Asutuse sertifikaatide kasutustingimused (ASKT)

Kehtiv alates 20.06.2014

MÕISTED

Asutuse sertifikaat (ka sertifikaat) - digitaalsed andmed, mis on välja antud võimaldamaks digitaalse dokumendi tervikluse kinnitamist, digitaalse dokumendiga seotuse tõestamist, seadmetuvastust, turvalise andmeedastuse tagamist, tarkvara signeerimist ja/või andmete krüpteerimist ja mille avalikud võtmed on seotud üheselt juriidilise isikuga, kellele sertifikaat kuulub.

SK – sertifitseerimisteenuse osutaja, AS Sertifitseerimiskeskus.
Sertifikaadi omanik – juriidiline isik, kelle andmed on sertifikaati kantud.
CP – (Certificate Policy) asutuse sertifikaatide sertifitseerimispoliitika. Reeglid, mille alusel SK teostab vastavat sertifitseerimisteenust (dokument on leitav SK koduleheküljelt www.sk.ee repositooriumist).
CPS - (Certification Practice Statement) Sertifitseerimispõhimõtted on raamdokument, mis kirjeldab SK tegevust sertifitseerimisteenuse osutamisel, sealhulgas teenusega seotud mõisteid ja protseduure (dokument on leitav SK koduleheküljelt www.sk.ee repositooriumist).

1. ÜLDTINGIMUSED

1.1. SK väljastab juriidilistele isikutele sertifikaate (edaspidi: klient) digitaalseks tembeldamiseks, digitaalseks seadmetuvastuseks, turvalise andmeedastuse tagamiseks, tarkvara signeerimiseks ja andmete krüpteerimiseks ning osutab teenust sertifikaatide kehtivuse kontrollimise võimaldamiseks ning sertifikaatide kehtivuse peatamiseks, kehtivuse peatatuse lõpetamiseks ja kehtetuks tunnistamiseks (sertifitseerimisteenuse osutamine)

1.2. Veebiserveri sertifikaate väljastatakse kliendile, kellele kuuluvate seadmete domeeninimed ja/või aadressid on registreeritud vastavates avalikes andmebaasides (juhul, kui seade on kättesaadav üldkasutatava arvutivõrgu kaudu).

1.3. Sertifikaadi taotlemiseks kohustub kliendi seaduslik esindaja või tema poolt volitatud isik esitama taotluse elektroonilisel kujul, mis võimaldab kontrollida kliendi esindaja isikusamasust ning taotlust esitades kinnitab ta esitatud andmete õigsust ning võtab täieliku vastutuse ebaõigete andmete esitamise eest.

1.4. Esmaseks eelduseks taotluse rahuldamisel on kliendi seaduslike esindajate ning veebiserveri seadme administraatori identiteedi taotlusele vastavuse kontroll ning vajadusel avalike andmebaaside positiivne vastus seadme ja domeeninime seotuse kohta.

1.5. SK-l on õigus ASKT-d ja CP-d muuta igal ajal kui selleks tekib SK seisukohalt põhjendatud vajadus. Info muudatustest avaldatakse SK koduleheküljel http://www.sk.ee/.

1.6. ASKT ning CP on sertifikaadi omanikuga siduvad kogu sertifikaadi kehtivusaja jooksul ning ka pärast selle kehtetuks tunnistamist seni, kui sel ajahetkel kehtinud sertifikaadiga tehtud toimingutest on tekkinud õiguslikud tagajärjed ning nende vaidlustamine ei ole aegunud.

2. SERTIFIKAADI OMANIKU ÕIGUSED JA KOHUSTUSED

2.1. Sertifikaadi omanikul on õigus ja kohustus kasutada sertifikaate vastavalt kehtivatele asutuse sertifikaatide kasutustingimustele ja digitaalallkirja seadusele. SK ei vastuta kliendile väljastatud sertifikaadi kasutamisest tulenevate mistahes tagajärgede eest.

2.2. Sertifikaadi omanik kohustub kaitsma sertifikaadi salajast võtit parimal võimalikul viisil. Digitaalse templi sertifikaadi omanik kohustub hoidma salajast võtit turvalises allkirja andmise vahendis (HSM, krüptopulk, kiipkaart).

2.3. Juhul, kui sertifikaadi salajane võti on väljunud sertifikaadi omaniku kontrolli alt või on tekkinud selline oht, kohustub sertifikaadi omanik esitama SK-le koheselt taotluse kliendile väljastatud sertifikaadi peatamiseks (ainult digitaalse templi puhul) või kehtetuks tunnistamiseks.

2.4. Sertifikaadi omanik kohustub sertifikaadi kehtetuks tunnistamisel kontrollima vastava kande olemasolu tühistusnimekirjas.

2.5. Sertifikaadi omanik kohustub koheselt SK-d teavitama kontaktisikute vahetumisest.

2.6. Sertifikaadi omanik kohustub koheselt teavitama SK-d tema suhtes alustatud pankrotimenetlusest, asutuse likvideerimisest või tegevuse peatamisest või muust sellesarnasest olukorrast oma asukohariigi seadusandluse mõistes.
2.7. Sertifikaadi omanik kohustub koheselt teavitama SK-d, kui sertifikaadis märgitud serveri ja/või seadme nimi või IP aadress on muutunud.

3. SK ÕIGUSED JA KOHUSTUSED

3.1. SK-l on õigus sertifikaadi väljastamisest keelduda CP-s toodud alustel.
3.2. SK-l on õigus enda poolt väljastatud sertifikaadid omaalgatuslikult kehtetuks tunnistada digitaalallkirja seadusest ja CP-st tulenevatel alustel. Sertifikaadid tunnistatakse kehtetuks juhul, kui:
- Sertifikaat ei ole väljastatud CP või CPS-i alusel;
- SK saab teate või on muul viisil teada saanud, et Klient on rikkunud ühte või mitut ASKT ja/või CP järgset olulist kohustust;
- Klient teatab, et esialgne sertifikaadi taotlus ei olnud volitatud ja Klient ei anna tagasiulatuvalt volitust;
- SK saab piisavad tõendid, et Kliendi salajane võti (mis vastab sertifikaadi avalikule võtmele) on väljunud Kliendi kontrolli alt või on tekkinud selline oht või seda sertifikaati on muul viisil väärkasutatud;
- Kui sertifikaadi omanik on esitanud ebaõigeid andmeid või andmed on oluliselt muutunud ja sertifikaadi omanik ei ole esitanud avaldust andmete muutmiseks või parandamiseks;
- SK saab teate või on muul viisil teada saanud, mis tahes asjaolust, mis viitab sellele, et sertifikaadi domeeninime ja/või IP-aadressi kasutus ei ole enam õiguslik (näiteks kohus on tühistanud Kliendi õiguse kasutada domeeninime mis on sertifikaadis, asjakohane suhe registri ja domeeni omaniku vahel on lõpetatud);
- SK saab teada, et sertifikaati on kasutatud kuriteo toimepanemiseks, nagu näiteks arvutikelmus, nuhkvara, pahavara ja arvutiviiruse levitamine jne;
- Kui sertifikaadi omanik ei ole määratud aja möödudes tasunud sertifikaadi väljastamise eest;
- SK lõpetab tegevuse mistahes põhjusel ja ei ole organiseerinud teist sertifitseerimisteenuse pakkujat sertifikaatide tühistusteenust pakkuma;
- On tekkinud kahtlus, et SK salajane võti, mida kasutati sertifikaadi väljastamiseks, on väljunud SK kontrolli alt.

3.3. SK esitab taotlejale keeldumise ning sertifikaadi omanikule sertifikaadi(tide) kehtetuks tunnistamise põhjuse kirjalikult.

4. VASTUTUS

4.1. Sertifikaadi omanik vastutab mistahes kahju eest, mis tekkis ASKT-s, CP-s ja/või Eesti Vabariigi õigusaktides fikseeritud kohustuste täitmata jätmise või mittenõuetekohase täitmise tõttu.
4.2. Sertifikaadi omanik vastutab kliendile eraldatud kehtivate sertifikaatide kasutamisest tulenevate mistahes tagajärgede eest ainuisikuliselt ning täies ulatuses.
4.3. Sertifikaadi omanik on teadlik, et aegunud ja/või kehtetuks tunnistatud sertifikaadi alusel tehtud toimingud on kehtetud.
4.4. SK ei vastuta, kui temast mitteolenevatel põhjustel (vääramatu jõud, kolmanda osapoole tegevus/tegevusetus) ei saa sertifikaadi omanik sertifikaate kasutada; huvitatud osapool kontrollida sertifikaatide kehtivust või pole võimalik teostada muud päringut/toimingut.
4.5. SK vastutab sertifitseerimisteenuse osutajale seadustega pandud kohustuste täitmise või täitmata jätmise eest.

5. SERTIFIKAADI KEHTIVUS JA KEHTIVUSE KONTROLL

5.1. Sertifikaat hakkab kehtima sertifikaadis märgitud kehtivusaja algusest, kuid mitte enne sertifikaadi kandmist SK poolt peetavasse kehtivate sertifikaatide andmebaasi.

5.2. Sertifikaadi kehtivus lõpeb sertifikaati märgitud kehtivuse aegumisel või sertifikaadi kehtetuks tunnistamisel.
5.3. SK on kohustatud sertifikaadi kehtivuse peatama (ainult digitaalse templi sertifikaadi puhul) või kehtetuks tunnistama, kui seda nõuab sertifikaadi omanik või muudel seadustes sätestatud aluste olemasolul.
5.4. SK-l on õigus peatada sertifikaadi kehtivus (ainult digitaalse templi sertifikaadi puhul) või sertifikaat tühistada, kui tal tekib põhjendatud kahtlus, et sertifikaati on kantud ebaõiged andmed või sertifikaat on sertifikaadi omaniku kontrolli alt väljas ja seda on võimalik kasutada ilma tema nõusolekuta.
5.5. SK teavitab sertifikaadi kehtivuse peatamisest (ainult digitaalse templi sertifikaadi puhul) või tühistamisest viivitamatult sertifikaadi omanikku. Juhul kui sertifikaadi kehtivust ei peatanud või tühistanud sertifikaadi omanik, edastatakse teade sertifikaadi omaniku kontaktisiku e- posti aadressile.
5.6. Sertifikaatide kehtivuse kontrollimiseks on võimalik kasutada tühistusnimekirja. Tühistusnimekirja alusel kontrolli teostamisel on huvitatud osapool kohustatud lähtuma kõige uuemast tühistusnimekirjast. Tühistusnimekiri sisaldab peatatud kehtivusega ja kehtetuks tunnistatud sertifikaate, nende kehtivuse muutmise aega ja põhjust. Tühistusnimekirju avaldatakse perioodiliselt iga 12 tunni järel SK koduleheküljel https://www.sk.ee/repositoorium/crl/.

6. ANDMETE TÖÖTLEMINE

6.1. SK töötleb sertifikaadi omaniku isikuandmeid vastavalt isikuandmete kaitse seadusele ja muudele Eesti Vabariigi seadustele. SK Kliendiandmete kaitse põhimõtted on avaldatud SK koduleheküljel http://www.sk.ee/ettevottest/andmekaitse.
6.2. Sertifikaadi omanik on teadlik ja nõustub enda nimetuse ja registrikoodi avaldamisega kehtivate sertifikaatide andmebaasis.
6.3. SK-l on õigus avaldada infomatsiooni sertifikaadi omaniku kohta kolmandale isikule, kelle õigus informatsiooni saada tuleneb Eesti Vabariigi seadustest.
6.4. Sertifikaadi omanik on teadlik sellest, et kasutades sertifikaate digitaalse dokumendi terviklikkuse kinnitamiseks, lisatakse digitaalselt kinnitatud dokumendile tema sertifikaat, milles sisalduvad tema nimetus ja registrikood.