PRIEDAS NR. 1
APIBENDRINTI SERTIFIKAVIMO VEIKLOS NUOSTATAI (G-CPS)

1. Įvadas

Šis dokumentas yra sertifikavimo tarnybų sertifikavimo veiklos nuostatų apibendrinimas, nusakantis aplinką, kurioje yra kuriami kvalifikuoti sertifikatai, teikiami TELIA Lietuva AB mobiliojo ryšio abonentams (toliau - *abonentams*).

Šis dokumentas nėra taikomas konkrečiai sertifikavimo tarnybai, tačiau visų sertifikavimo tarnybų, teikiančių kvalifikuotus sertifikatus TELIA Lietuva AB *abonentams*, nuostatai yra suderinami su teiginiais, išsakytais šiame dokumente. Šiame dokumente pateikti pagrindiniai ir esminiai teiginiai, su kuriais klientui būtina susipažinti prieš pradedant naudoti savo kvalifikuotą sertifikatą. Šalims, kurios pasitiki sertifikatais, šis dokumentas nėra pakankamas – šios šalys privalo analizuoti sertifikavimo veiklos nuostatus kiekvienos tarnybos, teikiančios kvalifikuotus sertifikatus TELIA Lietuva AB *abonentams*.

2. Taikymo sritis

2.1 Sertifikavimo Tarnyba (toliau vadinama CA)

CA sukuria kvalifikuotus sertifikatus, atitinkančius sertifikato taisykles (**toliau tekste vadinama CP**. Žiūr. priedą Nr.2 „Sertifikato taisyklės“), prisilaikydama savo veiklos nuostatų. Sertifikavimo tarnyba rūpinasi kvalifikuoto sertifikato gyvenimo ciklo užtikrinimu.

2.2 Registravimo Tarnyba (toliau vadinama RA)

RA veikia kaip CA atstovas santykiuose tarp *vartotojo* ir CA.

2.3 Vartotojas

2.3.1. Klientas

Klientas yra kvalifikuoto sertifikato turėtojas (TELIA Lietuva AB mobiliojo ryšio abonentas).

2.3.2. Pasitikinčioji šalis

Pasitikinčioji šalis yra šalis, kuri nusprendžia pasitikėti konkrečios CA išduotu kvalifikuotu sertifikatu.

Pasitikinčioji šalis:

- įvertina CA sertifikavimo veiklos nuostatus, sertifikato taisykles, registracijos taisykles (RP), kitus susijusius dokumentus;
- patikrina kvalifikuoto sertifikato galiojimą;
- patikrina kvalifikuoto sertifikato atitikimą jo taikymo sričiai;
- patikrina parašą ir susijusius duomenis, bei identifikuoja pasirašiusįjį asmenį.

3. Bendrosios sąlygos

3.1. Pareigos

3.1.1. Sertifikavimo tarnybų pareigos

Sertifikavimo tarnybos užtikrina, kad:

- Sertifikavimo paslaugos teikiamos prisilaikant EIDAS reglamento (EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS (ES) Nr. 910/2014, 2014 m. liepos 23 d.,dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB) reikalavimų dėl patikimumo užtikrinimo paslaugų;
- Sertifikavimo paslaugos teikiamos prisilaikant savo sertifikavimo veiklos nuostatų, suderintų su šiuo (G-CPS) dokumentu.

Sertifikavimo tarnybos:

- viešai skelbia savo sertifikavimo veiklos nuostatus ir sertifikato taisykles (CP), ir šie dokumentai yra pasiekiami internetu;
- užtikrina neskelbiamų asmens duomenų konfidencialumą;
- palaiko savo išduotus sertifikatus (valdo jų gyvenimo ciklą);
- priima kvalifikuotų sertifikatų atšaukimo užklausas 24 valandas per parą;
- užtikrina galimybę patikrinti savo išduotų sertifikatų galiojimą;
- išsaugoja visus su išduotais sertifikatais susijusius dokumentus;
- atlieka savo sistemų auditą ir viešai publikuoja audito išvadas;
- internete skelbia savo privalomojo veiklos draudimo polisus.

Sertifikavimo tarnybos užtikrina, jog jų darbuotojai neturi teistumo dėl tyčinių nusikaltimų

3.1.2. Registravimo tarnybos pareigos

RA priima paraiškas kvalifikuotiems sertifikatams gauti ir jiems panaikinti, šias paraiškas patikrina, prisilaikydama procedūrų, aprašytų registracijos taisyklėse (RP). RA pateikia klientams pasirašymo įrangą (SIM korteles) ir perduoda surinktus asmens duomenis į CA sertifikatų gamybai.

3.1.3. Kliento pareigos

Klientas privalo pateikti apie save teisingą ir išsamią informaciją. Pasikeitus asmens duomenims, klientas privalo apie tai informuoti RA. Klientas privalo nedelsiant pranešti, jei jam suteikta pasirašymo įranga galimai pasinaudojo tretieji asmenys. Klientas yra išimtinai atsakingas už jam suteiktos pasirašymo įrangos priežiūrą. Klientas privalo žinoti, jog pasirašinėti atšauktais arba pasibaigusio galiojimo sertifikatais yra neleistina.

3.1.4. Pasitikinčiosios šalies pareigos

Pasitikinčioji šalis išanalizuoja atsakomybes ir rizikas, susijusias su pasitikėjimu panaudojant sertifikatą. Atvejais, kai nėra pakankamai įrodymų dėl sertifikato galiojimo jo panaudojimo momentu, pasitikinčioji šalis privalo analizuoti atšauktų sertifikatų sąrašą, galiojusį tuo metu, kai buvo panaudotas sertifikatas. Pasitikinčioji šalis privalo sekti sertifikato taisyklėse numatytus apribojimus ir naudoti sertifikatą tik pagal paskirtį.

3.1.5. Publikavimo tarnybos pareigos

Publikavimo tarnyba privalo pateikti visoms suinteresuotoms šalims informaciją apie sertifikatus ir jų galiojimą:

- Tarnyba saugo visus galiojančius sertifikatus ir jų statusą;
- Tarnyba veikia 24 valandas per parą;
- Tarnyba turi apsaugos priemones nuo simuliacijos ir užtikrina pateikiamų duomenų integralumą.

3.2. Atsakomybė

CA atsakinga už savo pareigų, įvardintų punktuose 3.1.1 ir 3.1.5 vykdymą. CA nėra atsakinga už klientų privačių raktų apsaugą, neteisingą sertifikatų panaudojimą, neadekvačius pasitikinčiųjų šalių tikrinimus.

Nenugalimos jėgos (Force majeure) įvykių atvejais, sertifikavimo veiklos nuostatų (CPS) nevykdymas nėra laikomas pareigų nesilaikymu.

RA atsakinga už savo pareigų, įvardintų 3.1.2. prisilaikymą.

3.3. Ginčų sprendimas

Visi ginčai tarp šalių sprendžiami derybų būdu. Šalims nepavykus susitarti, ginčas sprendžiamas teisme, Vilniuje. Susijusios šalys informuojamos apie problemą/ieškinį ne daugiau, kaip per 30 dienų įvykus problemai, išskyrus įstatymuose numatytus atvejus.

4. Fizinės ir organizacinės saugumo priemonės

Saugumo valdymo prasme CA vadovaujasi visuotinai pripažintais standartais, pvz. ISO 13335, ISO 13569. Kiekviena CA laikosi vietos įstatymų/reglamentų, reguliuojančių kvalifikuotų sertifikatų išdavimą. Atvejais, kai vietos įstatymai nenusako kitaip, laikoma, kad CA užtikrina saugomų objektų saugumą su EAL-4 patikimumo lygiu, nustatomu standarte ISO/IEC 15408-1.

Privatiesiems raktams techninės saugumo priemonės aprašomos CP dokumente. Kiti techniniai saugumo klausimai (pvz., CA sistemų saugumas prieigos kontrolei, programinės įrangos saugumas, tinklų saugumas ir pan.), slaptos informacijos apsauga ir t.t. aprašomi kiekvienos CA sertifikavimo veiklos nuostatose.

5. Žodynas ir sutrumpinimai

Kursyvu paryškinti žodžiai šiame dokumente turi sekančią prasmę:

Raktinis žodis	Apibrėžimas
Autentifikacija	Asmens tapatybės nustatymas
Kvalifikuotas sertifikatas	Įstatymų reikalavimus atitinkantis paliudijimas, jog konkrečios pasirašymo įrangos turėtojas yra konkretus fizinis asmuo
Sertifikavimo tarnyba (CA)	Tarnyba, savo *skaitmeniniu parašu* pasirašanti elektroninius asmens tapatybės paliudijimus ir vėliau tuos paliudijimus prižiūrinti
Sertifikato taisyklės (CP)	Dokumentas, nusakantis sertifikato savybes, turinį bei sertifikato panaudojimo sritis
Sertifikavimo veiklos nuostatos (CPS)	Rinkinys taisyklių, nusakančių kaip sertifikavimo tarnyba vykdo savo veiklą
Sertifikavimo paslaugos	Sekančios paslaugos: sertifikatų sukūrimas, sertifikatų patikrinimo priemonių palaikymas, sertifikatų atšaukimas
Pasirašymo įranga	Techninė priemonė sauganti slaptus raktus panaudojamus *skaitmeniniams parašams* sukurti
Klientas	Fizinis asmuo, sertifikato turėtojas , TELIA Lietuva AB mobiliojo ryšio abonentas
Negaliojančių sertifikatų registras (CRL)	Sąrašas sertifikatų, paskelbtų negaliojančiais
Skaitmeninis parašas	Speciali informacija (pridedama prie pasirašomo dokumento), leidžianti dokumento gavėjui nustatyti kas dokumentą pasirašė ir ar nebuvo dokumentas pakeistas po pasirašymo
Publikavimo tarnyba	Sertifikatų galiojimo informacijos publikavimo tarnyba
Pasitikinčioji šalis	Šalis, kuri priima sprendimą remdamasi skaitmeniniu parašu
Privatusis raktas	Slaptas raktas, saugomas *pasirašymo įrangoje*. Šiuo raktu *užkoduojamas* pasirašomas turinys
Registracijos taisyklės	Taisyklės, nusakančios kaip RA suteikia *klientui pasirašymo įrangą* ir kaip inicijuojamas *kvalifikuoto sertifikato* sukūrimas
Registravimo tarnyba (RA)	Tarnyba, veikianti kaip CA atstovas, priimantis vartotojų paraiškas *kvalifikuotiems sertifikatams* gauti, šias paraiškas patikrinanti ir perduodanti surinktus asmens duomenis į CA.
sPIN	Signataro (pasirašančiojo asmens) PIN kodas, aktyvuojantis *privatųjį raktą* prieš kiekvieną pasirašymą (*skaitmeninio parašo* sukūrimą)
Užkodavimas	Informacijos transformacija tokiu būdu, jog ją galima perskaityti tik turint atitinkamą raktą
Viešasis raktas	Raktas, leidžiantis patikrinti *skaitmeninio parašo* teisingumą (atkoduoti *privačiuoju raktu užkoduotą* informaciją)