SSC GDL TSPDS

Viešai skelbtina informacija

Versija 3.1

LT OID: 2.16.440.1.4.30003763.2.1.3.1
IANA OID: 1.3.6.1.4.1.22501.2.1.3.1

2017 m.

Peržiūrų istorija

Versija	Data	**Peržiūrų detalės**
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
3.0	2017.01.09	Atnaujintos eIDAS reglamento nuostatos
3.1	2017.04.29	CAB ataskaita

1. Sutarties visuma

Šiame dokumente teikiama pagrindinių ir pagalbinių SSC GDL TSP paslaugų teikimo taisyklių ir nuostatų santrauka, susijusi su jos pasitikėjimo paslaugomis, kaip apibrėžta Europos Parlamento ir Tarybos reglamente (ES) Nr. 910/2014 dėl Elektroninės identifikavimo ir pasitikėjimo paslaugos elektroniniams sandoriams vidaus rinkoje ir Direktyvos 1999/93/EB (eIDAS) panaikinimas.

TSP PKI sistemoje publikuojamos taisyklės, nuostatai taip pat kai kurie programiniu būdu atpažįstami objektai, identifikuojami per konkrečius OID (objektų 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 2.16.440.1.4.30003763.2.1.3.0 nurodo versijos numerį 3 ir modifikacijos dokumento numerį 0.

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.

Jei mašininio nuskaitymo komponentas SSC GDL TSP susijęs su nepaskelbtu žmogaus skaitymo dokumento darbine instancija, taikomas OID su tuo pačiu versijos numeriu ir artimiausiu didesniu pakeitimo numeriu, jei atitinkamas dokumentas yra tinkamai prieinamas visuomenei.

The Trust Services Certification Policy (TSCP), Sertifikavimo praktikos ataskaita (TSCPS), Laiko žymos politika ir pareiškimas (TSTPPS) yra pagrindinis TSP politikos ir praktikos šaltinis, tačiau daugeliui PKI vartotojų, paslaugų vartotojams, šiuos dokumentus gali būti sunku suprasti. Todėl reikalingas supaprastintas dokumentas, kuris PKI vartotojams gali padėti priimti patikimą sprendimą - Trust Services PKI Disclosure Statement (TSPDS).

Siekiant įvertinti ar SSC GDL TSP teikiama paslauga, ar išduotas sertifikatas tinka konkrečiam naudojimui, *Užsakovai* ir *Pasitikinčios šalys* PRIVALO susipažinti su šiuo dokumentu, taip pat su TSPDS, TSCP, TSCPS, TSTPPS ir kitais susijusiais dokumentais.

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

SSC GDL TSP 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
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 TSCP, SSC GDL TSCPS, SSC GDL TSTPPS ir visais aukščiau lentelėje išvardintais dokumentais galima susipažinti arba užklausti Talpykloje:

http://gdl.repository.ssc.lt

2. Kontaktinė informacija

PKI tvarko Skaitmeninio sertifikavimo centras (SSC), privati korporacija, registruota Vilniuje, Lietuvoje.

SSC GDL TSP 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 TSP **šakninių ir išduodančių tarnybų valdytojas:**

SSC GDL TSP

Skaitmeninio sertifikavimo centras

Jogailos g. 8, LT-01116, Vilnius,

LIETUVA Web: http://www.ssc.lt

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

[2]Konkliudentinis veiksmas pagal Lietuvos Respublikos civilinio kodekso 1.71 punktą.

El. paštas: info@ssc.lt

Faks.: +370.700.22715

SSC GDL laiko žymos tarnybos (TSA) valdytojas:

SSC GDL TSP

Skaitmeninio sertifikavimo centras

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

Web: http://www.ssc.lt

El. paštas: info@ssc.lt

Faks: +370.700.22715

Registravimo tarnybos (RA) paslaugas vykdo specialus SSC padalinys.

Ši trečiojo šalis patvirtinta teikti SSC GDL TSP platinimo (RA) paslaugą:

UAB „Officeday“

Vilkpėdės g. 4

LT-03151 Vilnius

LIETUVA

Kiti SSC GDL TSP paslaugų teikimo kontaktai:

Paslaug a	Aprašyma s	Paslaugos kontaktams adresas	El. pašto adresas
Sertifikatų užsakymas	Teikiama informacija apie sertifikatų užsakymus.	https://private.ssc.lt/order_n/	o@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 (QSCD).	http://support.ssc.lt	Pagalba@ssc.lt
Laiko žymos teikimas ir valdymas	Kuria laiko žymos tokenus. Valdo Teikia laiko žymų paslaugų (TSS) veikimą.	http://support.ssc.lt https://gdl.repository.ssc.lt/lt/kontaktai/susisiekti/	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/

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. Sertifikatų ir laiko žymų tipai, tikrinimo procedūros ir naudojimas

Sertifikatų tipai

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

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 tokenų tipai

SSC GDL TSP nėra apribotos konkretaus taikymo tipui ir palaiko kvalifikuotus elektroninius parašus kaip nurodyta eIDAS.

SSC GDL TSS palaiko sha256WithRSAEncryption (2048 bit) pasirašymo algoritmą ir priima įvairias užklausas su SHA-1, SHA-256, SHA-384 ir SHA-512.

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 TSP Subjektui išduoti sertifikatai yra skirstomi į keturias klases.

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

Jei TSP 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 TSP 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:

Elektroninio parašo ir spaudo sertifikatus - dokumentų pasirašymas/antspaudavimas, el. laiškų pasirašymas, programinio kodo pasirašymas, laiko žymos pasirašymas;

Šifravimo sertifikatai - dokumentų šifravimas ir dešifravimas, el. pašto šifravimas.

Autentifikavimo priemonės: kliento, serverio ir įrangos elektroninės identifikavimo priemonės.

Žemiau esanti lentelė parodo ryšį tarp naudojimo ir sertifikatų klasių:

Naudojimas		Klasė 1	Klasė 2	Klasė 3	Klasė 4
Pasirašymas	dokumentas	-	+	+	+
	el. paštas	+	+	+	+
	kodas	-	+	+	+
	laiko žyma	-	+	-	-
Šifravimas	dokumentas	-	+	+	-

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

	el. paštas	+	+	+	-
	Bendravimas tarp svetainės kliento ir serverio	+	+	-	-
	Bendravimas tarp el. pašto kliento ir serverio	+	+	-	-
Autentifikavimas	Svetainės klientas	-	+	+	+
	Elektroninio pašto klientas	+	+	+	+
	Elektroninio pašto serveris	+	+	-	-
	Svetainės serveris ar įranga	-	+	+	-

Pagal eIDAS 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 TSP nenustato finansinių atsakomybių ribų sertifikatų[6] ar laiko žymos paslaugų naudojimui.

TSS remiasi patikimais UTC laiko šaltiniais su 1 sekundės tikslumu.

5. Užsakovų įsipareigojimai

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

- ➢ Užtikrinti sertifikato paraiškoje pateiktos informacijos tikslumą.
- ➢ Prieš įdiegimą ir pirmą naudojimą patikrinti išduotą sertifikatą dėl joje esančios informacijos˙ tikslumo.

[6] Išskyrus QCP, QCP+, EVCP ir EVCP+ sertifikatai. Esant poreikiui SSC GDL TSP 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.

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

- ➢ Naudoti sertifikatą tik teisiniais tikslais.

- ➢ Pranešti SSC GDL Registracijos Tarnybai kuo įmanoma anksčiau apie galimą privataus rakto kompromitavimą, naudojant vieną iš aukščiau nurodytų paslaugų teikimo kontaktų 5 puslapyje aukščiau.

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 TSCP, TSCPS ir TSTPPS nuostatų laikymąsi, sertifikatų tipų ir laiko žymų atitikimą, jų patikrinimo ir naudojimo atžvilgiu.

7. Ribota garantija ir atsakomybės atsisakymas

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

SSC GDL TSP 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 TSP aplaidumu, tyčinio nusižengimo atvejais arba, kai to reikalauja taikytina teisė.

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

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

SSC GDL TSCP ir TSCPS 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 TSP taisyklių ir nuostatų dokumentai yra prieinami:

SSC GDL TSP GSA: http://gdl.repository.ssc.lt/gsa

SSC GDL TSP RPA: http://gdl.repository.ssc.lt/rpa

SSC GDL TSCP: http://gdl.repository.ssc.lt/cp

SSC GDL TSCPS: http://gdl.repository.ssc.lt/cps

SSC GDL TSTPPS: http://gdl.repository.ssc.lt/tssp

9. Privatumo taisyklės

SSC GDL TSP *Privatumo taisyklės* yra duomenų saugykloje:

https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/

10. Pinigų grąžinimo taisyklės

SSC GDL TSP nenumato grąžinti pinigų už išduotus sertifikatus.

11. Galiojantys įstatymai ir ginčų sprendimas

Ginčai sprendžiami laikantis tvarkos ir sąlygų, nurodytų atitinkamose paslaugų sutartyse, nurodytose 4 puslapyje. Kontaktiniai duomenys yra pateikiami šio dokumento 2 skyriuje.

SSC GDL TSP paslaugų nuostatos yra reglamentuojamos Lietuvos Respublikos įstatymų ir eIDAS. Visos šalys savo galimus ieškinius turi pateikti Lietuvos Respublikos teismui.

12. TSP ir Talpyklos licencijavimas, patikimumo žymės ir auditas

Priėjimui prie SSC GDL TSP Talpyklos nereikia pateikti jokių licencijų.

SSC GDL kvalifikuoto sertifikavimo tarnyba buvo akredituota pagal eIDAS.

SSC GDL TSP teikiamos paslaugos buvo vertinamos nepriklausomų auditorių pagal ETSI standartus.