PRIEDAS NR. 2

SERTIFIKATO TAISYKLĖS (CP)

Šis dokumentas pateikia sertifikato (elektroninio asmens tapatybės paliudijimo) ir šio sertifikato panaudojimo srities/sąlygų aprašymą. Šis dokumentas yra viešai prieinamas ir yra skirtas visiems sertifikato vartotojams. Visos sertifikavimo tarnybos, išduodančios TELIA Lietuva AB klientams elektroninius asmens tapatybės paliudijimus - sertifikatus, užtikrina, kad jų sukuriami sertifikatai atitinka šias Sertifikato Taisykles.

Reikalavimai sertifikatams, leidžiantiems identifikuoti asmenis ir kurti asmeninius elektroninius parašus

1. Įvadas

Ši dokumentas (Sertifikato Taisyklės arba CP) yra kvalifikuoto sertifikato kaip produkto aprašymas. CP aprašo šio produkto savybes ir panaudojimo principus.

Trumpas produkto aprašymas:

Klientui pateikiamas vienas kvalifikuotas sertifikatas, kuris gali būti naudojamas kurti **skaitmeniniams parašams** (turintiems tokias savybes ir tokią juridinę galią, kaip ir ranka pasirašytas asmens parašas) bei kliento **autentifikavimui** (privati elektroninės atpažinties schema). Sertifikatas yra susiejamas su privačiuoju raktu, kuris saugiai patalpintas pasirašymo įrangoje (specialioje SIM kortelėje) ir gali būti „aktyvuotas“ tik sertifikato turėtojo, žinančio slaptą pasirašymo PIN kodą - sPIN. Skaitmeninis parašas gali būti sukuriamas bet kokiems duomenims, jis yra unikalus būtent tiems pasirašomiems duomenims, nėra techninių priemonių, leidžiančių tokį pat parašą sukurti kitam asmeniui. Klientas vienu metu gali turėti tik vieną kvalifikuotą sertifikatą, susietą su pasirašymo įranga.

Šis dokumentas aprašo pagrindinius techninius aspektus, nusakančius TELIA Lietuva AB (veikiančios kaip registravimo tarnyba (RA)) klientams suteikiamus kvalifikuotus sertifikatus.

2. Taikymo sritis

2.1. Sertifikavimo tarnyba (CA)

Kvalifikuotus sertifikatus pagamina Sertifikavimo Tarnyba (CA). Yra keletas sertifikavimo tarnybų, bendradarbiaujančių su RA, pateikiant klientams kvalifikuotus sertifikatus ir juos vėliau prižiūrint. Kiekviena CA veikia skirtingoje saugioje aplinkoje, kuri aprašoma šių tarnybų patvirtintose sertifikavimo veiklos nuostatose (CPS), kurios yra vieši dokumentai, publikuojami internete. Klientui susipažinimui yra pateikiami "apibendrinti sertifikavimo veiklos nuostatai" (G-CPS), kurie yra suderinami su atskirų CA CPS ir yra sutrumpinta jų versija. Visų susijusių CA sąrašas yra pateikiamas kliento sutartyje. Atvejais, kai šiame CP dokumente pateikiami nuostatai prieštarauja CPS, yra laikoma, kad galioja CP teiginiai.

2.2. Registravimo tarnyba (RA)

RA veikia kaip CA atstovas santykiuose tarp kliento ir CA visais kvalifikuotų sertifikatų (siejamų su mobiliąja pasirašymo įranga SIM kortelėse) klausimais.

RA veikia pagal registracijos taisykles (**toliau tekste vadinama RP**. Žiūr. priedą Nr.3 „Registravimo taisyklės“) - viešai skelbiamą dokumentą. RA ir CA santykiai yra reguliuojami atskiru susitarimu ir atitinka CP bei RP. 24 valandas per parą veikianti klientų aptarnavimo/pagalbos telefono linija įgalina klientus atšaukti kvalifikuotus sertifikatus.

2.3. Klientas

Klientas yra fizinis asmuo, atstovaujantis save ir esantis aktyvus TELIA Lietuva AB mobiliojo ryšio abonentas. Klientui pateikiamas kvalifikuotas sertifikatas, atitinkantis šias CP ir RP. Sertifikatas (elektroninis asmens tapatybės paliudijimas) susieja viešąjį raktą (atitinkantį privatųjį raktą saugomą mobiliajame pasirašymo įrenginyje - SIM kortelėje) su kliento asmenine informacija.

2.4. Sertifikato taikymo sritys

Sertifikatas, išduodamas pagal šį CP yra laikomas **kvalifikuotu sertifikatu** ir gali būti naudojamas:

- **skaitmeniniam pasirašymui,** kaip tai apibrėžta LR Elektroninio Parašo Įstatyme,
- **elektroninei identifikacijai** nustatant sertifikato turėtojo tapatybę,
- **duomenų užkodavimui**.

Šios CP neriboja sertifikato panaudojimo kitiems uždaviniams.

3. Bendrosios sąlygos

3.1. Sertifikavimo tarnybų pareigos

CA teikia sertifikavimo paslaugas, derančias su šiomis CP ir su priedo Nr.1 G-CPS punktu 3.1.1. Atšaukti sertifikatai yra nedelsiant paskelbiami negaliojančių sertifikatų sąrašuose, kurie atnaujinami kas 12 valandų.

3.2. Registravimo tarnybų pareigos

Registravimo tarnyba priima iš klientų paraiškas dėl sertifikatų suteikimo ir jų atšaukimo. Paraiškose pateikiami duomenys patikrinami pagal procedūras, nustatytas RP. RA perduoda visus surinktus duomenis į CA.

3.3. Kitos 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.

4. Sertifikato gyvavimo ciklas

4.1. Kvalifikuoto sertifikato sukūrimas

Kvalifikuoto sertifikato sukūrimas vyksta tik kai:

- Mobiliojo ryšio funkcija išduotoje SIM kortelėje yra aktyvuota,
- Klientas patvirtina savo asmens duomenų, susietų su konkrečia SIM kortele teisingumą,

Sertifikato sukūrimo užklausa ir susiję asmens duomenys perduodami į CA, kvalifikuoto sertifikato sukūrimui. Sertifikato aktyvavimo informacija pateikiama vartotojui SMS žinute. Sukurti ir galiojantys kvalifikuoti sertifikatai talpinami viešoje sertifikatų saugykloje, pasiekiamoje Paslaugų Teikėjams.

4.2. Sertifikato atnaujinimas

Pasibaigus sertifikato galiojimo laikui arba panaikinus sertifikatą, RA įspėja apie tai klientą SMS žinute. Klientas gali aktyvuoti naują sertifikatą tik gavęs naują SIM kortelę.

4.3. Sertifikato sustabdymas

Sertifikato sustabdymas nepalaikomas. Esant reikalui, SIM kortelė gali būti blokuojama - tokiu būdu tik uždaroma prieiga prie pasirašymo įrenginio.

4.4. Sertifikato atšaukimas

Sertifikatas gali būti atšauktas:

- Kliento prašymu;
- Automatiškai, kai kliento mobiliojo ryšio paslauga atšaukiama, panaikinama;
- Kai klientas praneša apie galimai pamestą SIM arba neteisėtą SIM kortelės panaudojimą iš trečiųjų asmenų pusės;
- Kai sPIN tampa žinomas tretiesiems asmenims, arba įtarus, kad tretieji asmenys sužinojo sPIN;
- Kai tampa žinoma, jog klientas pažeidė savo įsipareigojimus;
- Kai pasikeičia kliento asmens duomenys (vardas, pavardė, asmens kodas);
- Kai to pareikalauja teismas ar ikiteisminio tyrimo institucijos, turinčios tam tinkamus įgaliojimus ir raštišką pagrindą;
- Kai RA įtaria, jog sertifikatą naudoja kiti asmenys ar RA įtarus, jog sPIN tapo žinomas tretiesiems asmenims.

RA perduoda sertifikato panaikinimo užklausą į CA. CA nedelsiant atšaukia sertifikatą ir atnaujina negaliojančių sertifikatų registrą (CRL).

4.5. Nenumatytų situacijų valdymas

Tuo atveju, jei konkretaus CA veikla netikėtai nutrūksta ir jos nepavyksta atstatyti per 24 valandas, RA suteikia galimybę klientams atšaukti savo sertifikatą ir aktyvuoti naują sertifikatą, sukuriamą kito veikiančio CA.

4.6. CA veiklos nutraukimas

Tuo atveju, kai konkretus CA nutraukia savo veiklą, visi jo sukurti sertifikatai yra atšaukiami. Klientas gali aktyvuoti naują sertifikatą, kuris bus sukurtas kitame CA.

5. Techninės saugumo priemonės

5.1. Kliento raktai

Kriptografiniai raktai yra generuojami arba saugiai patalpinami į SIM kortelę gamybos metu. Raktų kopijų nekuriama ir neegzistuoja žinomų būdų, kaip atstatyti privatųjį raktą SIM kortelę jau pagaminus. Privatusis raktas gali būti aktyvuojamas tik įvedant sPIN (nuo 4 iki 8 skaičių) kodą.
Pradinis sPIN yra atspausdintas ant SIM kortelės plastiko, paslėptas po nutrinamų dažų sluoksniu, sPIN kopijos niekur nesaugomos. RA garantuoja dėl pradinio sPIN apsaugos iki SIM kortelės perdavimo klientui momento, kliento prašoma įsitikinti sPIN kodo apsauga prieš priimant naują SIM kortelę.
Klientas yra įpareigojamas saugoti pasirašymo įrenginį, neleisti juo naudotis kitiems asmenims ir laikyti paslaptyje sPIN. Įtarus, kad sPIN tapo žinomas kitiems asmenims, vartotojas privalo arba pasikeisti sPIN, arba pakeisti SIM kortelę į naują.

5.2. Sistemų ir duomenų apsauga

Techninės saugumo priemonės, susijusios su CA veikla, aprašomos priede Nr. 1 (G-CPS).
Techninės priemonės, susijusios su RA veikla, aprašomos priede Nr. 3 (RP).

Neskelbiami asmens duomenys yra saugomi RA, CA ir pasitikinčiųjų šalių pagal galiojančius vietos įstatymus ir atitinka ES galiojančius reglamentus.

6. Techninis sertifikatų aprašymas

Sertifikatai apima sekančius duomenis:

- Sertifikato leidėjo duomenys (pavadinimas, registracijos numeris);
- Sertifikato turėtojo (subjekto) duomenys (žiūr. DN lauko aprašymą žemiau);
- Sertifikato galiojimo datas (nuo kada sertifikatas įsigalioja ir kada jo galiojimas baigiasi);
- Techninius duomenis, t.y.:
  1. Sertifikato formato versija;
  2. Sertifikato serijos numeris;
  3. Algoritmas, naudotas pasirašant sertifikatą;
  4. Sertifikate naudojamas viešasis raktas ir jo atvaizdavimo metodas;
  5. CA viešojo rakto identifikatorius;
  6. Asmens viešojo rakto identifikatorius;
  7. Rakto panaudojimo laukas;
  8. Sertifikato taisyklių, kurios atitinka šias taisykles, numeris;
  9. Nuoroda į negaliojančių sertifikatų skelbimo servisą (CDP);
  10. CA papildoma informacija;
  11. Išplėstinis raktų panaudojimo laukas (tik autentifikacijos sertifikate);
  12. CA papildomų paslaugų identifikatorius ir nuoroda.

6.1. Vardai sertifikatuose

Sertifikatas saugo 2 skiriamuosius vardus: sertifikato leidėjo ir sertifikato turėtojo. Šiems vardams taikomi kodavimo reikalavimai, aprašyti RFC3280.

Sertifikato turėtojo skiriamasi vardas (DN) apima sekančius atributus:

Atributas	**Aprašymas**	**Pavyzdys**
C (Country)	2-jų raidžių šalies kodas	**LT**
SN (Surname)	Asmens pavardė	**Pavardenis**
G (GivenName)	Asmens vardas	**Vardenis**
Serialnumber	Asmens kodas (žr. ETSI EN 319 412-1 V1.1.1 (2016-02))	**PNOLT-30001010004**
CN (CommonName)	Asmens parašo vizualizacijai skirtas laukas	**Vardenis, PAVARDENIS**

CA užtikrina, kad skiriamieji vardai to CA išleidžiamuose skirtingų subjektų sertifikatuose būtų skirtingi.

6.2. Techniniai sertifikato duomenys

Laukas ir OID	Privalomas	Pvz.	Aprašymas
Version	**Taip**	**V3**	**Sertifikato formato versija**
SerialNumber	**Taip**	**14 df 29 0a d8 91 33 d4 5a 9d 54 69 aa 9c 80 1d**	**Unikalus sertifikato serijos numeris šiame CA**
Signature Algorithm 1.2.840.113549.1.1.11	**Taip**	**sha256WithRSAEncryption**	**Pasirašymo algoritmas pagal RFC 5280**
Issuer Distinguished name			
Common Name (CN) 2.5.4.3	**Taip**	**EID-SK 2016**	**Sertifikavimo Tarnybos (CA) pavadinimas**
Organisation Identifier 2.5.4.97	**Taip**	**NTREE-10747013**	**Sertifikatą išleidžianti organizacija (žr. detaliau 5.1.4 ETSI EN 319 412-1)**
Organisation (O) 2.5.4.10	**Taip**	**AS Sertifitseerimiskeskus**	**Sertifikatą išleidžiančios organizacijos vardas**
Country (C) 2.5.4.6	**Taip**	**EE**	**Šalies kodas: (2 simbolių žymėjimas žr. ISO 3166 country code)**
Valid from	**Taip**	**2018 m. kovo 5 d., pirmadienis 17:30:00**	**Pirmoji sertifikato galiojimo diena ir laikas**
Valid to	**Taip**	**2023 m. kovo 5 d., sekmadienis 00:59:59**	**Paskutinė sertifikato galiojimo diena ir laikas**
Subject Distinguished Name			
Serial Number (S) 2.5.4.5	**Taip**	**PNOLT-37102230096**	**Asmens kodas pagal žymėjimą nustatytą 5.1.3 ETSI EN 319 412-1**
Given Name (G) 2.5.4.42	**Taip**	**VARDENIS**	**Asmens vardas UTF8 koduotėje žr. RFC5280**
Surname (SN) 2.5.4.4	**Taip**	**PAVARDENIS**	**Asmens pavardė UTF8 koduotėje žr. RFC5280**
Common Name (CN) 2.5.4.3	**Taip**	**VARDENIS, PAVARDENIS**	**Asmens parašo vizualizacijai skirta informacija (dažniausiai vardas ir pavardė)**
Country (C) 2.5.4.6	**Taip**	**LT**	**Subjekto identifikatoriaus kontekstas (Šalis, kurioje subjekto SerialNumber yra unikalus)**
Subject Public Key	**Taip**	**04 23 8f f1 2b df b1 01 ff 81 df 3a 99 a2 b7 b1 b5 2d ae b1 eb 91 52 1c 0d 77 79 36 55 ba d4 5d 92 f7 24 67 0d a7 7c 9f c0 b7 2a 2b 75 cf 0a 0a cc c3 a9 ea c8 42 ff db f6 bf 31 9f 05 bc 97 45 f0**	**RSA atveju 2048 eksponentės bitai (žr. RFC 4055) ECC rakto atveju 256 bitai (žr. RFC 5480)**
Public key parameters	**Taip**	**05 00 ECDSA_P256**	**RSA rakto atveju – modulis (n) ECC rakto atveju NIST P-256 kreivės informacija**

Papildoma sertifikato informacija

Naudojami sekantys nustatymai ("Kritinis" reiškia, jog programos naudojančios sertifikatą privalo patikrinti lauko turinį):

Nustatymo pavadinimas	Sertifikate	
	Nustatytas?	Kritinis?
AuthorityKeyIdentifier	TAIP	NE
SubjectKeyIdentifier	TAIP	NE
KeyUsage	TAIP	TAIP
CertificatePolicies	TAIP	NE
SubjectAltName	TAIP	NE
CRLDistributionPoints	TAIP	NE
ExtKeyUsage	TAIP	TAIP (autentifikacijai)
Authority Information Access	TAIP	NE

Detalesnis sertifikatų ir jų laukų aprašymas pateikiamas konkretaus CA CP dokumente.