Sertifikavimo veiklos nuostatai

SSC GDL CA

Versija 4.10

2015

Pakeitimų istorija

Versija	Data	Paaiškinimai
4.6	06/25/13	Suderinta su CPS redakcija anglų kalba
4.7	04/22/14	Informacija apie EV CA
4.8	08/01/14	Atnaujinta OID lentelė ir 1.2
4.9	02/16/15	Atnaujintas 3 sk.
4.10	04/01/15	Bendra redakcija ir 4 sk. atnaujinimas

TURINYS

1 ĮŽANGA

Sertifikavimo tarnyba SSC GDL CA gamina įvairios paskirties skaitmeninius sertifikatus. Sertifikatų gamyba SSC GDL CA tarnyboje paremta Viešojo rakto infrastruktūra (angl. *Public Key Infrastructure* - PKI).

Šiame dokumente naudojama terminologija iš esmės atitinka [RFC3647].

Raktiniai žodžiai „PRIVALO“ („REIKALAUJAMA“, „TURI“), „DRAUDŽIAMA“ („NETURI“), „TURĖTŲ“ („REKOMENDUOJAMA“), „NETURĖTŲ“ („NE REKOMENDUOJAMA“), „GALI“ („PASIRINKTINAI“) šiame dokumente turi būti aiškinami taip, kaip tai aprašyta [RFC2119].

Priklausomai nuo konteksto frazė “*Sąlygų nėra*“ šiame dokumente gali reikšti:

a) *taikomos SSC GDL CA Sertifikato taisyklų sąlygos*;

b) *taikomos atitinkamų normatyvinių dokumentų (žr. sk.) sąlygos*;

c) *taikomos sertifikavimo tarnybos vidinių dokumentų sąlygos*.

“SSC GDL CA” šiame dokumente reiškia sertifikavimo tarnybą, kurios veikla atitinka reikalavimus, išdėstytus dokumente [SSC_CP].

1.1 Bendra apžvalga

Šie nuostatai aprašo SSC GDL CA pagrindines tarnybos, užtikrinančios atitikimą patikimumo statusui taikomų saugos standartų reikalavimus. Sertifikavimo veiklos nuostatų (angl. *Certificate Practice Statement* - CPS arba *Nuostatai*) kontekste SSC GDL CA turi šias pagrindines tarnybas:

- Šakninių CA;
- Išduodančių CA, apimančių:
  - ✔ Registravimo tarnyba – vykdo *Subjektų* tapatybės tikrinimą;

- ✔ Sertifikatų generavimo tarnyba – gamina sertifikatus;
- ✔ Pristatymo tarnyba – pristato *Subjektams* sertifikatus ir kitą informaciją;
- ✔ Atšaukimo valdymo tarnyba – apdoroja gautus prašymus dėl atšaukimo;
- ✔ Sertifikatų būsenos tarnyba – pateikia sertifikato būsenos informaciją *Pasitikinčioms šalims*;

SSC GDL CA taip pat turi papildomas tarnybas:

- ✔ *Subjektų* sertifikatų laikmenos paruošimo tarnyba – paruošia parašo formavimo duomenų laikmenas (angl. *Signature Creation Device* – SSCD) naudojimui;
- ✔ *Laiko žymos tarnyba (angl. Time Stamp Authority – TSA arba SSC GDL TSA) – generuoja laiko žymas (angl. Time Stamp Token);*
- ✔ Subjektų autentifikavimo On-line režimu tarnyba (*id.ssc.lt*);
- ✔ Pagalbos tarnyba[1] (support.ssc.lt);
- ✔ El. parašo *kūrimo* tarnyba, pristatoma kaip SaaS (angl. *Software as a Service – SaaS*);
- ✔ El. parašo tikrinimo programine įranga, veikianti kaip WEB taikomoji programa.

Šis dokumentas gali būti naudojamas siekiant išsiaiškinti SSC GDL CA išduodamų sertifikatų taikymo sritį bei įvertinti sertifikavimo tarnybos patikimumą.

SSC GDL CA funkcijos atitinka saugos reikalavimus, nustatytus dokumente [SSC_CP].

Nors CPS nesiekiama aprašyti visų tipų išduodamų sertifikatų specifikacijų, tačiau aspektai, susiję su kvalifikuotais sertifikatais, pateikti taip, kad demonstruotų atitiktį El. parašo Direktyvos [Dir1999/93/EC] prieduose I ir II nurodytiems reikalavimams.

1.2 Dokumento pavadinimas ir identifikacija

SSC GDL CA CPS dokumento struktūra atitinka [SSC_CP]. SSC GDL CA veiklos nuostatai (CPS) identifikuojami bendru OID kodu:

IANA: **1.3.6.1.4.1.22501.0.2**

Nacionalinis OID Registras[2]: **2.16.440.1.4.30003763.0.2**

1 Apima realaus laiko bendravimo (angl. live chat) ir Pagalbos (angl. help desk) tarnybas.
2 Po Lietuvos kompetentingos institucijos pritarimo.

Konkretaus versijos CPS identifikuojamas pridedant prie bendro OID kodo atitinkamo dokumento versijos (v) ir modifikacijos (m) numerius, pvz.:

IANA: 1.3.6.1.4.1.22501.0.2.v.m

Nacionalinis OID Registras: 2.16.440.1.4.30003763.0.2.v.m

Visuose SSC GDL CA išduotuose sertifikatuose yra nurodomas taikomų reikalavimų objekto registruotas identifikatorius (angl. *Object Identifier - OID*). Kai kurie iš šių OID ir atitinkami reikalavimai tvarkomi trečiųjų šalių, su kuriomis SSC GDL CA dėl jų naudojimo turi tiesioginį ar netiesioginį susitarimą. Nors ir šiame dokumente yra aprašyta dauguma naudojamų trečiųjų šalių OID reikalavimų, tačiau vertinant konkretaus tipo sertifikato tinkamumą, pačiame sertifikate nurodyto OID kodui atitinkantys reikalavimai visada taikomi prioritetine tvarka. Dėl patogumo šiame dokumente pateikiami atitinkami OID kodai. Sertifikatai išduoti pagal šiuos CPS nurodo bent jau vieną iš šių taikomų *Taisyklių* OID kodų:

Taisyklės	**OID**
NCP	0.4.0.2042.1.1
NCP+	0.4.0.2042.1.2
EVCP	0.4.0.2042.1.4
EVCP+	0.4.0.2042.1.5
DVCP	0.4.0.2042.1.6
OVCP	0.4.0.2042.1.7
QCP + SSCD	0.4.0.1456.1.1
QCP	0.4.0.1456.1.2
CAB Forum EV SSL	2.23.140.1.1
CAB Forum BR (*Subjekto* tapatybė patikrinta)	2.23.140.1.2.2
CAB Forum BR (*Subjekto* tapatybė nepatikrinta)	2.23.140.1.2.1
anyPolicy	2.5.29.32.0
ETSI TS 102 023 Bazinės laiko žymos taisyklės	0.4.0.2023.1.1
LTV laiko žyma *kvalifikuotam parašui* (v - versija, m – modifikacija)	1.3.6.1.4.1.22501.0.6.v.m 2.16.440.1.4.30003763.0.6.v.m
GDL CA CP	1.3.6.1.4.1.22501.0.1

Taisyklės	OID
(Bendras CP nuorodos OID)	2.16.440.1.4.30003763.0.1
SSC GDL CA CP (Konkretaus CP nuorodos OID, v – versijos numeris, m – modifikacijos numeris)	1.3.6.1.4.1.22501.0.1.v.m 2.16.440.1.4.30003763.0.1.v.m
SSC GDL CA CPS (Bendras CPS nuorodos OID)	1.3.6.1.4.1.22501.0.2 2.16.440.1.4.30003763.0.2
SSC GDL CA CPS (Konkretaus CPS nuorodos OID, v – versijos numeris, m – modifikacijos numeris)	1.3.6.1.4.1.22501.0.2.v.m 2.16.440.1.4.30003763.0.2.v.m
SSC_Authentication_Only	1.3.6.1.4.1.22501.9.6.2.0 2.16.440.1.4.30003763.9.6.2.0
SSC_AIO	1.3.6.1.4.1.22501.9.8.1.0 2.16.440.1.4.30003763.9.8.1.0

Teikiant paslaugas pagal šiuos CPS, kai kurios šio dokumento struktūros temos gali būti tiesiogiai netaikytinos, jos yra paliktos tik dokumento struktūros suderinamumo sumetimais.

Sąveikumas su sertifikavimo tarnybomis, išduodančiomis sertifikatus pagal kitas Taisykles, gali būti pasiektas naudojant Patikimų paslaugų teikėjų sąrašus (angl. *Trust Lists* - TSL), Taisyklių tarpusavyje prilyginimo būdu (angl. *mapping*) arba kryžminio sertifikavimo metodu. Ši sertifikavimo tarnyba yra įtraukta į Microsoft Windows Trust Program, Lietuvos ir Europos TSL[3], Google Chrome Root Certificate Program, Opera Software, Adobe Acrobat Trust List[4] ir yra Mozilla CA Certificate Inclusion Program[5] Apple iOS Root Certificate Program[6] ir Android Root Certificate[7] Program dalyvė.

1.3 PKI dalyviai

Šioje dokumento dalyje pristatomi SSC GDL CA PKI sistemos dalyviai. Jeigu teikiant paslaugas SSC GDL CA tam tikras savo funkcijas perduoda trečiajai šaliai, tokie santykiai yra įforminti atitinkamu rašytiniu susitarimu. Priklausomai nuo perduotų funkcijų charakteristikos, šių funkcijų vykdytojai gali būti atskleisti dokumente SSC_PDS.

3 https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf
4 Laukiama patvirtinimo.
5 Laukiama patvirtinimo.
6 Laukiama patvirtinimo.
7 Laukiama patvirtinimo.

1.3.1 Sertifikavimo tarnybos

SSC GDL CA PKI sistemoje skiriamos dviejų pagrindinių tipų sertifikavimo tarnybos: Šakninė sertifikavimo tarnyba (angl. *Root CA*) ir Išduodanti sertifikavimo tarnyba (angl. *Issuing CA*). Šiuo metu į SSC PKI sistemos hierarchiją įeina šios tarnybos:

Šakninė tarnyba	**Išduodanti tarnyba**	**Paaiškinimai**
Root A	SSC GDL Class 1-2 CA	Išduoda sertifikatus asmenims, kurių tapatybė nėra patikimai patikrinama, ir nekvalifikuotus sertifikatus.
	SSC GDL Class 2-4 QCA	Išduoda kvalifikuotus sertifikatus plačiajai visuomenei.
Root B	SSC GDL NH CA	Išduoda įvairius sertifikatus įrangai arba el. paslaugoms.
	SSC GDL EV CA	Išduoda EV SSL sertifikatus.
VS Root	SSC GDL VS Class 2-4 QCA	Išduoda kvalifikuotus sertifikatus Viešojo sektoriaus *Subjektams*.

Šakninės tarnybos. Užtikrina *Išduodančių tarnybų* patikimumą. *Šakninės tarnybos* išduoda sertifikatus tik sertifikavimo tarnyboms, kurios laikosi reikalavimų, nustatytų atitinkamose *Taisyklėse*, ir yra atsakingos už šių tarnybų valdymą ir šių *Nuostatų* įgyvendinimą.

Išduodančios tarnybos. Išduoda sertifikatus tik galutiniams naudotojams – *Užsakovams,* ir teikia kitas susijusias paslaugas. SSC GDL CA tarnyba yra valdoma pagal teisės aktų [Dir1999/93/EC] ir [LT-ES-LAW] reikalavimus.

Jeigu kokia nors iš aukščiau išvardintų tarnybų pati tampa trečiosios šalies išduoto sertifikato *Subjektu*, atitinkama tarnyba turės atskleisti visus kryžminiu būdu pasirašytus sertifikatus.

1.3.2 Registravimo tarnybos

Šiuo metu registravimo tarnybos funkcijas vykdo SSC struktūrinis padalinys. Be prašymų apdorojimo, tapatybės patikrinimo ir prašymą pateikusių asmenų identifikavimo ir autentifikavimo, registravimo tarnyba taip pat išplatina Šakninių ir Išduodančių tarnybų sertifikatus ir atlieka kitas funkcijas, aprašytas šiuose Nuostatuose.

1.3.3 *Užsakovai* ir *Subjektai*

Kai kuriais atvejais asmuo, kuris prašo sertifikato (pvz. organizacija), vadinamas *Užsakovu*, prašo išduoti sertifikatą kitam asmeniui, vadinamam *Subjektu*. Tas pats *Užsakovas* gali atstovauti keliems *Subjektams,* kurių vardu pagal šio dokumento nuostatus išduodami sertifikatai ir kurių *skiriamieji vardai* ir viešieji raktai bus įrašyti sertifikatuose.

Santykiuose su SSC GDL CA už privataus rakto, susijusio su viešuoju raktu naudojimą, atsakingu laikomas *Užsakovas*, o *Subjektas* yra asmuo, kuris yra autentifikuojamas pagal privatų raktą ir kuris valdo jo naudojimą. Kai sertifikatas yra išduodamas asmeniui savarankiškam naudojimui, tuomet *Užsakovas* ir *Subjektas* yra tas pats asmuo.

Remiantis [CABF-EV] reikalavimais sertifikavimo tarnyba gali išduoti EV sertifikatus privačiųjų organizacijų, viešojo sektoriaus institucijų ir nekomercinių įstaigų *Subjektams*.

Sertifikatai yra išduodami tik remiantis su *Užsakovais* pasirašytų sutarčių pagrindu.

1.3.4 Pasitikinčios šalys

Juridiniai ir fiziniai asmenys, kurie pasitiki SSC GDL CA išduotais sertifikatais, vadinasi *Pasitikinčiomis šalimis*[8]. Kaip yra aprašyta [SSCGDLRPA], kiekvienas siekiantis tikrinti sertifikato galiojimą turi naudotis *Sertifikatų būsenos tarnybos* paslaugomis.

1.3.5 Kiti dalyviai

Išduodant EVCP ir EVCP+ tipo sertifikatus yra apibrėžti šių dalyvaujančių asmenų vaidmenys:

Sertifikato prašytojas: fizinis asmuo, turintis įgaliojimą atstovauti *Pareiškėją* arba trečioji šalis, kuris pateikia prašymą išduoti EV sertifikatą *Pareiškėjo* vardu;

Sertifikato tvirtintojas: fizinis asmuo, kuris yra arba *Pareiškėjas, Pareiškėjo* darbuotojas, arba įgaliotas atstovauti *Pareiškėją* (i) kaip *Sertifikato prašytojas*, ir suteikti kitiems darbuotojams

8 *pasikliaujančioji šalis – fizinis arba juridinis asmuo, kuris pasikliauja elektronine atpažintimi ar patikimumo užtikrinimo paslauga*, 2014 m. liepos 23 d. EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.

ar trečiosioms šalims *Sertifikato prašytojo* įgaliojimus ir (ii) tvirtinti prašymus išduoti EV sertifikatus, kuriuos pateikia kiti *Sertifikato prašytojai*;

Sutarties pasirašytojas: fizinis asmuo, kuris yra arba *Pareiškėjas*, *Pareiškėjo* darbuotojas arba įgaliotas atstovauti *Pareiškėją* ir kuris yra įgaliotas *Pareiškėjo* vardu pasirašyti paslaugų teikimo sutartis;

Pareiškėjo atstovas: fizinis asmuo, kuris yra arba *Pareiškėjas*, *Pareiškėjo* darbuotojas, arba įgaliotas atstovauti *Pareiškėją* ir Pareiškėjo vardu pritarti, pripažinti ir sutikti su Sertifikato naudojimo sąlygomis;

Subrangovas – prieglobos paslaugų teikėjas;

Taikomosios programinės įrangos teikėjas: fizinis arba juridinis asmuo, su kuriuo SSC GDL CA pasirašo sutartį dėl jos (Šakninės CA ir/ar Išduodančios CA) sertifikato platinimo kartu su programine įranga.

Pareiškėjas gali įgalioti vieną asmenį vykdyti du ar daugiau iš aukščiau išvardintų vaidmenų.

1.4 Sertifikato naudojimas

Priklausomai nuo tapatybės tikrinimo lygmens ir saugumo reikalavimų, sertifikatai, išduodami pagal šiuos Nuostatus, gali būti grupuoti į klases:

1 klasė – Sertifikato *Subject* laukas nurodo *Vardą*, kuris nėra susietas su kokiu nors fiziniu asmeniu, kurio tapatybė buvo patikrinta. Garantuojamas tik nurodyto komunikavimo resurso (pvz. el. pašto adreso, tel. numerio ir pan.) egzistavimas. Sertifikato *Subjektu* gali būti žmogus, organizacija, įranga arba el. paslauga.

2 klasė – Sertifikato *Subject* laukas nurodo *Vardą*, kuris yra susietas su asmeniu, kurio tapatybė buvo patikimai patikrinta. Sertifikato *Subjektu* gali būti žmogus, organizacija, įranga arba el. paslauga.

3 klasė – Sertifikato *Subject* laukas nurodo *Vardą*, kuris yra susietas su asmeniu, kurio tapatybė buvo patikimai patikrinta. Atitinkamas privatus raktas yra saugomas laikmenoje, kurią

išskirtinai valdo *Subjektas*. Sertifikato *Subjektu* gali būti žmogus, organizacija, įranga arba el. paslauga.

4 klasė – Sertifikato *Subject* laukas nurodo *Vardą* ir biometrinius duomenis, kurie susieti su asmeniu, kurio tapatybė buvo patikimai patikrinta. Atitinkamas privatus raktas yra saugomas laikmenoje, kurią išskirtinai valdo *Subjektas*. Sertifikato *Subjektu* gali būti tik žmogus.

Sertifikavimo tarnyba išduoda skirtingų tipų sertifikatus, kurie remiasi trečiųjų šalių nustatytomis Taisyklėmis (pvz. [CABF-BR], [CABF-EV]), kurios šiuose Nuostatuose vadinamos remiamomis Taisyklėmis (angl. Reference Policy). Remiamų Taisyklių naudojimą iliustruoja žemiau pateikta lentelė:

Išduodanti tarnyba	***Remiamos Taisyklės***				
	QCP[9]/QCP+[10]	**NCP[11]/NCP+[12]**	**EVCP[13]/EVCP+[14]**	**DVCP[15]**	**OVCP[16]**
SSC GDL Class 1-2 CA	-	+	-	+	-
SSC GDL Class 2-4 QCA	+	-	-	-	+
SSC GDL NH CA	+	-	-	-	+
SSC GDL EV CA	-	-	+	-	-
SSC GDL VS Class 2-4 QCA	+	-	-	-	-

Konkretaus sertifikato kontekste jame nurodyti *Remiamų Taisyklių* reikalavimai visada turi dominuojančią reikšmę[17]. Sertifikavimo tarnyba nagrinėja sertifikato naudotojų ir *Pasitikinčių šalių prašymus* dėl testinių sertifikatų išdavimo ir jų tikrinimo.

SSC GDL CA veikla atitinka dokumentų [CABF-BR] ir [CABF-EV][18] einamųjų versijų reikalavimus. Atsiradus nesuderinamumui tarp šių Nuostatų ir minėtų dokumentų, pastarieji turi pirmenybę.

SSC GDL CA taip pat įgyvendino [CABF-NCSSR] reikalavimus, kurie yra integruoti į vidinę dokumentaciją.

9 Sertifikato taisyklės kvalifikuotiems sertifikatams plačiajai visuomenei, kaip nurodyta [ETSITS101456].
10 QCP su SSCD kaip nurodyta [ETSITS101456].
11 Normalizuota CP kaip nurodyta [ETSITS101042] ir atitinka kvalifikuotų sertifikatų kokybę, tačiau be sąryšio su [Dir1999/93/EC].
12 NCP su saugia laikmena.
13 Extended Validation Certificates Policy (EVCP) programinės įrangos pasirašymui arba TLS/SSL protokolui kaip nurodyta [CABF-EV].
14 EVCP su saugia laikmena.
15 Domain Validation Certificates Policy (DVCP) TLS/SSL sertifikatams kaip nurodyta [CABF-BR].
16 Organizational Validation Certificates Policy (OVCP) TLS/SSL sertifikatams kaip nurodyta [CABF-BR].
17 Taikomi [ETSITS101042] [ETSITS101456] reikalavimai.
18 Skelbiama http://www.cabforum.org

1.4.1 Tinkamas sertifikato naudojimas

Nepaneigiamumo ir šifravimo/dešifravimo funkcijos vykdomos skirtingais sertifikatais.

Užsakovo pageidavimu pasirašymo ir autentifikavimo funkcijos gali būti užtikrintos viename sertifikate (SSC_AIO).

1.4.2 Draudžiamas sertifikato naudojimas

Iki šiol nėra aptikta taikomųjų sistemų, kuriose būtų buvę uždrausti sertifikatai, išduodami pagal šiuos Nuostatus.

SSC GDL CA išduodami sertifikatai nėra suprojektuoti, paskirti arba įgalioti naudojimui pavojingose aplinkose arba jų valdymo įrangoje, atominių elektrinių valdymo priemonėse, navigacinėse, komunikacinėse arba bet kuriose valdymo sistemose, kur klaida gali tiesiogiai sukelti mirties arba sužalojimo riziką arba sunkią žalą aplinkai.

1.5 Nuostatų administravimas

Nauja šių *Nuostatų* redakcija yra prieinama *Užsakovams* ir *Pasitikinčioms šalims* Talpyklos rengiamų dokumentu skiltyje iki tol, kol jai pritars Nuostatų 1.5.3 poskyryje nurodytas asmuo.

SSC GDL CA dėkoja ir vertina rekomendacijas ir pasiūlymus siunčiamus el. pašto adresu nurodytų Nuostatų 1.5.1 poskyryje pildant parsisiunčiamą pastabų ir pasiūlymų formą.

1.5.1 Nuostatus administruojanti organizacija

Šį dokumentą administruoja:

Skaitmeninio sertifikavimo centras (SSC)

Jogailos 8, LT-01116, Vilnius, LIETUVA

Web: http://www.ssc.lt

El. paštas: info@ssc.lt

Faksas: +370.700.22715

1.5.2 Kontaktinis asmuo

Klausimus dėl šių Nuostatų prašome pateikti:

Skaitmeninio sertifikavimo centras (SSC)

Jogailos 8, LT-01116, Vilnius, LIETUVA

Web: http://www.ssc.lt

Tel.: +370.700.22722

El. paštas: info@ssc.lt

Faksas: +370.700.22715

1.5.3 Kas nustato CPS atitiktį Taisyklėms

Skaitmeninio sertifikavimo centras (SSC)

Taisyklių valdytojui

Jogailos 8, LT-01116, Vilnius, LIETUVA

Tel.: +370.700.22722

Faksas: +370.700.22715

El. paštas: info@ssc.lt

1.5.4 Pritarimo procedūra

Bet kuriai šių Nuostatų redakcijai turi pritarti SSC GDL CA Taisyklių valdytojas. Numatomi pakeitimai gali būti skelbiami SSC GDL CA Talpykloje siekiant gauti visuomenės pasiūlymus ir pastabas. Priklausomai nuo numatytų pakeitimų specifikos, Taisyklių valdytojas nusprendžia, ar atnaujinti Nuostatai reikalauja OID kodų pakeitimo išduotuose sertifikatuose.

1.6 Apibrėžimai ir sutrumpinimai

Šiame dokumente naudojama terminologija ir apibrėžimai iš [CWA14167-1] , [ETSITS101042], [ETSITS101456], [ETSITS102023], [CABF-BR] ir [CABF-EV].

2 TALPYKLA IR JOS VALDYTOJAS

2.1 Talpykla

Talpyklą https://gdl.repository.ssc.lt betarpiškai valdo SSC GDL CA.

SSC GDL CA Talpykloje *Užsakovams, Subjektams* ir *Pasitikinčioms šalims* prieinami:

a) Šie Nuostatai (http://gdl.repository.ssc.lt/CPS);

b) Šakninių ir Išduodančių tarnybų sertifikatai (http://gdl.repository.ssc.lt/certs);

c) Išduodančių tarnybų CRL sąrašų einamosios versijos:

http://gdl.repository.ssc.lt/rootacrl

http://gdl.repository.ssc.lt/rootbcrl

http://gdl.repository.ssc.lt/rootvs

2.2 Sertifikatų skelbimas

Sugeneruoti sertifikatai yra pristatomi atitinkamiems *Užsakovams* ir *Subjektams*. Sertifikatai gali būti prieinami nuolat SSC GDL CA Talpykloje, jeigu tam yra gautas *Subjekto* pritarimas.

Sertifikatų naudojimo sąlygos yra prieinamos *Pasitikinčioms šalims* tarptautiniu mastu 24 val. per parą ir 7 d. per savaitę, taip pat SSC GDL CA *Talpykloje*.

Už SSC GDL CA galimybių ribų įvykusių nenumatytų gedimų atveju, sertifikavimo tarnyba užtikrina Talpyklos veikimo atstatymą ne ilgiau kaip per 48 val.

2.3 Skelbimo laikas ir dažnumas

Sertifikatai ir kita atitinkama informacija yra skelbiama iškart po išdavimo arba priėmimo SSC GDL CA.

2.4 Prieiga prie Talpyklos

Šie Nuostatai, CA sertifikatai ir CRL sąrašai yra prieinami Talpykloje per Internet tinklą. Prieiga prie kitos informacijos SSC GDL CA Talpykloje nustatoma remiantis procedūromis, kurioms pritarė SSC GDL CA.

SSC GDL CA gali tikslingai apriboti prieigą prie Talpyklos siekiant apsisaugoti nuo kenksmingų kompiuterinių atakų.

3 IDENTIFIKAVIMAS IR AUTENTIFIKAVIMAS

3.1 Vardai

Subjektai, sertifikato leidėjai X.509 standarto sertifikatuose ir CRL sąrašuose identifikuojami naudojant t.v. *skiriamuosius vardus* (angl. *distinguished names)*. *Skiriamųjų vardų* atributai pateikiami pagal t.v. *DirectoryString*[19] sintaksę, kuri leidžia išreikšti vardus įvairių kodų lentelių išraiška: *PrintableString*, *TeletexString*, *BMPString*, *UniversalString* ir *UTF8String*.

Vardų vienoda išraiška yra svarbi vykdant sertifikato kelio tikrinimą[20] (angl. *Path validation*), vardų grandinės atkūrimą (angl. *Name chaining*) ir vardo apribojimo vertinimą (angl. *Name constrains computation*), kai vardai turi būti palyginami. Užtikrindama nurodytos kodų lentelės ir *Vardą* sudarančių raidžių atitikimą, sertifikavimo tarnyba prisideda prie teisingo *kelio tikrinimo* rezultato.

Kartais sertifikate gali būti nurodyti tam tikri vardų naudojimo apribojimai. Tokiu atveju apribotas vardas turi būti palygintas su *Subjekto* vardais per visą sertifikatų grandinę. Siekiant užtikrinti korektišką vardų apribojimo taikymą, visuose atitinkamuose grandinės sertifikatuose vardo atributai turi būti užkoduoti tuo pačiu metodu.

3.1.1 Vardų tipai

Ar *Subjektas*, nurodytas sertifikate, išduotame pagal šiuos Nuostatus, yra žmogus, organizacija, įranga ar paslauga, gali būti nustatytas pagal *Skiriamąją vardą* sertifikate taip, kaip apibrėžta EN 319 412 1-5 serijos standartuose.

Vardai, pavardės ir pseudonimai turi įprastą semantiką, kuri leidžia tikrinti *Subjekto* tapatybę.

3.1.2 Vardų reikšmingumas

Siekiant identifikuoti kiekvieną sertifikato *Subjektą, skiriamieji vardai* sertifikatuose, išduotuose SSC GDL CA, priskiriami prasmingai. Atributas CN rodo sertifikato *Subjektą* žmogui

19 Directory Access Protocol (v3): Attribute Syntax Definitions, RFC 2522, December 1997.
20 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, May 2008

lengvai suprantama forma. Pvz., fizinio asmens atveju, tai yra to asmens oficialus vardas:

CN=*Vardas Pavardė*

3.1.3 Anonimiškumas ir pseudonimai

SSC GDL CA anonimiškų sertifikatų neišduoda, tačiau sertifikate gali būti nurodytas asmens pseudonimas.

Sertifikatai su pseudonimais gali būti išduoti tiek fiziniams, tiek ir juridiniams asmenims pagal jų organizacinį vaidmenį.

3.1.4 Skirtingų vardų interpretavimo taisyklės

Skiriamųjų vardų (DN) interpretavimo taisyklės yra nustatytos X.501 standarte, o el. pašto adresų interpretavimas – [RFC2822].

Kadangi (X.509) sertifikato *Subjekto* atributas *serialNumber* neatskleidžia jo reikšmes semantika, šiam tikslui naudojama standarte RFC 3739 numatytas "*qcStatement-2*".

3.1.5 Vardų unikalumas

SSC GDL CA užtikrina *Subjekto su skiriamuoju* vardu unikalumą visuose išduotuose sertifikatuose. Sertifikatai išduoti tam pačiam asmeniui leidžia vienareikšmiškai nustatyti asmens tapatybę kaip nurodyta 3.1.4.

3.1.6 Prekinių ženklų pripažinimas, autentifikavimas ir vaidmuo

SSC GDL CA neišduos sertifikato, jeigu tai tai pažeidžia kito asmens teisę į prekinį ženklą.

3.2 Pradinis tapatybės tikrinimas

Pradinės tapatybės tikrinimo funkcijas, užtikrinančias patikimą tapatybes informaciją sertifikate, atlieka SSC GDL CA Registravimo tarnyba.

Sertifikate pateikiamų asmens duomenų tikrinimo patikimumo užtikrinimo prasme šie Nuostatai apibrėžia keturi pradines tapatybes tikrinimo klases (lygius) - 1 klase nurodo į žemesne patikimumą, o 4 – į aukščiausią.

Kaip konkrečioms taikomosioms sistemoms ir tranzakcijoms tinkančių sertifikatų išrinkimo kriterijus privačiųjų ir viešųjų asmenų teikiamas el. paslaugas, atlikę susijusių rizikų ir jų atsitikimo tikimybė ir atsižvelgiant į 1.4 p. nuostatas, nustato jiems priimtino asmens tapatybės tikrinimo lygius, kuri naudojasi *Užsakovai*.

Jeigu sertifikato *Subjektas* yra fizinis asmuo, asmens tapatybė (pvz. vardas, pavardė) tikrinama betarpiškai, pateikiant asmens tapatybės dokumentus arba būdais, kurie gali būti laikomi ekvivalentiški fiziniam prisistatymui[21].

SSC GDL CA saugoja visą asmens tapatybės tikrinimo metu surinktą informaciją, visas nuorodas į dokumentus, kurie buvo naudoti tikrinant asmens tapatybę, ir visą informaciją apie dokumentų galiojimą.

Jeigu SSC GDL CA paslauga teikiama per *Užsakovą*, surenkama pakankamai įrodymų, kad pastarasis turėjo tinkamą įgaliojimą veikti *Subjekto vardu*, (pvz., gali atstovauti identifikuotą organizaciją). *Užsakovas* PRIVALO pranešti savo adresą arba kitus atributus, kurių pagalba būtų įmanoma susisiekti su juo.

Jeigu sertifikatas išduodamas įrangai arba paslaugai, laikoma, kad privataus rakto naudojimą kontroliuoja atsakingas asmuo. SSC GDL CA šią informacija fiksuoja ir saugoja. Sertifikatuose, išduotuose pagal šiuos Nuostatus, DN laukas gali nurodyti įrangą arba paslaugą, kuri sertifikuojama. Sertifikato diegimą galutinėje įrangoje arba paslaugoje turi užtikrinti *Užsakovo* paskirtas atsakingas asmuo.

Asmens tapatybės tikrinimas išduodant EVCP ir EVCP+ sertifikatus atliekamas pagal [CABF-EV] reikalavimus.

EVCP ir EVCP+ sertifikatų užsakymams SSC GDL CA turi specialias formas, kuriose numatyti tikrinimo reikalavimai visiems potencialiems dalyviams, nurodytiems 1.3.5 p.

21 Netiesioginio tikrinimo įrodymu gali būti dokumentas, kurių gavimui būtinas asmeninis apsilankymas, pateikimas.

3.2.1 Privataus rakto turėjimo įrodymas

Jeigu *Užsakovas* pats generuoja raktų porą, reikalaujama, kad būtų pateiktas privataus rakto, atitinkančio viešąjį raktą pateiktame CSR, valdymo įrodymas.

El. parašo sertifikato atveju, tai daroma prašant *Subjektą* pasirašyti SSC GDL CA siūlomus duomenis. SSC GDL CA toliau tikrina šį parašą to asmens pateiktu viešuoju raktu.

Privataus rakto valdymo įrodymas nėra reikalaujamas, jeigu raktų generavimas vykdomas CA arba RA tiesiogiai kontroliuojant procesą.

3.2.2 Organizacijos autentifikacija

Jeigu sertifikato *Subjektas* yra juridinis asmuo, tapatybė nustatoma pagal pilną organizacijos pavadinimą ir pagal duomenis apie jos registravimą valstybės pripažįstamame registre.

Jeigu sertifikato *Subjektas* yra įranga arba paslauga, valdoma organizacijos arba jos vardu, reikalaujama nurodyti įrangos/paslaugos identifikavimo duomenis, pilną organizacijos pavadinimą ir nacionaliniu mastu pripažįstamą registracijos identifikatorį.

EVCP ir EVCP+ sertifikatų atveju *Pareiškėjo* tapatybė, įskaitant jo tariamą vardą, juridinį ar fizinį, ir veiklos buveinė bei domeno srities vardo nuosavybės teisė yra tikrinama pagal [CABF-EV] reikalavimus.

3.2.3 Individualaus asmens autentifikacija

Jeigu sertifikato *Subjektas* yra fizinis asmuo, nesusijęs su juridiniu asmeniu, turi būti nurodyti vardas, pavardė (nacionalinių teisės aktų nustatyta forma), gimimo data ir vieta, asmens tapatybės dokumento duomenys arba kiti atributai (pvz. biometriniai), kurie gali būti naudojami vienareikšmiškai skiriant šį asmenį nuo kitų, turinčių tokį pat vardą ir pavardę.

Jeigu sertifikato *Subjektas* yra fizinis asmuo, susijęs su juridiniu arba organizaciniu asmeniu, turi būti nurodyti vardas, pavardė (nacionalinių teisės aktų nustatyta forma), gimimo data ir vieta, asmens tapatybės dokumento duomenys arba kiti atributai (pvz. biometriniai), kurie gali būti naudojami vienareikšmiškai skiriant šį asmenį nuo kitų, turinčių tokį pat vardą ir pavardę, pilnas

juridinio ar kito asocijuoto organizacinio asmens pavadinimas, jo juridinis statusas ir visi juridinio arba asocijuoto organizacinio asmens registravimo duomenys, santykiai tarp *Subjekto* ir juridinių arba asocijuotų organizacinių asmenų.

Sertifikato atšaukimo atveju gali būti naudojamos alternatyvios procedūros, pvz., prašant per saugų kanalą įvesti PIN (angl. *Personal Identification Number*) kodą.

3.2.4 Įrangos autentifikavimas

Jeigu sertifikato *Subjektas* yra techninė įranga, *Užsakovas* privalo pateikti atitinkamą įrangą identifikuojančia informacija ir priimtina įrangos nuosavybes teises įrodymą, kuriame turi būti gamintojo priskirtas įrangos/produkto pavadinimas, serijinis numeris, įrangos atributai, kurias prašoma įrašyti į sertifikatą, jeigu tokiu yra, ir įrangos savininko kontaktine informacija.

CA patikrins, kad *Užsakovas* yra įgaliotas prašyti sertifikatą šiai įrangai.

Jeigu pati įranga teikia save identifikuojančia informacija (pvz., sertifikatą), įrangos tapatybe yra autentifikuojama.

Papildoma informacija apie įrangos registravimą teikiama 4 skyriuje.

3.2.5 Paslaugos autentifikavimas

Jeigu sertifikato *Subjektas* yra paslaugą teikiamą per tinklą, Užsakovas privalo pateikti identifikuojanti informacija ir priimtina nuosavybės teises įrodymą, kuriame turi būti unikalus programines įrangos ar paslaugos pavadinimas (e.g. domeno vardas), paslaugos atributai, kurias prašoma įrašyti į sertifikatą, jeigu tokiu yra, ir savininko kontaktine informacija.

CA patikrins, kad *Užsakovas* yra:

(a) įgaliotas prašyti sertifikatą šiai paslaugai;

(b) ikras paslaugos savininkas (per atitinkamą patikimą 3-jų šalių duombaze);

(c) galintis demonstruoti domeno informacijos valdymą (manipuliuojant DNS įrašais ir serverio konfigūraciją).

Papildoma informacija apie paslaugos registravimą teikiama 4 skyriuje.

3.2.6 Netikrinama informacija

Informacija apie *Subjektą*, įskaitant ir el. pašto adresą, įrašoma tik po patikimo patikrinimo.

3.2.7 Įgaliojimų tikrinimas

Išduodant CA ir el. parašo sertifikatą, kuriame bus nurodytas organizacijos pavadinimas, SSC GDL CA tikrina asmens įgaliojimus veikti organizacijos vardu. Jeigu sertifikate nurodomas pseudonimas, identifikuojantis *Subjektą* pagal organizacinį vaidmenį, SSC GDL CA įsitikina, kad asmuo yra įgaliotas pasirašyti to vaidmens vardu.

3.2.8 Sąveikumo kriterijai

SSC GDL PKI sistema suprojektuota tokiu būdu, kad galėtų sąveikauti su kitomis pasitikėjimo paslaugų tarnybomis šiais tikslais:

- *registruoti Subjektą*;
- pristatyti raktus ir/ar sertifikatus;
- autentifikuoti *Subjektus* on-line režimu;
- teikti kitas abipusiškai naudingas paslaugas.

3.3 Identifikavimas ir autentifikavimas sertifikavimo tikslais

3.3.1 Identifikavimas ir autentifikavimas įprastam sertifikavimui

Atstatant (angl. re-key) *Užsakovo* sertifikatą, asmens tapatybė gali būti nustatyta remiantis galiojančiu sertifikatu, su sąlyga, kad tapatybė pakartotinai tikrinama kas tris metus įprastu registravimo būdu.

Atstatant įrangos sertifikatus, tapatybė gali būti nustatyta remiantis galiojančiu įrangos arba asmens, atsakingo už įrangą, sertifikatu, su sąlyga, kad tapatybė pakartotinai tikrinama kas trys

metus įprastu registravimo būdu.

3.3.2 Identifikavimas ir autentifikavimas po atšaukimo

Po sertifikato atšaukimo naujas sertifikatas visada išduodamas praėjus įprastą registravimo procesą, aprašytą aukščiau.

3.4 Identifikavimas ir autentifikavimas atšaukimo tikslais

Prašymai atšaukti sertifikatą visada reikalauja autentifikacijos. Autentifikacija gali būti atlikta remiantis galiojančiu sertifikatu, su sąlyga, kad atitinkamas privatus raktas nėra kompromituotas.

4 REIKALAVIMAI SERTIFIKAVIMO VEIKLAI

Bendru atveju SSC GDL CA išduotu sertifikatu gyvavimo ciklas apima: *Subjekto* registravimą, sertifikato išdavimą, sertifikato naudojimą, sertifikato atšaukimą, sertifikato galiojimo pasibaigimą, Sertifikato atstatymą/atnaujinimą.

Siekiant atlikti patikimą registravimo procesą CA remiasi modeliu kurio pagrindo sudaro:

1. Sertifikato *prašytojas*:

(a) yra fizinis asmuo – kuris turi galiojanti tikrinamą asmens tapatybes dokumentą;

(b) yra įgaliotas atstovauti *Užsakovui* ir/ar *Subjektui*;

(c) yra asmuo su kuriu galima bendrauti per viešai identifikuojama komunikacinį kanalą.

2. Sertifikato *Užsakovas*:

(a) yra arba prašytojas arba kitas fizinis ar juridinis asmuo, turintis galiojanti tikrinamą asmens tapatybes dokumentą;

(b) yra įgaliotas atstovauti *Subjektą*, jeigu taikoma;

(c) yra asmuo su kuriu galima bendrauti per viešai identifikuojama komunikacinį kanalą.

3. Sertifikato *Subjektas*:

(a) yra arba *Užsakovas* arba kitas fizinis ar juridinis asmuo, turintis galiojanti tikrinamą asmens tapatybes dokumentą;

(b) turi atitinkamą įgaliojimą, jeigu taikoma;

(c) sutinka su sertifikavimo paslaugų teikimo sąlygomis;

(d) yra asmuo su kuriu galima bendrauti per viešai identifikuojama komunikacinį kanalą.

Registravimo procesas, kuris gali būti vykdomas nuotoliniu būdu arba Subjektu asmeniškai apsilankant[22], užtikrina patikimą proceso dokumentavimą, kad išvengti galimą registravimo fakto neigimą, reikalauja, kad Užsakovas įrodytu:

1. *Subjektas*, kurio prašoma registruoti iš tikrųjų yra tas asmuo kuriu prisistato;
2. *Subjektas* egzistuoja pareikštų identifikatorių ir atributais;
3. *Subjekto* identifikatorius yra unikalus tam tikroje aplinkoje arba domene.

22 Naudojant metodus, užtikrinančius fiziniam apsilankymui ekvivalentiška patvirtinimą kuri gali demonstruoti patikimumo paslaugų teikėjas.

SSC GDL CA palaiko dokumentų ir informacijos šaltinių, kuri pripažinti kaip patikimi asmens tapatybes patvirtinimu, sąrašą. Priklausomai nuo sertifikato klases savo tapatybe asmuo gali patvirtinti fiziškai apsilankant arba nuotolinių būdu, jeigu to leidžia taikoma tapatybes tikrinimo procedūra.

Būdai kaip sertifikatas yra užsakomas ir kaip tikrinama Užsakovo tapatybe sertifikato gyvavimo cikle tūri esmine saugumo reikšme. Bendru atveju Registravimas apima:

1) užsakymo išduoti sertifikatą priėmimą;
2) *sertifikato prašytojo* identifikavimą ir jo įgaliojimo tikrinimą;
3) priimtino ryšio kanalo tarp prašytojo ir RA suderinimo;
4) pradines informacijos teikimą (sertifikavimo paslaugos teikimo sąlygos, prašymo formos, prieigos duomenų prie užsakymo aplinkos teikimą ir pan.);
5) paraiškos ir visų susijusiu dokumentų priėmimą;
6) *Užsakovo* identifikavimą, jo įgaliojimų tikrinimą;
7) *Užsakovo* egzistavimo formų nustatymą;
8) santykių tarp *Užsakovo* ir kitų asmenų, turinčių reikšminga įtaka į arba prisiimančių atsakomybe už sutartinių įsipareigojimų su CA vykdymo, tikrinimą;
9) informacijos, kurios prašomą įrašyti į sertifikato Subjektą, tikrinimą;
10) kitų atributų (pvz., el. pašto adreso, domeno vardo ir pan.), kuriu prašoma sertifikate, tikrinimą;
11) Paraiškos priėmimą.

Tikrinimo procese RA pirma tikrina *prašytojo* pateiktos informacijos ir dokumentu galiojimą ir po to prašytojo/Užsakovo egzistavimo forma naudojant savo pasirinkta patikimą ir nepriklausomą informacijos šaltinį.

Kai tik susijusiu asmenų tapatybe yra nustatyta, RA tikrina bet kuria kitą informacija, kuri prašoma sertifikate. Patikrinimas vykdomas tiek fizinių taip pat skaitmeninių išteklių atžvilgių.

Technines įrangos atveju Užsakovas turi pateikti produkto identifikuojanti informacija (pvz., pavadinimą, serijinį numerį ir pan.) ir nuosavybes teises įrodymą (pvz., įrangos naudojimo vieta, siuntimo/pristatymo dokumentus, sąskaita-faktūra ir pan.). Pateikta informacija tikrinama kryžinų būdu kai tam yra galimybių.

Skaitmeninių ištekliu atveju, kai jų identifikatorius skiria tretieji asmenys (pvz., el. pašto adresus, domeno vardus ir pan.), RA tikrina išteklių veiklos egzistavimą per betarpišką priėjimą prie resurso ar jo naudojimą, o teisine egzistavimą – gavę atitinkamo registruojančio asmens patvirtinimą dėl nuosavybes.

Aukšto patikimumo sertifikatu atveju RA prašo demonstruoti atitinkamų išteklių valdymo sugebėjimą (pvz., keisti DNS įrašus, serverio konfigūracija ir pan.).

Apibendrinant konstatuotina, kad SSC GDL CA:

a) Supažindina *Užsakovus* ir *Pasitikinčias šalis* su teikiamų paslaugų sąlygomis, išdėstytomis dokumente „Viešai skelbtina informacija“ (SSC GDL CA PDS);
b) Turi valdymo organą, kuris galutinai tvirtina CPS ir užtikrina tinkamą jų įgyvendinimą;
c) Informuoja apie planuojamus CPS pakeitimus ir nedelsiant skelbia patikslintus ir patvirtintus CPS;
d) Dokumentuoja taikomus algoritmus ir parametrus.

Dokumente „ASMENŲ REGISTRAVIMO SERTIFIKATAMS GAUTI IR KONSULTAVIMO TAISYKLĖS“ CA aprašo asmens tapatybes nustatymo procedūras darbiniame lygmenyje. Šis dokumentas audituojamas.

4.1 Prašymas išduoti sertifikatą

Prieš sudarant sutartį[23] su *Užsakovu,* SSC GDL CA supažindina asmenį su sertifikatų naudojimo sąlygomis[24], nurodytomis viešai prieinamame dokumente – „Viešai skelbtina informacija“[25].

Tapatybės nustatymui SSC GDL CA remiasi tiesioginiais įrodymais arba atitinkamų įgaliotų šaltinių pateiktais patvirtinimais. *Subjekto* tapatybės nustatymui naudojama procedūra yra tinkamai apibrėžta nacionalinę teisę atitinkančiuose vidiniuose dokumentuose.

23 Teikiant sertifikavimo paslaugas plačiajai visuomenei, atkreipiamas dėmesys, kad sutarties sąlygos atitiktų naudotojų teisių apsaugos įstatymų reikalavimus, įskaitant ir Direktyvos 93/13/EEB dėl nesąžiningų sąlygų sutartyse su naudotojais įgyvendinimą.
24 Jei sertifikato *Subjektas* ir *Užsakovas* yra ne tas pats žmogus, sertifikato *Subjektas* yra informuojamas apie jo/jos įsipareigojimus.
25 Dokumento OID: 2.16.440.1.4.30003763.0.3.1.0, 1.3.6.1.4.1.22501.0.3.1.0

SSC GDL CA registracijos proceso metu užtikrina ES ir nacionalinių asmens duomenų apsaugos įstatymų reikalavimų laikymąsi ir tikrinimo taisykles bei reikalauja surinkti pakankamai duomenų, kad asmens tapatybės patvirtinimas atitiktų sertifikato naudojimo reikalavimus.

SSC GDL CA registracijos metu atlieka tapatybės patikrinimą kaip aprašyta nacionalinę teisę atitinkančiuose vidiniuose dokumentuose, ir esant poreikiui, patikrina ir specialius asmens, kuriam yra išduodamas kvalifikuotas sertifikatas, požymius. Asmens tapatybė nustatoma fiziniam asmeniui dalyvaujant betarpiškai arba netiesiogiai – naudojant metodus, prilygstančius betarpiškam asmens dalyvavimui[26].

Jei dėl paslaugų suteikimo į SSC GDL CA kreipiasi ne pats sertifikato *Subjektas*, tuomet *Užsakovas* turi pateikti įrodymus, kad gali atstovauti sertifikato *Subjektą*, o prašymas dėl sertifikato išdavimo, kuriame įtraukti sertifikato *Subjekto* įsipareigojimai, privalo būti pasirašytas tiek sertifikato *Subjekto*, tiek *Užsakovo*. Prašymo forma identifikuoja kiekvieno dalyvio vaidmenį kaip aprašyta skyriuose 1.3.3, 1.3.5. Sertifikatų prašymo formos pateikiamos *Užsakovams* po užsakymo pateikimo.

EVCP ir EVCP+ sertifikatų atveju yra taikomos papildomos tikrinimo priemonės, aprašytos [CABF-EV], nustatant *Užsakovo* teisinį[27], fizinį[28] ir veiklos egzistavimą. Siekiant autentifikuoti parašus EVCP ir EVCP+ sertifikatų prašymų formose[29], turi būti įrodomas atstovavimas ir įgalinimai veikti *Pareiškėjo* vardu.

Į sutartį su *Užsakovu* SSC GDL CA įtraukia *Užsakovo* sutikimą:

a) su jo įsipareigojimais;

b) naudoti saugų įrenginį[30];

c) SSC GDL CA saugotų informaciją, naudojamą registravimo metu[31], sertifikato laikmenos informaciją, *Užsakovo* duomenis, kai sertifikatą užsako ne pats *Subjektas*,

26 Netiesiogiai patikrinti įrodymai, nedalyvaujant fiziniam asmeniui, yra dokumentai pateikti registravimui, kuris atliekamas gavus prašymą, reikalaujantį fizinio asmens dalyvavimo. Įrodymai gali būti pateikti popierine arba elektronine dokumentų forma.
27 Juridinio asmens vardo, kuris nurodomas EV sertifikatų prašymuose, teisėtumą ir tikrumą RA tikrina oficialiuose duomenų registruose (Juridinių asmenų, mokesčių mokėtojų ir socialinės apsaugos DB).
28 RA patikrina Pareiškėjo oficialų pašto (buveinės) adresą ir pagrindinį telefono numerį.
29 Tuo atveju, jeigu sertifikato prašo techninis kontaktinis asmuo, neturintis sertifikato užsakymo teisių, sertifikato prašymo forma turi būti pasirašyta kito asmens, kurio įgaliojimas ir bus tikrinamas. RA su pasirašančiu asmeniu susisiekia telefonu siekiant patvirtinti jo įgaliojimą. RA taip pat gali susisiekti su pasirašančiu asmeniu paštu, išsiunčiant pareiškėjui laišką į jo verslo veiklos vietą.
30 Jei reikalaujama sertifikavimo tarnybos.
31 Įskaitant asmens priėmusio prašymą, tapatybės tikrinimo metodą, jei toks yra, ir su tuo susijusį CA ir RA pavadinimą, jeigu taikoma.

taip pat bet kokią būsimą informaciją dėl sertifikato atšaukimo, asmens ir jo specialiųjų požymių, nurodytų sertifikate, ir visos šios informacijos perdavimą trečiosioms šalims, kai SSC GDL CA nutraukia savo veiklą pagal šiuos *Nuostatus*;

d) leisti arba ne skelbti jo sertifikatą;

e) su jo patvirtinimu, kad sertifikate nurodyta informacija yra teisinga;

f) *su Užsakovo* arba *Subrangovo* įsipareigojimais ir garantija EVCP ir/arba EVCP+ sertifikatų atveju:

- imtis visų protingų priemonių, kad visais atvejais tinkamai apsaugoti EVCP ir EVCP+ sertifikatų privatųjį raktą, jo slaptažodį ir laikmeną;
- nediegti ir nenaudoti EVCP ar EVCP+ sertifikato, prieš tai neatlikus sertifikate nurodytų duomenų peržiūros ir patikrinimo;
- įdiegti EVCP ar EVCP+ sertifikatą tik į tarnybinę stotį, kurios Domeno Vardas yra nurodytas sertifikate ir naudoti EV sertifikatą laikantis teisės aktų, išskirtinai tinkamoje kompanijos veikloje ir laikantis Sutarties sąlygų;

g) su įsipareigojimu ir garantija nedelsiant kreiptis į CA dėl sertifikato atšaukimo, kai:

- bet kokia SSC GDL CA išduoto sertifikato informacija yra/ar tampa neteisinga ar klaidinga;
- yra patvirtinta arba tariama informacija apie *Užsakovo* sertifikato privataus rakto netinkamą naudojimą arba sukompromitavimą.

h) informacija yra saugojama tiek, kiek nurodyta aukščiau arba tiek, kiek gali prireikti sertifikavimo fakto įrodymui atliekant teisines procedūras[32].

Jei raktų porą generuoja ne SSC GDL CA, tai prašymo išduoti sertifikatą apdorojimo procesas užtikrina, kad sertifikato *Subjektas* valdo privatųjį raktą.

32 Tais atvejais, kai sertifikato *Subjektai* per RA yra registruojami kitoje šalyje, kurioje įkurta CA, RA registravimo atveju turi taikyti savo šalies taisykles. Jei *Užsakovai* gyvena kitoje šalyje, turi būti atsižvelgta į sutartinius ir kitus teisinius reikalavimus taikomus *Užsakovui* pagal RA šalies reikalavimus.

SSC GDL CA taiko specialias procedūras aukštą riziką keliantiems prašymams tikrinant organizacijų, prieš kurias dažniausiai būna nukreipti „apsimestinių nuorodų“ (angl. *phishing*) tipo sukčiavimo atakos, sąrašus, įtartini prašymai apdorojami atliekant papildomus patikrinimus „apsimestinių nuorodų“ sąrašuose, kurį skelbia APWG[33] ir kituose šaltiniuose, kuriuos naudoja CA siekiant įsitikinti, kad pareiškėjas ir prašyme nurodytas asmuo yra ta pati organizacija.

4.1.1 Kas gali prašyti išduoti sertifikatą

Prašymą dėl CA sertifikato sudarymo gali pateikti įgaliotas SSC GDL CA atstovas.

Prašymą dėl *Subjekto* sertifikato sudarymo gali pateikti arba sertifikato *Subjektas,* arba *Užsakovas*.

Prašymą dėl įrenginio/paslaugos sertifikato sudarymo gali pateikti asmuo atsakingas už įrenginį ar paslaugą.

4.1.2 Išdavimo procesas ir atsakomybės

Visa bendravimo tarp RA ir *Užsakovo* informacija, įskaitant ir informaciją išdavimo procese, tikrinama ir apsaugojama nuo pakeitimų. Slaptų duomenų perdavimas apsaugojamas specialiomis priemonėmis.

Bendraujant elektroniniu būdu yra naudojamas kriptografinis šifravimo mechanizmas.

Už tikslios informacijos pateikimą registravimo proceso metu atsako *Užsakovas*.

4.2 Prašymo išduoti sertifikatą apdorojimas

Prašymo išduoti sertifikatą apdorojimo procesas kryptingai veda ir padeda *Užsakovui* iki galutinio sertifikato gavimo.

Prašymų EVCP ir EVCP+ sertifikatams gauti apdorojimas užbaigiamas, kai kitas darbuotojas, nei tas, kuris atliko pradinę Prašymo informacijos patikrinimą, atlieka papildomą

33 The Anti-Phishing Work Group

kryžminį duomenų sutikrinimą, kruopščiai tikrina visą informaciją ir sprendžia išduoti ar ne sertifikatą.

4.2.1 Identifikavimo ir autentifikavimo funkcijų vykdymas

Užsakovo identifikavimas ir autentifikavimas vykdomas atitinkamai pagal šių CPS reikalavimus, aprašytus aukščiau.

Užsakovo tapatybės nustatymas yra tinkamai dokumentuota RA pareiga.

4.2.2 Prašymo išduoti sertifikatą priėmimas arba atsisakymas

Prašymo išduoti sertifikatą priėmimo arba atsisakymo sąlygos yra nurodomos paslaugų teikimo sutartyje.

4.2.3 Prašymo apdorojimo laikas

Prašymas išduoti sertifikatą turi būti apdorotas per tris darbo dienas, o sertifikatas turi būti išduotas per penkias darbo dienas nuo RA patvirtinimo.

4.3 Sertifikato išdavimas

Gavus prašymą išduoti sertifikatą, RA patikrina *Užsakovo* tapatybę ir įgaliojimus bei informacijos tikslumą, nurodytą prašyme išduoti sertifikatą. Esant teigiamam patikrinimui, siunčiama užklausa SSC GDL CA sertifikato generavimui.

4.3.1 CA veiksmai išduodant sertifikatą

SSC GDL CA užtikrina, kad anksčiau SSC GDL CA registruoto sertifikato *Subjekto* prašymai yra išsamūs, tikslūs ir tinkamai įgaliojantys. Tai apima sertifikatų atnaujinimą, kai išduodamas sertifikatas su nauju *Subjekto* raktu po sertifikato atšaukimo arba prieš pasibaigiant sertifikato galiojimui ir keičiant *Subjekto* duomenis sertifikate.

Kai prašoma atnaujinti sertifikatą, SSC GDL CA patikrina, ar jis egzistuoja ir galioja, bei, ar informacija, kuri buvo naudojama sertifikato *Subjekto* tapatybės nustatymui, vis dar galioja. Jeigu paaiškėja, kad sertifikuota informacija, pvz., vardas, pasikeitė arba sertifikatas yra atšauktas, registravimo duomenys patikslinami, iš naujo užregistruojami ir patvirtinami *Užsakovo*.

SSC GDL CA neišduoda naujo sertifikato anksčiau sertifikuotam viešajam raktui.

Sertifikate išduotame pagal šiuos CPS įrašoma:

a) SSC GDL CA tarnybos identifikatorius ir šalis;
b) sertifikato *Subjekto* vardas arba slapyvardis;
c) viešasis raktas, atitinkantis privatųjį raktą, kurį valdo sertifikato *Subjektas*[34];
d) nuoroda į sertifikato galiojimo pradžios ir pabaigos laikotarpį;
e) sertifikato identifikavimo kodas;
f) išdavusios CA elektroninis parašas.

QCP ir QCP+ sertifikatai išduoti pagal šiuos CPS apima[35]:

a) požymį, kad sertifikatas yra kvalifikuotas;
b) SSC GDL CA ir šalies, kurioje įkurta sertifikavimo tarnyba, identifikavimą;
c) pasirašančio asmens vardą arba slapyvardį;
d) pasirašančio asmens specifinius požymius, jei taikoma;
e) parašo tikrinimo duomenis, atitinkančius parašo formavimo duomenis;
f) nuorodą į sertifikato galiojimo pradžios ir pabaigos laikotarpį;
g) sertifikato identifikavimo kodą (pvz. sertifikato serijinį numerį);
h) saugų elektroninį parašą sertifikavimo paslaugų teikėjo, kurį jis išduoda;
i) apribojimus dėl sertifikato naudojimo paskirties, jei taikoma;
j) ribas sandorių vertei, kuriuose gali būti naudojamas sertifikatas, jei taikoma[36];
k) nuorodą į SSC GDL CA PDS.

EVCP ir EVCP+ sertifikatai, išduoti pagal šiuos CP apima:

34 QCP+ sertifikatai *Subjekto* išskirtinė kontrolė.
35 Kaip nurodyta EN 319 412-5.
36 Taikoma visiems QCP+ sertifikatams.

Laukas	OID
subject:organizationName	2.5.4.10
subject:commonName[37]	2.5.4.3
subject:businessCategory	2.5.4.15
subject:jurisdictionOfIncorporationLocalityName	1.3.6.1.4.1.311.60.2.1.1
subject:jurisdictionOfIncorporationStateOrProvinceName	1.3.6.1.4.1.311.60.2.1.2
subject:jurisdictionOfIncorporationCountryName	1.3.6.1.4.1.311.60.2.1.3
subject:serialNumber	2.5.4.5
subject:streetAddress	*2.5.4.9*
subject:localityName	*2.5.4.7*
subject:stateOrProvinceName	*2.5.4.8*
subject:countryName	*2.5.4.6*
subject:postalCode	*2.5.4.17*

SSC GDL CA užtikrina, kad kvalifikuotame sertifikate nurodytas *Subjekto skiriamasis vardas* (DN) sertifikavimo tarnybos ribose visada liks unikalus[38].

Sertifikato išdavimo procedūra yra dokumentuota ir patikimai susieta su raktų poros generavimu[39] ir su tuo susijusio registravimo, sertifikato atstatymo ar atnaujinimo duomenimis.

Jei sertifikatas įrašomas į saugų įrenginį, SSC GDL CA užtikrina, kad tai būtų atliekama saugiai:

- CA užtikrintai kontroliuoja saugaus įrenginio paruošimą;
- Saugus įrenginys yra saugojamas ir pristatomas saugiai.

4.3.2 CA pranešimas užsakovui apie sertifikato išdavimą

RA informuoja *Užsakovą* apie sertifikato išdavimą ir pristatymo galimybę. Įrenginių ar paslaugų sertifikatų atveju, RA informuoja atsakingą asmenį.

4.4 Sertifikato priėmimas

Sertifikato išdavimo procese yra etapas, kai *Užsakovas* aiškiai patvirtina sertifikato

37 arba *subjectAltName:dNSName*
38 Per visą CA egzistavimo laikotarpį *skiriamasis vardas,* nurodytas išduotame sertifikate, niekada nebus panaudotas pakartotinai.
39 Sertifikatai visada išduodami remiantis atitinkamu privačiu raktu pasirašytos PKC#10 užklausos.

priėmimą. Priimdamas sertifikatą *Užsakovas* sutinka su sąlygomis, išdėstytomis šiuose CPS.

4.4.1 Sertifikato priėmimą patvirtinantis elgesys

Sertifikavimo procese yra numatytas etapas, kuriame *Užsakovas* aiškiai priima sertifikatą.

4.4.2 Sertifikato skelbimas

SSC GDL CA skelbia sertifikatus viešai, jei tam pritaria *Užsakovas* ir jeigu tai atitinka duomenų apsaugos reikalavimus.

4.4.3 CA pranešimas kitiems asmenims apie sertifikato išdavimą

Šalys dalyvaujančios sertifikato išdavimo procese taip pat gali gauti pranešimą apie sertifikato išdavimą.

4.5 Raktų poros ir sertifikato naudojimas

4.5.1 Privataus rakto ir sertifikato naudojimas

Konkretūs raktų poros ir/ar naudojimo apribojimai yra išreikšti per sertifikato *Basic constraints* ir *Key usage* plėtinius.

4.5.2 Viešojo rakto ir sertifikato naudojimas pasitikinčioms šalimis

CA, veikiančios pagal šiuos CPS, sudaro CRL sąrašus, nurodančius visų sertifikatų[40] būseną, kurią *Pasitikinčios šalys* PRIVALO patikrinti kiekvieną kartą norėdamos pasitikėti sertifikatu.

40 Išskyrus OCSP atsakiklio sertifikatus su *id-pkix-ocsp-nocheck* plėtiniu.

4.6 Sertifikato pratęsimas

Ši CA pratęsia egzistuojantį sertifikatą išduodant naują sertifikatą naujai raktų porai.

4.6.1 Sertifikato pratęsimo aplinkybės

SSC GDL CA patikrina pratęsiamo sertifikato buvimą ir jo bei informacijos, naudojamos sertifikato *Subjekto* tapatybės ir požymių patvirtinimui, galiojimą.

4.6.2 Kas gali prašyti pratęsti sertifikatą

Tik sertifikato *Subjektas* arba jo įgaliotas *atstovas* GALI prašyti pratęsti sertifikatą.

4.6.3 Prašymo pratęsti sertifikatą apdorojimas

Pratęsimo prašymai ir procedūros yra paprastai tokios pat kaip ir naujo sertifikato išdavimo metu, o *Užsakovo* bet kokie pateikiami dokumentai GALI būti pasirašyti elektroniniu būdu.

4.6.4 Pranešimas užsakovui apie naujo sertifikato išdavimą

SSC GDL CA praneša *Užsakovui* apie naujo sertifikato išdavimą tokiu būdu, kuris atitinka taikomus Taisyklių reikalavimus.

4.6.5 Pratęsto sertifikato priėmimą patvirtinantis elgesys

Pratęstas sertifikatas laikomas priimtu, kai *Užsakovas* raštiškai patvirtina pristatymo faktą arba kai *Užsakovas* per 15 dienų po pratęsimo panaudoja sertifikatą.

4.6.6 Pratęsto sertifikato skelbimas

Remiantis *Užsakovo* sutikimu, pratęstas sertifikatas yra skelbiamas SSC GDL CA Talpykloje.

4.6.7 Pranešimas kitiems asmenims apie sertifikato išdavimą

Jei kiti subjektai buvo susiję su sertifikato išdavimo procesu, jie taip pat gali būti informuoti apie sertifikato išdavimą.

4.7 Sertifikato atstatymas

Sertifikato atstatymas yra tas pats, kas naujo sertifikato su nauju viešuoju raktu išdavimas, kai kita sertifikato *Subjekto* informacija sertifikate lieka nepakitusi. Atstatytas sertifikatas gali būti su skirtingu sertifikato pasibaigimo laikotarpiu, o informacija, susijusi ne su sertifikato *Subjektu*, taip pat GALI keistis sertifikate.

4.7.1 Sertifikato atstatymo aplinkybės

Iki dviejų sertifikato pratęsimo/atstatymo kartų, kurių dažnumas ne ilgesnis nei 25 mėnesiai, pratęsimas/atstatymas gali būti atliekamas nuotoliniu būdu, be *Užsakovo* asmeninio pasirodymo tarnyboje. Atšaukti ar pasibaigę sertifikatai nėra pratęsiami.

4.7.2 Kas gali prašyti sertifikato atstatymo

Prieš pasibaigiant raktų poros galiojimo laikotarpiui, *Užsakovas* gali prašyti išduoti naują sertifikatą, jei ankstesnis sertifikatas nebuvo atšauktas, o *Užsakovas* ir reikalavimai sertifikatui vis dar egzistuoja.

4.7.3 Prašymo atstatyti sertifikatą apdorojimas

SSC GDL CA patikrina atstatomo sertifikato buvimą ir jo bei informacijos, naudojamos sertifikato *Subjekto* tapatybės ir požymių patvirtinimui, galiojimą.

Jei sertifikuoti vardai ar požymiai pasikeitė arba ankstesnis sertifikatas buvo atšauktas, tuomet registracijos informacija yra tikrinama, saugoma, o *Užsakovas* sutinka su ja.

4.7.4 Pranešimas užsakovui apie naujo sertifikato išdavimą

Kai tik sertifikatas yra sugeneruotas, *Užsakovai* nedelsiant yra informuojami apie naujo sertifikato išdavimą.

4.7.5 Atstatyto sertifikato priėmimą patvirtinantis elgesys

Atstatytas sertifikatas laikomas priimtu, kai *Užsakovas* raštiškai patvirtina pristatymo faktą arba kai *Užsakovas* per 15 dienų po atstatymo panaudoja sertifikatą.

4.7.6 Atstatyto sertifikato publikavimas

Remiantis *Užsakovo* sutikimu, atstatytas sertifikatas gali būti skelbiamas SSC GDL CA Talpykloje.

4.7.7 Pranešimas kitiems asmenims apie sertifikato išdavimą

Jei kiti asmenys buvo susiję su sertifikato išdavimo procesu, jie taip pat gali būti informuoti apie sertifikato išdavimą.

4.8 Sertifikato pakeitimas

Sertifikato pakeitimas yra tas pats, kas naujo sertifikato su nauju viešuoju raktu išdavimas, kai bet kokia sertifikato *Subjekto* informacija sertifikate taip pat gali keistis. Pakeistas sertifikatas gali būti su skirtingu sertifikato pasibaigimo laikotarpiu, o informacija, susijusi ne su sertifikato *Subjektu*, taip pat GALI keistis sertifikate.

4.8.1 Sertifikato pakeitimo aplinkybės

SSC GDL CA patikrina keičiamo sertifikato buvimą ir jo bei informacijos, naudojamos sertifikato *Subjekto* tapatybės ir požymių patvirtinimui, galiojimą.

4.8.2 Kas gali prašyti pakeisti sertifikatą

Tik sertifikato *Subjektas* arba įgaliotas *Subjekto* atstovas GALI prašyti pakeisti *Subjekto* sertifikatą.

4.8.3 Prašymų pakeisti sertifikatą apdorojimas

Pakeitimo prašymai ir procedūros yra paprastai tokios pat kaip ir naujo sertifikato išdavimo metu, o *Užsakovo* bet kokie pateikiami dokumentai GALI būti pasirašyti elektroniniu būdu

4.8.4 Pranešimas užsakovui apie naujo sertifikato išdavimą

SSC GDL CA praneša *Užsakovui* apie pakeisto sertifikato išdavimą tokiu būdu, kuris atitinka taikomų Taisyklių reikalavimus.

4.8.5 Pakeisto sertifikato priėmimą patvirtinantis elgesys

Pakeistas sertifikatas laikomas priimtu, kai *Užsakovas* raštiškai patvirtina pristatymo faktą arba kai *Užsakovas* per 15 dienų po pakeitimo panaudoja sertifikatą.

4.8.6 Pakeisto sertifikato skelbimas

Remiantis *Užsakovo* sutikimu, pakeistas sertifikatas yra skelbiamas SSC GDL CA Talpykloje.

4.8.7 Pranešimas kitiems asmenims apie sertifikato išdavimą

Jei kiti subjektai buvo susiję su sertifikato išdavimo procesu, jie taip pat gali būti informuoti apie sertifikato pakeitimą.

4.9 Sertifikato atšaukimas ir sustabdymas

SSC GDL CA užtikrina, kad sertifikatai būtų atšaukiami laiku, remiantis leistinu ir patikrintu sertifikato atšaukimo prašymu. SSC GDL CA atšaukimo procedūros yra dokumentuotos.

Maksimalus laikotarpis nuo prašymo atšaukti sertifikatą gavimo ir sertifikatų atšaukimo statuso atnaujinimo yra 48 valandos[41].

Prašymai ir pranešimai, susiję su sertifikatų atšaukimu[42], yra tvarkomi juos gavus,

41 QCP, QCP+, EVCP ir EVCP+ - 24 valandos.
42 Pvz. dėl *Subjekto* privataus rakto kompromitacijos, *Subjekto* mirties, netikėtos sutarties arba veiklos nutraukimo, sutarties sąlygų pažeidimo.

patvirtinus juos ir patikrinus, kad jie gauti iš įgalioto šaltinio. Gauti prašymai ir pranešimai patvirtinami kaip tai reikalauja SSC GDL CA procedūros.

Sertifikato *Subjektas*, o kur taikoma ir *Užsakovas,* po sertifikato atšaukimo, yra informuojamas apie sertifikato būsenos pasikeitimą. Atšauktas sertifikatas nebus niekada atkurtas.

Sertifikatų atšaukimo būsenos informacija yra tarptautiniu mastu viešai prieinama 24 valandos per parą, 7 dienas per savaitę. Esant sistemos gedimui dėl teikiamų paslaugų ar kitų veiksnių įtakos, kurių SSC GDL CA negali kontroliuoti, SSC GDL CA imasi visų priemonių siekiant užtikrinti, kad ši atšauktų sertifikatų tikrinimo paslauga būtų pasiekiama per ne ilgiau kaip 72 valandas.

SSC GDL CA palaiko CRL, OCSP ir bet kokie sertifikatų statuso pasikeitimai po atšaukimo atsispindi abejuose metoduose. CA užtikrina pakankamus išteklius, kad gaunamos užklausos dėl bet kurio sertifikato būsenos būtų apdorojamos komerciškai prasmingu greičiu.

Sertifikato būsenos informacijos vientisumas ir autentiškumas yra apsaugotas. Sertifikato būsenos informacija yra prieinama tol, kol sertifikato galiojimas pasibaigia.

Prašymas atšaukti sertifikatą gali būti patvirtintas, jei yra pasirašytas patikrinamu elektroniniu parašu arba pasirašytas raštiškai. Sertifikatas gali būti atšaukiamas sertifikato *Subjekto, Užsakovo* arba įgalioto asmens prašymu.

4.9.1 Atšaukimo aplinkybės

SSC GDL CA atšaukia sertifikatą:

a) remiantis sertifikato *Subjekto* ar *Užsakovo* prašymu;

b) kai prarandama privataus rakto kontrolė;

c) kai sertifikato gavimui buvo pateikti klaidingi duomenys;

d) laikantis apribojimų, nurodytų sertifikate;

e) kai sertifikato *Subjektas* tampa neveiksnus arba miršta;

f) kai sertifikato *Subjektas* pažeidė sutartį ar kitus taikomus teisės nuostatus;

g) kitais atvejais, atitinkančiais reglamentuojančius teisės aktus.

Užsakovams, naudojantiems SSCD laikmenas, atšaukimas yra neprivalomas, jei laikomasi visų šių sąlygų:

- atšaukimo priežastis nėra "*rakto kompromitavimas*";
- susijęs privatus raktas negali būti eksportuojamas;
- laikmena buvo grąžinta CA, buvo inicializuota, suformatuota ar sunaikinta iškart po pristatymo;
- laikmena buvo apsaugota nuo neteisėto naudojimo per laikotarpį tarp perdavimo ir inicializavimo, formatavimo ir sunaikinimo.
- visais kitais atvejais sertifikatų atšaukimas yra privalomas. Net ir jei visos aukščiau minėtos sąlygos yra įvykdytos, tokių sertifikatų atšaukimas yra rekomenduojamas.

h) *Užsakovas* nurodo, kad originalus EVCP ir/arba EVCP+ sertifikato prašymas nebuvo įgaliotas ir vis dar nėra įgaliojimų pateikti prašymą;

i) CA gauna pagrįstų įrodymų, kad EVCP ir/arba EVCP+ sertifikatas naudojamas netinkamai;

j) CA gauna pranešimą arba kitaip sužino, kad teismas arba arbitražas panaikino *Užsakovo* teisę naudoti domeno vardą, kuris buvo nurodytas EVCP ir/arba EVCP+ sertifikate, arba kad *Užsakovui* nepavyko laiku atnaujinti savo domeno vardo;

k) CA gauna pranešimą arba kitaip sužino apie esminės informacijos pasikeitimą, nurodytą EVCP ir/arba EVCP+ sertifikate ;

l) CA, savo nuožiūra nustačius, kad EVCP ir/arba EVCP+ sertifikatas buvo išduotas nesilaikant sąlygų, nurodytų [CABF-EV];

m) CA nustačius, kad bet kokia informacija nurodyta EVCP ir/arba EVCP+ sertifikatuose, yra netiksli;

n) CA dėl bet kokios priežasties nutraukus veiklą ir nesant susitarimui su kita CA teikti atšaukimo paslaugos EVCP ir/arba EVCP+ sertifikatams;

o) CA teisė išduoti EVCP ir/arba EVCP+ sertifikatus pasibaigė arba buvo atšaukta ar nutraukta, nebent CA susitaria ir toliau teikti CRL/OCSP paslaugas;

p) Įtarus, kad CA šakninio sertifikato privatus raktas, kuris buvo naudojamas EVCP ir/ar EVCP+ sertifikatų išdavimui, buvo kompromituotas;

q) CA gauna pranešimą arba kitaip sužino, kad *Užsakovas* yra nurodomas kaip nepageidaujama šalis arba įtrauktas į juoduosius sąrašus, arba pagal CA jurisdikcijos įstatymus veikia draudžiamoje vietoje;

r) Atšaukimo prašo *Taikomosios programinės įrangos teikėjas*;

s) Sertifikatas buvo naudojamas pasirašyti arba platinti kenksmingą kompiuterinę programą, kuri buvo įkelta be naudotojo sutikimo.

4.9.2 Kas gali prašyti atšaukti sertifikatą

Tai apima:

- sertifikato *Subjektą arba Užsakovą*;
- išdavusią CA;
- įgaliotą organizaciją arba teisėsaugos pareigūnus.

Atšaukimo prašymai nedelsiant yra perduodami SSC GDL CA arba RA, įtarus ar nustačius rakto kompromitavimo atvejį arba bet kokį kitą įvykį, reikalaujantį atšaukimo.

4.9.3 Atšaukimo apdorojimo procedūra

Atšaukimo prašyme TURI būti nurodyti sertifikato *Subjektas* ir atšaukimo priežastys.

SSC GDL CA reikalauja pareiškėjo autentifikacijos arba patvirtinimo dėl atšaukimo kitais būdais (pvz. telefonu, faksu, el. paštu, asmeniškai atvykus). Po prašymo patvirtinimo visada seka sertifikato atšaukimas.

Trečiųjų šalių pateiktus atšaukimo prašymus SSC GDL RA išnagrinėja per 24 valandas po jų gavimo ir priima sprendimą remiantis: pareiškėjo autentifikacija, atšaukimo priežasties pobūdžiu ir atitinkamais teisės aktais. RA patvirtinus atšaukimo prašymus, po to visada seka sertifikato atšaukimas.

4.9.4 Atšaukimo uždelsimas

Sąlygų nėra.

4.9.5 Laikas per kurį atšaukimą privaloma apdoroti sertifikavimo tarnyboje

Sertifikatų atšaukimo prašymai gauti likus dviem valandoms iki CRL generavimo yra apdorojami iki kito CRL publikavimo.

4.9.6 Reikalavimas pasitikinčioms šalims tikrinti atšaukimą

Pasitikinčios šalys pačios priima sprendimą dėl sertifikatų atšaukimo tikrinimo, remiantis rizikos įvertinimu, atsakomybe ir įvertinus atšauktų sertifikatų naudojimo pasekmes.

4.9.7 CRL išdavimo dažnumas

CRL yra skelbiamas ne vėliau nei iki kito suplanuoto paskelbimo. CA sudaro CRL bent kartą per savaitę ir CRL lauko *nextUpdate reikšmė* negali būti ilgesnė nei 168 valandos nuo CRL sugeneravimo.

4.9.8 Maksimalus CRL uždelsimas

CRL yra skelbiamas iš karto kai tik sugeneruojamas bet ne vėliau nei 2 valandos po generavimo. CRL yra generuojamas ne vėliau nei nurodytas einamojo CRL lauke *nextUpdate*.

4.9.9 Galimybė tikrinti atšaukimą/būseną On-line būdu

Visų SSC GDL CA išduotų sertifikatų būsenos patikrinimas yra prieinamas per CRL.

Sertifikatų būsenos patikrinimas On-line būdu yra galimas sertifikatams išduotiems pagal QCP, QCP+, EVCP ir EVCP+ Taisykles.

4.9.10 Reikalavimai tikrinti atšaukimą/būseną On-line būdu

Prieš pasitikint bet kokiu SSC GDL CA išduotu sertifikatu, pasitikinčios šalys PRIVALO patikrinti sertifikatų galiojimą.

4.9.11 Kitos atšaukimo skelbimo formos

Sąlygų nėra.

4.9.12 Specialūs reikalavimai rakto kompromitavimo atveju

SSC GDL CA naudos tinkamus būdus siekiant informuoti *Užsakovus* ir *Pasitikinčias šalis* apie bet kokį SSC GDL CA privataus rakto sukompromitavimą. SSC GDL CA sprendimas bus priimtas remiantis tvirtais įrodymais dėl privataus rakto sukompromitavimo arba remiantis didele tikimybe dėl tokio pažeidžiamumo.

4.9.13 Aplinkybės galiojimo sustabdymui

Sąlygų nėra.

4.9.14 Kas gali prašyti sustabdyti galiojimą

Sąlygų nėra.

4.9.15 Sustabdymo prašymo procedūra

Sąlygų nėra.

4.9.16 Sustabdymo periodo ribos

Sąlygų nėra.

4.10 Sertifikato būsenos tikrinimo paslaugos

SSC GDL CA teikia sertifikatų statuso tikrinimo paslaugą naudojant CRL arba OCSP. OCSP paslauga galima sertifikatų tipams nurodytiems šių CPS skyriuje “Galimybė tikrinti atšaukimą/būseną On-line būdu“, 4.9.9

4.10.1 Veikimo principas

CRL ir OCSP paslaugų buvimą ir adresus nurodo sertifikato plėtiniai *CRL DP* ir *AIA*.

4.10.2 Paslaugos prieinamumas

SSC GDL CA CRL ir OCSP paslaugos yra prieinamos tarptautiniu mastu 24 x 7 režimu.

4.10.3 Pasirinktinos galimybės

Sąlygų nėra.

4.11 Paslaugos teikimo pabaiga

SSC GDL CA *Užsakovai* gali nutraukti paslaugų naudojimą pagal atitinkamas paslaugų teikimo Sutarties sąlygas, kaip nurodyta 9 skyriuje.

4.12 Raktų atsarginis saugojimas ir atstatymas

Sąlygų nėra.

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

5.1 Fizinė kontrolė

Siekiant kontroliuoti prieigą prie SSC GDL sertifikavimo tarnybos techninės ir programinės įrangos yra įgyvendintos fizinės saugumo priemonės.

Fizinė prieiga prie SSC GDL sertifikavimo tarnybos personalo kompiuterių leidžiama tik darbuotojams, turintiems tam priskirtus vaidmenis. Prieigos kontrolė vykdoma laikant SSC GDL sertifikavimo tarnybos kompiuterius ir su jais susijusią įrangą rakinamose patalpose, prie kurių prieigą turi tik personalas.

Asmenys, patenkantys į sertifikatų generavimo, sertifikatų laikmenos paruošimo ir atšaukimo patalpas, negali būti paliekami patalpoje be priežiūros ar be įgalioto asmens palydos.

SSC GDL CA sertifikavimo tarnybos patalpų saugumas reguliariai tikrinamas. Saugumo patikra apima vaizdinį kriptografinių laikmenų patikrinimą, jei įrenginiai nenaudojami, ar saugiai uždarytos durys ir užrakintos spynos, ir ar nebūta įsilaužimo žymių.

SSC GDL sertifikavimo tarnybos patalpose rezervinės kopijos ir kitos laikmenos saugomos tokiu būdu siekiant išvengti praradimo, sugadinimo arba saugojamos informacijos neteisėto naudojimo. Atsarginės kopijos saugojamos duomenų atstatymo ir archyvavimo tikslais. Bent viena atsarginė kopija saugoma kitoje patalpoje, skirtingoje nuo pagrindinės, bet turinčioje tokį patį saugumo lygmenį, kad įvykus avarijai pagrindinėje patalpoje, duomenis būtų galima atstatyti iš šios kopijos. Atsarginės kopijos laikmena saugojama nuo neleistinos prieigos taip kaip ir pagrindinė.

Jautrūs duomenys saugomi tokiu būdu siekiant išvengti jų atskleidimo neįgaliotiems asmenims (pvz: ištrinti failai).

Registravimo tarnybai privaloma fizinio saugumo priemonė yra rakinamos spintos ar kitos panašios priemonės, tinkančios registravimo metu surinktų dokumentų saugojimui.

5.1.1 Patalpų vieta ir statyba

SSC GDL sertifikavimo tarnybos patalpos yra trijose skirtingose vietose atskiriant jos sertifikavimo tarnybos sistemos branduolį, sertifikavimo bei registravimo tarnybas, kas leidžia užtikrinti patikimą apsaugą nuo nesankcionuotos prieigos prie bendros PKI infrastruktūros, kadangi visi trys elementai veikia nepriklausomai.

5.1.2 Fizinė prieiga

Sertifikavimo tarnybos įrangos fizinės prieigos kontrolė ir nuolatinis stebėjimas užtikrina, kad prie įrangos nebus patekta neteisėtais būdais. Prieiga prie kritinių sertifikavimo tarnybos komponenčių, įskaitant kriptografinį modulį, reikalauja bent dviejų žmonių dalyvavimo. Aktyvavimo duomenys saugomi atskirai nuo kriptografinio modulio. SSC GDL sertifikavimo tarnybos darbo vietos saugumo patikrinimas įtraukia durų bei ventiliavimo angų patikrinimą, bei tinkamą funkcionavimą, aplinkos patikrą nuo nesankcionuotos prieigos.

Registravimo tarnybos fizinės prieigos kontrolė sumažina įrangos sugadinimo riziką.

5.1.3 Elektra ir oro kondicionavimas

SSC GDL sertifikavimo tarnyba palaiko tinkamą elektros energijos aprūpinimo bei oro kondicionavimo infrastruktūrą, užtikrinančią sertifikavimo tarnybos paslaugų stabilumą.

5.1.4 Vandentiekio gedimai

SSC GDL sertifikavimo tarnyba užtikrina, jog sertifikavimo tarnybos paslaugos yra apsaugotos nuo galimo vandentiekio avarijos poveikio.

5.1.5 Gaisro prevencija ir saugumas

SSC GDL sertifikavimo tarnyba užtikrina, jog sertifikavimo tarnybos paslaugos yra apsaugotos patikimomis priešgaisrinės apsaugos ir gaisro prevencijos priemonėmis.

5.1.6 Laikmenų saugojimas

SSC GDL sertifikavimo tarnyba saugo savo duomenų laikmenas siekdama apsaugoti jas nuo atsitiktinio sugadinimo ar neleistinos prieigos. Atsarginės kopijos daromos pagal nustatytus grafikus ir yra saugomos vietoje, atskiroje nuo pagrindinio pastato. Duomenų apsaugos procedūros apsaugo laikmenas nuo jų senėjimo ir būklės blogėjimo.

5.1.7 Atliekų šalinimas

SSC GDL sertifikavimo tarnyba užtikrina, jog duomenų saugojimo laikmenos prieš jas pašalinant būtų sunaikinamos.

5.1.8 Rezervinė kopija saugojama išorėje

Duomenų ir sistemos atsarginės kopijos daromos ir saugomos kartą per savaitę.

5.2 Procedūrų kontrolė

5.2.1 Patikimi vaidmenys

Patikimu laikomas tas vaidmuo, kuris gali kelti saugumo problemą. Šios funkcijos sudaro visą PKI saugumo pagrindą. Siekiant užtikrinti, kad vaidmenys būtų vykdomi patikimu būdu, buvo imtasi dviejų būdų: patikimą vaidmenį atliekantis asmuo yra tinkamai apmokytas ir yra patikimas; vaidmenys yra paskirstomi tarp keleto asmenų, tad norint atlikti kenkėjišką veiklą reikėtų kelių asmenų susitarimo. Pirminiai SSC GDL sertifikavimo bei registravimo tarnybų vaidmenys apima:

1. Informacinės Sistemos Saugos vadovas – atsakingas už Saugos Taisyklių vykdymą.
2. Administratoriai – yra įgalioti įdiegti, sukonfigūruoti bei prižiūrėti SSC GDL sertifikavimo tarnybos sistemas.
3. Sertifikavimo tarnybos operatoriai – atsakingi už kasdieninę SSC GDL sertifikavimo tarnybos veiklą.

4. Registravimo tarnybos operatoriai – atsakingi už sertifikatų duomenų tikrinimą ir tvirtinimą, sertifikatų generavimą, atšaukimą ar sustabdymą.
5. Sistemos Auditorius – įgaliotas peržiūrėti SSC GDL sertifikavimo tarnybos audito žurnalus.

Personalas paskiriamas vykdyti patikimą vaidmenį tik atlikus būtiną biografijos patikrą.

5.2.2 Būtinas personalo skaičius per užduotį

Bent du asmenys dalyvauja ir yra informuoti, kai yra atliekamos šios operacijos:

- Atjungiant Operacinės Sistemos apsaugą – netikėto sistemos gedimo atveju;
- Kopijuojant/keičiant kietuosius diskus ar sistemos laikmenas;
- Atstatant sistemą iš atsarginės kopijos;
- Šakninės ar išduodančios sertifikavimo tarnybos raktų poros generavime, atšaukime, atsarginės kopijos gamyboje ar atstatyme.

Administratoriai neišduoda sertifikatų.

Šakninių sertifikavimo tarnybos sertifikatų išdavimas yra operacija, kurią atlieka keli įgalioti asmenys ir kurių vaidmenys apibrėžti raktų generavimo ceremonijos dokumentacijoje.

Dalyvaujantys asmenys yra apmokyti IT, PKI bei saugumo reikalavimų ir išmano operacijas, kurias atlieka ar paliudija.

5.2.3 Identifikavimas ir autentifikavimas kiekvienam vaidmeniui

Vykdomas remiantis įprastiems jautriems vaidmenims taikoma praktika.

5.2.4 Vaidmenys, reikalaujantys pareigybių atskyrimo

SSC GDL sertifikavimo tarnyba palaiko šiuos atskirtus vaidmenis:

- Sertifikavimo tarnybos administratorius;
- Sistemos administratorius;
- Informacinės sistemos saugos vadovas.

Registravimo tarnybai nėra numatyta vaidmenų išskyrimo.

Asmuo, pašalinantis SSC GDL sertifikavimo tarnybos audito žurnalus, nepriklauso asmenų grupei, vykdančiai operacijas su SSC GDL sertifikavimo tarnybos kriptografiniais raktais.

5.3 Personalo valdymas

SSC GDL sertifikavimo tarnyboje dirba personalas[43], turintis žinias[44], patirtį ir kvalifikaciją, reikalingą darbo funkcijų atlikimui. Atitinkamos sankcijos taikomos darbuotojams, pažeidusiems sertifikavimo tarnybos taisykles ar procedūras.

Patikimi vaidmenys, nuo kurių priklauso SSC GDL sertifikavimo tarnybos saugumas, yra aiškiai identifikuoti.

Sertifikavimo tarnybos darbuotojai turi pareigybines instrukcijas, kuriose apibrėžtas kiekvieno vaidmens jautrumas, remiantis vykdomų funkcijų, biografijos patikros, mokymo ir jautrios informacijos valdymo aspektais.

Visi sertifikavimo tarnybos darbuotojai priklausantys patikimiems vaidmenims yra laisvi nuo interesų konflikto.

SSC GDL sertifikavimo tarnyba užtikrina, kad asmenys, vykdantys registravimo tarnybos funkcijas, yra apmokyti naudotis darbine programine įranga ir registravimo taisyklėmis bei nuostatais.

5.3.1 Kvalifikacija, patirtis ir leidimo reikalavimai

43 CA personalas apima darbuotojus, dirbančius pagal sutartį ir vykdančius su CA susijusias paslaugų teikimo funkcijas. Personalas, vykdantis CA paslaugų stebėjimo funkcijas CA personalu nelaikomas.

44 CA personalas turi atitikti reikalavimą turėti "*eksperto lygio žinias, patirtį ir kvalifikaciją*" per mokymus, faktišką patirtį arba jų kombinaciją. Į tai įeina reguliarūs kursai, nerečiau 12 mėn., apie naujas saugos grėsmes ir galiojančias saugos Taisykles.

Asmenys, priklausantys patikimiems vaidmenims, pasirenkami remiantis jų lojalumu, patikimumu bei sąžiningumu ir privalo būti Europos Sąjungos šalių piliečiai.

5.3.2 Biografijos tikrinimo procedūros

SSC GDL sertifikavimo tarnyba užtikrina, kad patikimą vaidmenį atlikti atrinkto asmens biografija yra patikrinta. Kiekvieno atrinkto kandidato asmenybė yra patikrinama įgalioto sertifikavimo tarnybos darbuotojo, tam panaudojant valstybinius asmens tapatybės dokumentus (pasas ar asmens tapatybės kortelė).

Tapatybės patikrinimas apima: darbo istoriją, išsilavinimą, rekomendacijas, socialinio draudimo numerio patikrinimą, gyvenamųjų vietų bei galimos kriminalinės praeities patikrą. Patikrinimas apima paskutiniųjų penkerių metų laikotarpį. SSC GDL sertifikavimo tarnyba neskiria patikimam vaidmeniui asmens, turinčio kriminalinių ar kitų nusižengimų. Kandidatas yra prašomas pateikti informaciją apie nusižengimus (teistumą). Kandidatui atsisakius pateikti šią informaciją, jo kandidatūra toliau nėra svarstoma.

5.3.3 Mokymo reikalavimai

Sertifikavimo, registravimo ir laiko žymos tarnybų personalas yra apmokomas šiose srityse:

- sertifikavimo ir registravimo tarnybų saugumo procedūros ir principai;
- autentifikavimo ir tapatybės tikrinimo taisyklės ir procedūros;
- sertifikavimo ir registravimo tarnybų programinė įranga;
- nelaimių likvidavimas ir veiklos tęstinumo procedūros;
- potencialios grėsmės tapatybės tikrinimo procese;
- kitos taikytinos rekomendacijos ir gairės.

Mokymo periodas turėtų trukti bent tris mėnesius ir būti vykdomas vyresniųjų sertifikavimo ar/ir registravimo tarnybos darbuotojų. SSC GDL sertifikavimo tarnyba registruoja mokymus ir nurodo, kokio lygio mokymas buvo baigtas.

Registravimo tarnybos darbuotojai, atliekantys tapatybės tikrinimą, prieš paskyrimą, TURI turėti žinių ir įgūdžių, įgalinančių atlikti šias funkcijas[45].

5.3.4 Mokymų dažnumas ir reikalavimai

Numatant esminius SSC GDL sertifikavimo ar registravimo tarnybų veiklos pokyčius, turi būti užtikrintas personalo supažindinimo planas.

5.3.5 Darbuotojų rotacijos dažnumas ir eiliškumas

SSC GDL sertifikavimo tarnyba užtikrina, kad pokyčiai jos personalo sudėtyje neturės jokios įtakos sertifikavimo paslaugų teikimui.

5.3.6 Sankcijos už neleistinus veiksmus

Asmenis, pažeidusius reikalavimus, taisykles ar procedūras, SSC GDL sertifikavimo tarnyba patraukia administracinėn atsakomybėn.

5.3.7 Reikalavimai dirbantiems pagal sutartį

SSC GDL sertifikavimo tarnybos taisyklės bei reikalavimai vienodai taikoma visiems dirbantiems pagal sutartį.

5.3.8 Dokumentacija personalui

SSC GDL sertifikavimo tarnybos dokumentacija skirta personalui apima:

45 Po vidinio žynių apie tapatybės patikrinimo principus pagal [CABF-BR] ir [CABF-EV] patikrinimo.

- SSC GDL CA Sertifikavimo taisykles, SSC GDL CA Sertifikavimo veiklos nuostatus, SSC GDL CA Sutartis su pasitikinčiomis šalimis, SSC GDL CA Privatumo taisykles, SSC GDL CA viešai skelbtiną informaciją;

- Atitinkamą techninę ir eksploatacinę dokumentaciją, skirtą palaikyti atitinkamas personalo pareigas bei funkcijas;

- Įrašus apie praeitus mokymus ir personalo žinių įvertinimo rezultatus.

5.4 Audito žurnalo procedūros

Visos aplikacijos, palaikančios SSC GDL sertifikavimo tarnybos darbą, pildo audito žurnalą. Audito žurnaluose sieja kiekvieno sertifikato gyvavimo ciklo įvykius su konkrečiu darbuotoju.

5.4.1 Registruojamų įvykių tipai

Kiekvienas audito įrašas apima šią informaciją: įvykio tipą, jo datą ir laiką, ar sertifikatas sėkmingai/nesėkmingai išduotas arba atšauktas, darbuotojo, vykdančio atitinkamą vaidmenį, duomenis.

Bet kokio šaltinio kreipimasis į SSC GDL sertifikavimo tarnybą yra laikomas stebimu įvykiu. Jam priskirtas audito įrašas privalo savyje talpinti įvykio datą, laiką, šaltinį, gavimo vietą bei turinį.

5.4.2 Žurnalo apdorojimo dažnumas

Audito žurnalai automatiškai apdorojami ir periodiškai peržiūrimi siekiant atmesti bet kokią įtartiną veiklą bei po kiekvienos svarbios operacijos.

5.4.3 Audito žurnalų saugojimo periodas

Audito žurnalai privalo būti saugomi ne trumpiau nei septynis metus.

5.4.4 Audito žurnalų apsauga

Sertifikavimo tarnybos sistemos konfigūracija ir procedūros užtikrina, kad tik įgalioti asmenys archyvuoja ir naikina audito žurnalus. Procedūros įgyvendintos taip, jog apsaugotų duomenis, kuriems nesuėjo senaties laikas, nuo ištrynimo ar sunaikinimo.

5.4.5 Audito žurnalo rezervinio kopijavimo procedūros

Kintančios informacijos atsarginės kopijos daromos kasdien. Pilna atsarginė kopija daroma kas savaitę.

5.4.6 Audito žurnalų surinkimo sistema (vidinė ir išorinė)

Audito žurnalų surinkimo sistema yra sistemos vidinis procesas. Automatiniai audito procesai paleidžiami sistemos ar aplikacijos starto metu.

5.4.7 Įvykį sukėlusio asmens informavimas

Sąlygų nėra.

5.4.8 Pažeidžiamumo kontrolė

SSC GDL sertifikavimo tarnyba reguliariai atlieka saugumo kontrolę pagal nustatytas vidaus procedūras.

5.5 Archyvas

5.5.1 Archyvo sudėtis

Archyvo įrašai yra išsamūs siekiant patvirtinti tinkamą SSC GDL sertifikavimo tarnybos veikimą ir kiekvieno išduoto sertifikato tikrumą. Archyve kaupiami šie duomenys: Sertifikavimo tarnybos akreditacijos, CP, CPS, sutarčių šablonai, Sistemų/įrenginių/aplikacijų konfigūracijos, sistemos ar konfigūracijos pokyčiai bei atnaujinimai, įrašai apie *Subjektų* raktų generavimus, sertifikato užklausas (CSR), visus pasirašytus sertifikatus, atšaukimo užklausas, gautus ir

patvirtintus sertifikatus, Sutartis su klientais, laikmenos gavimo patvirtinimus, paskelbtus CRL, informaciją apie audito parametrų pokyčius (dažnis, stebimų įvykių tipas), mėginimus ištrinti ar modifikuoti audito žurnalus, sertifikavimo tarnybos ar klientų raktų generavimas, privačių raktų eksportavimas, sertifikatų statuso keitimo patvirtinimai ar atsisakymai, vaidmenų skyrimas patikimam asmeniui, kriptografinių modulių sunaikinimas, visi pranešimai apie sertifikatų kompromitaciją, SP, CP, CPS pažeidimus.

5.5.2 Archyvo saugojimo periodas

Archyvo saugojimo periodas 10 metų.

5.5.3 Archyvo apsauga

Archyvo duomenų apsauga užtikrinama naudojant el. parašo ir laiko žymų technologijas.

5.5.4 Archyvo rezervinės kopijavimo procedūros

Sąlygų nėra.

5.5.5 Reikalavimai dėl laiko žymėjimo

Sąlygų nėra.

5.5.6 Archyvo surinkimo sistema (vidinė ir išorinė)

Sąlygų nėra.

5.5.7 Archyvinės informacijos gavimo ir tikrinimo procedūros

Archyviniai duomenys periodiškai tikrinami siekiant įsitikinti duomenų pasiekiamumu ir vientisumu. Archyvo patikrinimas atliekamas automatiškai su patikimų darbuotojų priežiūra.

5.6 Raktų keitimas

Kiekviena šakninė ir išduodanti sertifikavimo tarnyba turi vieną pasirašymo raktą, kuriuo atlieka visus sertifikavimo tarnybos pasirašymo veiksmus. Sertifikavimo tarnyba negali išduoti sertifikatų, kurie galioja ilgiau nei jų pačių sertifikatai ar viešieji raktai, todėl jų turimų sertifikatų galiojimo laikas yra ilgesnis nei išduodamų naudotojams. Siekiant sumažinti sertifikavimo tarnybos sertifikato pasibaigimo pasekmes, raktai yra keičiami prieš pasibaigiant SSC GDL sertifikavimo tarnybos sertifikatui. Nuo to laiko sertifikavimo tarnybos pasirašymo tikslams naudojamas tik naujas raktas. Senas, bet dar galiojantis sertifikavimo tarnybos sertifikatas, yra prieinamas kol nenustoja galioti visi juo pasirašyti sertifikatai.

5.7 Kompromitacija ir veiklos tęstinumas

Sertifikavimo tarnybos kompromitacijos atveju, remiantis vidinėmis procedūromis SSC GDL sertifikavimo tarnybos sertifikatas yra atšaukiamas (jei įmanoma), SSC GDL sertifikavimo tarnyba iš naujo atkuria visą savo sistemą ir iš naujo pasirašo sertifikavimo tarnybos sertifikatą, tuomet iš naujo pasirašomi visi kryžminiai ir naudotojų sertifikatai.

Jei nelaimės atveju SSC GDL sertifikavimo tarnybos raktai sukompromituojami ar yra pagrįstas įtarimas jog taip galėjo nutikti nelaimės arba jos pasekmių šalinimo atveju, tokiu atveju SSC GDL sertifikavimo tarnyba turi atstatyti raktus tokiu būdu kaip buvo minėta anksčiau.

Informacija apie visus esamus ar numanomus sertifikavimo tarnybos vientisumo ar saugumo pažeidimus pranešama atitinkamoms institucijoms.

5.7.1 Procedūros incidentų ir kompromitacijų atveju

SSC GDL sertifikavimo tarnyba yra numačiusi kompetentingų priežiūros institucijų, kitų trečiųjų asmenų, kaip programinės įrangos ar sistemų teikėjų, kurie remiasi sertifikavimo tarnybos infrastruktūra, duomenų apsaugos priežiūros institucijų informavimo procedūra apie sistemos saugos pažeidimą arba jos integralumo praradimą, įtakojantį teikiamas paslaugas ir saugojamus asmens duomenis.

5.7.2 Kompiuterinių resursų, programinės įrangos ir/ar duomenų pažeidimai

Programinės įrangos pažeidimo ar duomenų praradimo atvejais SSC GDL sertifikavimo tarnyba veikia pagal savo veiklos atkūrimo planą.

5.7.3 Procedūros sertifikavimo tarnybos privataus rakto kompromitavimo atveju

Tokiu atveju, jei SSC GDL sertifikavimo tarnybos privatus raktas sukompromituotas (ar numanoma, kad taip įvyko), sertifikavimo tarnyba turi atlikti nustatytą tyrimą ir nuspręsti, ar raktas turėtų būti atšauktas. Jei nuspręsta raktą atšaukti, apie tai pranešama, esant susisiekimo galimybėms, visiems *Užsakovams* ir sugeneruojama nauja sertifikavimo tarnybos raktų pora arba naudojama kita SSC GDL sertifikavimo tarnyba, kuri gali generuoti sertifikatus *Užsakovams*.

5.7.4 Veiklos tęsimo galimybės po avarijos

SSC GDL sertifikavimo tarnyba turi veiklos atstatymo planą po avarijos, kurio pagalba tarnybos funkcijos atstatomos pagal nustatyta prioritetą. Aukščiausias prioritetas suteikiamas statuso tikrinimo ir SSC GDL sertifikavimo tarnybos Talpyklos atstatymui.

5.8 CA arba RA veiklos nutraukimas

SSC GDL sertifikavimo tarnybos veiklos nutraukimo atveju turi būti atšauktas sertifikavimo tarnybos sertifikatas ir apie nutraukimą visiems *Užsakovams*, *Subjektams*, Programinės įrangos teikėjams ir asmenims, turintiems kryžminiu būdu pasirašytus sertifikatus, turi būti pranešta elektroniniu paštu ir tarnybos tinklalapyje. Taip pat sertifikavimo tarnyba:

a) remiantis šiais CPS nustoja išdavinėti sertifikatus;

b) archyvuoja visus audito žurnalus ir kitus įrašus;

c) sunaikina visus susijusius privačius raktus;

d) teisės aktų nustatyta tvarka perduoda visus archyvuotus įrašus įgaliotiems asmenims;

e) praneša naudotojams, jog jie turi panaikinti EV CA (tarnybą, išduodančią EV SSL) ir pasirūpinti savo aplikacijomis.

Tuo atveju, jei įgaliota institucija neegzistuoja, SSC GDL sertifikavimo tarnyba:

a) tinkamai įforminant perduoda funkcijas ir visus atitinkamus duomenis patikimai trečiajai šaliai;

b) atšaukia visus sertifikatus ir publikuoja galutinius CRL tai dienai, kuri buvo nurodyta išplatintame pranešime;

c) sunaikina visus privačius raktus.

SSC GDL yra sudariusi draudimo sutartį padengti išlaidas, susijusias su šiais reikalavimais tuo atveju, jei bankrutuotų ar negalėtų padengti išlaidų.

6 TECHNINĖS SAUGOS PRIEMONĖS

6.1 Raktų poros generavimas ir įdiegimas

SSC GDL sertifikavimo tarnyba, išduodama sertifikatus remdamasi šiuo dokumentu, užtikrina, kad SSC GDL sertifikavimo tarnybos raktų generavimas būtų vykdomas fiziškai apsaugotoje patalpoje dalyvaujant patikimam personalui ir pagal patvirtintą sertifikavimo tarnybos raktų generavimo ceremoniją.

6.1.1 Raktų poros generavimas

SSC GDL sertifikavimo tarnyba užtikrina kad:

a) *Subjekto* raktai generuojami naudojant pramonėje pripažintus algoritmus;

b) *Subjekto* rakto ilgis ir naudojami viešojo rakto algoritmai atitinka pripažintus pramonėje[46];

c) *Subjekto* raktai generuojami ir saugiai saugomi, kol neperduodami *Subjektui*;

d) Privatus raktas naudotojui pateikiamas tokiu būdu, kad jo saugumas ir vientisumas nebūtų pažeisti;

e) Laikmenų paruošimą[47] kontroliuoja saugiai.

Kai su laikmena yra susiję aktyvavimo duomenys, pastarieji paruošiami ir pristatomi atskirai nuo parašo formavimo įrangos (laikmenos)[48].

6.1.2 Privataus rakto pristatymas užsakovui

SSC GDL sertifikavimo tarnybos pristatymo procedūra vykdoma tokiu būdu, jog galima būtų įsitikinti, kad teisinga laikmena ir aktyvavimo duomenys perduoti teisingam *Užsakovui*. SSC GDL sertifikavimo tarnyba atsako už laikmenos vietą ir būseną, kol jos neatsiima *Užsakovas*.

SSC GDL sertifikavimo tarnyba fiksuoja informaciją apie *Užsakovų* atsiimtas laikmenas.

46 Algoritmai ir parametrai pasirenkami pagal ETSI TS 102 176-1.
47 Taikoma QCP+ sertifikatams.
48 Atskyrimas gali būti pasiektas pristatant aktyvavimo duomenis ir SSCD skirtingu laiku arba skirtingais būdais.

6.1.3 Viešojo rakto pristatymas sertifikato tarnybai

Kai raktų poros yra sugeneruotos *Užsakovo* arba RA, viešasis raktas ir *Užsakovo* tapatybės duomenys privalo būti saugiai pristatyti SSC GDL sertifikavimo tarnybai sertifikato išdavimui. Pristatymo mechanizmas susieja *Užsakovo* tapatybę su jo viešuoju raktu. Kriptografija naudojama tokiam susiejimui yra tokia pat stipri kaip SSC GDL sertifikavimo tarnybos raktas naudojamas sertifikatams pasirašyti.

6.1.4 CA viešojo rakto pristatymas pasitikinčioms šalims

Kai sertifikavimo tarnyba atnaujina savo pasirašymą raktų pora, ji platinama saugiu būdu. Naujas viešasis raktas gali būti pristatytas sertifikate, pasirašyto kryžminiu metodu arba savarankiškai.

Savarankiškai pasirašyto sertifikato įdiegimas į laikmenas taikant saugius mechanizmus:

a) Sertifikatas įrašomas į laikmeną *Užsakovui* apsilankius RA arba remiantis 6.1.2 skyriumi;
b) Sertifikatas įrašomas į laikmeną, kai RA generuoja užsakovo raktų porą, kuri pristatoma *Užsakovui* remiantis 6.1.2 skyriumi;
c) Platinant sertifikatą per programinės įrangos tiekėjus[49] arba pasitikėjimo sąrašus.

6.1.5 Raktų ilgis

Pripažinti ir rekomenduojami kriptografiniai algoritmai ir raktų ilgiai užtikrina, kad pasirašyti sertifikatai patvirtins elektroninį parašą visą jo galiojimo laikotarpį.

6.1.6 Viešojo rakto parametrų generavimas ir kokybės tikrinimas

SSC GDL sertifikavimo tarnybos viešojo rakto parametrai nustatyti pagal ETSI, FIPS ir kitų patikimų šaltinių[50] informaciją.

49 Apima operacines sistemas, naršykles ir kitas populiarias aplikacijas.
50 ECRYPT II Yearly Report on Algorithms and Key sizes, Katholieke Universiteit Leuven, 2012

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

Galutinio naudotojo sertifikatuose, turinčiuose *sscAuthenticationPolicy* OID, nurodomas tik *digitalSignature bitas*. El. parašo sertifikatuose gali būti nurodytas arba *digitalSignature* arba *nonRepudiation*[51].

Išduodančių tarnybų sertifikatai naudojami tik *Subjektų* sertifikatų ir CRL pasirašymui ir juose nurodomas *keyCertSign* bitas. Sertifikatuose, skirtuose CRL parašo tikrinimui, nurodomas *cRLSign* bitas.

Sertifikatuose, skirtuose OCSP parašo tikrinimui, nurodomi *digitalSignature ir/*ar *nonRepudiation* bitai.

Įrangos sertifikatuose, skirtuose pasirašymui, nurodomas *digitalSignature* bitas. Įrangos sertifikatuose taip pat gali būti nurodytas *nonRepudiation* bitas.

6.2 Privataus rakto saugumas ir kriptografinio modulio techninės kontrolės priemonės

SSC GDL CA HSM sertifikuoti pagal FIPS 140-2 Level 3 arba/ir EAL 4 saugumo standartus.

HSM tvarkomi, saugomi ir tikrinami griežtai laikantis gamintojo dokumentacijos.

6.2.1 Kriptografinio modulio standartai ir valdymas

Sąlygų nėra.

6.2.2 Privataus rakto (n iš m) daugiasmens naudojimas

SSC GDL sertifikavimo tarnybos privačių raktų kriptografinės operacijos vykdomos pagal vidiniuose dokumentuose aprašytas kelių asmenų atliekamas procedūras, kurios reikalauja daugialaipsnės prieigos prie privačių raktų ir atitinkamoje darbo aplinkoje. SSC GDL sertifikavimo tarnybos raktų saugykla, šakniniai raktai ir pasirašymo raktų duomenys visada apsaugomi 3 iš 5 principų.

51 Taip pat vadinama *contentCommitment*.

6.2.3 Privataus rakto atsarginis saugojimas

SSC GDL sertifikavimo tarnyba neperduoda trečiajai šaliai atsarginiam saugojimui savo pasirašymo raktų ar *Užsakovų* privačių raktų.

6.2.4 Privataus rakto rezervinė kopija

SSC GDL sertifikavimo tarnybos privačių raktų atsarginės kopijos daromos laikantis tokios pat tvarkos kaip darant pagrindinius raktus ir saugomos atskirai. Atsarginės raktų kopijos saugomos pagal tą pačią tvarką kaip ir originalai.

6.2.5 Privataus rakto archyvavimas

SSC GDL sertifikavimo tarnyba nearchyvuoja privačių raktų duomenų.

6.2.6 Privataus rakto perkėlimas į arba iš kriptografinio modulio

Kai SSC GDL sertifikavimo tarnybos privatus pasirašymo raktas perkeliamas į išorinį parašo kūrimo įrenginį, jis saugomas tokiu pat lygiu kaip parašo kūrimo įrenginys:

a) SSC GDL sertifikavimo tarnybos privataus pasirašymo rakto atsarginių kopijų gamyba, saugojimas ir atstatymas vykdomas fiziškai saugioje aplinkoje dalyvaujant patikimam personalui.
b) SSC GDL sertifikavimo tarnybos privataus rakto atsarginėms kopijoms taikomas toks pat saugumo lygis kaip ir naudojamiems raktams.

6.2.7 Privataus rakto saugojimas kriptografiniame modulyje

SSC GDL sertifikavimo tarnybos privatūs raktai laikomi *FIPS 140-2 level 3* sertifikuotuose įrenginiuose.

6.2.8 Privataus rakto aktyvavimo metodas

Privačių raktų aktyvavimas grindžiamas HSM gamintojo metodika ir savarankiškai sukurta ir palaikoma kelių asmenų daugialaipsniu apsaugos mechanizmu.

6.2.9 Privataus rakto deaktyvavimo metodas

SSC GDL sertifikavimo tarnybos personalo privatūs raktai gali būti deaktyvuoti po kiekvienos procedūros, atsijungiant iš sistemos.

SSC GDL sertifikavimo tarnyba užtikrina, jog aktyvuotas HSM nepaliekamas be priežiūros ar kitaip nesudaroma galimybė nesankcionuotai prieigai. Tik iš anksto žinomi SSC GDL sertifikavimo tarnybos personalo veiksmai sukuria sąlygas privataus rakto pasirašymui. Privatūs raktai perkeliami į HSM tik tuomet, kai atitinkama sertifikavimo tarnyba vykdo operacijas.

6.2.10 Privataus rakto sunaikinimo metodas

Kai tai būtina, sertifikavimo tarnyba sunaikina privačius raktus pagal tvarką, užtikrinančią, kad neliks jokių duomenų, pagal kuriuos galima būtų atstatyti raktą. Kalbant apie kriptografinį modulį, sertifikavimo tarnyba naudoja "*zeroisation*" funkciją ir kitas atitinkamas priemones siekiant užtikrinti tinkamą sertifikavimo tarnybos rakto sunaikinimą.

6.2.11 Kriptografinio modulio rūšys

Žr. 6.2.7 .

6.3 Kiti raktų poros valdymo aspektai

6.3.1 Viešojo rakto archyvavimas

Sąlygų nėra.

6.3.2 Sertifikato ir raktų poros naudojimo periodai

Raktų poros naudojimo periodas yra toks pat kaip susieto su ja sertifikato galiojimo periodas, išskyrus tai, jog privatus raktas gali būti toliau naudojamas iššifravimui, o viešasis raktas - parašo patikrinimui.

Užsakovo privataus ir viešojo rakto naudojimo periodas sutampa.

6.4 Aktyvavimo duomenys

6.4.1 Aktyvavimo duomenų generavimas ir įdiegimas

Aktyvavimo duomenų generacija ir diegimas atliekamas laikantis SSC GDL sertifikavimo tarnybos raktų generavimo ceremonijos dokumentacijos. Aktyvavimo duomenys saugomi lustinėse kortelėse sugrupuotose į tris atskirus saugojimo paketus.

6.4.2 Aktyvavimo duomenų apsauga

Aktyvavimo duomenys ir laikmenos yra apsaugotos nuo atskleidimo kriptografinio ir fizinio prieinamumo kontrolės mechanizmų.

6.4.3 Kiti aktyvavimo duomenų aspektai

Faktiškas aktyvavimo duomenų panaudojimas įmanomas esant ne mažiau kaip dviejų iš trijų atskirai saugomų duomenų laikmenų.

6.5 Kompiuterinės saugos priemonės

SSC GDL sertifikavimo tarnyba, veikianti pagal šiuos CPS užtikrina, kad jos sistema prieinama tik įgaliotiems asmenims:

a) tinklo kontrolė apsaugo SSC GDL sertifikavimo tarnybos vidinį tinklą nuo neteisėtos prieigos apimant *Užsakovus* bei trečiuosius asmenis;

b) jautrūs duomenys yra apsaugoti nuo neautorizuotos prieigos, pakeitimo ir nėra keičiami per nesaugius tinklus;

c) sistemos saugumą palaiko veiksmingas naudotojų[52] administravimas, audito žurnalai ir

52 CA ir RA operatoriai, administratoriai ir auditoriai.

nuolatiniai nuotolinės prieigos pakeitimai;

d) prieiga prie informacijos ir taikomųjų programų funkcijų yra ribojama remiantis prieigos kontrolės tvarka;

e) SSC GDL sertifikavimo tarnyba palaiko pakankamas kompiuterinio saugumo priemones patikimų vaidmenų atskyrimui, įskaitant administracinių ir eksploatavimo funkcijų atskyrimą;

f) Sertifikavimo tarnybos personalas tinkamai identifikuojamas ir autentifikuojamas prieš naudojantis kritinėmis aplikacijomis;

g) Sertifikavimo tarnybos personalas atsako už savo veiksmus;

h) Sertifikato generavimas ir atšaukimas yra dokumentuotas procesas, kuris apsaugo nuo šališkų operacijų;

Sertifikato pridėjimo ir ištrynimo operacijos pristatymo ir atšaukimo valdymo aplikacijose kontroliuojamos per prieigos kontrolę.

6.5.1 Specifiniai kompiuterinės saugos techniniai reikalavimai

Toliau išvardinti kompiuterinio saugumo reikalavimai taikomi SSC GDL sertifikavimo tarnybos sistemai:

- kiekvienas naudotojas autentifikuojamas prieš prieinant prie SSC GDL sertifikavimo tarnybos sistemos ar aplikacijų;
- naudotojai turi privilegijas, atitinkančias jiems skirtas vykdyti funkcijas;
- visoms operacijoms generuojami ir saugomi audito žurnalai;
- kritiški saugos procesai vykdomi operacinėje aplinkoje su nustatytomis vientisumo ribomis;
- gedimo atveju palaikomas rakto ar sistemos atstatymas.

6.5.2 Kompiuterinės saugos lygiai

SSC GDL sertifikavimo tarnybos PKI sistema įvertinta kaip atitinkanti industrinius reikalavimus keliamus patikimoms sistemoms.

6.6 Techninės gyvavimo ciklo valdymo priemonės

6.6.1 Sistemos kūrimo priemonės

SSC GDL sertifikavimo tarnybos saugos reikalavimai sistemos kūrimui apima:

SSC GDL sertifikavimo tarnybos naudojama programinė įranga sukurta remiantis dokumentuota specifikacija;

Infrastruktūros, skirtos SSC GDL sertifikavimo tarnybos darbui ir sistemos vystymui, yra realiai atskirtos;

SSC GDL sertifikavimo tarnybos veikla palaiko kelias sertifikavimo tarnybas;

Buvo imtasi tinkamų priemonių siekiant užkirsti kelią kenksmingos programinės įrangos atakoms.

6.6.2 Saugos valdymo priemonės

SSC GDL sertifikavimo tarnybos sistemos konfigūracija yra dokumentuota. Naudojamas mechanizmas leidžia pastebėti neleistinus pakeitimus programinės įrangos konfigūracijoje. SSC GDL sertifikavimo tarnyba periodiškai tikrina programinės įrangos vientisumą.

6.6.3 Gyvavimo ciklo saugos priemonės

Sistemos ištekliai yra stebimi, todėl ateities pajėgumo poreikiai užtikrinami pagal turimą pakankamą duomenų apdorojimo galią ir saugojimo talpą.

6.7 Tinklo saugos priemonės

Prieiga prie SSC GDL sertifikavimo tarnybos sistemos apribojama ugniasiene, kuri apriboja sertifikavimo tarnybos atliekamas funkcijas. Sertifikavimo tarnybos įranga yra apsaugota nuo žinomų tinklo atakų. Visi nenaudojami prievadai ir paslaugos yra išjungtos. SSC GDL sertifikavimo tarnybos įrangoje yra tik įranga reikalinga tinkamam SSC GDL sertifikavimo tarnybos funkcionavimui.

6.8 Laiko žymėjimas

SSC GDL sertifikavimo tarnybos tvirtinimo laikas palaikomas vienos minutės tikslumu.

7 SERTIFIKATŲ, CRL IR OCSP PROFILIAI

7.1 Sertifikato profilis

Sertifikatų, išduotų pagal šiuos Nuostatus, profiliai atitinka [RFC5280] specifikaciją, papildomi reikalavimai gali būti taikomi priklausomai nuo sertifikato klasės ir taikomų *Taisyklių* OID nurodyto sertifikate.

Sertifikatų profiliai aprašyti atskiruose dokumentuose, turinčiuose žemiau pateiktus OID kodus:

Sertifikato klasė	Sertifikato tipas	Profilio OID
I klasė	Visi	1.**3.6.1.4.1.22501.9.1.3.0** **2.16.440.1.4.30003763.9.1.3.0**
II klasė	Visi	1.**3.6.1.4.1.22501.9.2.3.0** **2.16.440.1.4.30003763.9.2.3.0**
III klasė	Visi	1.**3.6.1.4.1.22501.9.3.3.0** **2.16.440.1.4.30003763.9.3.3.0**
IV klasė	Visi	1.**3.6.1.4.1.22501.9.4.1.0** **2.16.440.1.4.30003763.9.4.1.0**

Sertifikato profiliai pateikiami *Užsakovams*, *Subjektams* ir *Pasitikinčioms šalims* jų prašymu.

EVCP ir EVCP+ sertifikatų profiliai yra aprašyti II ir III klasės sertifikatų profilius aprašančiuose dokumentuose, nurodytuose aukščiau pateiktoje lentelėje.

7.1.1 Versijos numeris(-iai)

SSC GDL CA išduoti sertifikatai atitinka X.509 standarto 3 versiją.

7.1.2 Sertifikato plėtiniai

Žr. lentelę, pateiktą 7.1.p.

7.1.3 Algoritmų OID kodai

SSC GDL CA išduotuose sertifikatuose naudojami šie algoritmai:

Algoritmas	OID
sha-1WithRSAEncryption	1.2.840.113549.1.1.5
sha256WithRSAEncryption	1.2.840.113549.1.1.11
id-RSASSA-PSS	1.2.840.113549.1.1.10

7.1.4 Vardų formos

Žr. lentelę, pateiktą 7.1.p.

7.1.5 Vardų apribojimai

SSC GDL CA gali išduoti sertifikatus su vardų apribojimais.

7.1.6 Sertifikato taisyklių OID kodas

Žr. lentelę, pateiktą 7.1.p.

7.1.7 *Policy Constraints* plėtinio naudojimas

Sąlygų nėra.

7.1.8 *Policy* plėtinio parinkčių sintaksė ir semantika

Žr. lentelę, pateiktą 7.1.p.

7.1.9 Kritinio *Certificate Policies* plėtinio apdorojimo semantika

Žr. lentelę, pateiktą 7.1.p.

7.2 CRL profilis

CRL profilis išleistas atskirame dokumente su šiuo OID:

1.3.6.1.4.1.22501.9.5.2.0

2.16.440.1.4.30003763.9.5.2.0

CRL profiliai pateikiami *Užsakovams*, *Subjektams* ir *Pasitikinčioms šalims Talpykloje*:

http://gdl.repository.ssc.lt/CRLprofile

7.2.1 Versijos numeris(-iai)

SSC GDL CA CRL sąrašai atitinka [RFC5280] 2 versiją.

7.2.2 CRL ir CRL įrašų plėtiniai

Žr. lentelę, pateiktą 7.1.p.

7.3 OCSP profilis

Žr. lentelę, pateiktą 7.1.p.

7.3.1 Versijos numeris(-iai)

Žr. lentelę, pateiktą 7.1.p.

7.3.2 OCSP plėtiniai

Žr. lentelę, pateiktą 7.1.p.

8 ATITIKTIES AUDITAS IR KITI TIKRINIMAI

SSC GDL CA yra numačiusi atitikties audito mechanizmą, užtikrinantį šių Nuostatų reikalavimų įgyvendinimą ir laikymąsi.

8.1 Patikrinimų dažnumas ir aplinkybės

Sertifikavimo paslaugų atitiktį reikalavimams, nurodytiems standartuose [ETSITS101042], [ETSITS101456], ir [ETSITS102023] užtikrina kasmetinis nepriklausomas auditas.

8.2 Auditorius ir jo kvalifikacija

SSC GDL CA auditą atliko TÜV Informationstechnik GmbH (VFR), kuri yra akredituota "DAkkS Deutsche Akkreditierungsstelle GmbH" pagal DIN EN 45011. Auditas atliekamas remiantis:

"Zertifizierungsschema für Zertifikate des akkreditierten Bereichs der Zertifizierungsstelle der TÜV Informationstechnik GmbH", ver. 1.2, 2011-01-28, TÜV Informationstechnik GmbH.

8.3 Auditorių ir sertifikavimo tarnybos santykiai

SSC GDL CA išrinko Audito paslaugų teikėją visiškai nepriklausomą nuo sertifikavimo tarnybos atlikus tarptautiniu mastu priimtas pirkimo procedūras.

8.4 Audito apimtis

Auditas užtikrina, kad SSC GDL CA ir RA tarnybas vykdo veiklą, atitinkančią visus reikalavimus, nurodytus SSC GDL CP ir CPS einamosiose versijose. Auditas apima visus CA/RA veiklos aspektus, reikalaujančius nepriklausomo patikrinimo.

8.5 Veiksmai dėl audito metu nustatytų trūkumų

Jeigu audito metu nustatoma neatitiktis taikomoms teisės normoms, SSC GDL CA CP/CPS arba

bet kuriems kitiems įsipareigojimams, susijusiems su sertifikavimo tarnybos paslaugomis, SSC GDL CA TURI numatyti veiksmų planą, užtikrinantį pastabų šalinimą.

8.6 Audito rezultatai

Audito ataskaita turi būti pateikta SSC GDL CA *Taisyklių valdytojui* tam, kad būtų parengtas atitinkamų veiksmų planas.

9 KITI VEIKLOS IR TEISINIAI KLAUSIMAI

Pagal šiuos Nuostatus teikiamų paslaugų verslo ir teisiniai aspektai yra sugrupuoti į atskirus dokumentus, kaip tai pateikta žemiau esančioje lentelėje:

Paslaugų teikimo sutartis	Dokumento OID
Paslaugų teikimo sutartis su fiziniu asmeniu	1.3.6.1.4.1.22501.8.3.1.0 2.16.440.1.4.30003763.8.3.1.0
Paslaugų teikimo sutartis su įmone	1.3.6.1.4.1.22501.8.3.2.0 2.16.440.1.4.30003763.8.3.2.0
OCSP paslaugų teikimo sutartis	1.3.6.1.4.1.22501.8.3.3.0 2.16.440.1.4.30003763.8.3.3.0
Laiko žymos paslaugos teikimo sutartis	1.3.6.1.4.1.22501.8.3.4.0 2.16.440.1.4.30003763.8.3.4.0
Autentifikavimo paslaugos teikimo sutartis	1.3.6.1.4.1.22501.8.3.5.0 2.16.440.1.4.30003763.8.3.5.0
Pasitikinčių šalių sutartis	1.3.6.1.4.1.22501.8.3.7.0 2.16.440.1.4.30003763.8.3.7.0

9.1 Mokesčiai

9.1.1 Sertifikato išdavimo ir pratęsimo mokesčiai

Sertifikatų išdavimo, atstatymo, pratęsimo ir pakeitimo kainos yra skelbiamos SSC GDL CA tinklalapyje.

9.1.2 Priėjimo prie sertifikatų mokesčiai

SSC GDL CA pasilieka teisę nustatyti mokesčius už priėjimą prie sertifikatų domenų bazės.

9.1.3 Atšaukimo arba priėjimo prie būsenos informacijos mokesčiai

Iki dešimties OCSP užklausų per dieną apdorojama be atlygio. *Pasitikinčios šalys,* ketinančios siųsti daugiau užklausų per dieną, PRIVALO susisiekti su SSC GDL CA dėl komercinės OCSP

paslaugos sąlygų[53].

9.1.4 Mokesčiai už kitas paslaugas

SSC GDL CA pasilieka sau teisę imti mokesčius už bet kurias kitas teikiamas paslaugas.

9.1.5 Mokesčių grąžinimas

Pagal 9 sk. pateiktų paslaugų teikimo sutarčių sąlygas.

9.2 Finansinė atsakomybė

SSC GDL CA užtikrina pakankamus finansinius resursus, kad palaikytų savo veiklą ir vykdytų šiuose Nuostatuose numatytus įsipareigojimus.

9.2.1 Draudimo apimtis

SSC GDL CA turi veiklos draudimą, kaip to reikalauja Europos Sąjungos ir Lietuvos Respublikos teisės aktai.

9.2.2 Kitas turtinis padengimas

Sąlygų nėra.

9.2.3 Draudimo ir garantijos padengimas galutiniam naudotojui

SSC GDL CA atlygina tiesioginę žalą klientams už jos padarytas klaidas pagal savo atsakomybę.

53 Taikoma QCP ir QCP+.

9.3 Verslo informacijos konfidencialumas

Žr. 9 sk.

9.3.1 Konfidencialios informacijos apimtis

Visa pagal šiuos Nuostatus surinkta informacija apie *Subjektus*/*Užsakovus* laikoma konfidencialia ir negali būti atskleista trečiosioms šalims be *Užsakovų* ir *Subjektų* pritarimo, išskyrus atvejus, numatytus teisės aktuose.

Informacija apie SSC GDL CA PKI sistemos projektą, įskaitant visas CA/RA informacines sistemas, bendrą architektūrą ir veikimo principus, yra konfidenciali. Taip pat, žemiau išvardinta informacija nėra viešai prieinama:

- gauti prašymai;
- sertifikatų užklausos;
- privatūs raktai (jeigu tokių yra) ir bet kokie jų atstatymo duomenys;
- visi audito įrašai;
- *Force* majeure planai;
- veiklos tęstinumo planai;
- saugos priemonės kompiuterinės ir programinės įrangos valdymui;
- visi techniniai ir technologiniai sertifikavimo ir registravimo procesų aspektai;
- visi veiklos ir paslaugų teikimo rodikliai, išskyrus numatytus teisės aktuose.

9.3.2 Nekonfidenciali informacija

Visa informacija, įrašyta į sertifikatą, laikoma nekonfidencialia. Sertifikato būsenos tikrinimo paslaugos pateikiama informacija taip pat laikoma vieša.

9.3.3 Atsakomybė už konfidencialios informacijos apsaugą

Sąlygų nėra.

9.4 Asmens duomenų privatumas

SSC GDL CA yra duomenų valdytoja ir registruota asmens duomenų valdytojų valstybės registre, registracinis numeris: P-3069.

9.4.1 Privatumo politika

SSC GDL CA privatumo politika yra paskelbta viešai:

https://gdl.repository.ssc.lt/pp

9.4.2 Privati informacija

Informacija apie *Subjektą,* neįrašyta į sertifikatą ar CRL, laikoma privati.

9.4.3 Neprivati informacija

Bet kokia informacija apie asmenį ar organizaciją, įrašyta į sertifikatą, CRL, nėra laikoma privati.

9.4.4 Atsakomybė už privačios informacijos apsaugą

Tiek SSC GDL CA, tiek ir *Užsakovai* turi saugoti privačios informacijos konfidencialumą tokiu pačiu lygiu, kaip tai daroma nuosavos informacijos atžvilgiu.

9.4.5 Pranešimai ir sutikimai dėl privačios informacijos naudojimo

SSC GDL CA gali naudoti privačią informaciją *Subjektui* pritarus arba teisės aktų nustatyta tvarka.

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

Visa informacija šiuose Nuostatuose pateikta *SSC GDL CA* vardu ar asocijuota su *SSC GDL CA* vardu yra organizacijos, nurodytos 1.5.2 p., nuosavybė. Ši organizacija gali turėti neregistruotus prekybinius ar paslaugų ženklus, tačiau jie saugomi kaip intelektinė nuosavybė. Visi SSC GDL CA išduoti sertifikatai yra išskirtinė sertifikavimo tarnybos nuosavybė. *Užsakovams* ir *Pasitikinčioms* šalims leidžiama kopijuoti ar kitaip naudotis sertifikatais neišskirtinėmis sąlygomis. SSC GDL CA, kaip sertifikato leidėjas, pasilieka teisę bet kada savo nuožiūra atšaukti sertifikatą.

9.5.1 Sertifikatai ir CRL

Sąlygų nėra.

9.5.2 CP/CPS

Visos CP ir CPS autorių teisės yra saugomos.

9.5.3 Prekių ženklai

Sąlygų nėra.

9.5.4 Parašo formavimo duomenys

Visos Šakninių ir Išduodančių tarnybų raktų poros ir atitinkami sertifikatai yra SSC GDL CA nuosavybė.

9.6 Atstovavimas ir garantijos

SSC GDL CA išduotiems EVCP ir EVCP+ sertifikatams taikomos [CABF-EV] numatytos garantijos *Užsakovams*, *Subjektams*, *Taikomųjų programinių įrangų teikėjams* ir *Pasitikinčioms šalims*.

9.6.1 CA atstovavimas ir garantijos

Žr. 9 sk.

9.6.2 RA atstovavimas ir garantijos

Žr. 9 sk.

9.6.3 Užsakovo atstovavimas ir garantijos

Žr. 9 sk.

9.6.4 Pasitikinčios šalies atstovavimas ir garantijos

Atstovavimo ir garantijos sąlygos *Pasitikinčioms šalims* yra numatytos atitinkamoje sutartyje, kuri yra viešai prieinama SSC GDL CA Talpykloje.

9.6.5 Kitų dalyvių atstovavimas ir garantijos

Sąlygų nėra.

9.7 Garantijos atsižadėjimas

Žr. 9 sk. Be to, jokiais būdais SSC GDL CA negali būti laikoma atsakinga už bet kurį arba visus žemiau išvardintus atvejus:

- Atsitiktinė ar priežastinė netiesioginė žala;
- Duomenų ar pelno praradimas;
- Mirtis arba asmens sužalojimas;
- Atsakomybė už sertifikate nurodyto sandorio vertės apribojimo viršijimą;

- Atsakomybė už *Užsakovo* naudojamos kompiuterinės ar programinės įrangos pasekmes;
- Atsakomybė už privataus rakto kompromitacijos pasekmes.

9.8 Atsakomybės ribojimas

Žr. 9 sk.

9.9 Kompensacijos

Žr. 9 sk.

9.10 Sąlygų galiojimas ir nutraukimas

9.10.1 Galiojimas

Žr. 9 sk.

9.10.2 Nutraukimas

Žr. 9 sk.

9.10.3 Sąlygų nutraukimo ir išlikimo poveikis

Žr. 9 sk.

9.11 Individualūs pranešimai ir komunikavimas su dalyviais

Atskiri pranešimai ir informacija, susijusi su SSC GDL CA CPS, yra priimama per paslaugų kontaktinius taškus, nurodytus dokumente SSC GDL CA PDS.

9.12 Pakeitimai

9.12.1 Pakeitimo procedūra

Žr. 9 sk. Be to, keičiant CPS taip pat keičiasi dokumento versijos dalis – modifikacijos numeris. SSC GDL CA palaiko procedūras, užtikrinančias, kad šie Nuostatai negali būti pakeisti ir/ar paskelbti be tinkamo SSC GDL CA Taisyklių valdytojo pritarimo.

9.12.2 Pranešimo būdas ir periodas

Žr. 9 sk.

9.12.3 OID pakeitimo būtinybės aplinkybės

Bet kurio OID kodo, nurodyto 1.2 p., pakeitimai, reikalauja naujos CPS versijos paskelbimo.

9.13 Ginčių sprendimo sąlygos

Skundai ar raginimai turi būti tiesiogiai adresuoti SSC GDL CA. Sertifikavimo tarnyba, prieš taikant ginčo sprendimo mechanizmus, pasistengs išspręsti ginčą abipusiškai priimtinu būdu. Jeigu šalims pasiekti sutarimo nepavyko, ginčas turi būti sprendžiamas Lietuvos Respublikos teisme. Išsamesnė informacija – žr. 9 sk.

9.14 Taikomoji teisė

Žr. 9 sk.

9.15 Atitiktis taikomam įstatymui

Žr. 9 sk.

9.16 Įvairios sąlygos

9.16.1 Sutarties visuma

Žr. 9 sk.

9.16.2 Perleidimas

Žr. 9 sk.

9.16.3 Sutarties dalinis taikymas

Žr. 9 sk.

9.16.4 Prievolės (advokato mokesčiai ir išimties teisės)

Žr. 9 sk.

9.16.5 Force Majeure

Žr. 9 sk.

9.17 Kitos sąlygos

Sąlygų nėra.

10 NUORODOS

10.1 Normatyvinės nuorodos

Žemiau pateiktų dokumentų reikalavimai, jeigu yra taikytini konkretaus tipo sertifikatams, laikytini šių Nuostatų 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] Policy requirements for certification authorities issuing public key certificates (Normalized level only).

[ETSIEN319411-3] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates.

[ETSITS101456] ETSI TS 101 456 Policy, Requirements for Certification Authorities Issuing Qualified Certificates.

[ETSIEN319411-2] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: 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

[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.

[SSC_CP] SSC GDL CA Sertifikato taisyklės.

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.Certificates for

[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.

[RFC2822] RFC 2822, Internet Message Format, IETF, 2001

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

[RFC3039] RFC3039, 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.

[SSCGDLRPA] SSC GDL CA Pasitikinčio šalies sutartis.
[SSC_PDS] SSC GDL CA Viešai skelbtina informacija.

