

KVALIFIKUOTO ELEKTRONINIO PARAŠO PASLAUGŲ TEIKIMO SUTARTIES BENDROSIS SĄLYGOS

Kvalifikuoto elektroninio parašo paslaugas teikia:

- valstybės įmonė Registrų centras, V. Kudirkos g. 18, LT-03105 Vilnius, veikianti kaip sertifikavimo tarnyba (**toliau vadinama CA**),
- UAB „Tele2“, Upės g. 23, LT-08128, Vilnius, veikianti kaip registravimo tarnyba (**toliau vadinama RA**) ir atstovaujanti CA,

Sertifikavimo tarnybos (CA) funkcijų vykdytojas gali būti keičiamas be išankstinio kliento informavimo. Tuo atveju, jei sertifikavimo paslaugas teikia kita CA, nei nurodyta aukščiau, ir atskirai nėra susitarta kitaip, yra laikoma, jog visos Elektroninio parašo paslaugų teikimo sutarties bendrosios sąlygos (toliau - „Bendrosios sąlygos“) galioja be pakeitimų.

1. Apimtis.

Bendrosiomis sąlygomis reglamentuojamas CA vykdomas sertifikavimo paslaugų teikimas klientui ir kliento naudojimas sertifikavimo paslaugomis.

2. Objektas.

Pagal šią sutartį CA sudaro kvalifikuotą sertifikatą kvalifikuotam elektroniniam parašui sudaryti ir autentifikavimo sertifikatą, skirtą asmens tapatybei elektroninėje erdvėje nustatyti (abu toliau vadinami sertifikatais), o RA įsipareigoja CA sudarytą sertifikatą perduoti klientui, RA patikrinus kliento tapatybę bei surinkus reikiamus dokumentus / duomenis.

Klientui sertifikavimo paslaugos teikiamos pagal:

- 2.1. CA sertifikavimo veiklos nuostatus (toliau - CPS) ir kvalifikuotų sertifikatų taisyklės (toliau - CP), kurie viešai skelbiami <http://www.elektroninis.lt/dokumentai>;
- 2.2. Europos Parlamento ir Tarybos reglamentu (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (toliau - eIDAS);
- 2.3. Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymą (toliau - PUP);
- 2.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą;
- 2.5. Europos Parlamento ir Tarybos reglamentą (ES) dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas);
- 2.6. Lietuvos Respublikos Vyriausybės patvirtintais Reikalavimais kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, Reikalavimais elektroninio parašo įrangai, Kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarka, Elektroninio parašo priežiūros reglamentą.

4. CA atsakomybė.

4.1. Teikiant sertifikavimo paslaugas CA vykdo įsipareigojimus, įvardintus CPS, CP, eIDAS, PUP. Klientui patvirtinus sertifikatą galiojimą, CA garantuoja savo įsipareigojimų įvykdymą.

4.2. CA atsako už:

- 4.2.1. Sudaryto sertifikato duomenų tikslumą;
- 4.2.2. Tai, kad sertifikate nurodytas asmuo yra parašo formavimo duomenų, atitinkančių sertifikate nurodytus parašo tikrinimo duomenis, turėtojas;
- 4.2.3. Parašo formavimo duomenų ir parašo tikrinimo duomenų atitikimą, kai jis asmens prašymu sukuria šiuos duomenis;
- 4.2.4. Sertifikato galiojimo nutraukimą laiku;
- 4.3. Klientas atlygina CA patirtus nuostolius, jei:
 - 4.3.1. Pateikė klaidingus ar ne visus duomenis, reikalingus kvalifikuotam elektroniniam parašui sudaryti;
 - 4.3.2. Neapsaugo savo saugios parašo formavimo įrangos nuo kompromitacijos.
 - 4.4. CA neatsako, jei nuostoliai buvo patirti dėl:
 - 4.4.1. Trečiųjų šalių ir galimų vartotojų naudojamos neautorizuotos aparatinės ir programinės įrangos kriptografiniams raktams generuoti, duomenis šifruoti, elektroniniams parašams kurti;
 - 4.4.2. Neleistino sertifikato naudojimo;
 - 4.4.3. Teikiamų paslaugų prieinamumo ir kokybės, jei sutrikimai fiksuojami ne CA veikimo ribose, kurios detalizuotos CP, CPS.

5. Duomenų registravimo funkcijų perdavimas.

RA veikia kaip CA atstovas. RA tarpininkauja tarp kliento ir CA, teikdami šias paslaugas:

- 5.1. prašymo dėl sertifikato išdavimo priėmimas ir apdorojimas;
- 5.2. prašančiojo asmens tapatybės nustatymas;
- 5.3. sutarties pasirašymas RA vardu;
- 5.4. kriptografinių laikmenų (SIM kortelių) pateikimas klientams.
- 5.5. prašymo dėl sertifikato atšaukimo priėmimas ir apdorojimas;
- 5.6. asmens, prašančio atšaukti sertifikatą, tapatybės nustatymas;
- 5.7. asmens duomenų saugojimas, atsižvelgiant į Bendrajame duomenų apsaugos reglamente bei Lietuvos Respublikos teisės aktuose numatytus reikalavimus;

6. Kliento sutikimas.

Pasirašydamas šias Bendrąsias sąlygas klientas pripažįsta ir sutinka, kad:

- 6.1 Galiojančio sertifikato panaudojimas atitinka ranka pasirašomą parašą ir sukuria tokias pat juridines pasekmes;
- 6.2 klientas perskaitė dokumentus CPS ir CP;
- 6.3 klientas gavo instrukciją apie sertifikato aktyvavimą, panaudojimą bei įspėjimus dėl jo saugumo;
- 6.4 klientas supranta CA paslaugų pobūdį ir pobūdį paslaugų, kurias teikia trečiosios šalys - paslaugų teikėjai, savo veikloje taikantys sertifikatus;
- 6.5 klientas supranta CA įsipareigojimus ir atsakomybę bei šios atsakomybės ribas, aprašomas dokumentuose CPS ir CP;

7. Kliento įsipareigojimai ir atsakomybė.

7.1 Pateikdamas užklausą sertifikatui gauti klientas sutinka:

- 7.1.1. pateikti tikslią ir visą informaciją RA, kaip to reikalauja CPS;
- 7.1.2. naudoti viešojo ir privaciojo raktų porą tik CPS ir CP nurodytiems tikslams, laikantis sertifikate nurodytų apribojimų;
- 7.1.3. leisti naudoti ir saugoti šiuos asmens duomenis: asmens kodą, vardą, pavardę, asmens tapatybės dokumento (paso, tapatybės kortelės) ar leidimo gyventi Lietuvoje numerį, telefono numerį, el. pašta;
- 7.1.4. leisti 7.1.3 p. nurodytus asmens duomenis perduoti kitoms informacinėms sistemoms ir Registrų centro partneriams su sąlyga, kad asmens duomenys bus perduodami tik siekiant įgyvendinti sutartį bei užtikrinti visavertišką sertifikatų panaudojimą;
- 7.1.5. tinkamai pasirūpinti, kad jo privaciojo raktu nepasinaudotų kiti asmenys;
- 7.1.6. sertifikatą naudoti tik parašams, kuriamiems eIDAS reikalavimus atitinkančia saugia formavimo įranga, tvirtinti;
- 7.1.7. nedelsiant, bet ne vėliau kaip per 12 valandų, informuoti Registrų centro sertifikavimo tarnybą, kai sertifikato galiojimo laikotarpiu atsitinka bent vienas iš šių įvykių:
- 7.1.8. pametamas, pavagiamas ar kitaip sukompromituojamas privatusis raktas;
- 7.1.9. atskleidžiami privaciojam raktui panaudoti reikalingi identifikavimo duomenys (SPIN kodas, kt.);
- 7.1.10. pastebimi netikslumai sertifikate arba jame prireikia daryti pakeitimus;
- 7.1.11. privaciojo rakto kompromitacijos atveju, nedelsiant nutraukti jo naudojimą;

8. Sertifikato priėmimas.

Sertifikatas laikomas kliento priimtu/patvirtintu po sertifikato aktyvavimo procedūros įvykdymo.

9. Sertifikato galiojimo terminai ir apmokėjimo sąlygos.

Klientui išduotas sertifikatas galioja 3 (tris) metus. Sertifikato galiojimas nutraukiamas užblokavus kriptografinių raktų laikmeną. Klientas apmoka už sertifikavimo paslaugas pagal RA pateikiamas sąskaitas.

10. Sertifikato laikinas sustabdymas.

Klientų sertifikato laikinas sustabdymas neatliekamas.

11. Atsakomybės apribojimai.

CA atsakomybės teiginiai, išdėstyti dokumentuose CPS ir CP, yra taikomi visiems ieškiniams, kylantiems dėl sertifikatų ir sertifikavimo paslaugų, atliekamų iš CA ir RA pusės, teikimo. Atsakomybės apribojimai yra taikomi visiems ieškiniams prieš CA ir/ar RA. Apribojimai taikomi konkrečiam sertifikatui, nežiūrint į tai, kiek operacijų atliktą, kiek dokumentų pasirašyta, kiek įvyko priežastinių pasekmių ar kiek suteikta paslaugų dėl sertifikato panaudojimo. Šie apribojimai yra taikomi bet kokiam atsakomybei, kylančiai dėl sutarčių, civilinės teisės pažeidimų (įskaitant aplaidumą) ar atsakomybei pagal Lietuvos Respublikos įstatymus.

12. Duomenų apsauga ir privatumas.

Klientas suteikia teisę viešai publikuoti duomenis, pažymėtus kaip „sertifikato informacija“ ir „sertifikato statusas“. Šis publikavimas bus atliekamas internete ar kitomis CA pasirinktomis priemonėmis tam, kad būtų teikiamos sertifikavimo paslaugas. Klientas suteikia teisę CA ar RA atskleisti bet kokią su sertifikatais susijusią informaciją, kaip būdą išsiaiškinti sertifikatų patikimumą arba išsiaiškinti sertifikatų bei jais paremtų elektroninių parašų juridinės galios statusą, nežiūrint į tai, jog konkretus sertifikatas yra galiojantis, sertifikato galiojimas nutrauktas arba jo galiojimo laikas pasibaigęs.

13. Nuostolių padengimas.

Klientas įsipareigoja padengti nuostolius ir atleisti nuo atsakomybės CA, RA, jų vadovus bei darbuotojus, agentus ar susijusius asmenis, jei klientas naudoja sertifikatus kitiems tikslams ar pažeidžia sertifikatų naudojimo taisykles, kaip tai numatyta Bendrosiose sąlygose ir su jomis susijusiose dokumentuose.

14. Elektroninės sutartys.

Pasirašydamas Bendrąsias sąlygas bei sutartį dėl kvalifikuoto elektroninio parašo paslaugų teikimo, klientas sutinka, jog sutarčių sudarymas, pranešimų siuntimas ir komunikacija gali būti atliekami elektroniniais būdais.

15. Nutraukimas.

Sutartį dėl elektroninio parašo paslaugų teikimo gali nutraukti bet kuri iš pasirašiusių šalių bet kuriuo metu. Sutartis yra nutraukiama, jei pasikeitė kliento informacija, pateikta šios sutarties duomenų laukeliuose 1, 3 arba 8. Visais atvejais kliento sumokėti mokesčiai negražinami.

16. Vientisumas.

Jei bet kuris Bendrųjų sąlygų punktas, sakiny ar frazė yra pripažįstami kaip negaliojantys ar prieštaraujantys įstatymams, tuomet tai neįtakoja kitų Bendrųjų sąlygų punktų, sakinių ar frazių galiojimo.

17. Taikoma teisė.

Bendrosios sąlygos bei sutartis dėl kvalifikuoto elektroninio parašo paslaugų teikimo yra interpretuojamos pagal Lietuvos Respublikos įstatymus ir šalys sutinka vadovautis išskirtinai Lietuvos teismų jurisdikcija.

18. Asmens duomenų tvarkymo nuostatos.

18.1 Kliento asmens duomenys tvarkomi siekiant išduoti kvalifikuotą elektroninį parašą bei įgyvendinti šią sutartį. Asmens duomenų tvarkymo teisinis pagrindas – asmens duomenis tvarkyti būtina siekiant įvykdyti sutartį, kurios šalis yra sertifikato savininkas (Bendrojo

- 6.6** CA ir/arba RA gali atsisakyti klientui suteikti sertifikavimo paslaugas, nepaaiškinant savo tokio atsisakymo priežasčių;
- 6.7** Sertifikato galiojimas nutraukimas:
- 6.7.1 kliento prašymu;
 - 6.7.2. paaiškėjus, kad sertifikato duomenys neteisingi;
 - 6.7.3. paaiškėjus, kad sertifikatas buvo sudarytas remiantis neteisingais duomenimis;
 - 6.7.4. sertifikatą sudariusi CA nutraukia savo veiklą ir jos kitas sertifikavimo paslaugų teikėjas neperima sertifikavimo veiklos;
 - 6.7.5. CA ar RA sprendimu, nustačius, jog klientas nesilaiko sertifikato naudojimo sąlygų;
 - 6.7.6. klientui praradus sertifikatą atitinkančių parašo formavimo duomenų kontrolę;
 - 6.7.7. remiantis sertifikato galiojimo apribojimais numatytais sertifikate jį sudarant (jei buvo nurodyti);
 - 6.7.8. kai klientas nutraukia sutartį su RA;
 - 6.7.9. kai pažeidžiamas CA privačiojo rakto ir naudojamos sertifikato tvarkymo sistemos saugumas ir kyla pavojus sudaryto sertifikato patikimumui;
 - 6.7.10. gavus informacijos, jog klientas tapo neveiksnius;
 - 6.7.11. gavus informacijos, jog klientas mirė;
 - 6.7.12. Buvo prarasta/pažeista privataus rakto kontrolė dėl "signataro PIN" (toliau vadinamas sPIN) kodo vagystės ar dėl kitų priežasčių;
- 6.8** Sertifikate pateikiami asmens duomenys (vardas, pavardė, asmens tapatybės kodas) yra traktuojami kaip vieša informacija, pasiekiami trečiosioms šalims;
- 6.9** CA sprendžia visus ginčus, susijusius su nesutarimais, liečiančiais sertifikavimo paslaugas, CA suteiktus sertifikatus ir elektroninius parašus, patvirtintus šiais sertifikatais. Bet kokios užklauskos, skundai, ieškiniai ar įspėjimai į CA patenka per RA, kuris gautą informaciją nukreipia į CA.

duomenų apsaugos reglamento 6 str. 1 d. b p.). Sertifikatų savininko pateiktų asmens duomenų valdytojas yra valstybės įmonė Registrų centras (buveinės adresas Vinco Kudirkos g. 18-3, 03105 Vilnius). Vykdamas minėtą kvalifikuoto elektroninio parašo paslaugų teikimo sutartį, RA veikia kaip CA įgaliotas duomenų tvarkytojas.

18.2. Asmens duomenys bus saugomi 10 (dešimt) metų po sutarties pasibaigimo.

18.3. Asmens duomenys gali būti perduodami trečiajai šaliai tik gavus sertifikatų savininko sutikimą, išskyrus atvejus, kai duomenų perdavimą nustato teisės aktai.

18.4. Klientas turi teisę:

18.4.1. prašyti, kad duomenų valdytojas leistų susipažinti su tvarkomais asmens duomenimis;

18.4.2. reikalauti ištaisyti netikslius asmens duomenis;

18.4.3. reikalauti ištrinti („teisė būti pamirštam“) asmens duomenis, jei jie nėra reikalingi, kad būtų pasiekti tikslai, dėl kurių buvo tvarkomi, arba asmens duomenys buvo tvarkomi neteisėtai;

18.4.4. apriboti, išskyrus saugojimą, asmens duomenų tvarkymo veiksmus, kai duomenys tvarkomi netiksliai;

18.4.5. pateikti skundą Valstybinei duomenų apsaugos inspekcijai.

18.5 Duomenų apsaugos pareigūno kontaktiniai duomenys:

18.5.1. duomenų valdytojo el. p.: duomenusauga@registrucentras.lt;

18.5.2. duomenų tvarkytojo el. p.: dpo.lt@tele2.com