SSC GDL CA

Viešai skelbtina informacija

Versija 2.3

LT OID: 2.16.440.1.4.30003763.2.1.2.3
IANA OID: 1.3.6.1.4.1.22501.2.1.2.3

2014 m.

Pakeitimų istorija

Versija	Data	Komentaras
2.1	2013.04.15	Pradinė redakcija
2.2	2014.04.15	Atnaujintos kontaktų ir tarnybų lentelės
2.3	2014.07.02	Papildyta informacija apie OID identifikavimą

1. Sutarties visuma

Šiame dokumente teikiama pagrindinių ir pagalbinių SSC GDL CA paslaugų teikimo taisyklių ir nuostatų santrauka.

SSC GDL CA PKI sistemoje publikuojamos taisyklės, nuostatai taip pat kai kurie programiniu būdu atpažįstami objektai, identifikuojami per konkrečius OID (objektu identifikavimo) kodus. Paskutiniai du OID kodo numeriai atskirti vienu tašku nurodo atitinkamo dokumento versijos ir modifikacijos numerius. Šie numeriai visada priskiriami nuosekliai, pvz., OID kodas 2.16.440.1.4.30003763.2.1.2.3 nurodo antros versijos ir trečios modifikacijos dokumentą.

Jeigu nauja dokumento publikacija nuo turimos to pačio dokumento publikacijos (jeigu tokia egzistuoja) skiriasi nestilistinio ir/ar neredakcinio pobūdžio pakeitimais, atnaujintos publikacijos versijos numeris OID kode inkrementuojamas iki to dokumento publikacijos, priešingu atveju inkrementuojama tik atitinkamo dokumento OID kodo modifikacijos dalis, nekeičiant jo versijos numerio. Naujos modifikacijos dokumentai gali būti publikuojami arba naudojami kaip vidiniai darbiniai egzemplioriai.

Tais atvejais, kai koks nors programiniu būdu atpažįstamas objektas nurodo į viešai nepublikuotą dokumento egzempliorių, laikoma, kad taikomas to dokumento viešai paskelbtas egzempliorius su tuo pačiu versijos ir artimiausiu didesniu modifikacijos numeriais.

Pagrindiniais šaltiniais apie SSC GDL CA teikiamas paslaugas laikomi dokumentai:

- Sertifikato taisyklės (CP);
- Sertifikavimo veiklos nuostatai (CPS);
- Laiko žymos taisyklės ir nuostatai (TSP-S).

Tačiau daugumai PKI naudotojų šiuos dokumentus sunku suprasti. Todėl yra poreikis apibendrintame dokumente - SSC GDL PKI *Viešai skelbtina informacija* (*angl. PKI Disclosure Statement* - PDS), kuris padėtų PKI naudotojams priimti pagrįstus sprendimus.

Siekiant įvertinti ar SSC GDL CA teikiama paslauga, ar išduotas sertifikatas tinka konkrečiam naudojimui, *Užsakovai* ir *Pasitikinčios šalys* PRIVALO susipažinti su šiuo dokumentu, taip pat su SSC GDL CA CP, SSC GDL CA CPS, SSC GDL CA TSP-S ir kitais susijusiais dokumentais.

Pasitikinčios šalys ir asmenys, ketinantys dalyvauti SSC GDL PKI, turi pasirašyti vieną iš paslaugų teikiamų sutarčių:

SSC GDL CA paslauga	**Dokumento IANA/LT identifikatorius (OID)[1]**
Bendros paslaugų teikimo sąlygos (sutartis)	1.3.6.1.4.1.22501.8.2.6.0 2.16.440.1.4.30003763.8.2.6.0

[1]OID – Object Identifier. http://www.oid-info.com/

Pasitikinčios šalies sutartis[2]	1.3.6.1.4.1.22501.8.2.7.0 2.16.440.1.4.30003763.8.2.7.0
Fizinio asmens sertifikavimo sutartis	1.3.6.1.4.1.22501.8.2.1.0 2.16.440.1.4.30003763.8.2.1.0
Juridinio asmens sertifikavimo sutartis	1.3.6.1.4.1.22501.8.2.2.0 2.16.440.1.4.30003763.8.2.2.0
OCSP paslaugos sutartis	1.3.6.1.4.1.22501.8.2.3.0 2.16.440.1.4.30003763.8.2.3.0
Laiko žymos paslaugos sutartis	1.3.6.1.4.1.22501.8.2.4.0 2.16.440.1.4.30003763.8.2.4.0
Autentifikacijos paslaugos sutartis	1.3.6.1.4.1.22501.8.2.5.0 2.16.440.1.4.30003763.8.2.5.0

Su SSC GDL CP, SSC GDL CPS, SSC GDL TSP-S ir visais aukščiau lentelėje išvardintais dokumentais galima susipažinti arba užklausti SSC GDL CA Talpykloje:

http://gdl.repository.ssc.lt

2. Kontaktinė informacija

SSC GDL CA viešojo rakto infrastruktūrą (angl. Public Key Infrastructure - PKI) valdo uždaroji akcinė bendrovė Skaitmeninio sertifikavimo centras (SSC).

SSC GDL CA taisyklių valdytojas:

Skaitmeninio sertifikavimo centras

Jogailos g. 8, LT-01116, Vilnius, LIETUVA

Web: http://www.ssc.lt

El. paštas: info@ssc.lt

Faks.: +370.700.22715

SSC GDL CA šakninių ir išduodančių tarnybų valdytojas:

Skaitmeninio sertifikavimo centras

Jogailos g. 8, LT-01116, Vilnius, LIETUVA

Web: http://www.ssc.lt

El. paštas: info@ssc.lt

Faks.: +370.700.22715

SSC GDL laiko žymos tarnybos (TSA) valdytojas:

Skaitmeninio sertifikavimo centras

[2]Konkliudentiniais veiksmais (LR Civilinio kodekso 1.71 straipsnis).

Jogailos g. 8, LT-01116, Vilnius, LIETUVA
Web: http://www.ssc.lt
El. paštas: info@ssc.lt
Faks: +370.700.22715

SSC GDL CA *Registravimo tarnybos* (RA) funkcijas vykdo specialus SSC GDL CA skyrius.

Teikiant SSC GDL CA paslaugas taip pat dalyvauja trečioji šalis:

UAB „Officeday“
Vilkpėdės g. 4
LT-03151 Vilnius
LIETUVA

Kiti SSC GDL CA paslaugų teikimo kontaktai:

Paslauga	Aprašymas	Paslaugos kontaktams adresas	El. pašto adresas
Sertifikatų užsakymas	Teikiama informacija apie sertifikatų užsakymus.	https://private.ssc.lt/order_n/	uzsakymai@ssc.lt
Užsakovo/Subjekto registracija	Teikiama registravimui reikalinga informacija.	https://private.ssc.lt/order_n/	dokumentai@ssc.lt
Sertifikato gamyba	Generuojami užsakyti sertifikatai.	http://support.ssc.lt	Pagalba@ssc.lt
Pristatymas	Sertifikatų ar kitų dokumentų pristatymas *Subjektui*.	http://support.ssc.lt	Pagalba@ssc.lt
Sertifikatų atšaukimas	Priima prašymus atšaukti sertifikatą.	http://support.ssc.lt	uzsakymai@ssc.lt
Sertifikatų būsena[3]	Pateikia informaciją apie sertifikato būseną (CRL ir OCSP).[4]	http://support.ssc.lt https://gdl.repository.ssc.lt/lt/kontaktai/susisiekti/	Pagalba@ssc.lt
Subjekto saugi įranga	Teikia informaciją apie saugią parašo formavimo įrangą (SSCD).	http://support.ssc.lt	Pagalba@ssc.lt
Laiko žymos teikimas	Teikia laiko žymos paslaugas (TSS).	http://support.ssc.lt https://gdl.repository.ssc.lt/lt/kontaktai/susisiekti/	Pagalba@ssc.lt
Subjekto autentifikacija	Autentifikuoja Subjektą prieš teikiant el. paslaugas.	id.ssc.lt/*service_name* kur *service_name* nurodo paslaugos pavadinimą pvz., egas.	Pagalba@ssc.lt
Subjekto asmens kodas	Suteikia asmens kodą pagal sertifikatą.	https://id.ssc.lt/verify.wsdl	Pagalba@ssc.lt
El. parašo tikrinimas	Tikrina ETSI parašo formatu pasirašytus dokumentus kaip Paslauga (SaaS).	https://jps.ssc.lt/verify	Pagalba@ssc.lt
Pagalbos tarnyba	Padeda klientams, naudojantiems sertifikatus.	http://support.ssc.lt	Pagalba@ssc.lt
Pokalbis gyvai	Teikia pagalbą bendraujant realiu laiku.	http://livechat.ssc.lt	
El. parašo kūrimo programinė įranga	JUSTA – El. parašo kūrimo programinė įranga kaip Paslauga (SaaS).	http://www.justa.lt/order/	Pagalba@ssc.lt

[3] Būsenos tikrinimo tarnybos adresas yra nurodomas kiekviename sertifikate.
[4] OCSP pasirašančių tarnybų sertifikatai pateikiami Talpykloje: https://gdl.repository.ssc.lt/lt/talpykla/tarnybiniai-sertifikatai-ir-crl-sarasai/

3. Sertifikatų ir laiko žymų tipai, tikrinimo procedūros ir naudojimas

Sertifikatų tipai

SSC GDL CA yra du pagrindiniai sertifikavimo tarnybų (CA) tipai: šakninės ir išduodančios tarnybos. Šiuo metu hierarchija susideda iš tokių sertifikavimo tarnybų:

Šakninė CA	Išduodanti CA	Sertifikato tipas
Root A	SSC Class 1-2 CA	Nepatikrintos tapatybės *Subjektų* sertifikatai ir nekvalifikuoto el. parašo sertifikatai.
	SSC Class 2-4 QCA	Visuomenei išduodami kvalifikuoto el. parašo sertifikatai.
Root B	SSC NH CA	Įrangos/Paslaugų sertifikatų tipai.
	SSC EV CA	EV SSL ir EV CS sertifikatai
VS Root	SSC VS Class 2-4 QCA	Kvalifikuoti el. parašo sertifikatai viešojo sektoriaus institucijų Subjektams.

Laiko žymų tipai

SSC GDL TSS nėra apribotos konkretaus taikymo tipui ir palaiko kvalifikuotus elektroninius parašus kaip nurodyta 1999 gruodžio 13 d. Europos Parlamento ir Tarybos dėl Bendrijos elektroninių parašų reguliavimo sistemos Direktyvoje 1999/93/EC.

SSC GDL CA laiko žymų paslaugas palaiko tokie parašo algoritmai:

- sha1WithRSAEncryption (2048 bit);
- sha256WithRSAEncryption (2048 bit).

SSC GDL priima įvairias užklausas su SHA-1, SHA-256, SHA-384 ir SHA-512 santraukomis.

SSC GDL TSS pasirašomi sertifikatai galioja iki 10 metų.

SSC GDL TSS yra komercinių paslaugų tarnyba.

Tikrinimo procedūra

Priklausomai nuo tapatybės tikrinimo ir saugumo reikalavimų lygio SSC GDL CA *Subjektui* išduoti sertifikatai yra skirstomi į klases.

Jei *Subjektas* yra fizinis asmuo, jo tapatybė yra tikrinama tiesiogiai arba netiesiogiai, naudojant priemones, kurios suteikia fizinio dalyvavimo[5] patikimumą.

[5] Pavyzdžiui, fizinis dalyvavimas netiesiogiai įrodomas patikrinus fizinio asmens pateiktą registracijos dokumentą, kuris buvo įgytas fiziškai dalyvaujant.

Jei paslauga yra teikiama *Užsakovui*, tada pateikiami įrodymai, kad *Užsakovas* yra įgaliotas veikti *Subjekto* vardu (pvz. yra įgaliotas tvarkyti užsakymus visiems organizacijos nariams). *Užsakovas* pateikia fizinį adresą ar kitą kontaktą, kuriuo būtų galima su juo susisiekti.

Sertifikatai yra išduodami įrangoje, su sąlyga, kad paskirtas atsakingas asmuo užtikrins tinkamą kontrolę ir naudojimą privačiais raktais. Paskirtas asmuo laikomas atsakingu už nuosavybės įrodymą ir užtikrinimą, kad raktai yra saugiai perkelti į įrenginį arba paslaugą.

Naudojimas

SSC GDL CA sertifikavimo ir laiko žymos paslaugos nenustato jokių apribojimų paslaugų naudotojų ratui (bendruomenei) ar sertifikato tinkamumui.

Pagal *Užsakovo* požiūrį SSC GDL sertifikatai gali būti skirstomi į:

Parašo sertifikatai:

- dokumentų pasirašymas;
- el. pašto pasirašymas;
- programinio kodo pasirašymas;
- laiko žymos pasirašymas.

Šifravimo sertifikatai:

- dokumentų šifravimas ir dešifravimas;
- el. pašto šifravimas.

Autentifikavimo sertifikatai:

- kliento autentifikavimas;
- serverio autentifikavimas;
- įrangos sertifikatai.

Žemiau esanti lentelė parodo ryšį tarp naudojimo ir sertifikatų klasių:

Naudojimas		**Klasė**			
		I	**II**	**III**	**IV**
Pasirašymas	dokumentai	–	+	+	+
	el. paštas	+	+	+	+
	programiniai kodai	–	+	+	+

	laiko žyma	–	+	–	–
Šifravimas	dokumentai	–	+	+	–
	el. paštas	+	+	+	–
	duomenų srautas tarp Web kliento ir serverio	+	+	-	-
	duomenų srautas tarp el. pašto kliento ir serverio	+	+	-	-
Autentifikavimas	web klientas	–	+	+	+
	el. pašto klientas	+	+	+	+
	el. pašto serveris	+	+	-	-
	web serveris ar įrenginys	–	+	+	–

Pagal taikytiną teisę pasirašymo ar autentifikavimo sertifikatai gali būti pripažinti kvalifikuotais ir nekvalifikuotais. Kvalifikuotais sertifikatais gali būti laikomi ne žemesni nei antros klasės sertifikatai, kurių sudėtyje yra ETSI standartais nustatyti kvalifikuoto sertifikato skiriamieji požymiai.

Pagal tarptautinių standartų reikalavimus, serverių ar įrenginių autentifikavimo sertifikatai (SSL), taip pat programinio kodo pasirašymo sertifikatai (CS) gali būti pripažinti atitinkančiais EV (angl. Extended Validation – pastiprinto patikimumo) skiriamaisiais ženklais. EV SSL arba EV CS sertifikatus išduoda SSC GDL CA tarnybos, kurios yra pripažintos atitinkančiomis ETSI arba kito analogiško lygio standarto reikalavimus.

4. Pasitikėjimo ribos

SSC GDL CA nenustato finansinių atsakomybių ribų sertifikatų[6] ar laiko žymos paslaugų naudojimui.

TSS remiasi patikimais UTC laiko šaltiniais su 1 sekundės tikslumu. Saugūs TSS veiklos įrašai yra taip pat prieinami.

5. *Užsakovų* įsipareigojimai

Užsakovai privalo susipažinti su SSC GDL CA paslaugų taisyklėmis ir sąlygomis, prieš sudarydami sutartį su CA. *Užsakovo* įsipareigojimai apima:

Užtikrinti sertifikato paraiškoje pateiktos informacijos tikslumą.

Prieš įdiegimą ir pirmą naudojimą patikrinti išduotą sertifikatą dėl joje esančios informacijos

[6] Išskyrus QCP, QCP+, EVCP ir EVCP+ sertifikatai. Esant poreikiui SSC GDL CA išduotiems kvalifikuotiems sertifikatams gali nustatyti apribojimus dėl sandorių vertės, kuriems sertifikatas gali būti naudojamas. *Užsakovai* ar *Pasitikinčios šalys* TURI nurodyti, kokius apribojimus, jei tokių yra, jie nori taikyti naudojamiems sertifikatams.

tikslumo.

Užtikrinti privačių raktų, susijusių PIN kodų, sertifikato atšaukimo slaptažodžių apsaugą nuo neteisėto naudojimo.

Naudoti sertifikatą tik teisiniais tikslais.

Pranešti SSC GDL RA kuo įmanoma anksčiau apie galimą privataus rakto kompromitavimą, naudojant vieną iš aukščiau nurodytų paslaugų teikimo kontaktų.

6. *Pasitikinčios šalies* įsipareigojimas tikrinti sertifikato būseną

Sprendimas tikrinti atšaukimą yra priimamas *Pasitikinčios šalies*, remiantis rizikos įvertinimu, atsakomybe ir vertinant galimomis atšaukto sertifikato naudojimo pasekmėmis. Prieš pasitikėdami sertifikatu, visada užtikrinkit CP, CPS ir TSP-S nuostatų laikymąsi, sertifikatų tipų ir laiko žymų atitikimą, jų patikrinimo ir naudojimo atžvilgiu.

7. Ribota garantija ir atsakomybės atsisakymas

SSC GDL CA neprisiima jokios atsakomybės, susijusios su sertifikatų ar viešojo/privataus raktų porų naudojimu, išskyrus naudojimą, kuris yra aprašytas SSC GDL CA paslaugų sutartyse. *Užsakovas* apsaugos CA nuo bet kokios atsakomybės, išlaidų kylančių iš bet kokio panašaus ieškinio reikalavimų.

SSC GDL CA neturi būti atsakingi už bet kokius aplinkybių sąlygojamus, netiesioginius ar atsitiktinius nuostolius, bet kokių verslo praradimų, negauto pelno ar valdymo nuostolius, ar iš anksto numatomus ar nenumatomus, kylančius iš išreikštų ar numanomų garantijų pažeidimų, sutarties pažeidimų, iškraipymų. Tačiau atsakomybė gali atsirasti dėl bet kokio sertifikato naudojimo ar pasitikėjimo jomis, ryšio su SSC GDL CA aplaidumu, tyčinio nusižengimo atvejais arba, kai to reikalauja taikytina teisė.

Ginčai turi būti sprendžiami laikantis SSC GDL CA pretenzijų teikimo procesų, nurodytų atitinkamoje paslaugų teikimo sutartyje. Paslaugų teikimo sutarčių projektai yra prieinami, paprašius iš aukščiau nurodytų kontaktų.

SSC GDL CA neapima jokios atsakomybės dėl bet kokių sandorių, tarp *Užsakovų/Subjektų* ir trečiųjų šalių..

SSC GDL CA CP ir CPS nuostatos galioja atskirai. Jei kuri nors dalis būtų teismo laikoma nepagrįsta ar netaikytina, kitos dalys lieka galioti.

8. Taikomos sutartys, sertifikavimo veiklos nuostatai ir sertifikato taisyklės

Pagrindiniai SSC GDL CA taisyklių ir nuostatų dokumentai yra prieinami šiais adresais:

SSC GDL CA GSA:	http://gdl.repository.ssc.lt/gsa
SSC GDL CA RPA:	http://gdl.repository.ssc.lt/rpa
SSC GDL CA CP:	http://gdl.repository.ssc.lt/cp
SSC GDL CA CPS:	http://gdl.repository.ssc.lt/cps
SSC GDL CA TSSP:	http://gdl.repository.ssc.lt/tssp

9. Privatumo taisyklės

SSC GDL CA *Privatumo taisyklės* yra duomenų saugykloje:

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

10. Pinigų grąžinimo taisyklės

SSC GDL CA nenumato grąžinti pinigų už išduotus sertifikatus.

11. Galiojantys įstatymai ir ginčų sprendimas

Ginčai sprendžiami laikantis tvarkos ir sąlygų, nurodytų atitinkamose paslaugų sutartyse, nurodytose 3 puslapyje. Kontaktiniai duomenys yra pateikiami šio dokumento 4 puslapyje.

SSC GDL CA paslaugų nuostatos yra reglamentuojamos Lietuvos Respublikos įstatymų ir taikomos Europos Sąjungos reglamentuose ir visos šalys savo galimus ieškinius turi pateikti Lietuvos Respublikos teismui.

12. CA, Talpyklos licencijavimas, patikimumo žymės ir auditas

Priėjimui prie SSC GDL CA Talpyklos nereikia pateikti jokių licencijų.

SSC GDL CA kvalifikuoto sertifikavimo tarnyba buvo akredituota Lietuvos Respublikos Vyriausybės.

SSC GDL CA teikiamos paslaugos buvo vertinamos nepriklausomų auditorių pagal ETSI TS 102 042[7], ETSI TS 101 456[8] ir ETSI TS 102 023[9] reikalavimus.

[7] Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
[8] Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.
[9] Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.