikatais, PRIVALO susipažinti su šiomis *Taisyklėmis*, CPS ir kitais dokumentais.

1.2 Dokumento pavadinimas ir identifikacija

Sertifikatai, išduoti pagal šias Taisykles, PRIVALO turėti OID, kuris turi būti naudojamas Pasitikinčioms šalimis apsisprendžiant dėl sertifikato tinkamumo ir patikimumo konkrečios aplikacijos atžvilgiu. SSC OID kodą sudaro – OID šaknis ir konkretaus objekto identifikatorius iš SSC OID registro jungtis. OID šaknį paskiria išorinis registras. Šiuo momentu SSC yra identifikuota dviejuose registruose: IANA[2] ir Lietuvos OID Registre[3].

IANA paskirtas SSC identifikatorius: 1.3.6.1.4.1.22501.

SSC OID identifikatorius pagal Lietuvos juridinių asmenų registrą: 2.16.440.1.4.30003763.

Tokiu būdu šios Taisyklės yra identifikuojamos kaip:

1.3.6.1.4.1.22501.0.1.4.4

2.16.440.1.4.30003763.0.1.4.4

1.3 PKI dalyviai

Šioje dokumento dalyje aprašomi vaidmenys, kuriuos atlieka asmenys dalyvaudami PKI sistemoje.

1.3.1 Sertifikavimo tarnybos

Sertifikavimo tarnybos (CA) – tai yra įmonės, kurios išduoda sertifikatus. Sertifikavimo tarnyba, veikianti pagal šias *Taisykles,* PRIVALO išleisti savo Nuostatus, kuriuose būtų aprašytos tarnybos ir jų santykiai su kitais PKI dalyviais.

1 ITU-T rekomendacija X.208 (ASN.1) arba ITU-T rekomendacija X.509 (ISO/IEC 8824).
2 Internet Assigned Numbers Authority.
3 Turi pritarti atsakinga Lietuvos institucija.

1.3.2 Registravimo tarnybos

Registravimo tarnybos (RA) – organizuoja prašymų dėl sertifikato išdavimo priėmimą, tikrina asmens tapatybę, vykdo pareiškėjų identifikaciją ir autentifikaciją. RA taip pat vykdo kitas funkcijas, kurias CA, veikianti pagal šias *Taisykles*, PRIVALO aprašyti savo *Nuostatuose*. CA GALI perduoti vykdyti RA funkcijas vienam ar daugeliui asmenų. Atitinkamuose *Nuostatuose* PRIVALO būti atskleistos visos RA ir jų santykiai su CA SSC PKI sudėtyje.

Jeigu RA funkcijos yra perduotos trečiajai šaliai, CA, veikianti pagal šias Taisykles, PRIVALO užtikrinti, kad informacija apsikeičiama tik su įgaliotais paslaugų teikėjais.

1.3.3 *Užsakovai* ir *Subjektai*

Užsakovu laikomas asmuo, kuriam pagal šias Taisykles yra išduodamas sertifikatas ir kuris sutinka su sąlygomis, išdėstytomis atitinkamuose Nuostatuose. Detalesnė informacija apie *Užsakovus* ir jų santykius su išduotais sertifikatais turi būti aprašyta CPS.

1.3.4 Pasitikinčios šalys

Pasitikinti šalis yra bet koks sertifikato gavėjas, kuris turi pasitikėti sertifikate nurodyta informacija ir sutinka naudotis sertifikatu pagal šių Taisyklių nuostatas.

1.3.5 Kiti dalyviai

Išduodant sertifikatus ir/ar teikiant kitas susijusias paslaugas CA, veikianti pagal šias Taisykles, GALI pasitelkti kitas šalis.

1.4 Sertifikato naudojimas

Sertifikatai, išduoti pagal šias Taisykles, yra tapatybės sertifikatai, kurie sieja asmens viešąjį raktą su asmeniu ir jo duomenimis sertifikate. Šiuose sertifikatuose NEBŪTINAI bus pateikta informacija apie asmens vaidmenį, teises, privilegijas ir įgaliojimus vykdomos veiklos atžvilgiu. Tačiau juose GALI būti informacija, kuri nurodo naudojimo apribojimus.

Taisyklės šiame dokumente taikomos sertifikatams, išduotiems plačiajai visuomenei ir nesukuria kokių nors apribojimų dėl naudotojų rato ar sertifikato tinkamumo.

1.4.1 Tinkamas sertifikato naudojimas

Pasinaudojant atitinkamais protokolais sertifikatai gali būti naudojami serverio arba kliento autentifikavimui, el. parašo kūrimui/tikrinimui, informacijos šifravimui ir dešifravimui.

1.4.2 Draudžiamas sertifikato naudojimas

Sąlygų nėra.

1.5 Taisyklių administravimas

Šio dokumento atnaujintos versijos yra prieinamos *Užsakovams* ir *Pasitikinčioms šalims*.

1.5.1 Taisykles administruojanti organizacija

Šias Taisykles administruoja:

Skaitmeninio sertifikavimo centras

Jogailos 8, LT-01116, Vilnius, LIETUVA

Web: http://www.ssc.lt

El. paštas: info@ssc.lt

Faks.: +370.700.22715

1.5.2 Kontaktinis asmuo

Klausimai dėl šio dokumento turi būti adresuoti:

Skaitmeninio sertifikavimo centras

Jogailos 8, LT-01116 Vilnius, LIETUVA

Tel.: +370.700.22722

Faks.: +370.700.22715

1.5.3 Kas nustato CPS atitiktį Taisyklėms

Įmonės valdybos paskirtas asmuo yra įgaliotas ir atsakingas už Nuostatų suderinimą.

1.5.4 Pritarimo procedūra

CA PRIVALO nurodyti, kokios iš šiame dokumente nurodytų taisyklių bus taikomos teikiant paslaugas ir kokios galimos variacijos pasirinktos.

Asmuo, turintis galutinio sprendimo teisę ir atsakomybę, peržiūri CPS ir vertina jų atitiktį šioms CP. CA PRIVALO paskelbti CPS savo naudotojų bendruomenei[4]. Kai ruošiami dokumento pakeitimai, apie tai PRIVALO būti pranešta iš anksto *Pasitikinčioms šalims* ir kryžminiu būdu sertifikuotoms tarnyboms.

1.6 Apibrėžimai ir sutrumpinimai

Šiame dokumente naudojama terminologija atitinka:

[CWA14167-1]

[ETSITS101042]

[ETSITS101456]

[ETSITS102023].

4 CA naudotojų bendruomenę sudaro: *Užsakovai*/*Subjektai* ir šalys, kurios ketina pasitikėti sertifikatais, išduotais pagal šias CP.

2 TALPYKLA IR JOS VALDYTOJAS

2.1 Talpykla

CA, išduodanti sertifikatus pagal šias Taisykles, privalo skelbti visus jos arba jai išduotus CA sertifikatus ir CRL savo Talpykloje, kuri turi būti pasiekiama per atitinkamą URI (angl. *Uniform Resource Identifier* – URI), nurodytą CA išduotuose sertifikatuose.

Talpykla GALI būti tvarkoma paties CA arba kito paskirto asmens. Pastaruoju atveju CA PRIVALO išlaikyti adekvačią kontrolę, kad užtikrintų atitiktį šioms Taisyklėms. Jeigu Talpyklos tvarkymas perduotas trečiajai šaliai, tai perdavimas PRIVALO būti tinkamai įformintas.

Šios Taisyklės yra skelbiamos viešai: http://gdl.repository.ssc.lt/CP

2.2 Sertifikatų skelbimas

CA PRIVALO užtikrinti, kad sertifikatai atitinkamu laiku yra prieinami *Užsakovams* ir *Subjektams*.

Jeigu įvyksta sistemos sutrikimai, kurie yra už CA kontrolės ribų, tai bus sutelktos visos pastangos, kad informacinė paslauga būtų atstatyta per laikotarpį, nurodytą jos CPS.

2.3 Skelbimo laikas ir dažnumas

Talpyklos informacija PRIVALO būti paskelbta iškart po išleidimo ar CA priėmimo.

2.4 Prieiga prie talpyklos

Prieiga prie CP, CPS ir CRL PRIVALO būti neatlygintina.

CA PRIVALO specialiomis priemonėmis kontroliuoti prieigą prie Talpyklos siekiant išvengti neteisėto Talpyklos informacijos įrašymo, pakeitimo arba ištrynimo.

3 IDENTIFIKAVIMAS IR AUTENTIFIKAVIMAS

Visuose sertifikatuose, išduotuose pagal šias Taisykles, PRIVALO būti X.501 standartui atitinkantis skiriamasis vardas (angl. *Distinguished Name* - DN).

3.1 Vardai

Šios Taisyklės kokių nors apribojimų Šakninių ir Išduodančių tarnybų vardams nenustato.

3.1.1 Vardų tipai

Vardų tipai PRIVALO būti nurodyti CPS.

3.1.2 Vardų reikšmingumas

Sertifikatai, išduoti pagal šias Taisykles, laikomi prasmingi, jeigu juose nurodyti *skiriamieji vardai* yra suprantami *Pasitikinčioms šalims*.

Nors išduodančios tarnybos pavadinimas įprastai nėra interpretuojamas *Pasitikinčios šalies*, šios Taisyklės reikalauja, kad jis būtų reikšmingas. Išduodančios tarnybos pavadinimas PRIVALO būti nurodytas CN atribute:

CN= *SSC GDL Class 1-2 CA*

3.1.3 Anonimiškumas ir pseudonimai

Anonimiškumas arba *Užsakovai* su pseudonimais PRIVALO būti aprašyti CPS.

3.1.4 Skirtingų vardų interpretavimo taisyklės

Vardų interpretavimo taisyklės PRIVALO būti nurodytos CPS.

3.1.5 Vardų unikalumas

CA, veikianti pagal šias Taisykles, PRIVALO užtikrinti, kad *skiriamieji vardai* yra unikalūs CA ribose.

3.1.6 Prekinių ženklų pripažinimas, autentifikavimas ir vaidmuo

Prekinių ženklų pripažinimas, autentifikavimas ir vaidmuo PRIVALO būti aprašytas CPS.

3.2 Pradinis tapatybės tikrinimas

CA, veikianti pagal šias *Taisykles,* PRIVALO užtikrinti, kad disponuoja *Užsakovo* ir *Subjekto* tapatybės nustatymo, jų vardų ir susijusių duomenų tikslumo įrodymais. Jeigu taikoma, asmens tapatybė gali būti nustatyta per atitinkamus ir įgaliotus šaltinius. RA PRIVALO užtikrinti, kad sertifikato prašymai yra tikslūs, įgalioti ir visiškai užpildyti kartu su surinkta tapatybės įrodymo ar patvirtinimo informacija.

Jeigu sertifikatai išduodami įrangai ar paslaugai, CA surinks atitinkamo atsakingo asmens dokumentus.

3.2.1 Privataus rakto turėjimo įrodymas

Registravimo procesas PRIVALO reikalauti iš *Subjekto* įrodyti privataus rakto disponavimo faktą. Šis procesas PRIVALO būti aprašytas CPS.

3.2.2 Organizacijos autentifikacija

Organizacijos tapatybės nustatymas PRIVALO būti aprašytas CPS. CA PRIVALO identifikuoti aukštą riziką keliančius prašymus ir atlikti papildomus būtinus prevencinius veiksmus.

3.2.3 Individualaus asmens autentifikacija

Įprastomis aplinkybėmis *Subjektas* PRIVALO asmeniškai apsilankyti RA ir būti vizualiai autentifikuotas. Ypatingomis sąlygomis, kai Subjekto apsilankymas būtų neįmanomas arba praktiškai sunkiai realizuojamas, GALI būti numatyta išimtis iš šio reikalavimo. Šios sąlygos ir įgaliojimo reikalavimai PRIVALO būti aprašyti CPS.

3.2.4 Netikrinama informacija

Nepatikrinti *Užsakovo* duomenys į sertifikatą nebus įrašomi.

3.2.5 Įgaliojimų tikrinimas

Įgaliojimo tikrinimo procedūra PRIVALO būti aprašyta CPS.

3.2.6 Sąveikumo kriterijai

CA gali teikti sąveikumo paslaugas kitoms CA arba taikomųjų sistemų kūrėjams. Sąveikumo sąlygos PRIVALO būti aprašytos sutartyje tarp šalių. Sutarties sąlygos NEGALI prieštarauti šioms Taisyklėms.

3.3 Identifikavimas ir autentifikavimas sertifikavimo tikslais

3.3.1 Identifikavimas ir autentifikavimas įprastam sertifikavimui

CA sertifikato atstatymo procedūra sutampa su pradiniu sertifikato išdavimu.

Subjekto sertifikato atstatymas PRIVALO būti aprašytas CPS.

3.3.2 Identifikavimas ir autentifikavimas po atšaukimo

Subjekto identifikavimas ir autentifikavimas sertifikato atstatymo tikslais po atšaukimo priklauso nuo atšaukimo priežasties. CPS PRIVALO aprašyti, kokiomis sąlygomis tai būtų leidžiama.

3.4 Identifikavimas ir autentifikavimas atšaukimo tikslais

Identifikavimas ir autentifikavimas atšaukimo tikslais PRIVALO būti aprašytas CPS.

4 REIKALAVIMAI SERTIFIKAVIMO VEIKLAI

CA PRIVALO turėti CPS ir procedūras, kurios įgyvendina šiose CP nurodytus reikalavimus. CPS PRIVALO nustatyti kitų organizacijų, dalyvaujančių CA veikloje, įsipareigojimus, įskaitant taikomas taisykles ir nuostatus. CA PRIVALO pateikti *Užsakovams* ir *Pasitikinčioms šalims* CPS ar kitus susijusius dokumentus, kurių reikia siekiant įvertinti Nuostatų atitiktį paslaugų Taisyklėms.

CA neprivalo atskleisti visų savo taikymo nuostatų viešai.

4.1 Prašymas išduoti sertifikatą

Prašymo išduoti sertifikatą proceso metu PRIVALO būti pateikiama pakankamai informacijos siekiant nustatyti *Užsakovo* įgaliojimus įsigyti sertifikatą, nustatyti *Užsakovo* tapatybę, gauti *sertifikato Subjekto* viešąjį raktą, nustatant, ar jis/ji valdo prašomo išduoti sertifikato privatųjį raktą, patikrinti bet kokią kitą informaciją, kuri įrašoma į sertifikatą.

4.1.1 Kas gali prašyti išduoti sertifikatą

Kas gali pateikti prašymą sertifikato išdavimui PRIVALO būti nurodyta CPS.

4.1.2 Išdavimo procesas ir atsakomybės

Išdavimo procesas ir atsakomybė PRIVALO būti aprašyta CPS.

4.2 Prašymo išduoti sertifikatą apdorojimas

CA, veikianti pagal šias CP, PRIVALO turėti prašymų išduoti sertifikatą tikrinimo procedūras. Siekiant išvengti *sukčiavimo apsimetant* ir kitų sukčiavimo atakų, CA, veikdama pagal šias CP, PRIVALO gebėti atpažinti aukštos rizikos sertifikatų prašymus.

4.2.1 Identifikavimo ir autentifikavimo funkcijų vykdymas

Identifikavimo ir autentifikavimo funkcijų vykdymas PRIVALO būti apibrėžtas CPS.

4.2.2 Prašymo išduoti sertifikatą priėmimas arba atsisakymas

CA PRIVALO atskleisti *Užsakovams* potencialias prašymo išduoti sertifikatą atmetimo

priežastis.

4.2.3 Prašymo apdorojimo laikas

Prašymo apdorojimo laikas PRIVALO būti apibrėžtas CPS.

4.3 Sertifikato išdavimas

Sertifikato išdavimas PRIVALO būti aprašytas CPS.

4.3.1 CA veiksmai išduodant sertifikatą

CA PRIVALO įsitikinti, kad prašymas išduoti sertifikatą yra užpildytas visiškai, tikslus ir tinkamai įgaliotas. Tai liečia sertifikatų atnaujinimą, sertifikatų su nauju raktu po atšaukimo arba prieš pasibaigiant sertifikato galiojimui išdavimą ir sertifikatų pakeitimą, kai keičiasi *sertifikato Subjekto* tapatybės informacija.

4.3.2 CA pranešimas užsakovui apie sertifikato išdavimą

CA, veikdama pagal šias Taisykles, PRIVALO informuoti *Užsakovą* apie sertifikato generavimą.

4.4 Sertifikato priėmimas

CA PRIVALO užtikrinti, kad po generavimo sertifikatai būtų tinkamai prieinami *Užsakovams*, sertifikatų *Subjektams*.

4.4.1 Sertifikato priėmimą patvirtinantis elgesys

CPS PRIVALO būti nurodoma kaip *Užsakovai* patvirtina sertifikato priėmimą.

4.4.2 Sertifikato skelbimas

CA PRIVALO skelbti savo Šakninius ir Išduodančios CA sertifikatus ir taip pat GALI skelbti sertifikato *Subjekto* sertifikatus.

4.4.3 CA pranešimas kitiems asmenims apie sertifikato išdavimą

Įmonės valdyba PRIVALO būti informuota, kai šakninė CA, veikianti pagal šiuos CP, išduoda CA sertifikatą.

4.5 Raktų poros ir sertifikato naudojimas

Raktų poros naudojimo apimtis PRIVALO būti nurodyta sertifikatų plėtiniuose. CPS TURĖTŲ būti nurodomi specialūs apribojimai, jei tokie yra.

4.5.1 Privataus rakto ir sertifikato naudojimas

Sąlygų nėra.

4.5.2 Viešojo rakto ir sertifikato naudojimas pasitikinčioms šalimis

Sąlygų nėra.

4.6 Sertifikato pratęsimas

Sertifikato pratęsimas reiškia naujo sertifikato išdavimą su tuo pačiu sertifikato *Subjektui priskirtu vardu (DN),* viešuoju raktu ir kita informacija nurodyta turimame sertifikate. Turimas sertifikatas pasirinktinai gali būti atšauktas.

CA GALI išduoti naują sertifikatą naudojant ankstesnį sertifikato *Subjekto* sertifikuotą viešąjį raktą, jei tik jo kriptografinis saugumas yra pakankamas naujo sertifikato galiojimo laikotarpiui ir nėra jokių požymių, kad sertifikato *Subjekto* privatus raktas buvo sukompromituotas.

4.6.1 Sertifikato pratęsimo aplinkybės

CA sertifikatai ir OCSP atsakiklio sertifikatai GALI būti pratęsti, jei bendras pratęsto sertifikato laikotarpis neviršija nustatyto sertifikato galiojimo laikotarpio.

4.6.2 Kas gali prašyti pratęsti sertifikatą

CA GALI prašyti pratęsti savo CA sertifikatą arba OCSP atsakiklio sertifikatą.

4.6.3 Prašymo pratęsti sertifikatą apdorojimas

Bet kokiam Šakninio ar Išduodančios CA sertifikato pratęsimui[5] PRIVALO būti SSC valdybos įgalioto asmens patvirtinimas.

4.6.4 Pranešimas užsakovui apie naujo sertifikato išdavimą

CA PRIVALO informuoti *Užsakovą* apie sertifikato pratęsimą.

4.6.5 Pratęsto sertifikato priėmimą patvirtinantis elgesys

Sąlygų nėra.

4.6.6 Pratęsto sertifikato skelbimas

Sąlygų nėra.

4.6.7 Pranešimas kitiems asmenims apie sertifikato išdavimą

Sąlygų nėra.

4.7 Sertifikato atstatymas

Sertifikato atstatymas reiškia naujo sertifikato su nauju viešuoju raktu generavimą, paliekant esamo sertifikato likusį turinį.

Naujas sertifikatas GALI turėti skirtingą galiojimo laikotarpį, nurodyti kitą *CRL DP* ar būti pasirašytas kitos *Išduodančios CA*.

CA PRIVALO užtikrinti, kad anksčiau CA registruoto *sertifikato Subjekto* prašymai yra užpildyti visiškai, tikslūs ir tinkamai įgaliojantys. Tai apima sertifikato atnaujinimą, kai

5 Dėl kitų priežasčių nei *Šakninės* CA sertifikato atstatymas.

išduodamas sertifikatas su nauju *Subjekto* raktu po sertifikato atšaukimo arba prieš pasibaigiant sertifikato galiojimui, arba apima pakeitimą siekiant pakeisti s*ertifikato Subjekto* atributus.

4.7.1 Sertifikato atstatymo aplinkybės

Sertifikato atstatymas galimas dėl šių aplinkybių kaip sertifikato galiojimo pasibaigimas, rakto kompromitacija ar laikmenos pakeitimas.

4.7.2 Kas gali prašyti sertifikato atstatymo

Užsakovai, turintys galiojantį sertifikatą, GALI prašyti sertifikato atstatymo. RA sertifikato *Subjekto* vardu GALI prašyti naujo viešojo rakto sertifikavimo. Įrenginių/paslaugų sertifikatų atveju, naujo viešojo rakto sertifikavimo GALI prašyti atsakingas asmuo.

4.7.3 Prašymo atstatyti sertifikatą apdorojimas

Prieš pradedant apdoroti prašymą, prašymas atstatyti sertifikatą PRIVALO būti patikrintas. Sertifikato atstatymo prašymas gali būti apdorotas pagal pradinio išdavimo procesus.

4.7.4 Pranešimas užsakovui apie naujo sertifikato išdavimą

Sąlygų nėra.

4.7.5 Atstatyto sertifikato priėmimą patvirtinantis elgesys

Sąlygų nėra.

4.7.6 Atstatyto sertifikato publikavimas

Sąlygų nėra.

4.7.7 Pranešimas kitiems asmenims apie sertifikato išdavimą

Sąlygų nėra.

4.8 Sertifikato pakeitimas

Sertifikato pakeitimas reiškia naujo sertifikato išdavimą, kuris turi tą patį arba naują raktą ir skiriasi vienu ar daugiau sertifikato laukų nuo senojo sertifikato.

Senasis sertifikatas GALI būti atšauktas pasirinktinai.

4.8.1 Sertifikato pakeitimo aplinkybės

Sąlygų nėra.

4.8.2 Kas gali prašyti pakeisti sertifikatą

Sąlygų nėra.

4.8.3 Prašymų pakeisti sertifikatą apdorojimas

Sąlygų nėra.

4.8.4 Pranešimas užsakovui apie naujo sertifikato išdavimą

Sąlygų nėra.

4.8.5 Pakeisto sertifikato priėmimą patvirtinantis elgesys

Sąlygų nėra.

4.8.6 Pakeisto sertifikato skelbimas

Sąlygų nėra.

4.8.7 Pranešimas kitiems asmenims apie sertifikato išdavimą

Sąlygų nėra.

4.9 Sertifikato atšaukimas ir sustabdymas

CA, veikdama pagal šiuos CP, PRIVALO išduoti CRL, apimančius visus galiojančius

sertifikatus, išskyrus OCSP atsakiklio sertifikatus su *id-pkix-ocsp-nocheck* išplėtimu.

CA, veikdama pagal šias Taisykles, PRIVALO viešai paskelbti, kaip gauti sertifikatų atšaukimo informaciją. Ši informacija PRIVALO būti perduodama *Užsakovams* sertifikato prašymo ar išdavimo metu ir PRIVALO būti lengvai prieinama bet kokiai *Pasitikinčiai šaliai.*

Atšaukimo prašymas PRIVALO būti patvirtintas. Prašymas atšaukti sertifikatą GALI būti patvirtintas naudojant atšaukiamo sertifikato privatųjį raktą.

CA sertifikatų sustabdymas nėra leidžiamas pagal šias Taisykles. Tačiau *Subjektų* sertifikatų sustabdymas GALI būti leistinas.

CA PRIVALO pateikti mechanizmą, užtikrinantį, kad anuliuoti sertifikatai būtų nedelsiant atšaukti. Atšaukimo mechanizmas PRIVALO leisti sertifikatų naudotojams kreiptis ir laiku gauti nedviprasmišką informaciją apie bet kokio CA išduoto sertifikato atšaukimo statusą. Atšaukimo mechanizmas PRIVALO būti nurodytas CPS.

4.9.1 Atšaukimo aplinkybės

Sertifikatai PRIVALO būti atšaukti, kai sukompromituojamas privatusis raktas arba su sertifikatu susiję aktyvavimo duomenys. Raktų kompromitacija apima neįgaliota prieiga prie privataus rakto arba aktyvavimo duomenų, privataus rakto arba aktyvavimo duomenų praradimas, raktų vagystė arba sunaikinimas.

4.9.2 Kas gali prašyti atšaukti sertifikatą

Asmenys, kurie GALI prašyti sertifikato atšaukimo, PRIVALO būti nurodyti CPS.

CA taip pat PRIVALO apibrėžti, kokiu būdu atšaukimo prašymas GALI būti sukurtas ir kaip jis bus apdorojamas. Visi atšaukimo prašymai, atšaukimo priežastys ir po to sekantys CA veiksmai PRIVALO būti dokumentuoti.

4.9.3 Atšaukimo apdorojimo procedūra

Prašymas atšaukti sertifikatą PRIVALO nurodyti atšaukiamą sertifikatą, atšaukimo priežastis ir būti autentifikuojamas. Sertifikato atšaukimo procesas PRIVALO būti aprašytas CPS.

4.9.4 Atšaukimo uždelsimas

Sąlygų nėra.

4.9.5 Laikas per kurį atšaukimą privaloma apdoroti sertifikavimo tarnyboje

CA PRIVALO atšaukti sertifikatus taip greitai, kaip praktiškai gaunamas tinkamas prašymas dėl atšaukimo.

Atšaukimo prašymai PRIVALO būti apdoroti iki CRL publikavimo, išskyrus prašymus, gautus likus 2 valandoms iki CRL generavimo.

4.9.6 Reikalavimas pasitikinčioms šalims tikrinti atšaukimą

Kadangi atšauktų sertifikatų naudojimas GALI sukelti kenksmingas pasekmes, tai *Pasitikinčioms šalims* rekomenduojama visada tikrinti sertifikatų galiojimą.

4.9.7 CRL išdavimo dažnumas

CRL PRIVALO būti išduodamas periodiškai, net jei nėra sertifikatų atšaukimo būsenos pasikeitimų. Sertifikatų statuso informacija GALI būti pateikiama dažniau nei numatytas CRL išdavimo dažnumas.

Kai CRL yra vienintelis būdas teikiant sertifikatų atšaukimo informaciją, tai:

- kiekvienas CRL PRIVALO nurodyti kito CRL išdavimo laiką;
- naujas CRL GALI būti generuojamas anksčiau nei numatytas CRL išdavimas;
- CRL PRIVALO būti pasirašytas CA arba kitos įgaliotos tarnybos.

Išsami CRL paskelbimo informacija PRIVALO būti nurodyta CPS.

4.9.8 Maksimalus CRL uždelsimas

CRL PRIVALO būti paskelbti kiek įmanoma greičiau po jų sugeneravimo.

4.9.9 Galimybė tikrinti atšaukimą/būseną On-line būdu

Sertifikato statuso informacija PRIVALO būti atnaujinama ir prieinama *Pasitikinčioms šalims* per 24 valandas nuo sertifikato atšaukimo ir CA PRIVALO palaikyti sertifikato statuso patikrinimą on-line būdu per OCSP [RFC2560] .

4.9.10 Reikalavimai tikrinti atšaukimą/būseną On-line būdu

Sąlygų nėra.

4.9.11 Kitos atšaukimo skelbimo formos

CA GALI naudoti kitas sertifikatų statuso atšaukimo skelbimo formas, kurios PRIVALO būti aprašytos CPS.

4.9.12 Specialūs reikalavimai rakto kompromitavimo atveju

CA sertifikatas PRIVALO būti atšauktas per 4 valandas nuo pranešimo gavimo.

4.9.13 Aplinkybės galiojimo sustabdymui

CA GALI teikti sertifikatų sustabdymo paslaugą. Skirtingai nuo atšaukimo, laikinas sertifikato sustabdymas leidžia iš naujo aktyvinti sertifikatą. Sustabdyto sertifikato galiojimo terminas lieka nepakitęs.

4.9.14 Kas gali prašyti sustabdyti galiojimą

Atvejais, kai CA teikia sertifikatų sustabdymo paslaugą, CA PRIVALO priimti *Užsakovo*

prašymą dėl sertifikato sustabdymo.

4.9.15 Sustabdymo prašymo procedūra

CA PRIVALO autentifikuoti asmenį, prašantį sertifikato sustabdymo.

4.9.16 Sustabdymo periodo ribos

Sąlygų nėra.

4.10 Sertifikato būsenos tikrinimo paslaugos

Sąlygų nėra.

4.10.1 Veikimo principas

Sąlygų nėra.

4.10.2 Paslaugos prieinamumas

Sąlygų nėra.

4.10.3 Pasirinktinos galimybės

Sąlygų nėra.

4.11 Paslaugos teikimo pabaiga

Sąlygų nėra.

4.12 Raktų atsarginis saugojimas ir atstatymas

CA privatieji raktai NEPRIVALO būti perduoti trečios šalies saugojimui.

4.12.1 Raktų atsarginio saugojimo ir atstatymo taisyklės ir nuostatai

Sąlygų nėra.

4.12.2 Seanso rakto saugojimo ir atstatymo taisyklės ir nuostatai

Sąlygų nėra.

5 PATALPOS, ADMINISTRAVIMAS IR VEIKLOS KONTROLĖ

Sertifikavimo tarnyba PRIVALO užtikrinti, kad administravimo ir valdymo procedūros taikomos laikantis pripažintos „geriausios praktikos“[6].

Sertifikavimo tarnyba PRIVALO prisiimti atsakomybę už visus savo veiklos aspektus, nepriklausomai nuo to, ar tam tikros jos funkcijos yra perduotos trečiosioms šalims. Sertifikavimo tarnyba PRIVALO aiškiai apibrėžti trečiųjų šalių atsakomybę ir atitinkamomis priemonėmis užtikrinti, kad trečiosios šalys yra įpareigotos įgyvendinti sertifikavimo tarnybos reikalavimus.

Informacijos saugos infrastruktūra, reikalinga valdyti sertifikavimo tarnybos saugumą, PRIVALO būti palaikoma visą laiką. Bet kokie pakeitimai, įtakojantys saugumo lygį, PRIVALO būti patvirtinti sertifikavimo tarnybos valdymo organo.

Sertifikavimo tarnybos saugumo politika (SP), apimanti CA patalpų, sistemų ir informacinių išteklių saugos valdymą ir darbines procedūras, PRIVALO būti dokumentuota[7], įgyvendinta ir palaikoma. Sertifikavimo tarnyba PRIVALO užtikrinti, kad sistemos komponentai yra saugūs ir funkcionuoja korektiškai priimtinos gedimo rizikos ribose:

- Sertifikavimo tarnybos komponentų ir informacijos vientisumas PRIVALO būti apsaugotas nuo virusų, kenkėjiškos ir neteisėtos programinės įrangos;
- Procedūros, skirtos pranešti apie įvykusius incidentus ir reaguoti į juos, PRIVALO būti įgyvendintos tokiu būdu, kad šių incidentų padaryta žala būtų sumažinta iki minimumo.
- Visiems patikimiems ir administraciniams vaidmenims, darantiems poveikį paslaugų tiekimui, turi būti nustatytos ir įgyvendintos atitinkamos procedūros.

Kada saugos bei kontrolės priemonės, kurių reikalauja šios Taisyklės, jau yra naudojamos sertifikavimo tarnybos veikloje, atitinkami dokumentai PRIVALO būti nurodyti CPS, panaudojant jų pavadinimus arba OID.

6 CA PRIVALO atlikti rizikos vertinimą siekiant įvertinti veiklos riziką, ir numatyti reikalingus saugos reikalavimus bei procedūras. Rizikos įvertinimas PRIVALO būti reguliariai peržiūrimas ir atnaujinamas (ISO/IEC 27001, ISO/IEC 27002). CA PRIVALO užtikrinti, kad jos turtas, įskaitant informacinius išteklius, yra tinkamai apsaugotas, identifikuojant visus informacinius išteklius ir priskiriant klasifikacinei grupei, atsižvelgiant į rizikos vertinimą.

7 Saugos taisyklės PRIVALO identifikuoti atitinkamus objektus ir potencialią grėsmę bei numatyti saugos priemones, kad atitinkamai su rizikos vertinimu apribotų galimų grėsmių pasekmes. PRIVALO būti aprašytos taisyklės, nurodymai ir procedūros kaip užtikrinamas reikalingas saugos lygis, papildomai nurodant veiksmus incidentų ir stambių avarijų atvejais.

5.1 Fizinė kontrolė

Visi fizinės kontrolės reikalavimai, nurodyti šiose Taisyklėse, taikytini šakninei sertifikavimo tarnybai, pasirašančiajai sertifikavimo tarnybai ir visoms sertifikavimo tarnybos bei RA sistemų kompiuterizuotoms darbo vietoms, išskyrus atvejus, kurie specialiai pažymėti.

Sertifikavimo tarnyba, išduodama sertifikatus pagal šias Taisykles, PRIVALO užtikrinti, kad fizinė prieiga prie svarbiausių paslaugų yra kontroliuojama ir rizika, siejama su fizine ir aplinkos sauga[8], yra minimizuota:

- fizinė prieiga prie įrenginių, palaikančių svarbias paslaugas, PRIVALO būti leidžiama tik tinkamai įgaliotiems asmenims;
- PRIVALO būti įgyvendintas valdymas, padedantis išvengti nuostolių, žalos ar grėsmės turtui ar veiklai;
- PRIVALO būti imtasi priemonių siekiant išvengti informacijos, informacijos laikmenų sukompromitavimo ar vagysčių.

Sertifikatų generavimo, laikmenos paruošimo bei atšaukimo funkcijos PRIVALO būti vykdomos aplinkoje, kuri fiziškai apsaugotų nuo neteisėtos prieigos prie sistemos ar duomenų. Asmenys, patenkantys į šią saugią zoną, NEGALI būti palikti be personalo priežiūros. Sertifikatų generavimo, laikmenų paruošimo bei sertifikatų atšaukimo vykdymo patalpos PRIVALO būti fiziškai atskirtos. Patalpų dalys negali būti dalijamos su kitomis organizacijomis.

Aplinkos ir fizinės saugos priemonės PRIVALO būti įgyvendintos siekiant apsaugoti patalpas su sistemine įranga, pačius sistemos resursus bei jų funkcionalumą palaikančią įrangą. Sertifikavimo tarnybos fizinė ir aplinkos saugos politika sertifikatų generavimo, laikmenos paruošimo ir sertifikatų atšaukimo vykdymo dalyje PRIVALO numatyti fizinės prieigos kontrolės, apsaugos nuo stichinių nelaimių, priešgaisrinės apsaugos priemones, priemones komunalinių sistemų infrastruktūros gedimo ir vandens nuotėkų atvejams, apsaugos nuo vagysčių, įsilaužimų, neteisėto patekimo ir veiklos atstatymo po avarijos priemones.

PRIVALO būti įgyvendinta kontrolė apsauganti nuo neautorizuoto įrangos, informacijos, duomenų laikmenų ir programinės įrangos, susijusios su sertifikavimo tarnybos paslaugomis, išnešimo.

8 Vadovaujantis ISO/IEC 27002.

5.1.1 Patalpų vieta ir statyba

Sertifikavimo tarnybos įrangos patalpų vieta ir konstrukcija, kaip ir sertifikavimo tarnybos patalpų, naudojamų administravimui, PRIVALO atitikti didelės vertės bei jautrios informacijos saugojimui skirtų patalpų reikalavimus.

5.1.2 Fizinė prieiga

Fizinės prieigos kontrolė PRIVALO užtikrinti, kad būtų neleidžiama nesankcionuota prieiga prie įrangos.

Jei patalpose nėra nuolatos dirbama, tai paskutinis jas paliekantis asmuo PRIVALO pažymėti patalpų palikimo laiką ir datą bei įsitikinti, kad visos būtinos fizinės apsaugos priemonės yra vietoje ir aktyvuotos.

5.1.3 Elektra ir oro kondicionavimas

Sertifikavimo tarnyba PRIVALO turėti pakankamai resursų, užtikrinančių automatinį atliekamų veiksmų bei duomenų išsaugojimą prieš sistemai išsijungiant nuo maitinimo, įtampos pertrūkio ar kondicionavimo sistemos gedimo.

Saugykloje PRIVALO būti įrengta nepertraukiamo maitinimo sistema, kurios resursų užtektų bent 8 darbo valandoms nesant pagrindinės maitinimo įtampos.

5.1.4 Vandentiekio gedimai

Sertifikavimo tarnybos įranga PRIVALO būti sumontuota ant paaukštintų grindų, kad išvengtų sąlyčio su vandeniu.

5.1.5 Gaisro prevencija ir saugumas

Sąlygų nėra.

5.1.6 Laikmenų saugojimas

Visos duomenų laikmenos PRIVALO būti saugomos saugiai, laikantis informacijos klasifikavimo schemos reikalavimų.

Nebereikalingos duomenų laikmenos, talpinančios svarbius duomenis, PRIVALO būti saugiai sunaikintos. Duomenų laikmenos, naudojamos sertifikavimo tarnybos sistemoje, PRIVALO būti saugiai tvarkomos siekiant apsaugoti jas nuo pažeidimų, vagysčių bei senėjimo.

5.1.7 Atliekų šalinimas

Nereikalingi svarbūs duomenys ir dokumentacija PRIVALO būti sunaikinti saugiu būdu.

5.1.8 Rezervinė kopija saugojama išorėje

Duomenų ir sistemos atsarginės kopijos, skirtos atstatymui po avarijos, PRIVALO būti daromos periodiškai ir aprašytos CPS.

5.2 Procedūrų kontrolė

Sertifikavimo tarnyba PRIVALO naudoti patikimas sistemas bei produktus, kurie yra apsaugoti nuo modifikacijos[9].

Siekiant užtikrinti saugos integraciją į sertifikavimo tarnybos sistemas, bet kokios sistemos projektavimo ir reikalavimų nustatymo fazėje, PRIVALO būti atliekama saugumo reikalavimų analizė. Pakeitimų kontrolės procedūros PRIVALO būti taikomas visoms naujoms versijoms, jų modifikacijoms bei skubiems naudojamos programinės įrangos pataisymams.

Šios saugumo operacijos PRIVALO būti atskirtos nuo kitų operacijų:

- atsakingos sertifikavimo tarnybos procedūros;
- saugių sistemų planavimas ir priėmimas;
- apsauga nuo kenksmingos programinės įrangos;

9 CA veiklos rizikos vertinimas PRIVALO identifikuoti kritinius komponentus, reikalaujančias patikimų sistemų, ir reikalaujamus atitikties lygius. Reikalavimai patikimoms sistemoms nustatomi pagal [CWA14167-1] arba tinkamą saugumo profilį, nustatytą pagal ISO/IEC 15408.

- atsarginės kopijos;
- tinklo valdymas;
- aktyvi audito žurnalų stebėsena, įvykių tyrimas ir iš to sekantys veiksmai;
- duomenų laikmenų tvarkymas ir apsauga;
- duomenų ir programinės įrangos pakeitimai.

Šios operacijos PRIVALO būti valdomos patikimo personalo, tačiau gali būti atliekamos ne specialistų, tinkamam personalui prižiūrint.

5.2.1 Patikimi vaidmenys

Sertifikavimo tarnyba, dirbanti pagal šias Taisykles, nustato patikimus vaidmenis savo CPS.

5.2.2 Būtinas personalo skaičius per užduotį

Sertifikavimo tarnyba, dirbanti pagal šias taisykles, savo CPS nustato kritines operacijas reikalaujančias dviejų ar daugiau žmonių[10].

5.2.3 Identifikavimas ir autentifikavimas kiekvienam vaidmeniui

Visi Sertifikavimo tarnybos vaidmenys PRIVALO reikalauti dviejų faktorių autentifikacijos prieš leidžiant atlikti bet kokį veiksmą skirtą tam vaidmeniui.

5.2.4 Vaidmenys, reikalaujantys pareigybių atskyrimo

Sertifikavimo tarnyba, dirbanti pagal šias Taisykles, PRIVALO skirti šiuos tris vaidmenis: Informacinių sistemų saugos vadovas, sistemos administratorius, sertifikavimo tarnybos administratorius.

Pareigybių atskyrimas PRIVALO būti priimtinas su sąlyga, jog atsparumas vidinei atakai yra stiprus ir vaidmenys identifikuoti CPS.

10 Dalyvaujančių ir žinančių apie vykdomų operacijų charakterį.

5.3 Personalo valdymas

Sertifikavimo tarnyba, dirbanti pagal šias Taisykles, užtikrina, jog darbuotojai ir įdarbinimo praktika palaiko sertifikavimo tarnybos operacijų patikimumą.

Svarbus sertifikavimo tarnybos personalas paskiriamas raštiškai ir PRIVALO gauti tinkamą apmokymą savo pareigų vykdymui.

5.3.1 Kvalifikacija, patirtis ir leidimo reikalavimai

Kvalifikacijos, patirties ir biografijos patikros reikalavimai vykdytojams, vadovams, prižiūrėtojams ir tikrintojams PRIVALO būti išdėstyti CPS.

5.3.2 Biografijos tikrinimo procedūros

Nepriklausomai nuo paskyrimo datos, aukštesnio išsilavinimo laipsnis PRIVALO būti patikrintas.

Sertifikavimo tarnybos personalas PRIVALO praeiti patikrinimą apimantį šias sritis: darbo, išsilavinimo, gyvenamosios vietos, teistumo ir rekomendacijų. Kiekvienos srities patikrinimas PRIVALO apimti bent paskutinių penkerių metų laikotarpį, išskyrus gyvenamosios vietos patikrinimą, kuris PRIVALO apimti bent trejų metų laikotarpį.

5.3.3 Mokymo reikalavimai

Sertifikavimo tarnybos ir RA personalas PRIVALO išklausyti išsamius mokymus.

5.3.4 Mokymų dažnumas ir reikalavimai

Personalas, atsakingas už PKI vaidmenis, PRIVALO būti informuojamas apie sertifikavimo tarnybos veiklos pokyčius.

5.3.5 Darbuotojų rotacijos dažnumas ir eiliškumas

Sąlygų nėra.

5.3.6 Sankcijos už neleistinus veiksmus

Sertifikavimo tarnyba PRIVALO imtis administracinių bei drausminių veiksmų prieš darbuotojus atlikusius neteisėtus veiksmus, susijusius su sertifikavimo tarnybos, RA veikla pagal šias Taisykles, CPS ar kitas nustatytas procedūras.

5.3.7 Reikalavimai dirbantiems pagal sutartį

Pagal sutartį dirbantiems ir vykdantiems patikimus vaidmenis, taikomi visi reikalavimai nurodyti šiose Taisyklėse.

5.3.8 Dokumentacija personalui

Kiekvienam vaidmeniui PRIVALO būti parengta dokumentacija, aprašanti priskiriamas pareigas ir procedūras.

5.4 Audito žurnalo procedūros

Audito žurnalų failai ar ataskaitos PRIVALO būti generuojami visiems įvykiams, susijusiems su sertifikavimo tarnybos sauga.

5.4.1 Registruojamų įvykių tipai

PRIVALO būti fiksuojami visos operacinės sistemos lygio saugumo ir CA/RA aplikacijų įvykiai. CPS ar kitas vidinis sertifikavimo tarnybos dokumentas PRIVALO detalizuoti įvykių tipus.

5.4.2 Žurnalo apdorojimo dažnumas

Audito žurnalų peržiūra ir patvirtinimas, kad žurnalai nebuvo pakeisti, PRIVALO būti vykdomas kiekvieną savaitę. Pastebėjus įtartinus įvykius, PRIVALO būti atliktas išsamesnis tyrimas.

5.4.3 Audito žurnalų saugojimo periodas

Audito žurnalai PRIVALO būti saugomi ne trumpiau nei 6 mėnesius.

5.4.4 Audito žurnalų apsauga

Sertifikavimo tarnyba PRIVALO įgyvendinti procedūras, užtikrinančias audito žurnalų apsaugą nuo praradimo iki audito žurnalų saugojimo periodo pabaigos.

Audito žurnalų saugojimo laikmena PRIVALO būti saugi, o saugojimo vieta būti skirtinga nuo jų sukūrimo vietos.

5.4.5 Audito žurnalo rezervinio kopijavimo procedūros

Audito žurnalų ir audito santraukų atsarginės kopijos PRIVALO būti daromos kas mėnesį. Audito žurnalų kopijos kas mėnesį PRIVALO būti išsiųstos į nutolusią saugojimo vietą.

5.4.6 Audito žurnalų surinkimo sistema (vidinė ir išorinė)

Audito žurnalų surinkimo sistema turi būti sukonfigūruota taip, kad apsaugotų žurnalus nuo praradimo.

5.4.7 Įvykį sukėlusio asmens informavimas

Sąlygų nėra.

5.4.8 Pažeidžiamumo kontrolė

Audito žurnalai PRIVALO būti stebimi ir reguliariai peržiūrimi siekiant identifikuoti kenksmingą veiklą.

5.5 Archyvas

Archyvo įrašai apima sertifikatų registravimo informaciją, įvykius reikšmingus

sertifikavimo tarnybos aplinkai, raktų ir sertifikatų valdymo įvykius.

Sertifikavimo tarnyba užtikrina, kad visa svarbi informacija, susijusi su paslaugomis, yra saugoma nustatytą laiko tarpą, visų pirma kaip įrodymas teisinio proceso metu.

5.5.1 Archyvo sudėtis

Sąlygų nėra.

5.5.2 Archyvo saugojimo periodas

Minimalus archyvo saugojimo laikotarpis yra 10 (dešimt) metų.

5.5.3 Archyvo apsauga

Joks neidentifikuotas asmuo NEPRIVALO turėti galimybės įrašyti į, redaguoti ar ištrinti archyvą. Archyvo laikmenos PRIVALO būti laikomos saugioje ir apsaugotoje saugojamoje patalpoje.

5.5.4 Archyvo rezervinės kopijavimo procedūros

Atsarginės kopijos su duomenimis, reikalingais atstatyti sertifikavimo tarnybos operacijas, PRIVALO būti daromos ir saugomos saugiose vietose, nelaimės atveju[11] leidžiančiose laiku atkurti sistemos funkcionalumą. Atsarginių kopijų darymo ir atstatymo operacijos turi būti daromos patikimų asmenų[12].

5.5.5 Reikalavimai dėl laiko žymėjimo

Sertifikavimo tarnybos archyvo įrašai juos sukuriant PRIVALO būti automatiškai pažymimi laiko žyma.

11 Atitinkamai su ISO/IEC 27002, 10.5.1 p.: Svarbios informacijos ir programinės įrangos rezervinės kopijos PRIVALO būti daromos reguliariai. PRIVALO būti aprūpinta tinkamomis rezervinio kopijavimo priemonėmis, užtikrinančiomis, kad svarbi informacija ir programinė įranga gali būti atstatyta. Kopijavimo priemonės PRIVALO būti reguliariai tikrinamos siekiant užtikrinti jų atitiktį veiklos tęstinumo planams.

12 Jeigu rizikos analizė identifikuoja informaciją, kurios tvarkymui reikalingas dviejų asmenų dalyvavimas, pvz., raktams, dviejų asmenų dalyvavimas PRIVALO būti taikomas ir atstatymo operacijoms.

5.5.6 Archyvo surinkimo sistema (vidinė ir išorinė)

Sąlygų nėra.

5.5.7 Archyvinės informacijos gavimo ir tikrinimo procedūros

Sąlygų nėra.

5.6 Raktų keitimas

Sertifikavimo tarnyba PRIVALO įsitikinti, kad jos privatūs pasirašymo raktai nebenaudojami, pasibaigus jų galiojimo laikui. Visos sertifikavimo tarnybos privačių raktų kopijos, pasibaigus jų galiojimo laikui, PRIVALO būti sunaikintos arba padaromos nebetinkamomis naudojimui.

5.7 Kompromitacija ir veiklos tęstinumas

Veiklos tęstinumas užtikrina, kad sistemos gedimo atveju sertifikavimo tarnybos paslaugos bus greitai ir saugiai atkurtos. Šios paslaugos PRIVALO būti atsparios gedimams ir veikti nepertraukiamai: Pristatymo tarnyba, Sertifikatų atšaukimo valdymo tarnyba, Atšaukimo būsenos tarnyba.

Sertifikavimo tarnyba nelaimės atveju PRIVALO garantuoti, kad jos paslaugos bus atkurtos kaip įmanoma greičiau, tai galioja ir privataus rakto kompromitacijos atveju. Visų pirma sertifikavimo tarnyba TURĖTŲ sudaryti ir valdyti veiklos tęstinumo planą kaip reaguoti nelaimės atveju.

Kompromitacijos atveju sertifikavimo tarnyba TURĖTŲ imtis bent šių veiksmų:

a) informuoti visus *Užsakovus* bei kitus asmenis, su kuriais sertifikavimo tarnyba turi sudariusi sutartis ar palaiko kitokius verslo santykius, įskaitant *Pasitikinčias šalis* bei kitas sertifikavimo tarnybas;

b) informuoti, jog sertifikatai ir atšaukimo statuso informacija, pasirašyta šios CA tarnybos raktu, tapo nebegaliojanti;

c) kai sertifikavimo tarnyba informuojama apie kitos sertifikavimo tarnybos

sukompromitavimą, visi sukompromituotosios sertifikavimo tarnybos sertifikatai yra atšaukiami.

Jei kuris iš algoritmų ar parametrų, naudojamų CA ar jos *Užsakovų,* tampa nepakankamai saugus tolimesniam naudojimui, sertifikavimo tarnyba PRIVALO:

- informuoti visus *Užsakovus* bei trečiąsias šalis su kuriomis sertifikavimo tarnyba turi sudariusi sutartis ar kitos formos susitarimą. Be to, ši informacija PRIVALO būti prieinama ir kitoms *Pasitikinčioms šalims*;
- atšaukti bet kurį paveiktą sertifikatą.

5.7.1 Procedūros incidentų ir kompromitacijų atveju

Sertifikavimo tarnyba PRIVALO veikti laiku ir koordinuotai, siekiant greitai sureaguoti į incidentus ir apriboti saugumo pažeidimų poveikį. Apie įvykusį incidentą PRIVALO būti pranešta kuo greičiau.

5.7.2 Kompiuterinių resursų, programinės įrangos ir/ar duomenų pažeidimai

Kai kompiuteriniai, programiniai ir/arba duomenų ištekliai sukompromituojami, sertifikavimo tarnyba, dirbanti pagal šias Taisykles, PRIVALO:

- Prieš atstatant veiklą įsitikinti, kad sistemos vientisumas yra užtikrintas;
- Jei sertifikavimo tarnybos pasirašymo raktai nėra sunaikinti, jos operacijos PRIVALO būti atkuriamos pirmenybę teikiant CRL generavimui pagal nustatytą grafiką;
- Jei CA raktai yra nebepanaudojami, sertifikavimo tarnybos operacijos PRIVALO būti atstatytos kaip įmanoma greičiau, pirmenybę teikiant rakto atstatymui ar naujos raktų poros generacijai.

5.7.3 Procedūros sertifikavimo tarnybos privataus rakto kompromitavimo atveju

CA veiklos tęstinumo plane[13] PRIVALO būti aprašytas sertifikavimo tarnybos privataus rakto

13 arba "veiklos atstatymo planas".

sukompromitavimo ar praradimo atvejis bei veiksmai skirti tokiam atvejui spręsti.

Atsitikus tokiam atvejui, sertifikavimo tarnyba PRIVALO imtis atitinkamų priemonių, kad būtų išvengta nelaimės pasikartojimo[14].

5.7.4 Veiklos tęsimo galimybės po avarijos

Sertifikavimo tarnyba, dirbdama pagal šias Taisykles, PRIVALO turėti procedūras, skirtas operatyviam sertifikavimo tarnybos darbo atstatymui. Tuo atveju, jei sertifikavimo tarnybos sistema fiziškai pažeista ir sertifikavimo tarnybos pasirašymo raktai sunaikinti, apie tai PRIVALO būti pranešta atitinkamai nacionalinei institucijai ir sertifikavimo tarnyba PRIVALO imtis visų veiksmų, kurie jai šioje situacijoje atrodo tinkami.

5.8 CA arba RA veiklos nutraukimas

Sertifikavimo tarnybos ar RA veikla gali būti nutraukta vienašališkai (angl. *Terminated for convenience*), dėl pasibaigusios sutarties, reorganizavimo ar kitų su saugumu nesusijusių priežasčių. Tokiu atveju sertifikavimo tarnyba PRIVALO pamėginti apie veiklos nutraukimą pranešti visiems *Subjektams, Užsakovams* ir *Pasitikinčioms šalims*. Pastarųjų nuožiūra turimi sertifikatai GALI būti ir toliau laikomi galiojančiais.

Apie CA darbo nutraukimą nedelsiant PRIVALO būti pranešta atitinkamoms institucijoms.

Sertifikavimo tarnyba turi užtikrinti, jog nutraukiant savo veiklą, *Užsakovai* ir *Pasitikinčios šalys* patirtų kuo įmanoma mažiau sutrikimų. Prieš sertifikavimo tarnybai nutraukiant veiklą, PRIVALO būti įvykdytos sekančios procedūros:

a) informuoti visus *Užsakovus* ir kitus asmenis su kuriais CA turi sutartis ar kitokios formos susitarimus;

b) visiems subrangovams nutraukiamas leidimas veikti CA vardu;

c) CA perduoda patikimai šaliai įpareigojimus bei visą informaciją, kurios gali prireikti teikiant įrodymus apie sertifikavimo tarnybos veiklą tam tikru laikotarpiu;

d) CA raktai, įskaitant jų atsargines kopijas, turi būti sunaikinti arba pašalinti tokiu būdu, jog privatūs raktai negalėtų būti atkurti.

14 Vadovaujantis ISO/IEC 27002.

Taip pat dėl reikalavimų:

- "*CA perduoda patikimai šaliai įpareigojimus bei visą informaciją, kurios gali prireikti teikiant įrodymus apie sertifikavimo tarnybos veiklą tam tikru laikotarpiu*" apima registravimo ir atšaukimo statuso informaciją už atitinkamą laikotarpį;
- "*CA savo Nuostatuose aprašys veiklos nutraukimo sąlygas*" taip pat apima nepasibaigusių sertifikatų atšaukimo statuso informaciją.

6 TECHNINĖS SAUGOS PRIEMONĖS

Šiame skyriuje pateikiamos taisyklės dėl CA, RA, *Subjektų* bei atitinkamos techninės kontrolės priemonės.

Sertifikavimo tarnyba PRIVALO užtikrinti, kad kriptografinis įrenginys per visą jo naudojimo laiką nėra sugadintas pervežant jį. Sertifikavimo tarnyba PRIVALO užtikrinti, jog pasirašymo raktai, saugomi kriptografiniame įrenginyje, yra sunaikinami pasibaigus įrenginio naudojimo laikui.

Kai saugumo sprendimai jau yra naudojami sertifikavimo tarnybos veikloje, jie PRIVALO būti cituojami CPS.

6.1 Raktų poros generavimas ir įdiegimas

Kiekviena išduodanti sertifikavimo tarnyba PRIVALO turėti savo pasirašymo raktų poras.

Užsakovai GALI generuoti savo raktų poras arba jų raktų poras gali sugeneruoti RA, ar kiti įgalioti asmenys su sąlyga, kad visi taikomi reikalavimai iš šių Taisyklių bus įvykdyti.

6.1.1 Raktų poros generavimas

Sertifikavimo tarnybos rakto generavimas PRIVALO būti atliekamas naudojant vieną iš šių įrenginių:

a) atitinkančių reikalavimus, nustatytus CEN CWA 14167-2, CEN CWA 14167-3 arba CEN CWA 14167-4;

b) patikima sistema, atitinkančia EAL4 ar aukštesnio lygio standartą pagal ISO/IEC 15408 ar lygiaverčius saugumo kriterijus.

Sertifikavimo tarnybos raktų generavimas PRIVALO būti atliekamas remiantis raktų generavimo ceremonijos dokumentu, naudojant pripažintus algoritmus, raktų ilgius bei stebint kvalifikuotam auditoriui visą procesą bei sertifikavimo tarnybos šakninių raktų generavimo vientisumą bei konfidencialumą užtikrinančias priemones. Visa raktų generavimo ceremonija PRIVALO būti filmuojama audito tikslais.

6.1.2 Privataus rakto pristatymas užsakovui

Privatūs raktai GALI būti pristatomi elektroniniu būdu arba per HSM. Bet kokiu atveju PRIVALO būti laikomasi sekančių reikalavimų:

Personalas, generuojantis pasirašymo raktą, NEGALI pasilikti jokios to rakto kopijos. Privatus raktas pristatymo procese PRIVALO būti apsaugotas nuo aktyvavimo, modifikavimo ar sukompromitavimo. *Užsakovas* PRIVALO patvirtinti privataus rakto gavimą.

6.1.3 Viešojo rakto pristatymas sertifikato tarnybai

Sertifikavimo tarnybos viešasis raktas pristatant jį naudotojui PRIVALO būti apsaugotas nuo pakeitimo ar sukeitimo. CPS PRIVALO aprašyti pristatymo specifiką.

6.1.4 CA viešojo rakto pristatymas pasitikinčioms šalims

Sertifikavimo tarnyba, pristatant viešąjį raktą *Pasitikinčioms šalims,* užtikrina jo ir kitų susijusių parametrų autentiškumą ir vientisumą. Sertifikavimo tarnybos viešieji raktai PRIVALO būti prieinami *Pasitikinčioms šalims* tokiu būdu, kad garantuotų raktų vientisumą ir patvirtintų jų šaltinį.

6.1.5 Raktų ilgis

Sertifikatai išduodami pagal šias Taisykles PRIVALO būti RSA ar elipsinės kreivės viešieji raktai su rekomenduojamu rakto ilgiu.

6.1.6 Viešojo rakto parametrų generavimas ir kokybės tikrinimas

Sąlygų nėra.

6.1.7 Raktų naudojimo tikslai (pagal X.509 v3 *key usage* reikšmę)

Specifinio rakto naudojimas GALI būti ribojamas „*KeyUsage*“ plėtinio ir visi sertifikatai PRIVALO turėti kritinio rakto panaudojimo plėtinį, jeigu taikoma. Viešieji raktai susieti su *Užsakovų* sertifikatais PRIVALO būti naudojami arba pasirašymui, arba atkodavimui, bet ne abiems.

6.2 Privataus rakto saugumas ir kriptografinio modulio techninės kontrolės priemonės

Sertifikavimo tarnybos sertifikatų pasirašymo raktai PRIVALO būti naudojami tik fiziškai saugiose patalpose. *Subjekto* privatieji raktai NEGALI būti prieinami niekam kitam tik jam.

6.2.1 Kriptografinio modulio standartai ir valdymas

Sertifikavimo tarnybos, pasirašančios sertifikatus pagal QCP+, PRIVALO naudoti FIPS 140 trečio ar aukštesnio lygio patvirtintą aparatinį kriptografinį modulį, atitinkantį CEN CWA 14168 „*Secure signature creation devices EAL 4*“ ir CEN CWA 14170 „*Security requirements for signature creation applications*“.

Sertifikavimo tarnybos privatūs pasirašymo raktai PRIVALO būti laikomi ir naudojami kriptografiniame įrenginyje, atitinkančiame: reikalavimus nurodytus ISO/IEC 19790 ar viename iš CEN CWA 14167-2, CEN CWA 14167-3, CEN CWA 14167-4, arba tai PRIVALO būti patikima sistema, atitinkanti EAL4 ar aukštesnio lygio pagal ISO/IEC 15408 ar lygiavertį saugumo įvertinimą.

6.2.2 Privataus rakto (n iš m) daugiasmens naudojimas

Vienam asmeniui neleistina aktyvuoti ar prieiti prie bet kokio HSM, saugančio sertifikavimo tarnybos privatų pasirašymo raktą. Sertifikavimo tarnybos pasirašymo raktų atsarginės kopijos PRIVALO būti daromos dalyvaujant dviem asmenims. Prieiga prie sertifikavimo tarnybos raktų atkūrimo ar atstatymo po nelaimės PRIVALO būti vykdoma dalyvaujant dviem asmenims. Dalyvaujančių asmenų vardai PRIVALO būti žymimi sąraše, kuris PRIVALO būti prieinamas audito patikros metu.

6.2.3 Privataus rakto atsarginis saugojimas

Sertifikavimo tarnyba nebesaugo *Užsakovų* raktų, kai jie yra pristatyti *Užsakovui*, jei *Užsakovo* privatus raktas yra naudojamas elektroniniam parašui pagal [1999/93/EC Direktyvą]. Sertifikavimo tarnyba, dirbanti pagal šias Taisykles, PRIVALO niekada neperduoti jos privataus rakto trečiajai šaliai atsarginiam saugojimui.

6.2.4 Privataus rakto rezervinė kopija

Atsarginių kopijų darymo procedūros PRIVALO būti aprašytos CPS.

6.2.5 Privataus rakto archyvavimas

Sertifikavimo tarnybos ir *Užsakovo* privatūs pasirašymo raktai NEGALI būti archyvuojami.

6.2.6 Privataus rakto perkėlimas į arba iš kriptografinio modulio

Sąlygų nėra.

6.2.7 Privataus rakto saugojimas kriptografiniame modulyje

Sertifikavimo tarnyba PRIVALO užtikrinti, kad jos privatūs raktai yra konfidencialūs, išlaiko savo vientisumą ir nėra naudojami pasibaigus jų galiojimo laikui.

6.2.8 Privataus rakto aktyvavimo metodas

Prieš išduodant *Užsakovui* el. parašo sertifikatą, PRIVALO būti įsitikinta, kad jis valdo naudojamą privatų raktą kriptografiniame įrenginyje. Aktyvuotas kriptografinis modulis NEPRIVALO būti prieinamas neįgaliotiems asmenims.

6.2.9 Privataus rakto deaktyvavimo metodas

Po panaudojimo kriptografinis modulis PRIVALO būti deaktyvuotas nuo jo atsijungiant arba automatiškai, praėjus tam tikram nenaudojimo laiko tarpui.

6.2.10 Privataus rakto sunaikinimo metodas

Kai privatūs raktai nebereikalingi, juos PRIVALO sunaikinti patikimi asmenys.

Kai kriptografinis modulis *Užsakovui* nebereikalingas ar kai baigiasi su juo susieto sertifikato galiojimo laikas, jis PRIVALO būti sunaikintas[15] savarankiškai arba sertifikavimo tarnybos pagalba.

6.2.11 Kriptografinio modulio rūšys

Pagal p. 6.2.1 .

6.3 Kiti raktų poros valdymo aspektai

6.3.1 Viešojo rakto archyvavimas

PRIVALO būti taikomi sertifikatų archyvavimo reikalavimai.

6.3.2 Sertifikato ir raktų poros naudojimo periodai

Šakninės bei *Išduodančios* sertifikavimo tarnybos raktų poros galiojimo laikas NEGALI būti ilgesnis nei 20 metų. *Užsakovo* raktų poros galiojimas NEGALI viršyti 8 metų.

Maksimalus OCSP sertifikato naudojimo periodas, remiantis šiomis Taisyklėmis, PRIVALO būti 5 metai.

6.4 Aktyvavimo duomenys

15 Pagal kriptografinio modulio gamintojo dokumentaciją.

6.4.1 Aktyvavimo duomenų generavimas ir įdiegimas

Privataus rakto aktyvavimo duomenys PRIVALO būti perduoti *Užsakovui* atitinkamais saugiais kanalais bei atskirai nuo susijusio kriptografinio modulio.

Aktyvavimo duomenys GALI būti pasirenkami *Užsakovo*.

6.4.2 Aktyvavimo duomenų apsauga

Aktyvavimo duomenys PRIVALO būti apsaugoti nuo atskleidimo kriptografinių ir fizinių prieigos kontrolės priemonių deriniu.

6.4.3 Kiti aktyvavimo duomenų aspektai

Sąlygų nėra.

6.5 Kompiuterinės saugos priemonės

Sertifikavimo tarnyba PRIVALO reikalauti kiekvieno naudotojo autentifikuoti save ir tik sėkmingai autentifikavusis, leisti atlikti veiksmus, susijusius su šio naudotojo vaidmeniu. Po atsijungimo PRIVALO būti privalomas pakartotinis autentifikavimas. Autentifikavimo duomenys PRIVALO būti unikalūs ir NEGALI būti panaudoti pakartotinai.

6.5.1 Specifiniai kompiuterinės saugos techniniai reikalavimai

Privalomos kompiuterinio saugumo kontrolės priemonės, nurodytos žemiau, PRIVALO užtikrinti, kad sertifikavimo tarnybos operacijos atliekamos pagal šias Taisykles:

- prieigos autentifikacija;
- saugos auditas;
- jautrioms funkcijoms skirtų vaidmenų/pareigų atskyrimas;

➢ sertifikavimo tarnybos sistemų bei raktų atstatymo mechanizmas.

Bet kokia komunikacija tarp patikimų vaidmenų ir sertifikavimo tarnybos PRIVALO būti autentifikuota ir apsaugota.

6.5.2 Kompiuterinės saugos lygiai

Sąlygų nėra.

6.6 Techninės gyvavimo ciklo valdymo priemonės

6.6.1 Sistemos kūrimo priemonės

Sistemos plėtros valdymo priemonės PRIVALO būti nurodytos CPS.

6.6.2 Saugos valdymo priemonės

Sertifikavimo tarnyba, dirbanti pagal šias Taisykles, PRIVALO naudoti prieigos prie sistemos kontrolės funkcijas, kurios kontroliuotų visų jautrių sertifikavimo tarnybos objektų naudojimą ir leistų jais naudotis tik autentifikuotam personalui. Sistemos prieigos kontrolė GALI būti vykdoma naudojamos operacinės sistemos arba tiesiogiai – pačio komponento programinės įrangos priemonėmis. Prieigos teisės prie tam tikro sertifikavimo tarnybos objekto nustatomos to objekto valdytojo, remiantis subjekto, prašančio prieigos, tapatybe.

6.6.3 Gyvavimo ciklo saugos priemonės

Sąlygų nėra.

6.7 Tinklo saugos priemonės

Sertifikavimo tarnyba PRIVALO užtikrinti, kad tinklo komponentai saugomi fiziškai saugioje aplinkoje ir jų konfigūracija yra periodiškai tikrinama.

PRIVALO būti įrengtas nuolatinis stebėjimas ir apsaugos sistema siekiant aptikti, užregistruoti ir laiku reaguoti į bet kokį neautorizuotą ar/ir neįprastą bandymą prieiti prie sistemos resursų.

6.8 Laiko žymėjimas

Sertifikavimo tarnyba PRIVALO užtikrinti, kad jos tinklas yra sinchronizuotas su oficialiais laiko šaltiniais. Šis reikalavimas yra atskirtas nuo laiko žymų paslaugos, teikiamos sertifikavimo tarnyboje.

7 SERTIFIKATŲ, CRL IR OCSP PROFILIAI

7.1 Sertifikato profilis

Sertifikatai, išduoti pagal šias Taisykles, PRIVALO atitikti X.509 standarto nustatytą profilį.

Tapatybės ir jos atributų duomenų reikšmės pateikiamos atitinkamuose X.509 v3 sertifikato plėtiniuose . Sertifikato kelias prasideda nuo pasitikėjimo „inkaro“ (angl. *trust anchor*). Pasitikėjimo „inkaras“ yra Šakninės CA sertifikatas, kuriuo naudotojai pasitiki per alternatyvias priemones.

Daugiau informacijos apie X.509 sertifikatus gali būti rasta X.509 rekomendacijose ir [RFC5280].

Sertifikatų, išduotų pagal šias CP, profiliai PRIVALO būti pateikti CPS.

7.1.1 Versijos numeris(ai)

CA PRIVALO išduoti X.509 standarto 3[16] versijos sertifikatus.

7.1.2 Sertifikato plėtiniai

Sertifikato plėtinių taisyklės PRIVALO būti pateiktos CPS.

7.1.3 Algoritmų OID kodai

Algoritmų OID taisyklės PRIVALO būti pateiktos CPS.

7.1.4 Vardų formos

Vardų formos PRIVALO būti pateiktos CPS.

7.1.5 Vardų apribojimai

Sertifikavimo tarnyba į CA sertifikatus GALI įrašyti vardų apribojimus.

16 Versijos numerio reikšmė yra 2.

7.1.6 Sertifikato taisyklių OID kodas

Sertifikato Taisyklių OID kodai PRIVALO būti pateikti CPS.

7.1.7 *Policy Constraints* plėtinio naudojimas

Sertifikavimo tarnyba į CA sertifikatus GALI įrašyti Taisyklių apribojimus (angl. *Policy Constraints*).

7.1.8 *Policy* plėtinio parinkčių sintaksė ir semantika

Sąlygų nėra.

7.1.9 Kritinio *Certificate Policies* plėtinio apdorojimo semantika

Sąlygų nėra.

7.2 CRL profilis

Apie sertifikato atšaukimą CA praneša skelbdama CRL. CRL yra saugomas Talpykloje ir tikrinamas *Pasitikinčių šalių* siekiant patikrinti sertifikato būseną. CRL sudėtyje yra informacija apie leidėją, jo generavimo data ir data, kada bus sugeneruotas kitas CRL, ir informacija apie atšauktus sertifikatus.

7.2.1 Versijos numeris(-iai)

CA PRIVALO išduoti X.509 standarto antros versijos profilio CRL.

7.2.2 CRL ir CRL įrašų plėtiniai

Sąlygų nėra.

7.3 OCSP profilis

OCSP pasirašymo sertifikatas PRIVALO būti pateiktas CPS.

7.3.1 Versijos numeris(-iai)

CA ,veikiantis pagal šias Taisykles, PRIVALO naudoti pirmos versijos numerį.

7.3.2 OCSP plėtiniai

Kritiniai OCSP plėtiniai NEPRIVALO būti naudojami.

8 ATITIKTIES AUDITAS IR KITI TIKRINIMAI

CA, veikiantis pagal šias Taisykles, PRIVALO turėti atitikties vertinimo mechanizmą. Šios Taisyklės nekelia kokių nors specialių atitikties vertinimo metodologijų, tačiau CA atitikimas PRIVALO būti įvertinamas reguliariai ir kaskart, kai įvyko esminiai veiklos pokyčiai.

CA laiko žymos paslauga PRIVALO atitikti [ETSITS102023] reikalavimus.

8.1 Patikrinimų dažnumas ir aplinkybės

CA ir RA, veikiančios pagal šias Taisykles, PRIVALO reguliariai atlikti atitikties vertinimą.

8.2 Auditorius ir jo kvalifikacija

Tikrinančio asmens pagrindinis darbas (veikla) PRIVALO būti auditas ir būti sertifikuotas informacinių sistemų auditoriaus.

8.3 Auditorių ir sertifikavimo tarnybos santykiai

Auditorius turėtų būti privati įmonė, nepriklausoma nuo sertifikavimo tarnybos, kurios veiklą audituoja.

8.4 Audito apimtis

CA turi sugebėti pademonstruoti, kad:

a) atitinka SSC GDL CA keliamus įpareigojimus ir garantijas kaip nurodyta šiose Taisyklėse;

b) yra įgyvendinęs priemones, atitinkančias CA veiklai keliamus reikalavimus;

c) jos CPS ir kita susijusi dokumentacija prieinama *Užsakovams* ir *Pasitikinčioms šalims*;

d) yra dokumentavusi naudojamus algoritmus ir parametrus.

8.5 Veiksmai dėl audito metu nustatytų trūkumų

Jeigu auditorius tikrinimo metu suranda neatitikimą tarp CP reikalavimų ir CA veiklos, PRIVALO būti imtasi šių veiksmų:

Auditorius PRIVALO fiksuoti neatitiktį;

CA PRIVALO pasiūlyti trūkumo pašalinimo būdą, įskaitant ir vykdymo datą.

Priklausomai nuo neatitikties charakteristikos, sunkumo ir pašalinimui siūlomos datos, CA GALI nuspręsti laikinai pristabdyti CA ar RA veiklą.

8.6 Audito rezultatai

Audito ataskaita PRIVALO būti pateikta CA.

9 KITI VEIKLOS IR TEISINIAI KLAUSIMAI

Šioje Taisyklių dalyje pateikiami dalyvaujančių šalių įsipareigojimai, atsakomybės sąlygos ir aptariami finansiniai/ekonominiai klausimai. Be to, konfidencialumo skyriuje aprašomi skirtumai tarp konfidencialios, viešai prieinamos ir platinamos informacijos. Taip pat nurodomi CA veiklos tikrinimo principai.

Pasitikinčioms šalims teikiama informacija apie paslaugų teikimo sąlygas TURI identifikuoti aplinkybes, kurių buvimas būtinas sprendžiant, ar pasitikėti atitinkama paslauga:

a) sertifikato galiojimas, sustabdymas ar atšaukimas turi būti patikrintas remiantis aktualios būsenos informacija;
b) turi būti atsižvelgta į sertifikato naudojimo apribojimus, nurodytus pačiame sertifikate arba paslaugų teikimo sąlygose;
c) turi būti atsižvelgta į kitas aplinkybes, nurodytas sutartyse arba kituose dokumentuose.

9.1 Mokesčiai

9.1.1 Sertifikato išdavimo ir pratęsimo mokesčiai

Mokesčiai taikomi sertifikato išdavimui ir atnaujinimui. Bet kuriuo atveju mokesčiai TURI BŪTI aiškiai nurodyti CPS.

9.1.2 Priėjimo prie sertifikatų mokesčiai

CA, veikianti pagal šias Taisykles, GALI taikyti mokesčius už prieigą prie tam tikrų jos išduodamų sertifikatų tipų.

9.1.3 Atšaukimo arba priėjimo prie būsenos informacijos mokesčiai

Sertifikato atšaukimas ir prieiga prie CRL teikiama neatlygintinai.

9.1.4 Mokesčiai už kitas paslaugas

Sąlygų nėra.

9.1.5 Mokesčių grąžinimas

Sąlygų nėra.

9.2 Finansinė atsakomybė

9.2.1 Draudimo apimtis

Šiose Taisyklėse nėra nustatomi finansiniai sertifikato naudojimo apribojimai, išskyrus QCP ir QCP+ sertifikatams. Finansiniai sertifikato naudojimo apribojimai gali būti nustatyti *Užsakovams* arba *Pasitikinčioms šalims*.

9.2.2 Kitas turtinis padengimas

Sąlygų nėra.

9.2.3 Draudimo ir garantijos padengimas galutiniam naudotojui

Sąlygų nėra.

9.3 Verslo informacijos konfidencialumas

Sąlygų nėra.

9.3.1 Konfidencialios informacijos apimtis

Sąlygų nėra.

9.3.2 Nekonfidenciali informacija

SSC išduotų sertifikatų turinys tarp jų ir informacija CRL sąrašuose nėra laikoma konfidenciali. Atšaukiant sertifikatą GALI BŪTI nurodyta priežastis. Sertifikato galiojimo laikas ir atšaukimo priežastis nėra laikoma konfidencialia. Bet kuriuo atveju, įprastomis aplinkybėmis,

jokia su sertifikatu susijusi informacija nebus laikoma neskelbtina.

9.3.3 Atsakomybė už konfidencialios informacijos apsaugą

Sąlygų nėra.

9.4 Asmens duomenų privatumas

9.4.1 Privatumo politika

CA, veikianti pagal šias Taisykles, TURI turėti privatumo ir asmens duomenų tvarkymo taisykles, užtikrinančias asmenį identifikuojančių duomenų apsaugą nuo atskleidimo pagal Lietuvos Respublikos įstatymų reikalavimus.

9.4.2 Privati informacija

CA, veikianti pagal šias Taisykles, saugos asmenį identifikuojančią informaciją nuo neįgalioto atskleidimo. Atskiri įrašai apie asmens atliktus sandorius GALI būti išduotas pačiam sandorio dalyviui arba jo teisėtai atstovaujančiam asmeniui. Sertifikavimo tarnybos saugomo archyvo turinys nebus atskleistas kitaip negu tai nustato įstatymai.

9.4.3 Neprivati informacija

Sąlygų nėra.

9.4.4 Atsakomybė už privačios informacijos apsaugą

Sąlygų nėra.

9.4.5 Pranešimai ir sutikimai dėl privačios informacijos naudojimo

Sąlygų nėra.

9.4.6 Informacijos atskleidimas dėl teisinių arba administracinių procesų

Sąlygų nėra.

9.4.7 Kitos informacijos atskleidimo aplinkybės

Sąlygų nėra.

9.5 Intelektinės nuosavybės teisės

Sąlygų nėra.

9.5.1 Sertifikatai ir CRL

Sąlygų nėra.

9.5.2 CP/CPS

Sąlygų nėra.

9.5.3 Prekių ženklai

Sąlygų nėra.

9.5.4 Parašo formavimo duomenys

Sąlygų nėra.

9.6 Atstovavimas ir garantijos

9.6.1 CA atstovavimas ir garantijos

CA TURI užtikrinti savo paslaugų prieinamumą, tikslumą ir kitus parametrus, paskelbtus paslaugų teikimo sąlygose. CA turi užtikrinti, kad visi jai keliami reikalavimai yra įgyvendinti atitinkamai pasirinkto CP. CA yra atsakinga už šių taisyklių reikalavimų vykdymą net ir tuo

atveju, kai jos funkcijos yra perduotos trečiosioms šalims.

9.6.2 RA atstovavimas ir garantijos

RA, vykdanti registravimo funkcijas pagal šias Taisykles, TURI atitikti šio dokumento sąlygas.

9.6.3 Užsakovo atstovavimas ir garantijos

CA TURI įpareigoti Užsakovus[17], kad:

a) informacija pateikiama CA pagal šio dokumento reikalavimus bus tiksli ir pilna;

b) raktų pora bus naudojama *Užsakovui* nurodytų apribojimų ribose;

c) bus imtasi tinkamų priemonių siekiant išvengti neteisėto privataus rakto naudojimo;

d) *Subjekto* raktų pora bus generuojama naudojant algoritmus, nurodytus CPS;

e) raktų ilgis ir algoritmas[18] bus naudojami pagal CPS reikalavimus[19];

f) *Subjekto* privatus raktas, naudojamas kriptografinėse funkcijose bus laikomas saugioje įrangoje[20];

g) jeigu sertifikato Taisyklės numato SSCD[21] naudojimą, el. parašo kūrimui bus naudojamas sertifikatas susietas su atitinkama saugia įranga;

h) jeigu sertifikato galiojimo metu kils viena iš šių aplinkybių, CA bus nedelsiant informuota:

- *Subjekto* privatus raktas prarastas arba pavogtas;
- *Subjekto* privatus raktas galimai kompromituotas arba prarasta jo išskirtinė kontrolė dėl aktyvavimo duomenų kompromitacijos ar kitų priežasčių;
- sertifikato turinio netikslumas arba pasikeitimai;
- atsitikus rakto kompromitavimui, privataus rakto tolimesnis naudojimas turi būti nedelsiant nutrauktas;

i) gavus pranešimą, kad CA sertifikatas yra sukompromituotas, bus užkirstas jo tolimesnis naudojimas *Subjektui*;

17 Jeigu *Užsakovas* nėra pats *Subjektas*, jis turi informuoti *Subjektą* apie jam taikomus įsipareigojimus.
18 Privaloma vadovautis ETSI TS 102 176-1.
19 Jeigu el. parašo raktų porą generuoja *Užsakovas* arba *Subjektas*, atitinkamas privatus raktas turi būti išskirtiniame *Subjekto* valdyme.
20 Taikoma NCP+ sertifikatams.
21 Taikoma QCP+ sertifikatams.

j) bus gautas pritarimas asmens duomenų tvarkymui ir saugojimui.

9.6.4 Pasitikinčios šalies atstovavimas ir garantijos

Pasitikinčioms šalims teikiama informacija apie paslaugų teikimo sąlygas TURI numatyti, kad priėmus sprendimą pasitikėti sertifikatu:

a) sertifikato galiojimas, sustabdymas ar atšaukimas bus tikrinamas remiantis aktualios būsenos informacija[22];
b) bus atsižvelgta į sertifikato naudojimo apribojimus, nurodytus pačiame sertifikate arba paslaugų teikimo sąlygose;
c) bus atsižvelgta į kitas aplinkybes, nurodytas sutartyse arba kituose dokumentuose.

9.6.5 Kitų dalyvių atstovavimas ir garantijos

Sąlygų nėra.

9.7 Garantijos atsižadėjimas

CA, veikianti pagal šias Taisykles, NEGALI atsisakyti atsakomybių, numatytų šiame dokumente.

9.8 Atsakomybės ribojimas

Bet koks atsakomybės atsisakymas ar ribojimas TURI būti atliekamas atitinkamai laikantis įstatymų reikalavimų.

9.9 Kompensacijos

Sąlygų nėra.

22 Informacija apie atšaukimą gali būti išplatinta ne ilgiau kaip per vieną parą.

9.10 Sąlygų galiojimas ir nutraukimas

9.10.1 Galiojimas

Šios Taisyklės galioja nuo sertifikavimo tarnybos paskirto įgalioto asmens tvirtinimo datos.

9.10.2 Nutraukimas

Sąlygų nėra.

9.10.3 Sąlygų nutraukimo ir išlikimo poveikis

Šių Taisyklių reikalavimai lieka galioti iki paskutinio išduoto sertifikato archyvavimo periodo pabaigos.

9.11 Individualūs pranešimai ir komunikavimas su dalyviais

Sąlygų nėra.

9.12 Pakeitimai

9.12.1 Pakeitimo procedūra

Sertifikavimo tarnybos Valdyba peržiūri šias Taisykles bent jau kartą per metus. Dokumento ištaisymai, atnaujinimai ar pakeitimai TURI būti prieinami viešai.

Pasiūlymai dėl šio dokumento pakeitimo TURI būti atliekami 1.5.2 p. nustatytu būdu ir turi nurodyti pakeitimų esmę, tikslingumą ir pakeitimo prašančio asmens kontaktinę informaciją.

9.12.2 Pranešimo būdas ir periodas

Sąlygų nėra.

9.12.3 OID pakeitimo būtinybės aplinkybės

Sąlygų nėra.

9.13 Ginčų sprendimo sąlygos

Sąlygų nėra.

9.14 Taikomoji teisė

Sąlygų nėra.

9.15 Atitiktis taikomam įstatymui

Šios Taisyklės TURI būti aiškinamos remiantis atitinkamai Lietuvos Respublikos ir Europos Sąjungos teisės aktais.

9.16 Įvairios sąlygos

9.16.1 Sutarties visuma

Sąlygų nėra.

9.16.2 Perleidimas

Sąlygų nėra.

9.16.3 Sutarties dalinis taikymas

Jeigu kokia nors šio dokumento dalis bus pripažįstama neteisinga ar negaliojančia, likusios šio dokumento dalys galioja iki kito atnaujinimo.

9.16.4 Prievolės (advokato mokesčiai ir išimties teisės)

Sąlygų nėra.

9.16.5 Force Majeure

Sąlygų nėra.

9.17 Kitos sąlygos

Sąlygų nėra.

10 NUORODOS

10.1 Normatyvinės nuorodos

Žemiau pateiktų dokumentų reikalavimai, jeigu yra taikytini konkretaus tipo sertifikatams, laikytini šių Taisyklių sudėtine dalimi. Jeigu nurodomas dokumentas atnaujinamas, nuoroda šiame dokumente nurodo ankstesnę versiją.

[CWA14167-1]	CEN CWA 14167-1, Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.
[ETSITS101042]	ETSI TS 101 042, Policy requirements for certification authorities issuing public key certificates (Normalized level only).
[ETSITS101456]	ETSI TS 101 456 Policy, Requirements for Certification Authorities Issuing Qualified Certificates.
[ETSITS102023]	ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities
[CABF-NCSSR]	Network and Certificate System Security Requirements, CA/Browser Forum, 2012
[CABF-BR]	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum, 2013
[CABF-EV]	EV SSL Certificate Guidelines Version, CA/Browser Forum, 2012
[CEN CMCSO-PP]	CWA 14167-2 Cryptographic Module for CSP Signing Operations – Protection Profile (CMCSO PP).
[CEN CMCKG-PP]	CWA 14167-3 Cryptographic Module for CSP Key Generation Services – Protection Profile (CMCKG-PP).
[CENSSCD]	CWA 14169 Secure Signature Creation Devices EAL4+.
[ALGO]	ETSI SR 002 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures.

10.2 Informacinės nuorodos

[LT-PDP-LAW]	Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas, Nr. X-1444, 2008.02.01 su pakeitimais.
[LT-ES-LAW]	Lietuvos Respublikos Elektroninio parašo įstatymas, Nr. VIII-1822, 2000.07.11 su pakeitimais.
[CWA14172-3]	CWA 14172-3: EESSI Conformity Assessment Guidance - Part 3: Trustworthy Systems Managing Electronic Signatures.
[RFC3647]	RFC3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices.
[RFC2119]	RFC 2119, Key words for use in RFCs to Indicate Requirement Levels. March 1997.

[RFC2560] RFC 2560, Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol, OCSP, June 1999.

[RFC5280] RFC 5280, Internet X.509 Public Key Infrastructure: Certificate and CRL Profile.

[Dir1999/93/EC] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[RFC2510] Internet X.509 Public Key Infrastructure Certificate Management Protocols, Adams, S. Farrell, March 1999.

[ETSI TS 101 862] Qualified Certificate Profile, DTS/SEC-004003

[RFC3039] RFC 3039, Internet X.509 Public Key Infrastructure Qualified Certificates Profile, Santesson, et al.).

[CC] Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408-1:1999, ISO/IEC 15408-2:1999, ISO/IEC 15408-3:1999.