Noteikumi un nosacījumi kvalificētu Smart-ID sertifikātu lietošanai

SK ID Solutions AS oriģinālā dokumenta ar nosaukumu „Terms and Conditions for Use of Certificates of Qualified Smart-ID“ tulkojums.

Spēkā no 01.01.2017

Definīcijas un akronīmi

Termins/akronīms	Definīcija
Autentifikācija	Personas unikāla identifikācija, pārbaudot viņa/viņas paziņoto identitāti
Autentifikācijas sertifikāts	Sertifikāts, kas paredzēts autentifikācijai un šifrēšanai.
SI	Sertificējošā iestāde
Sertifikāts	Publiskā atslēga kopā ar papildu informāciju, kas noteikta sertifikāta profilā, ir padarīta neviltojama ar šifrēšanu, izmantojot sertificējošās iestādes izsniegto privāto atslēgu.
Sertificējošā iestāde (SI)	SK struktūras daļa, kas atbild par elektronisko sertifikātu un atsaukto sertifikātu sarakstu ar savu elektronisko parakstu izsniegšanu un pārbaudi.
SP	Kvalificētu Smart-ID sertifikācijas politika.
SPP	SK ID Solutions AS – EID-SK sertifikācijas prakses paziņojums.
Smart-ID uzturētājs	Organizācija, kas ir juridiski atbildīga par Smart-ID sistēmu. SK ir Smart-ID uzturētājs.
Smart-ID sistēma	Tehniskā un organizatoriskā vide, kas padara iespējamu elektronisko autentifikāciju un elektroniskos parakstus elektroniskajā vidē. Smart-ID sistēma nodrošina pakalpojumus, kas abonentiem (kontu īpašniekiem) dod iespēju autentificēt sevi e-pakalpojumu sniedzējiem, izdot e-pakalpojumu sniedzēju pieprasītos elektroniskos parakstus un pārvaldīt savus Smart-ID kontus.
eIDAS	Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regula (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK.
E-pakalpojuma sniedzējs	Trešā persona, kas lieto Smart-ID sistēmas sniegtos pakalpojumus, lai autentificētu abonentus un abonentiem dotu iespēju elektroniski parakstīt dokumentus vai darījumus.
Palīdzības līnija	Palīdzības līnija sniedz lietotājiem atbalstu ar Q Smart-ID lietošanu saistīto problēmu risināšanā. Palīdzības līnija pieņem no abonentiem pieprasījumus Q Smart-ID sertifikātu atsaukšanai.
OCSP	Tiešsaistes sertifikātu statusa protokols
OID	Identifikators, kas piešķir objektam unikālu nosaukumu.
PIN kods	Aktivizācijas kods autentifikācijas sertifikātam un kvalificēta elektroniskā paraksta sertifikātam.
Privātā atslēga	Atslēga no atslēgu pāra, kura atslēgu pāra turētājam ir jātur slepenībā un kura tiek izmantota, lai izveidotu elektroniskos parakstus un/vai atšifrētu elektroniskos ierakstus vai failus, kas tika šifrēti ar atbilstošo publisko atslēgu. Smart-ID sistēmā pašas „privātās atslēgas“ vērtība nekad netiek ģenerēta un „privātā atslēga“ pastāv tikai tās sastāvdaļu veidā.
Publiskā atslēga	Tā atslēga no atslēgu pāra, kuru atbilstošās privātās atslēgas turētājs var publiski izpaust un kuru izmanto atkarīgās puses, lai pārbaudītu elektroniskos parakstus, kas izveidoti ar turētāja atbilstošo privāto atslēgu, un/vai lai šifrētu ziņojumus tā, lai tos varētu atšifrēt tikai ar turētāja atbilstošo privāto atslēgu. Smart-ID sistēmā publiskā atslēga pastāv tikai tās sastāvdaļu veidā un sastāv no šādām sastāvdaļām: „publiskās atslēgas lietojumprogrammas daļa“ un „publiskās atslēgas servera daļa“.
Q Smart-ID	Q Smart-ID ir jaunās paaudzes elektronisks identifikators, kas apgādā abonentu ar līdzekļiem elektroniskai autentifikācijai un ar kvalificētu elektronisko parakstu.
Kvalificēts elektroniskais paraksts	Uzlabots elektroniskais paraksts, kas izveidots ar kvalificētu elektroniskā paraksta izveides ierīci un kura pamatā ir kvalificēts sertifikāts elektroniskajiem parakstiem.
QSCD	Droša paraksta izveides ierīce, kas atbilst eIDAS Regulas noteiktajām prasībām.
Atkarīgā puse	Subjekts, kas paļaujas uz sertifikātā ietverto informāciju.
SK	SK ID Solutions AS, sertifikācijas pakalpojuma sniedzējs

SK PP	SK ID Solutions AS uzticamības pakalpojumu prakses paziņojums.
SLA	Servisa līmeņa līgums
Abonents	Pieaugusi fiziska persona ar aktīvu rīcībspēju, kurai ir izdoti Q Smart-ID sertifikāti.
Noteikumi un nosacījumi	Šis dokuments, kurā aprakstīti abonenta pienākumi un atbildība, izmantojot sertifikātus.

1. Vispārīgie noteikumi

1.1. Šajos noteikumos un nosacījumos ir aprakstītas galvenās politikas un prakses, saskaņā ar kurām rīkojas SK un kuras sniegtas SP par Q Smart-ID, SPP un SK PP (piem., Izpaušanas paziņojumā).

1.2. Noteikumi un nosacījumi reglamentē sertifikātu izmantošanas kārtību abonentam un veido juridiski saistošu līgumu starp abonentu un SK.

1.3. Abonentam ir jāpārzina un jāpieņem Noteikumi un nosacījumi.

1.4. SK ir tiesības grozīt Noteikumus un nosacījumus jebkurā laikā, ja SK ir pamatota vajadzība pēc šādiem grozījumiem. Informācija par grozījumiem tiks publicēta tīmekļa vietnē https://sk.ee/en.

1.5 Abonents var pieteikties Q Smart-ID tikai personīgi. Q Smart-ID nevar izdot pārstāvim.

2. Sertifikāta akceptēšana

2.1. Iesniedzot pieteikumu sertifikātam, kas paredzēts Q Smart-ID, abonents apliecina, ka viņš/viņa ir iepazinies ar Noteikumiem un nosacījumiem un piekrīt tiem. Atbilstošais apstiprinājums tiek uzskatīts par Q Smart-ID sertifikāta akceptēšanu.

2.2. Ja tiek veikta atkārtota sertifikāta atslēgas izsniegšana, abonents apliecina, ka viņš/viņa ir izlasījis Noteikumus un nosacījumus un piekrīt tiem.

3 Sertifikāta veids, validācijas procedūras un izmantošana

Sertifikāta veids	Izmantošana	Pielietotā un publicētā sertifikācijas politika	OID	Kopsavilkums
Smart-ID sertifikāti	Kvalificēts elektroniskā paraksta sertifikāts ir paredzēts:	SK ID Solutions AS – sertifikācijas politika kvalificētiem Smart-ID, publicēta https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.17.2	interneta atribūts(1.3.6.1) privāta subjekta atribūts(4) reģistrēta uzņēmuma atribūts, ko izdod privātās uzņēmējdarbības pārvaldnieks IANA(1) SK atribūts IANA reģistrā(10015) Sertifikācijas pakalpojuma atribūts(17.2)
	izveido eIDAS atbilstošu kvalificētu elektronisko parakstu.	ETSI EN 319 411-2 politika: QCP-n-qscd	0.4.0.194112.1.2	itu-t(0) identificēta-organizācija(4) etsi(0) kvalificētas-sertifikācijas-politikas(194112) politikas-identifikatori(1) qcp-natural-qscd(2)
	Autentifikācijas sertifikāts ir paredzēts:	SK ID Solutions AS – sertifikācijas politika kvalificētiem Smart-ID, publicēta https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.17.2	interneta atribūts(1.3.6.1) privāta subjekta atribūts(4) reģistrēta uzņēmuma atribūts, ko izdod privātās uzņēmējdarbības pārvaldnieks IANA(1) SK atribūts IANA reģistrā(10015) Sertifikācijas pakalpojuma atribūts(17.2)
	autentifikācija, šifrēšana.	ETSI EN 319 411-1 politika: NCP+	0.4.0.2042.1.2	itu-t(0) identificēta-organizācija(4) etsi(0) citas-sertifikācijas-politikas(2042) politikas-identifikatori(1) ncpplus (2)

3.1 Abonenta sertifikātu izmantošana ir aizliegta jebkuram no šiem mērķiem:

3.1.1 prettiesiska darbība (ieskaitot kiberuzbrukumus un mēģinājumu aizskart Q Smart-ID sertifikātu);

3.1.2 jaunu sertifikātu un informācijas par sertifikāta derīgumu izdošana;

3.1.3 pieļaušana citām personām izmantot abonenta privāto atslēgu;

3.1.4 pieļaušana, ka elektroniskajai parakstīšanai izsniegtais sertifikāts tiek izmantots automatizētā veidā;

3.1.5 elektroniskajai parakstīšanai izsniegtā sertifikāta izmantošana tādu dokumentu parakstīšanai, kas var radīt nevēlamas sekas (ieskaitot šādu dokumentu parakstīšanu testēšanas nolūkos).

3.2 Abonenta autentifikācijas sertifikātu nedrīkst izmantot, lai izveidotu eIDAS atbilstošus uzlabotos elektroniskos parakstus.

4 Uzticamības ierobežojumi

4.1 Sertifikāti stājas spēkā datumā, kas norādīts sertifikātā.

4.2 Sertifikāta derīgums beidzas sertifikātā norādītajā derīguma termiņa beigu datumā vai, ja sertifikāts tiek atsaukts.

4.3 Audita žurnāli tiek saglabāti uz vietas ne mazāk kā 10 gadus. Fiziskie vai digitālie arhīva ieraksti par sertifikātu pieteikumiem, reģistrācijas informāciju un lūgumiem vai pieteikumiem apturēšanai, apturēšanas izbeigšanu un atsaukšanu tiek saglabāti vismaz 10 gadus pēc tam, kad beidzies attiecīgā sertifikāta derīgums.

5 Abonenta tiesības un pienākumi

5.1 Abonentam ir tiesības iesniegt pieteikumu Q Smart-ID sertifikāta izsniegšanai.

5.2 Abonenta pienākums ir:

5.2.1 piekrist Noteikumiem un nosacījumiem;

5.2.2 ievērot SK sniegtās prasības;

5.2.3 izmantot viņa/viņas privāto atslēgu un sertifikātu saskaņā ar Noteikumiem un nosacījumiem, tostarp piemērojamiem līgumiem, kas izklāstīti 9. pantā, un Igaunijas Republikas un Eiropas Savienības likumiem;

5.2.4 nodrošināt, ka abonenta privātā atslēga tiek izmantota viņa/viņas kontrolē;

5.2.5 sniegt patiesu un pareizu informāciju Smart-ID sistēmai;

5.2.6 saprātīga laika posma ietvaros paziņot Smart-ID uzturētājam pareizo informāciju, ja viņa/viņas personas dati ir mainīti;

5.2.7 nekavējoties informēt SK par viņa/viņas privātās atslēgas neatļautas izmantošanas iespējamību un viņa/viņas sertifikātu atsaukšanu;
5.2.8 nekavējoties atsaukt viņa/viņas sertifikātus, ja viņš/viņa ir zaudējis kontroli pār savu privāto atslēgu.

6 SK tiesības un pienākumi

6.1 SK pienākums ir:
6.1.1 sniegt sertifikācijas pakalpojumu saskaņā ar piemērojamiem līgumiem, kas izklāstīti 10. pantā, un attiecīgiem tiesību aktiem;
6.1.2 veikt savu izsniegto sertifikātu un to derīguma uzskaiti;
6.1.3 uzturēt drošību ar savām iekšējās drošības procedūrām;
6.1.4 nodrošināt iespēju pārbaudīt sertifikātu derīgumu 24 stundas diennaktī;
6.1.5 sertifikācijas atslēgu aizsargāšanu ar aparatūras drošības moduļiem (piem., HSM) un to atrašanos tikai SK kontrolē;
6.1.6 sertifikācijas pakalpojuma sniegšanā izmantoto sertifikācijas atslēgu aktivizēšanu, pamatojoties uz dalītu kontroli.

7 Atkarīgo pušu pienākumi sertifikāta statusa pārbaudīšanai

7.1 Atkarīgā puse izpēta riskus un saistības, kas attiecas uz šī sertifikāta atzīšanu. Riski un saistības ir izklāstītas SPP un SP.
7.2 Ja sertifikātam vai kvalificētam elektroniskajam parakstam nav pievienots pietiekami daudz pierādījumu attiecībā uz sertifikāta derīgumu, atkarīgā puse pārbauda sertifikāta derīgumu, pamatojoties uz SK piedāvātajiem sertifikāta validācijas pakalpojumiem sertifikāta izmantošanas vai kvalificēta elektroniskā paraksta pievienošanas brīdī.
7.3 Atkarīgā puse ievēro sertifikātā noteiktos ierobežojumus un pārliecinās, ka akceptējamais darījums atbilst SPP un SP.
7.4 SK nodrošina sertifikātu statusa pakalpojumu pieejamību 24 stundas diennaktī, 7 dienas nedēļā ar vismaz 99,44% pieejamību kopumā gadā ar plānoto dīkstāves laiku, kas nepārsniedz 0,28% gadā.
7.5 SK piedāvā OCSP pakalpojumu sertifikāta statusa pārbaudei. Pakalpojums ir pieejams, izmantojot HTTP protokolu.
7.6 Atkarīgā puse pārliecinās par sertifikāta derīgumu, pārbaudot sertifikātu derīgumu pret OCSP. SK piedāvā OCSP ar šādām pārbaudes iespējām:
7.6.1 OCSP pakalpojums ir bez maksas un publiski pieejams vietnē http://aia.sk/eid2016;
7.6.2 SK piedāvā OCSP pakalpojumu ar labāku SLA saskaņā ar līgumu un cenu sarakstu.

8 Ierobežotā garantija un atruna / atbildības ierobežojumi

8.1 Abonents ir atbildīgs par savas privātās atslēgas uzturēšanu.
8.2 Abonents ir pilnībā atbildīgs par jebkādām digitālās identifikācijas un digitālā paraksta lietošanas sekām, izmantojot savus sertifikātus, gan to derīguma laikā, gan pēc tam.
8.3 Abonents ir atbildīgs par jebkādu kaitējumu, kas nodarīts Noteikumos un nosacījumos un/vai Igaunijas Republikas likumos norādīto viņa/viņas pienākumu neizpildes vai nepienācīgas izpildes rezultātā.
8.4 Abonents apzinās, ka elektroniskie paraksti, kas izdoti, pamatojoties uz sertifikātiem, kuriem beidzies derīguma termiņš vai kuri ir atsaukti, nav spēkā.
8.5 SK nodrošina:
8.5.1 to, ka sertifikācijas pakalpojums tiek sniegts saskaņā ar SPP, SP un attiecīgajiem Igaunijas Republikas un Eiropas Savienības tiesību aktiem;
8.5.2 sertifikācijas atslēgu aizsargāšanu ar aparatūras drošības moduļiem (piem., HSM) un to atrašanos tikai SK kontrolē;
8.5.3 sertifikācijas pakalpojuma sniegšanā izmantoto sertifikācijas atslēgu aktivizēšanu, pamatojoties uz dalītu kontroli;
8.5.4 ka tam ir obligātās apdrošināšanas līgumi, kas aptver visus SK pakalpojumus, lai nodrošinātu kompensāciju par zaudējumiem, kas radušies, SK pārkāpjot pienākumus;
8.5.5 ka tas informē visus abonentus, pirms SK pārtrauc sertifikācijas pakalpojumu, un uztur ar pārtraukto sertifikācijas pakalpojumu saistīto dokumentāciju un informāciju, kas nepieciešama saskaņā ar procedūru, kas noteikta SSP.
8.6 SK neatbild par:
8.6.1 abonentu privāto atslēgu slepenību, sertifikātu nepareizu lietošanu vai neatbilstošām sertifikātu pārbaudēm, vai par atkarīgās puses nepareiziem lēmumiem vai jebkādām sekām, kas radušās no kļūdām vai nepilnībām sertifikāta validācijas pārbaudēs;
8.6.2 savu pienākumu neizpildi, ja šāda neizpilde ir notikusi uzraudzības iestādes, datu aizsardzības uzraudzības iestādes, uzticamības saraksta vai jebkuras citas valsts iestādes kļūmju vai drošības problēmu dēļ;
8.6.3 nespēju veikt pienākumus, ja tā ir radušies nepārvaramas varas apstākļu dēļ.

9 Piemērojamie līgumi, SPP, SP

9.1 Attiecīgie līgumi, politikas un prakses paziņojumi, kas saistīti ar sertifikātu izmantošanas Noteikumiem un nosacījumiem, ir:
9.1.1 SK ID Solutions AS – sertifikācijas politika kvalificētiem Smart-ID, publicēta vietnē https://sk.ee/en/repository/CP/;
9.1.2 SK ID Solutions AS – EID-SK sertifikācijas prakses paziņojums, publicēts vietnē https://sk.ee/en/repository/CPS;
9.1.3 SK ID Solutions AS uzticamības pakalpojumu prakses paziņojums, publicēts vietnē: https://sk.ee/en/repository/sk-ps/;
9.1.4 Smart-ID sertifikāts un OCSP profils, publicēts vietnē: https://www.sk.ee/en/repository/profiles/;
9.1.5 Klienta datu aizsardzības principi https://www.sk.ee/en/repository/data-protection/.
9.2 Visu piemērojamo dokumentu pašreizējās versijas ir publiski pieejamas SK glabātavā https://www.sk.ee/en/repository/.

10 Konfidencialitātes politika un konfidencialitāte

10.1 SK ievēro klientu datu aizsardzības principus, kas sniegti SK glabātavā https://sk.ee/en/repository/data-protection/ un citos Igaunijas Republikas tiesību aktos, apstrādājot personas informāciju un reģistrēšanas informāciju.
10.2 Abonents ir informēts un piekrīt, ka sertifikātu izmantošanas digitālajā identifikācijā laikā personai, kura veic identifikāciju, tiek nosūtīts sertifikāts, kas ir iekļauts abonenta dokumentā un satur abonenta vārdu un personas kodu.

10.3 Visa informācija, kas kļuvusi zināma, sniedzot pakalpojumus, un kas nav paredzēta izpaušanai (piemēram, informācija, kas kļuvusi zināma SK uzticamības pakalpojumu pārvaldīšanas un sniegšanas rezultātā), ir konfidenciāla. Abonentam ir tiesības iegūt no SK informāciju par sevi saskaņā ar likumu.
10.4 SK nodrošina konfidenciālu informāciju un informāciju, kas paredzēta iekšējai lietošanai, pret kompromitēšanu un nepieļauj tās izpaušanu trešajām personām, īstenojot dažādus drošības uzraudzības pasākumus.
10.5 SK ir tiesības atklāt informāciju par abonentu trešajai personai, kurai saskaņā ar attiecīgajiem likumiem un tiesību aktiem ir tiesības saņemt šādu informāciju.
10.6 Turklāt nepersonalizēti statistikas dati par SK pakalpojumiem arī tiek uzskatīti par publisku informāciju. SK var publicēt nepersonalizētus statistikas datus par saviem pakalpojumiem.

11 Kompensāciju politika

11.1 SK apstrādā kompensācijas atsevišķi katrā gadījumā.

12 Piemērojamie tiesību akti, sūdzības un strīdu izšķiršana

12.1 Sertifikācijas pakalpojumu regulē Igaunijas un Eiropas Savienības kā vietu, kur SK ir reģistrēta kā SI, jurisdikcijas.
12.2 Visi strīdi starp pusēm tiks risināti pārrunu ceļā. Ja puses nespēj panākt mierizlīgumu, strīds tiek izšķirts tiesā SK atrašanās vietā.
12.3 Pārējie lietas dalībnieki tiks informēti par jebkuru prasību vai sūdzību ne vēlāk kā 30 kalendāro dienu laikā pēc atklāšanas, pamatojoties uz prasību, ja likumā nav noteikts citādi.
12.4 Abonents vai cita persona var iesniegt savu prasību vai sūdzību, izmantojot šo e-pasta adresi: info@sk.ee.
12.5 Visi pieprasījumi sakarā ar strīdiem ir jānosūta uz adresi, kas sniegta kontaktinformācijā šajos Noteikumos un nosacījumos.

13 SK un glabātavas licences, uzticamības zīmes un audits

13.1 Q Smart-ID sertifikācijas pakalpojumam ir kvalificēts statuss Igaunijas uzticamības sarakstā: https://sr.riik.ee/en/tsl/estonia.html. Obligāts priekšnoteikums šai reģistrācijai ir atbilstība piemērojamajiem noteikumiem un standartiem.
13.2 Atbilstības novērtēšanas iestāde saskaņā ar Regulu (EK) Nr. 765/2008 ir akreditēta kā kompetenta veikt kvalificētā uzticamības pakalpojumu sniedzēja un kvalificētu uzticamības pakalpojumu, ko tas sniedz, atbilstības novērtēšanu.
13.3 Audita secinājumi vai sertifikāti, kas balstīti uz audita rezultātiem atbilstības novērtēšanai, kas veikta saskaņā ar eIDAS Regulu, atbilstošajiem tiesību aktiem un standartiem, ir publicēti SK tīmekļa vietnē https://www.sk.ee/en/repository/.

14 Kontaktinformācija

14.1 Uzticamības pakalpojumu sniedzējs
SK ID Solutions AS
Reģistrācijas numurs 10747013
Pärnu mnt. 141, 113134
Tallina, IGAUNIJA
(Pirmd. - piektd. 9.00 - 18.00 pēc Austrumeiropas laika)
http://www.sk.ee/en
Tālrunis +372 610 1880
Fakss +372 610 1881
E-pasts: info@sk.ee

14.2 Pieteikumi Q Smart-ID sertifikātu atsaukšanai tiek pieņemti pa diennakts palīdzības līniju: 1777 vai (+ 372) 677 3377 un/vai pašapkalpošanās tīmekļa portālā.
14.3 Informācija un kontaktinformācija par palīdzības līniju un pašapkalpošanās tīmekļa portālu ir atrodamas SK tīmekļa vietnē https://www.sk.ee/en.