

# Kvalifitseeritud Smart-ID sertifikaatide kasutustingimused

Tõlge AS Sertifitseerimiskeskuse originaaldokumendile "Terms and Conditions for Use of Certificates of Qualified Smart-ID"

Kehtiv alates 01.01.2017

## 1. Määratlused ja lühendid

Termin/Lühend	Definitsioon
Autentimine	Unikaalne isiku identifitseerimine kontrollides tema väidetavat identiteeti.
Autentimissertifikaat	Autentimiseks ja krüpteerimiseks mõeldud sertifikaat.
CA	Sertifitseerimisasutus
Sertifikaat	Avalik võti koos täiendava teabega, mis on määratud sertifikaadi profiilis ja muudetud võltsimiskindlaks krüpteerimise kaudu, kasutades sertifitseerimisasutuse poolt väljastatud isiklikku võtit.
Sertifitseerimisasutus (CA)	SK struktuuriüksus, mis vastutab elektrooniliste sertifikaatide ning sertifikaatide tühistusnimekirjade väljastamise ja kontrollimise eest oma elektroonilise allkirjaga.
CP	Kvalifitseeritud Smart-ID sertifitseerimispoliitika.
CPS	AS Sertifitseerimiskeskus – EID-SK sertifitseerimise põhimõtted.
Smart-ID teenusepakkuja	Organisatsioon, mis on juriidiliselt vastutav Smart-ID süsteemi toimimise eest. Smart-ID teenusepakkuja on SK.
Smart-ID süsteem	Tehniline ja organisatsiooniline keskkond, mis võimaldab elektroonilist autentimist ja elektrooniliste allkirjade andmist elektroonilises keskkonnas. Smart-ID süsteem pakub teenuseid, mis võimaldavad klientidel (konto omanikel) ennast e-teenuste osutajate juures autentida, anda e-teenuste osutajate poolt nõutavaid elektroonilisi allkirju ja hallata oma Smart-ID kontosid.
eIDAS määrus	Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ.
E-teenuse pakkuja	Kolmas isik, kes kasutab Smart-ID süsteemi teenuseid klientide autentimiseks ja lubamaks klientidel elektrooniliselt allkirjastada dokumente või tehinguid.
Abiliin	Abiliin pakub kasutajatuge Q Smart-ID kasutamisest tekkinud probleemide lahendamiseks. Abiliin võtab klientidelt vastu taotlusi Q Smart-ID sertifikaatide tühistamiseks.
OCSP	Protokoll sertifikaadi kehtivuse kontrolliks.
OID	Objekti identifikaator.
PIN-kood	Autentimissertifikaadi ja kvalifitseeritud elektroonilise allkirja sertifikaadi aktiveerimiskood.
Isiklik võti	Võti võtmepaarist, mida võtmepaari omanik hoiab salajas ja mida kasutatakse elektrooniliste allkirjade loomiseks ja/või selliste elektrooniliste dokumentide või failide dekrüpteerimiseks, mida krüpteeriti vastava avaliku võtmega. Smart-ID süsteemis ei genereerita kunagi isikliku võtme väärtust tervikuna ja isiklik võti eksisteerib üksnes osadeks jaotatuna.
Avalik võti	Võtmepaar, mida vastava isikliku võtme omanik võib avalikustada ja mida huvitatud isik kasutab selleks, et tõendada omaniku vastava isikliku võtmega elektroonilisi allkirju ja/või krüpteerida teateid sellisel, et neid saaks dekrüpteerida vaid omaniku vastava isikliku võtmega. Avalik võti eksisteerib Smart-ID süsteemis üksnes osadeks jaotatuna ja koosneb järgmistest osadest: rakenduses ja serveris asuvatest osadest.
Q Smart-ID	Q Smart-ID on uue põlvkonna elektrooniline ID, mis võimaldab kliendil end elektrooniliselt autentida ja anda kvalifitseeritud elektroonilise allkirja.
Kvalifitseeritud elektrooniline allkiri	Täiustatud elektrooniline allkiri, mis luuakse kvalifitseeritud elektroonilise allkirja andmise vahendiga ja mis põhineb elektrooniliste allkirjade kvalifitseeritud sertifikaadil.

QSCD	Turvalise allkirja andmise vahend, mis vastab eIDAS määruses kehtestatud nõuetele.
Huvitatud isik	Isik, kes toetub sertifikaadis sisalduvale teabele.
SK	AS Sertifitseerimiskeskus, sertifitseerimisteenuste osutaja.
SK PS	AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted.
SLA	Teenustaseme leping.
Klient	Füüsiline isik, kellele on väljastatud Q Smart-ID sertifikaadid.
Kasutustingimused	Käesolev dokument, mis kirjeldab kliendi kohustusi ja vastutust sertifikaatide kasutamisel.

## 2. Üldtingimused

- 2.1. Käesolevad Kasutustingimused kirjeldavad peamisi poliitikaid ja põhimõtteid, mida SK järgib ja mis on esitatud Q Smart-ID sertifitseerimispoliitikas, sertifitseerimispõhimõtetes ja SK usaldusteenuste põhimõtetes.
- 2.2. Kasutustingimused reguleerivad Sertifikaatide kasutamist Kliendi poolt ning moodustavad Kliendi ja SK vahel õiguslikult siduva kokkuleppe.
- 2.3. Klient peab olema Kasutustingimustega tuttav ja nendega Sertifikaatide kättesaamisel nõustuma.
- 2.4. SK-l on õigus muuta Kasutustingimusi igal ajal, kui SK peab nende muutmist põhjendatuks. Teave muudatuste kohta avaldatakse veebilehel <https://sk.ee/>.
- 2.5. Klient saab taotleda Q Smart-ID-d üksnes isiklikult. Q Smart-ID-d ei väljastata esindajale.

## 3. Sertifikaadi vastuvõtmine

- 3.1. Q Smart-ID Sertifikaadi taotluse esitamisel kinnitab Klient, et ta on tutvunud ja nõustub Kasutustingimustega. Vastavat kinnitust loetakse Q Smart-ID Sertifikaadi vastuvõtmiseks.
- 3.2. Sertifikaadi võtmevahetuse korral kinnitab Klient, et ta on läbi lugenud Kasutustingimused ja nõustub nendega.

## 4. Sertifikaatide liigid ja kasutamine

Sertifikaadi liik	Kasutamine	Kohalduv ja avaldatud sertifitseerimispoliitika	OID	Kokkuvõte
Smart-ID sertifikaadid	Kvalifitseeritud elektroonilise allkirja sertifikaadi kasutamine:	AS Sertifitseerimiskeskus – kvalifitseeritud Smart-ID sertifitseerimispoliitika, avaldatud <a href="https://sk.ee/repositoorium/CP/">https://sk.ee/repositoorium/CP/</a>	1.3.6.1.4.1.10015.17.2	interneti tunnus (1.3.6.1) eraettevõtte tunnus(4) eraettevõtteid haldava IANA poolt registreeritud ettevõtte tunnus(1) IANA registris SK-le antud tunnus (10015) sertifitseerimisteenuse tunnus (17.2)
	eIDAS määrusega vastavuses olevate kvalifitseeritud elektrooniliste allkirjade loomiseks	ETSI EN 319 411-2 poliitika: QCP-n-qscd	0.4.0.194112.1.2	itu-t(0) identifitseeritud-asutus (4) etsi(0) kvalifitseeritud-sertifikaadi-poliitikad (194112) poliitika-identifikaatorid (1) qcp-natural-qscd(2)
	Autentimis-sertifikaadi kasutamine:	AS Sertifitseerimiskeskus – kvalifitseeritud Smart-ID sertifitseerimispoliitika, avaldatud <a href="https://sk.ee/repositoorium/CP/">https://sk.ee/repositoorium/CP/</a>	1.3.6.1.4.1.10015.17.2	interneti tunnus (1.3.6.1) eraettevõtte tunnus(4) eraettevõtteid haldava IANA poolt registreeritud ettevõtte tunnus(1) IANA registris SK-le antud tunnus (10015) sertifitseerimisteenuse tunnus (17.2)
	autentimiseks, krüpteerimiseks.	ETSI EN 319 411-1 poliitika: NCP+	0.4.0.2042.1.2	itu-t(0) identifitseeritud-asutus(4) etsi(0) muud-sertifikaadi-poliitikad(2042) poliitika-identifikaatorid(1) ncplus (2)

- 4.1. Kliendi sertifikaate on keelatud kasutada järgmistel eesmärkidel:
  - 4.1.1. ebaseaduslikuks tegevuseks (sealhulgas küberrünnakuteks ja katseks rikkuda Q Smart-ID Sertifikaati);
  - 4.1.2. uute Sertifikaatide ja Sertifikaatide kehtivuse info väljastamiseks;
  - 4.1.3. võimaldamaks teistel kasutada Kliendi Isikliku võtit;
  - 4.1.4. võimaldamaks kasutada elektrooniliseks allkirjastamiseks väljastatud Sertifikaadi automaatsel viisil;
  - 4.1.5. kasutada elektrooniliseks allkirjastamiseks väljastatud Sertifikaati selliste dokumentide allkirjastamiseks, mis võivad kaasa tuua soovimatuid tagajärgi (sealhulgas selliste dokumentide allkirjastamiseks testimise eesmärkidel).
- 4.2. Kliendi Autentimissertifikaati ei saa kasutada eIDAS määrusega vastavuses olevate Kvalifitseeritud elektrooniliste allkirjade loomiseks.

## 5. Sertifikaadi kasutusiga ja kontrolljälgede säilitamine

- 5.1. Sertifikaadid hakkavad kehtima Sertifikaadis määratud kuupäeval.
- 5.2. Sertifikaat kaotab kehtivuse Sertifikaadis määratud kuupäeval või Sertifikaadi tühistamisel.
- 5.3. Kontrolljälgi säilitatakse kohapeal vähemalt 10 aastat. Füüsilisi või digitaalseid arhiivmaterjale Sertifikaadi taotluste ja registreerimisteebe ning taotlusi tühistamise kohta säilitatakse vähemalt 10 aastat pärast vastava Sertifikaadi aegumist.

## 6. Kliendi õigused ja kohustused

- 6.1. Kliendil on õigus esitada taotlus Q Smart-ID Sertifikaadi väljastamiseks.

- 6.2. Klient on kohustatud:
  - 6.2.1. nõustuma Kasutustingimustega;
  - 6.2.2. pidama kinni SK sätestatud nõuetest;
  - 6.2.3. kasutama oma Isikliku võtit ja Sertifikaati vastavalt Kasutustingimustele, sealhulgas vastavalt punktis 10 toodud kohaldatavatele kokkulepetele ning Eesti Vabariigi ja Euroopa Liidu õigusaktidele;
  - 6.2.4. tagama, et tema Isikliku võtme kasutamine toimuks tema kontrolli all;
  - 6.2.5. esitama Smart-ID süsteemile õiget ja täpset teavet;
  - 6.2.6. oma isikuandmete muutumisel mõistliku aja jooksul teatama Smart-ID teenusepakkujale õiged andmed;
  - 6.2.7. viivitamatult teavitama SK-d oma Isikliku võtme võimalikust volitamata kasutamisest ja tühistama oma Sertifikaadid;
  - 6.2.8. viivitamatult tühistama oma Sertifikaadid, kui tema Isiklik võti on väljunud tema kontrolli alt.
7. **SK õigused ja kohustused**
  - 7.1. SK on kohustatud:
  - 7.2. osutama sertifitseerimisteenust kooskõlas punktis 10 toodud kokkulepete ja kohalduvate õigusaktidega;
  - 7.3. pidama arvet tema poolt väljastatud Sertifikaatide ja nende kehtivuse üle;
  - 7.4. tagama turvalisuse oma sisemiste turvaprotseduuride abil;
  - 7.5. pakkuma ööpäevaringselt võimalust Sertifikaatide kehtivuse kontrollimiseks;
  - 7.6. tagama, et sertifitseerimisvõtmed on kaitstud riistvara turvamoodulitega (HSM-ga) ja need on SK ainuisikulise kontrolli all;
  - 7.7. tagama, et sertifitseerimisteenuste osutamiseks kasutatavad sertifitseerimisvõtmed aktiveeritakse jagatud kontrolli alusel.
8. **Huvitatud isiku kohustused sertifikaadi staatuse kontrollimisel**
  - 8.1. Huvitatud isik uurib Sertifikaadi vastuvõtmisega seotud riske ja kohustusi. Riskid ja kohustused on sätestatud CPS-s ja CP-s.
  - 8.2. Kui Sertifikaat või elektrooniline allkiri ei sisalda piisavalt tõendeid Sertifikaadi kehtivuse kohta, kontrollib Huvitatud isik Sertifikaadi kehtivust Sertifikaadi kasutamise või Kvalifitseeritud elektroonilise allkirja lisamise hetkel SK poolt pakutud Sertifikaadi staatust kontrollida võimaldavate teenuste alusel.
  - 8.3. Huvitatud isik järgib Sertifikaadi sees sätestatud piiranguid ja veendub, et vastuvõetav toiming on kooskõlas CPS-i ja CP-ga.
  - 8.4. SK tagab Sertifikaadi staatust kontrollida võimaldavate teenuste kättesaadavuse 24 tundi päevas ja 7 päeva nädalas. Viidatud teenuste kättesaadavus on aastas minimaalselt 99,44% ja kavandatud seisakuueg ei ületa iga-aastaselt 0,28%.
  - 8.5. SK pakub Sertifikaadi staatuse kontrollimiseks OCSP teenust. Teenus on kättesaadav üle HTTP protokolliga.
  - 8.6. Huvitatud isik tuvastab Sertifikaadi kehtivuse kontrollides seda vastu OCSP-d. Sertifikaadi kehtivuse kontrollimiseks pakub SK OCSP teenust järgnevalt:
    - 8.6.1. avalikult ja tasuta veebilehe <http://aia.sk/eid2016> kaudu;
    - 8.6.2. lepingu ja hinnakirja alusel. Sellisel juhul pakub SK OCSP teenust parema SLA-ga kui on punktis 8.6.1 toodud teenusel;
    - 8.6.3. OCSP teenuse URL kantakse Sertifikaati *Authority Information Access (AIA)* väljale kooskõlas Sertifikaadi profiiliga.
9. **Vastutus**
  - 9.1. Klient vastutab ainuisikuliselt oma Isikliku võtme haldamise eest.
  - 9.2. Klient vastutab ainuisikuliselt ja täielikult Autentimise ja elektroonilise allkirja andmisega kaasnevate tagajärgede eest Sertifikaatide kehtivuse ajal kui ka pärast seda.
  - 9.3. Klient vastutab ainuisikuliselt igasuguse kahju eest, mis tuleneb Kasutustingimustest ja/või Eesti Vabariigi seadustes sätestatud kohustuste täitmata jätmisest või nende sobimatust täitmisest.
  - 9.4. Klient on teadlik, et aegunud või tühistatud Sertifikaatide alusel antud elektroonilised allkirjad on kehtetud.
  - 9.5. SK tagab, et:
    - 9.5.1. sertifitseerimisteenuse osutamine toimub kooskõlas CPS-i ja CP-ga ning Eesti Vabariigi ja Euroopa Liidu õigusaktidega;
    - 9.5.2. sertifitseerimisvõtmed on kaitstud riistvara turvamoodulitega (HSM-ga) ja need on SK ainuisikulise kontrolli all;
    - 9.5.3. sertifitseerimisteenuse osutamiseks kasutatavad sertifitseerimisvõtmed aktiveeritakse jagatud kontrolli alusel;
    - 9.5.4. tal on kohustuslikud kindlustuslepingud, mis katavad kõiki SK teenuseid ja tagavad SK kohustuste rikkumise tagajärjel tekitatud kahjude hüvitamise;
    - 9.5.5. enne sertifitseerimisteenuste osutamise lõpetamist teavitab ta vastavast asjaolust kõiki oma Kliente ja säilitab lõpetatud sertifitseerimisteenustega seotud vajalikku dokumentatsiooni ja informatsiooni kooskõlas CPS-s sätestatud protsessiga.
  - 9.6. SK ei vastuta:
    - 9.6.1. Kliendi Isiklike võtmete salajas hoidmise, mistahes Sertifikaatide väärkasutuse või Sertifikaatide ebapiisava kontrollimise või Huvitatud isiku valede otsuste eest või mistahes tagajärgede eest, mis on põhjustatud vigadest või tegevusetusest Sertifikaadi kehtivuse kontrollimisel;
    - 9.6.2. oma kohustuste mittetäitmise eest, kui see on põhjustatud järelevalveasutuse, Andmekaitse Inspeksiooni, Usaldusnimekirja või muu asutuse süü, vigade või turvaprobbleemide tõttu;
    - 9.6.3. oma kohustuste mittetäitmise eest, kui see on põhjustatud vääramatute jõude tõttu.
10. **Kohaldatavad kokkulepped, CPS, CP**
  - 10.1. Sertifikaatide Kasutustingimustega seotud asjakohased kokkulepped, poliitika ja põhimõtted:
    - 10.1.1. AS Sertifitseerimiskeskus – kvalifitseeritud Smart-ID sertifitseerimispoliitika, avaldatud: <https://sk.ee/repositoorium/CP/>;
    - 10.1.2. AS Sertifitseerimiskeskus – EID-SK sertifitseerimise põhimõtted, avaldatud: <https://sk.ee/repositoorium/CPS/>;
    - 10.1.3. AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted, avaldatud: <https://sk.ee/repositoorium/sk-ps/>;
    - 10.1.4. Smart-ID sertifikaadi ja OCSP profiil, avaldatud: <https://www.sk.ee/repositoorium/profiil/>;
    - 10.1.5. Kliendiandmete kaitse põhimõtted, avaldatud: <https://www.sk.ee/ettevottest/andmekaitse/>.
  - 10.2. Kõikide kohalduvate dokumentide kehtivad versioonid on avalikult kättesaadavad SK repositooriumis <https://sk.ee/repositoorium/>.
11. **Privaatsuspoliitika ja konfidentsiaalsus**
  - 11.1. SK järgib isikuandmete ja kontrolljälgede töötlemisel SK lehel <https://www.sk.ee/ettevottest/andmekaitse/> toodud kliendiandmete kaitse põhimõtteid ja muid Eesti Vabariigi õigusakte.
  - 11.2. Klient teab ja nõustub, et Sertifikaatide kasutamisel Autentimise ajal saadetakse Autentimist läbi viivale isikule Kliendi Sertifikaat, mis sisaldab Kliendi nime ja isikukoodi.

- 11.3. Kogu teave, mis tuleb ilmsiks teenuste osutamisel ja mis ei ole mõeldud avalikustamiseks (näiteks teave, mida SK teab tulenevalt usaldusteenuste toimimisest ja osutamisest), on konfidentsiaalne. Kliendil on õigus saada SK-lt enda kohta teavet vastavalt seadustele.
- 11.4. SK tagab konfidentsiaalse ja asutusesiseseks kasutamiseks mõeldud teabe ohutuse ja hoidub selle teabe avaldamisest kolmandatele pooltele läbi erinevate turvameetmete rakendamise.
- 11.5. SK-l on õigus avaldada kolmandale poolele teavet Kliendi kohta, kui kolmandal poolel on tulenevalt õigusaktidest õigus vastavat teavet saada.
- 11.6. SK teenuste kohta käivad mitteisikustatud statistilised andmed on avalik teave. SK võib avaldada oma teenuste kohta käivaid mitteisikustatud statistilisi andmeid.

## 12. Tagastamispoliitika

- 12.1. SK tegeleb hüvitamise taotlustega üksikjuhul.

## 13. Kohaldatav seadus, kaebused ja vaidluste lahendamine

- 13.1. Sertifitseerimisteenust reguleerib Eesti ja Euroopa Liidu seadusandlus tulenevalt asukohast, kus SK on sertifitseerimisasutusena registreeritud.
- 13.2. Kõik poolte vahelised vaidlused lahendatakse läbirääkimiste teel. Kui pooltel ei õnnestu läbirääkimiste teel kokkuleppele jõuda, lahendatakse vaidlus SK asukoha kohtus.
- 13.3. Teist poolt teavitatakse mistahes nõudest või kaebusest hiljemalt 30 kalendripäeva jooksul pärast nõude või kaebuse aluse avastamist, välja arvatud juhul, kui seaduses on sätestatud teisiti.
- 13.4. Klient või muu pool saab esitada oma nõude või kaebuse e-posti aadressil: [info@sk.ee](mailto:info@sk.ee).
- 13.5. Kõik nõuded või kaebused tuleb edastada Kasutustingimustes toodud kontaktandmetele.

## 14. SK litsentsid, usaldusmärgid ja audit

- 14.1. Q Smart-ID sertifitseerimisteenus on kvalifitseeritud teenusena registreeritud Eesti usaldusnimekirjas: <https://sr.riik.ee/en/tsl/estonia.html>. Registreerimise eeltingimuseks on sertifitseerimisteenuse vastavus kohalduvate õigusaktide ja standarditega.
- 14.2. Vastavushindamisasutus on akrediteeritud kooskõlas määrusega (EÜ) nr 765/2008 kui pädev asutus läbi viima kvalifitseeritud usaldusteenuste osutaja ja tema osutatavate kvalifitseeritud usaldusteenuste vastavushindamist.
- 14.3. Järeldused või sertifikaadid, mis põhinevad vastavushindamise tulemustel ja on läbi viidud kooskõlas eIDAS määruse, vastavate õigusaktide ja standarditega on avaldatud SK veebilehel: <https://www.sk.ee/repositoorium/>.

## 15. Kontaktandmed

- 15.1. Usaldusteenuste osutaja  
AS Sertifitseerimiskeskus  
Registrikood 10747013  
Pärnu mnt 141, 113134  
Tallinn, EESTI  
(E-R 9.00 - 18.00, Ida-Euroopa aja järgi)  
<http://www.sk.ee/>  
Telefon +372 610 1880  
Faks +372 610 1881  
E-post: [info@sk.ee](mailto:info@sk.ee)
- 15.2. Taotlusi Q Smart-ID Sertifikaatide tühistamise kohta võetakse vastu 24/7 Abiliinil 1777 või (+ 372) 677 3377 ja/või iseteeninduses ja/või klienditeeninduspunktis.
- 15.3. Abiliini ja iseteeninduse teave ja kontaktandmed on kättesaadavad SK kodulehel <https://www.sk.ee/>.