

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 17.02.2022

Definīcijas un akronīmi

Termins/akronīms	Definīcija
Autentifikācija	Personas unikāla identifikācija, pārbaudot viņa/viņas paziņoto identitāti
Autentifikācijas sertifikāts	Sertifikāts, kas ir paredzēts autentifikācijai.
SI	Sertificējošā iestāde
Sertifikāts	Publiskā atslēga kopā ar papildu informāciju, kas noteikta sertifikāta profilā, un ir padarīta neviltojama ar šifrēšanu, izmantojot certificējošās 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	SK ID Solutions AS – sertifikācijas politika kvalificētiem Smart-ID.
SPP	SK ID Solutions AS – EID-Q SK sertifikācijas prakses paziņojums.
Klientu apkalpošanas vieta	Klientu apkalpošanas vietā tiek pieņemti pieteikumi Q Smart-ID sertifikātu izsniegšanai un sertifikātu pieprasījumi tiek nosūtīti SK. Klientu apkalpošanas vietā tiek pieņemti un nosūtīti SK arī pieteikumi sertifikātu atsaukšanai.
Klientu apkalpošanas vietas palīdzības līnija	Palīdzības līnija, ko uztur klientu apkalpošanas vieta. Pa klientu apkalpošanas vietas palīdzības līniju tiek pieņemti pieprasījumi Q Smart-ID sertifikātu atsaukšanai no abonentiem, kuri pieteikušies Q Smart-ID ar klientu apkalpošanas vietas starpniecību.
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.
Identitātes sniedzējs	Organizācija, kas nodrošina elektroniskās autentifikācijas līdzekļus atbilstoši elektroniskās identifikācijas shēmai un kura ir atbildīga par to elektronisko identitāšu izveidošanu, kuras tiek lietotas Q Smart-ID sertifikātu izsniegšanai. Smart-ID uzturētājs pārliecinās, vai identitātes sniedzējs atbilst <u>prasībām identitātes sniedzējiem</u> kvalificētiem sertifikātiem.
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 privātajai atslēgai.
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.
Q Smart-ID	Smart-ID, kas satur vienu sertifikātu pāri, kas sastāv no autentifikācijas sertifikāta un kvalificēta elektroniskā paraksta sertifikāta, un satur tiem atbilstošās privātās atslēgas.
Kvalificēts elektroniskais paraksts	Kvalificēts elektroniskais paraksts pēc eIDAS Regulas.
Reģistrācijas iestāde	Iestāde, kas ir atbildīga par sertifikātu subjektu identificēšanu un autentifikāciju. Papildus reģistrācijas iestāde var pieņemt sertifikātu pieteikumus un sertifikāta atsaukšanas pieteikumus, pārbaudīt pieteikumus un/vai pārsūtīt pieteikumus sertificēšanas iestādei.
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
<u>Sekundārās Abonentu Autentifikācijas Nodrošinātājs</u>	<u>Organizācija, kura atbalsta vai izpilda Sekundāro Abonentu Autentifikāciju reģistrācijas procesa laikā, lai apliecinātu Abonenta informētību.</u> Sekundārā abonenta autentifikācijas sniedzējs ir atbildīgs par autentifikācijas ziņojumu piegādi Abonentam vai sekundārās abonenta autentifikācijas veikšanu ar elektroniskās identifikācijas līdzekli. Smart-ID nodrošinātājs ir pārbaudījis sekundārā abonenta autentifikācijas nodrošinātāju, lai ievērotu sekundārā abonenta autentifikācijas pakalpojumu sniedzēju prasības.
Smart-ID	Smart-ID ir jaunās paaudzes elektronisks identifikators, kas apgādā abonentu ar līdzekļiem elektroniskai autentifikācijai un ar elektronisko parakstu.
Smart-ID konts	Lai izmantotu Smart-ID sistēmas sniegtos pakalpojumus, abonentam ir jāreģistrē Smart-ID konts. Smart-ID konts saista Smart-ID lietotnes instanci ar Abonenta identitāti Smart-ID sistēmā. Smart-ID konta izveides un reģistrācijas gaitā Reģistrācijas iestāde apliecina Smart-ID konta īpašnieka (Abonenta) identitāti un saistību starp identitāti un atslēgu pāri apliecina sertificējusi sertificējusi sertificēšanas iestāde. Smart-ID kontam ir uzlabotā vai kvalificētā elektroniskā paraksta atslēga un autentifikācijas atslēga.
Smart-ID aplikācija	Smart-ID sistēmas tehniska komponente. Smart-ID aplikācija ir instalēta Abonenta mobilajā iekārtā un tā nodrošina piekļuvi kvalificētajiem Smart-ID pakalpojumiem
Smart-ID portāls	Abonenta mijiedarbības ar Smart-ID sistēmu punkts, kas ir pieejams, izmantojot tīmekļa pārlūkprogrammu. Portāls sniedz piekļuvi Smart-ID konta reģistrācijas un pārvaldības funkcijām.
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 pakalpojumiem, izdot elektroniskos parakstus un pārvaldīt savus Smart-ID kontus.
Abonents	Fiziska persona, 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://www.skidsolutions.eu/en>.
- 1.5. Abonents var pieteikties Q Smart-ID tikai personīgi, izņemot nepilngadīgo, kurš var pieteikties Q Smart-ID ar sava likumīgā pārstāvja starpniecību. Q Smart-ID nevar izdot pārstāvim.

2. Sertifikāta akceptēšana

- 2.1. Pēc tam, kad SK ir izsniedzis sertifikātus, abonents pārbauda sertifikātos esošo datu pareizību. Ja abonents ir pārliecinājies, ka dati sertifikātos ir pareizi, abonents apstiprina šīs informācijas pareizību. Atbilstošais apstiprinājums tiek uzskatīts par 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: izveido eIDAS atbilstošu kvalificētu elektronisko parakstu.	SK ID Solutions AS – sertifikācijas politika kvalificētiem Smart-ID, publicēta https://www.skidsolutions.eu/en/repository/C/P/ .	2.3.6.1.4.1.1001 5.17.1	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).
		ETSI EN 319 411-2 politika: QCP-n-qscd.	0.4.0.194112.1. 0	itu-t(0) identificēta-organizācija(4) etsi(0) kvalificētas-sertifikācijas-politikas(194112) politikas-identifikatori(1) qcp-natural(0).
	Autentifikācijas sertifikāts ir paredzēts: autentifikācijai.	SK ID Solutions AS – sertifikācijas politika kvalificētiem Smart-ID, publicēta https://www.skidsolutions.eu/en/repository/C/P/ .	2.3.6.1.4.1.1001 5.17.1	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).

Sertifikāta veids	Izmantošana	Pielietotā un publicētā sertifikācijas politika	OID	Kopsavilkums
		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) ncplus (2).

3.1. Abonenta sertifikātu izmantošana ir aizliegta jebkuram no šiem mērķiem:

- 3.1.1. prettiesiska darbība (ieskaitot kiberuzbrukumus un mēģinājumu aizskart Smart-ID sistēmu);
- 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 atsaukšanai 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. pieņemt Piekrišanu Automatizētai Biometriskās Identitātes Pārbaudei, ja tiek veikta Automatizēta Biometriskās Identitātes Pārbaude.
- 5.2.3. ievērot SK sniegtās prasības;
- 5.2.4. lietot SK nodrošināto Smart-ID aplikāciju,
- 5.2.5. izmantot viņa/viņas privātās atslēgas tikai kvalificētu elektronisko parakstu izveidošanai;
- 5.2.6. izmantot viņa/viņas privāto atslēgu un sertifikātu saskaņā ar Noteikumiem un nosacījumiem, tostarp piemērojamiem līgumiem, kas izklāstīti 10. pantā, un Igaunijas Republikas un Eiropas Savienības likumiem;
- 5.2.7. saņemot informāciju, ka viņa/viņas sertifikāts ir atsaukts vai izsniedzošā SI ir apdraudēta, turpmāk vairs neizmantot viņa/viņas privāto atslēgu;
- 5.2.8. nodrošināt, ka abonenta privātā atslēga tiek izmantota viņa/viņas kontrolē;
- 5.2.9. sniegt patiesu un pareizu informāciju Smart-ID sistēmai;

- 5.2.10. saprātīga laika posma ietvaros paziņot Smart-ID uzturētājam pareizo informāciju un atsaukt viņa/-as Sertifikātu, ja viņa/viņas personas dati ir mainīti;
- 5.2.11. nekavējoties informēt SK par viņa/viņas privātās atslēgas neatļautas izmantošanas iespējamību un atsaukt savus sertifikātus;
- 5.2.12. nekavējoties atsaukt viņa/viņas sertifikātus, ja viņš/viņa ir zaudējis kontroli pār savu privāto atslēgu vai PIN kodu.

6. SK tiesības un pienākumi

- 6.1. SK ir tiesības, ja drošības apsvērumu dēļ nepieciešams, ierobežot Smart-ID konta izmantošanu uz saprātīgu termiņu.
- 6.2. SK pienākums ir:
 - 6.2.1. sniegt sertifikācijas pakalpojumu saskaņā ar piemērojamiem līgumiem, kas izklāstīti 10. pantā, un attiecīgiem tiesību aktiem;
 - 6.2.2. nodrošināt, ka Q Smart-ID ir atzīts kā QSCD;
 - 6.2.3. nodrošināt, ka Smart-ID aplikācija ietver komponentes, kas ir atzītas kā daļa no QSCD;
 - 6.2.4. veikt savu izsniegto sertifikātu un to derīguma uzskaiti;
 - 6.2.5. atsaukt sertifikātus, ja to pieprasa Abonents vai jebkuros citos SP vai tiesību aktos noteiktos apstākļos;
 - 6.2.6. uzturēt drošību ar savām iekšējās drošības procedūrām;
 - 6.2.7. nodrošināt iespēju pārbaudīt sertifikātu derīgumu 24 stundas diennaktī;
 - 6.2.8. nodrošināt, ka sertifikācijas atslēgas ir aizsargātas ar aparatūras drošības moduļiem (piem., HSM) un atrodas tikai SK kontrolē;
 - 6.2.9. nodrošināt, ka sertifikācijas pakalpojuma sniegšanā izmantotās sertifikācijas atslēgas tiek aktivizētas, 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 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, uz kuru ir atsauce Sertifikāta Iestādes Informācijas Piekļuves paplašinājumā;
 - 7.6.2. SK piedāvā OCSP pakalpojumu ar labāku SLA saskaņā ar līgumu un cenu sarakstu;
 - 7.6.3. OCSP pakalpojuma URL ir iekļauts sertifikāta laukā „Piekļuve informācijai par sertificēšanas iestādi” (AIA) saskaņā ar sertifikāta profilu.

- 7.7. Sertifikāta, kam beidzies derīguma termiņš, atsaukšanas statusa informāciju var pieprasīt, rakstot uz e-pasta adresi info@skidsolutions.eu
- 7.8. OCSP pakalpojums ietver sertifikāta statusa informāciju līdz sertifikāta derīguma termiņa beigām.

8. Citu dalībnieku pienākumi

- 8.1. Smart-ID uzturētājs garantē, ka:
 - 8.1.1. tas ievēro atslēgas ģenerēšanas un uzglabāšanas darba kārtību, kas ir tā kontrolē un aprakstīta SPP;
 - 8.1.2. tas ievēro samaksas noteikumus, kas aprakstīti SPP;
 - 8.1.3. tas pārsūta pareizo sertifikātu un pareizu sertifikāta statusa informāciju.
- 8.2. Smart-ID uzturētājs ir tiesīgs anulēt identitātes sniedzēja statusu, ja ir ieguvis pierādījumus, ka identitātes sniedzējs neievēro prasības identitātes sniedzējiem kvalificētiem sertifikātiem.
- 8.3. Identitātes sniedzējs nodrošina atbilstību prasībām identitātes sniedzējiem kvalificētiem sertifikātiem.
- 8.4. Biometriskās Verifikācijas Pakalpojumu Sniedzējs ievēro ar SK noslēgtajā līgumā noteiktās prasības.
- 8.5. Sekundārās Abonenta Autentificēšanas Pakalpojumu Sniedzējs ievēro Autentifikācijas Pakalpojumu Sniedzēju Prasības.

9. Ierobežotā garantija un atruna / atbildības ierobežojumi

- 9.1. Abonents ir atbildīgs par daļu no privātās atslēgas uzturēšanu un PIN kodiem, kas ir viņa / -as īpašumā.
- 9.2. Abonents ir pilnībā atbildīgs par jebkādam autentifikācijas un elektroniskā paraksta lietošanas sekām, izmantojot savus sertifikātus, gan to derīguma laikā, gan pēc tam.
- 9.3. 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.
- 9.4. Abonents apzinās, ka elektroniskie paraksti, kas izdoti, pamatojoties uz sertifikātiem, kuriem beidzies derīguma termiņš vai kuri ir atsaukti, nav spēkā.
- 9.5. SK nodrošina:
 - 9.5.1. to, ka sertifikācijas pakalpojums tiek sniegts saskaņā ar SPP, SP un attiecīgajiem Igaunijas Republikas un Eiropas Savienības tiesību aktiem;
 - 9.5.2. sertifikācijas atslēgu aizsargāšanu ar aparātūras drošības moduļiem (piem., HSM) un to atrašanos tikai SK kontrolē;
 - 9.5.3. sertifikācijas pakalpojuma sniegšanā izmantoto sertifikācijas atslēgu aktivizēšanu, pamatojoties uz dalītu kontroli;
 - 9.5.4. ka tam ir obligātās apdrošināšanas līgumi, kas aptver visus SK pakalpojumus, lai nodrošinātu kompensāciju par zaudējumiem, kas radušies, SK pārkāpjot pienākumus;
 - 9.5.5. 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.
- 9.6. SK neatbild par:
 - 9.6.1. abonentu privāto atslēgu slepenību, sertifikātu nepareizu lietošanu vai neatbilstošām sertifikātu pārbaudēm, vai par atkarīgās puses nepareiziem lēmumiem vai jebkādam sekām, kas radušās no kļūdām vai nepilnībām sertifikāta validācijas pārbaudēs;
 - 9.6.2. 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;

9.6.3. nespēju veikt pienākumus, ja tā ir radušies nepārvaramas varas apstākļu dēļ.

10. Piemērojamie līgumi, SPP, SP

- 10.1. Attiecīgie līgumi, politikas un prakses paziņojumi, kas saistīti ar sertifikātu izmantošanas Noteikumiem un nosacījumiem, ir:
 - 10.1.1. SK ID Solutions AS – sertifikācijas politika kvalificētiem Smart-ID, publicēta <https://www.skidsolutions.eu/en/repository/CP/>;
 - 10.1.2. SK ID Solutions AS – EID-Q SK sertifikācijas prakses paziņojums, publicēts vietnē <https://www.skidsolutions.eu/en/repository/CPS/>;
 - 10.1.3. SK ID Solutions AS uzticamības pakalpojumu prakses paziņojums, publicēts vietnē <https://www.skidsolutions.eu/en/repository/sk-ps/>;
 - 10.1.4. Smart-ID sertifikāts un OCSP profils, publicēts vietnē <https://www.skidsolutions.eu/en/repository/profiles/>;
 - 10.1.5. Personas datu apstrādes principi, publicēti vietnē: <https://www.skidsolutions.eu/en/repository/data-protection/>;
 - 10.1.6. Piekrišana Automatizētai Biometriskās Identitātes Pārbaudei, publicēta vietnē: <https://www.skidsolutions.eu/en/repository/data-protection/>.
- 10.2. Visu piemērojamo dokumentu pašreizējās versijas ir publiski pieejamas SK glabātavā <https://www.skidsolutions.eu/en/repository/>.

11. Konfidencialitātes politika un konfidencialitāte

- 11.1. SK ievēro personas datu apstrādes principus, kas sniegti SK glabātavā <https://www.skidsolutions.eu/en/repository/data-protection/> un citos Igaunijas Republikas tiesību aktos, apstrādājot personas informāciju un reģistrēšanas informāciju.
- 11.2. Abonents ir informēts un piekrīt, ka sertifikātu izmantošanas autentifikācijas laikā personai, kura veic identifikāciju, tiek nosūtīts sertifikāts, kas ir iekļauts abonenta Q Smart-ID un satur abonenta vārdu un personas kodu.
- 11.3. Izmantojot sertifikātu kvalificētam elektroniskajam parakstam, abonents ir informēts un piekrīt, ka sertifikāts, kas ievadīts abonenta Q Smart-ID un satur abonenta vārdu un personas kodu, tiek pievienots dokumentam, ko abonents elektroniski paraksta.
- 11.4. 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.
- 11.5. SK nodrošina konfidenciālu informāciju un informāciju, kas paredzēta iekšējai lietošanai, pret kompromitēšanu un nepieļauj tās izpaušanu trešajām personām, īstenojot dažādus drošības uzraudzības pasākumus.
- 11.6. SK ir tiesības atklāt informāciju par abonentu trešajai personai, kurai saskaņā ar attiecīgajiem likumiem un tiesību aktiem ir tiesības saņemt šādu informāciju.
- 11.7. Turklāt nepersonalizēti statistikas dati par SK pakalpojumiem arī tiek uzskatīti par publisku informāciju. SK var publicēt nepersonalizētus statistikas datus par saviem pakalpojumiem.
- 11.8. SK ir tiesības kopīgāt attiecīgos datus ar Atkarīgo Pusi, lai nodrošinātu sertifikātu izmantošanas drošību.

12. Kompensāciju politika

- 12.1. SK apstrādā kompensācijas atsevišķi katrā gadījumā.

13. Piemērojamie tiesību akti, sūdzības un strīdu izšķiršana

- 13.1. Sertifikācijas pakalpojumu regulē Igaunijas un Eiropas Savienības kā vietu, kur SK ir reģistrēta kā SI, jurisdikcijas.
- 13.2. Visi strīdi starp pusēm tiks risināti pārrunu ceļā. Ja puses nespēj panākt mierizlīgumu, strīds tiek izšķirts tiesā SK atrašanās vietā.
- 13.3. 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.
- 13.4. Abonents vai cita persona var iesniegt savu prasību vai sūdzību, izmantojot šo e-pasta adresi: info@skidsolutions.eu
- 13.5. Visi pieprasījumi sakarā ar strīdiem ir jānosūta uz adresi, kas sniegta kontaktinformācijā šajos Noteikumos un nosacījumos.

14. SK un glabātavas licences, uzticamības zīmes un audits

- 14.1. Q Smart-ID sertifikācijas pakalpojumam ir kvalificēts statuss Igaunijas uzticamības sarakstā: <https://sr.riik.ee/en/tl.html>. Obligāts priekšnoteikums šai reģistrācijai ir atbilstība piemērojamajiem noteikumiem un standartiem.
- 14.2. 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.
- 14.3. 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.skidsolutions.eu/en/repository/>

15. Kontaktinformācija

- 15.1. Uzticamības pakalpojumu sniedzējs
 SK ID Solutions AS
 Reģistrācijas numurs 10747013
 Pārnu mnt. 141, 11314
 Tallina, IGAUNIJA
 (Pirmd. - piektd. 9.00 - 18.00 pēc Austrumeiropas laika)
<https://www.skidsolutions.eu/en>
 Tālrunis +372 610 1880
 Fakss +372 610 1881
 E-pasts: info@skidsolutions.eu
- 15.2. Pieteikumi Q Smart-ID sertifikātu atsaukšanai tiek pieņemti pa diennakts palīdzības līniju. Sazināšanās ar palīdzības līniju:
 - 15.2.1. no Igaunijas uz help.ee@smart-id.com vai pa tālr. 9001807 vai +372 715 1606;
 - 15.2.2. no Latvijas uz help.lv@smart-id.com vai pa tālr. 1807 vai +371 6766 5001;
 - 15.2.3. no Lietuvas uz help.lt@smart-id.com vai pa tālr. 1807 vai +370 670 41807.
- 15.3. Pieteikumi Q Smart-ID sertifikātu atsaukšanai tiek pieņemti arī pa klientu apkalpošanas vietas palīdzības līniju. Sazināšanās ar palīdzības līniju:
 - 15.3.1. no Igaunijas pa tālr. +372 6 310 310 (jebkurā laikā);
 - 15.3.2. no Latvijas pa tālr. +371 67 444 444 (jebkurā laikā);
 - 15.3.3. no Lietuvas pa tālr. 1884 vai +370 5 268 4444 (pirmd. - piektd. 8.00 - 20.00, sestd. 9.00 - 16.00).
- 15.4. Pieteikumi Q Smart-ID sertifikātu atsaukšanai tiek pieņemti arī pašapkalpošanās tīmekļa portālā un/vai Smart-ID pieteikšanas vietās, un/vai klientu apkalpošanas vietās.

15.5. Informācija un kontaktinformācija par palīdzības līniju un Smart-ID portālu ir pieejama SK tīmekļa vietnē <https://www.skidsolutions.eu/en> un <https://www.smart-id.com/>.