Valsts akciju sabiedrības

"Latvijas Valsts Radio un Televīzijas centrs"

# Sertificēšanas institūciju sertifikācijas NOTEIKUMI

SAGATAVOJA: Informācijas sistēmu daļa

## SAISTĪTIE DOKUMENTI:

[1] Latvijas Republikas Elektronisko dokumentu likums, 2002.g. novembris.

[2] eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Sertifikātu politika.

[3] eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Drošības noteikumi.

[4] RFC 3280 "Interneta X.509 publiskās atslēgas infrastruktūra: sertifikāti un CRL profils" (angliski: *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*).

[5] Likums "Par tiesu varu", 1992.g. 15. decembris.

[6] ETSI TS 101 456 V1.3.1 (05.2005) "Elektroniskie paraksti un infrastruktūra; Kvalificēto sertifikātu izsniedzošo sertifikācijas institūciju politikas prasības" (angliski: *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified Certificates*).

[7] RFC 2560 "Interneta X.509 publiskās atslēgas infrastruktūra: tiešsaistes sertifikātu statusa protokols, 1999.g. jūnijs (angliski: *Internet Public Key Infrastructure: Online Certificate Status Protocol, June 1999*).

[8] ETSI TS 101 861 V1.4.1 (07.2011) "Elektroniskie paraksti un infrastruktūra; Laika zīmogošanas profils" (angliski: *Electronic Signatures and Infrastructures (ESI); Time stamping profile*).

## DOKUMENTA IZMAIŅU VĒSTURE:

| Pārskatītā varianta nr. | Spēkā stāšanās datums | Izmaiņu kopsavilkums |
|---|---|---|
| 1.0 | 12.02.2010. | Gala versija. |
| 1.1. | 01.12.2010. | Pievienota informācija par jaunajiem WEB portāla sertifikātiem. |
| 1.2. | 06.01.2011. | Redakcionālas izmaiņas. |
| 1.3. | 12.01.2011. | Redakcionālas izmaiņas. |
| 1.4 | 08.04.2011. | Redakcionālas izmaiņas. |
| 1.5 | 28.04.2011. | Redakcionālas izmaiņas. |
| 1.6 | 12.05.2011. | Laboti OCSP sertifikātu derīguma termiņi. |
| 1.7. | 27.05.2011. | Papildināts ar informāciju, par iespēju apstiprināt WEB portāla sertifikātu pieteikumu izmantojot trešās puses. |
| 1.8 | 18.08.2011. | Papildināta informācija par SSL un koda paraksta sertifikātu pieteikumu pārbaudi 4.1.3.1. |
| 1.9 | 23.08.2011. | Redakcionālas izmaiņas. |
| 1.9.1. | 20.03.2012. | Veikta pāreja no E-ME identifikatora uz eParaksts.lv identifikatoru. Pievienoti eID sertifikātu profili. Mainīti sertifikātu OID. Grozīti URL no eme.lv uz eparaksts.lv. 1.4.1.punktā labota hierarhiskā struktūra. Dzēsta atļauja izsniegt 512 bitu atslēgas. |
| 1.9.2. | 09.11.2012. | Redakcija papildināta ar Mobilo kodu, pieteikšanās, autentificēšanās. |
| 1.9.3. | 10.01.2015. | Veikta pāreja no eParaksts.lv identifikatora uz LVRTC identifikatoru. Papildināts ar eZīmoga pakalpojumu, laboti RI norādot saites, sakarā ar viedkartēs esošo sertifikātu attālinātu jaunizdošanu pievienoti 3.3.4 |

| | | |
|---|---|---|
| | | un 4.1.2.10 punkti. Precizēts OCSP sertifikāta profils sakarā ar *„OCSP No Revocation Checking”* paplašinājuma iekļaušanu. Papildināta definīciju sadaļa.<br>Dokuments vairs nesatur OID.<br>Papildus veiktas noteikumu redakcionālās korekcijas. |
| 1.9.4. | 15.08.2016. | 1.3.11.2 punktā mainīts Palīdzības dienesta tālruņa numurs;<br>3.1.1.3. punkts papildināts ar jauna izsniedzēja datiem<br>7.4. punkts papildināts ar papildus Izsniegšanas SI Parakstītāja datiem. |

# Saturs

# 1. Ievads

## 1.1. Dokumenta nolūks

1.1.1. Šie Sertificēšanas institūciju sertifikācijas noteikumi (turpmāk – Sertifikācijas noteikumi jeb SN) apraksta praktiskās darbības kārtību, ko eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Sertificēšanas institūcijas ievēro procedūrām, kas attiecas uz sertifikātu pieteikšanu, izsniegšanu, lietošanu, pārbaudi, anulēšanu un to darbības termiņa izbeigšanu, kā arī eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Sertificēšanas institūciju darbības uzturēšanu.

1.1.2. Sertifikācijas noteikumi ir attiecināmi arī uz Valsts akciju sabiedrības "Latvijas Valsts radio un televīzijas centrs" sniegtajiem sertifikācijas pakalpojumiem, kas balstās uz elektroniskiem sertifikātiem ar iekļautu identifikatoru "E-ME".

1.1.3. Sertifikācijas noteikumos aprakstītas praktiskās darbības kārtība kopā ar tehnoloģijām, politikām un procesiem, uz ko ir atsauces šajos noteikumos, lai radītu uzticamību, nodrošinot eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Sertificēšanas institūciju augsta līmeņa drošību.

1.1.4. Sertifikācijas noteikumi tiek regulāri pārskatīti , ņemt vērā tehnoloģijas un informācijas drošības attīstību, kā arī citus būtiskus apstākļus.

1.1.5. Sertifikācijas noteikumu struktūra pamatos balstās uz RFC 3647 standarta.

1.1.6. Sertifikācijas noteikumu nosaka visiem parakstītājiem, pasūtītājiem un potenciālajiem pārbaudītājiem noteikumus, kas jāievēro izmantojot eParaksts.lv Sertifikācijas pakalpojumu sniedzēja laika zīmogošanas pakalpojumus.

1.1.7. Sertifikācijas noteikumi nosaka praktiskās darbības kārtību, kas saistīta ar eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Sertificēšanas institūciju, un ietver atslēgu un sertifikātu dzīves cikla pārvaldības procedūras:

1.1.7.1. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Saknes sertificēšanas institūcijas atslēgu pārim un pašparakstītam sertifikātam, ko izmanto sertifikātu un Atsaukto sertifikātu saraksta parakstīšanai;

1.1.7.2. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Politikas sertificēšanas institūcijas sertifikātam, kurus izmanto sertifikātu un Atsaukto sertifikātu saraksta parakstīšanai;

1.1.7.3. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Izsniegšanas sertificēšanas institūcijas sertifikātam, kurus izmanto sertifikātu un Atsaukto sertifikātu saraksta parakstīšanai;

1.1.7.4. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja uzticama Tiešsaistes sertifikātu statusa pārbaudes servisa sertifikātam;

1.1.7.5. gala lietotāju kvalificētiem sertifikātiem drošu parakstu izveidei;

1.1.7.6. gala lietotāju nekvalificētiem sertifikātiem drošai autentifikācijai;

1.1.7.7. tīmekļa vietnes autentifikācijas sertifikātiem;

1.1.7.8. koda parakstīšanas sertifikātiem;

1.1.7.9. domēna kontroliera sertifikātiem;

1.1.7.10. eZīmoga sertifikātiem;

1.1.7.11. laika zīmogošanas iekārtas sertifikātiem.

1.1.8. Sertifikācijas noteikumu lietotāju kopa ir visas puses, kas uzticas sertifikātiem, ko ir izsniegusi eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Sertificēšanas institūcija.

1.1.9. Sertifikācijas noteikumi nosaka darbības un pārvaldīšanas procesus saistītus ar eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Laika zīmogošanas institūciju tā, lai parakstītāji un pārbaudītāji varētu novērtēt savu uzticību laika zīmogošanas pakalpojumiem.

1.1.10. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Laika zīmogošanas institūcijas darbības nolūks ir piegādāt laika zīmogošanas pakalpojumus, kas ir izmantojami, lai atbalstītu drošos elektroniskos parakstus, kā arī saskaņā ar attiecīgajiem Latvijas Republikas normatīvajiem aktiem.

1.1.11. Sertifikācijas noteikumu dokumenta pamata valoda ir latviešu valoda.

## 1.2. Dokumenta nosaukums un identifikācija

| | |
|---|---|
| **Nosaukums** | Sertificēšanas institūciju sertifikācijas noteikumi |
| **Derīguma termiņš** | Šī dokumenta versija ir derīga līdz nākamās versijas publicēšanai |

1.2.1. Sertifikācijas noteikumi ir publicēti https://www.eparaksts.lv/lv/repozitarijs

1.2.2. Sertifikācijas noteikumi darbojas atbilstoši eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Sertifikātu politikai [2] ar **OID 1.3.6.1.4.1.32061.1.1.2**, kas minēts Sertifikātu politikas punktā 1.1.

## 1.3. Publiskās atslēgas infrastruktūras dalībnieki

1.3.1. Publiskās atslēgas infrastruktūras dalībnieki ir:

1.3.1.1. Saknes Sertificēšanas institūcija;

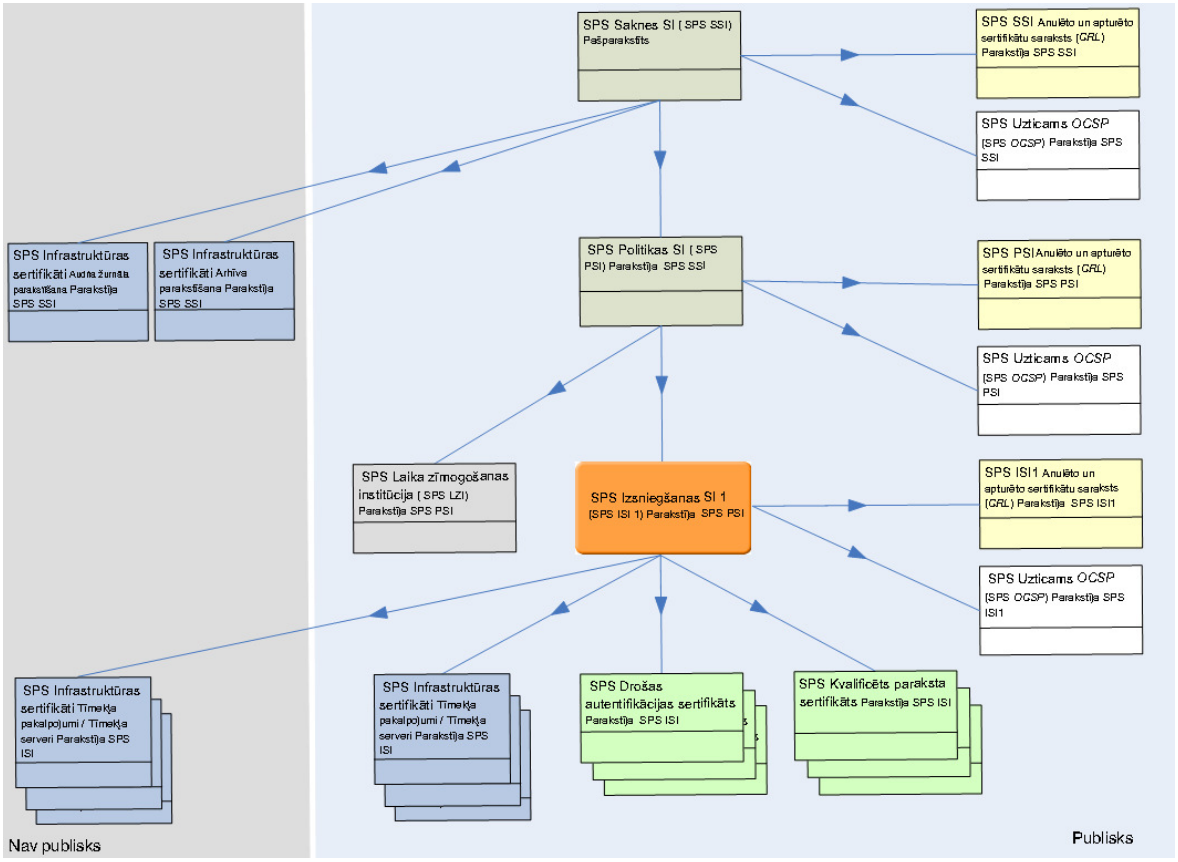
1.3.1.2. Politikas Sertificēšanas institūcija;

1.3.1.3. Izsniegšanas Sertificēšanas institūcija;

1.3.1.4. Reģistrācijas institūcija;

1.3.1.5. Parakstītājs un pasūtītājs;

1.3.1.6. Pārbaudītāji.




Attēls nr.1. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Sertificēšanas institūciju struktūra

1.3.2. **Saknes Sertificēšanas institūcijas apraksts un pienākumi:**

1.3.2.1. Saknes Sertificēšanas institūcija izsniedz sertifikātus un anulēto un apturēto sertifikātu sarakstus:

1.3.2.1.1. Politikas Sertificēšanas institūcijai,

1.3.2.1.2. uzticamam Sertifikātu statusa tiešsaistes pārbaudes servisam (atbilstoši RFC 2560 standartam),

1.3.2.1.3. audita notikumu žurnālu parakstošajai komponentei,

1.3.2.1.4. arhīvu parakstošajai komponentei.

1.3.2.2. Saknes Sertificēšanas institūcija ir augstākais uzticības pamats eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Publiskās atslēgas infrastruktūras hierarhijā.

1.3.2.3. Saknes Sertificēšanas institūcijas svarīgākās funkcijas ir apstrādāt sertifikātu pieteikumus, izsniegt sertifikātus un pārvaldīt tās izsniegto sertifikātu dzīves ciklu, kā arī darbināt un uzturēt Sertifikātu tiešsaistes statusa pārbaudes pakalpojumus.

1.3.2.4. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja ar šo garantē, ka veicot tā Saknes Sertificēšanas institūcijas un tai pakļauto sertificēšanas institūciju, un sertifikātu pārbaudes pakalpojumu operatora funkcijas, tas:

1.3.2.4.1. administrēs un publicēs šos Sertifikācijas noteikumus un citu būtisku un publisku informāciju saskaņā ar 2.2. nodaļu;

1.3.2.4.2. veiks un ir veicis atbilstības auditus saskaņā ar 8. nodaļu;

1.3.2.4.3. rīkosies ar konfidenciālu informāciju, personas datiem un informācijas izpaušanu saskaņā ar 9.3. nodaļu;

1.3.2.4.4. veiks identitātes pārbaudes funkcijas saskaņā ar 3.1.5. nodaļu;

1.3.2.4.5. veiks sertifikātu pieteikuma procesus, sertifikātu izsniegšanu un sertifikātu dzīves cikla pārvaldību saskaņā ar 4. nodaļu;

1.3.2.4.6. būs atbildīgs par Saknes Sertificēšanas institūcijas un globālās pārbaudes pakalpojumu darbību saskaņā ar 5. un 6. nodaļu;

1.3.2.4.7. uzturēs Sertifikācijas pakalpojumu sniedzēja informācijas sistēmu pēcavārijas atjaunošanas plānu saskaņā ar 5.7. nodaļu.

1.3.2.5. eParaksts.lv Sertifikācijas pakalpojumu sniedzējs garantē un paziņo, ka saknes kriptogrāfiskā atslēga nav kompromitēta un informācija, kas ir tā izsniegtajos sertifikātos, saskaņā ar eParaksts.lv Sertifikācijas pakalpojumu sniedzējam zināmo nav nepatiesa.

1.3.2.6. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja neuzņemas nekādas papildus garantijas vai saistības šo Sertifikācijas noteikumu aprakstīto aktivitāšu darbības laukā.

1.3.3. **Politikas Sertificēšanas institūcijas apraksts un pienākumi:**

1.3.3.1. Politikas sertificēšanas institūcija izsniedz sertifikātus un anulēto un apturēto sertifikātu sarakstus Izsniegšanas Sertificēšanas institūcijai un Laika zīmogošanas institūcijai.

1.3.3.2. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Politikas sertificēšanas institūcijas ir augsta līmeņa uzticamas sertificēšanas institūcijas, kuru sertifikātu izsniegusi eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Saknes sertificēšanas institūcija un kam var būt pakārtoti vienumi – citas uzticamas sertificēšanas institūcijas. Tās drīkst izsniegt sertifikātus arī citām pakārtotām Sertificēšanas institūcijām. Tām jāatbilst eParaksts.lv Sertifikācijas noteikumiem.

1.3.3.3. eParaksts.lv Sertifikācijas pakalpojumu sniedzējs pārvalda Politikas sertificēšanas institūciju. Tā nodrošina sertifikācijas pakalpojumus pakārtotām Izsniegšanas sertificēšanas institūcijām. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Politikas sertificēšanas institūcijas pienākumi ir šādi:

1.3.3.3.1. publicēt šos Sertifikācijas noteikumu un citu publisku informāciju saskaņā ar 2.2. nodaļu;

1.3.3.3.2. veikt un būt veikušam atbilstības auditus saskaņā ar 8. nodaļu;

1.3.3.3.3. rīkoties ar konfidenciālu informāciju, personas datiem saskaņā ar 9.3. nodaļu;

1.3.3.3.4. veikt identitātes pārbaudes funkcijas saskaņā ar 4. nodaļu;

1.3.3.3.5. veikt sertifikātu pieteikumu procesus, sertifikātu izsniegšanu un sertifikātu dzīves cikla pārvaldību saskaņā ar 4. nodaļu;

1.3.3.3.6. uzturēt un darbināt notikumu reģistrēšanas un audita sistēmas saskaņā ar 5.4. nodaļu;

1.3.3.3.7. uzturēt un arhivēt ierakstus saskaņā ar 5.5. nodaļu;

1.3.3.3.8. sniegt Politikas sertificēšanas institūcijas un sertifikātu pārbaudes pakalpojumus saskaņā ar 5.6., 5.8. nodaļu un 6. nodaļu;

1.3.3.3.9. uzturēs Sertifikācijas pakalpojumu sniedzēja informācijas sistēmu pēcavārijas atjaunošanas plānu saskaņā ar 5.7. nodaļu;

1.3.3.4. eParaksts.lv Sertifikācijas pakalpojumu sniedzējs garantē un paziņo, ka saknes kriptogrāfiskā atslēga nav kompromitēta un informācija, kas ir tā izsniegtajos sertifikātos, saskaņā ar eParaksts.lv Sertifikācijas pakalpojumu sniedzējam zināmo ir patiesa.

1.3.4. **Izsniegšanas Sertificēšanas institūcijas apraksts un pienākumi:**

1.3.4.1. Izsniegšanas sertificēšanas institūcija definē sertifikātu veidnes gala lietotāju sertifikātu tipiem, izsniedz gala lietotāju sertifikātus, infrastruktūras sertifikātus un anulēto un apturēto sertifikātu sarakstus.

1.3.4.2. eParaksts.lv SPS Sertificēšanas institūcijas ir balstītas uz eParaksts.lv SPS Saknes sertificēšanas institūcijas vai eParaksts.lv SPS Politikas

sertificēšanas institūcijas izsniegtajiem sertifikātiem, kas atbilst eParaksts.lv SI SN (šim dokumentam).

1.3.4.3. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Izsniegšanas sertificēšanas institūcijas pienākumi ir šādi:

1.3.4.3.1. par sertifikāta izsniegšanu informēt pasūtītāju, kurš ir izsniedzamā sertifikāta parakstītājs;

1.3.4.3.2. ja nepieciešams, informēt par sertifikāta izsniegšanu citus (ne tikai sertifikāta parakstītāju);

1.3.4.3.3. informēt par sertifikāta anulēšanu vai apturēšanu parakstītāju (pasūtītāju), kura sertifikāts tiek anulēts vai apturēts.

1.3.5. **Reģistrācijas institūcijas apraksts, pienākumi un funkcijas:**

1.3.5.1. Reģistrācijas institūcija ir nepieciešama vienumu identifikācijai un autentifikācijai. Reģistrācijas institūcija ir fiziska vai juridiska persona vai struktūrvienība, kurai eParaksts.lv Sertifikācijas pakalpojumu sniedzējs deleģē zemāk uzskaitītās funkcijas:

1.3.5.1.1. parakstītāja personiska identificēšana un reģistrēšana;

1.3.5.1.2. pārbaudītu un pilnīgu datu sertifikātu izsniegšanai un anulēšanai pārsūtīšana eParaksts.lv Sertificēšanas institūcijai;

1.3.5.1.3. viedkaršu izsniegšana parakstītājam un sertifikātu aktivizēšana;

1.3.5.1.4. viedkaršu dzīves cikla loģistikas izsekošana.

1.3.5.2. Reģistrācijas institūcijas konkrētas funkcijas un pienākumi tiek norādīti attiecīgajos eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Izsniegšanas sertificēšanas institūcijas Sertifikācijas noteikumi.

1.3.5.3. Reģistrācijas institūcijas pienākumi:

1.3.5.3.1. parakstītāju un pasūtītāju identificēšana un autentifikācija;

1.3.5.3.2. apturēšanas un anulēšanas pieprasījumu pārbaude.

1.3.5.4. Parakstītāja, kas iesniedz pieteikumu sertifikāta saņemšanai, personīga identifikācija drīkst notikt ikvienā šim nolūkam izmantojamā Reģistrācijas institūcija.

1.3.5.5. Reģistrācijas institūcija funkcijas veic:

1.3.5.5.1. Klientu apkalpošanas centri

| |
|---|
| https://www.eparaksts.lv/lv/biznesam/eparaksts-viedkarte/klientu-apkalposanas-centri |
| https://www.eparaksts.lv/lv/virtualais-eparaksts/klientu-apkalposanas-centri |

1.3.5.5.2. mobilā Reģistrācijas institūcija (identificē un autentificē parakstītājus klienta telpās);

1.3.5.5.3. Interneta portāla parakstītāju un pasūtītāja pirmreizējā identificēšana un autentifikācija tiek veikta izmantojot iespēju pieteikumu apstiprināt elektroniski, izmantojot, kādu no trešās puses drošajiem autorizācijas veidiem.

1.3.5.5.4. AS “Latvijas Mobilais telefons” klientu apkalpošanas centros, piesakoties pakalpojumam „Mobilais kods”;

1.3.5.5.5. LR Pilsonības un migrācijas lietu pārvaldes teritoriālajās nodaļās, piesakoties eID kartei.

1.3.6. **Parakstītājs un pasūtītājs**

1.3.6.1. Pasūtītājs un parakstītājs var būt dažādas personas

1.3.6.2. Tīmekļa vietnes autentifikācijas sertifikātam, domēna kontroliera sertifikātam, eZīmoga sertifikātam un laika zīmogošanas iekārtas sertifikātam pasūtītājs ir iekārta vai serveris, pēc kura ģenerēta pieprasījuma sertifikāts ir

izsniegts. Koda paraksta sertifikātam parakstītājs ir programmatūra, kas izmanto ar sertifikātu apliecinātās atslēgas.

1.3.6.3. **Pasūtītāja pienākumi:**

1.3.6.3.1. sniegt precīzu informāciju sertifikāta pieteikumā;

1.3.6.3.2. aizsargāt pasūtītāja privātās atslēgas;

1.3.6.3.3. ievērot privātās atslēgas un sertifikāta lietošanas ierobežojumus;

1.3.6.3.4. informēt par privātās atslēgas kompromitēšanu.

1.3.6.4. **Parakstītāja pienākumi:**

1.3.6.4.1. aizsargāt parakstītāja privātās atslēgas;

1.3.6.4.2. ievērot privātās atslēgas un sertifikāta lietošanas ierobežojumus;

1.3.6.4.3. informēt par privātās atslēgas kompromitēšanu;

1.3.6.4.4. pārbaudīt, vai laika zīmoga marķieris ir pareizi parakstīts un vai eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Laika zīmogošanas institūcijas sertifikāts nav anulēts.

1.3.6.4.5. pasūtītājiem jāizmanto pieejamie rīki, lai pieprasītu un saņemtu laika zīmogus no eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Laika zīmogošanas institūcijas, ja vien netiek rakstiski norādīts savādāk.

1.3.7. **Pārbaudītāji**

1.3.7.1. Pārbaudītājs ir jebkurš publisko vai privāto tiesību subjekts, kas pieņem lēmumus, uzticoties eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Sertificēšanas institūciju izsniegtajiem sertifikātiem. Pārbaudītājs, kurš uzticas sertifikātam, pārbauda sertifikāta derīgumu, izmantojot svaigāko anulēšanas un apturēšanas statusa informāciju un pieejamos pārbaudes pakalpojumus.

1.3.7.2. **Pārbaudītāja pienākumi:**

1.3.7.2.1. būt atbildīgam par elektroniskā paraksta pārbaudi;

1.3.7.2.2. atzīt atbilstošos atbildības ierobežojumus un garantijas.

1.3.7.3. paļauties uz elektroniskajiem parakstiem un sertifikātiem, tikai ievērojot sekojošo:

1.3.7.3.1. elektroniskais paraksts ir izveidots sertifikāta derīguma termiņa laikā;

1.3.7.3.2. elektroniskais paraksts var tikt sekmīgi pārbaudīts;

1.3.7.3.3. visi publiskās atslēgas jaucējsummas rezultāti (izvilkumi) sertifikātam atbilstošajā sertifikātu hierarhijā ir sekmīgi pārbaudīti;

1.3.7.3.4. sertifikātiem sertifikātu hierarhijā nav beidzies derīguma termiņš;

1.3.7.3.5. sertifikāts un sertifikātu hierarhija ir sekmīgi pārbaudīta;

1.3.7.3.6. nav nekādu citu apstākļu, kuri varētu ietekmēt elektroniskā paraksta, sertifikāta, sertifikātu hierarhijas vai anulēto un apturēto sertifikātu saraksta uzticamību.

1.3.7.4. Paļaujoties uz Laika zīmogošanas marķieri, pārbaudītājam ir jāpārbauda, ka sertifikāts, ar ko laika zīmogs ir ticis parakstīts, ir derīgs tā pārbaudes brīdī.

1.3.7.5. Ja pārbaudes laiks pārsniedz attiecīgā sertifikāta derīguma periodu, ir jāizpildās šādiem nosacījumiem:

1.3.7.5.1. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Laika zīmogošanas institūcijas privātā atslēga nav tikusi diskreditēta nevienu brīdi līdz brīdim, kad pārbaudītājs pārbauda Laika zīmogošanas marķieri;

1.3.7.5.2. jaucējfunkcijas algoritmu izpilde, kas tiek izmantoti Laika zīmogošanas marķierim, uzrāda sekmīgu rezultātu;

1.3.7.5.3. Laika zīmogošanas marķierī izmantotā paraksta algoritms un paraksta atslēgas garums pārbaudes laikā vēl joprojām ir ārpus kriptogrāfisko

uzbrukumu sasniedzamības.

1.3.8. **eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Laika zīmogošanas institūcija**

1.3.8.1. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Laika zīmogošanas institūcija pa tiešo pakļauta Politikas sertificēšanas institūcijai.

1.3.8.2. eParaksts.lv Sertifikācijas pakalpojumu sniedzējs atbild par to, ka šī dokumenta 2.nodaļā ietvertās prasības ir nodrošinātas saskaņā ar Sertifikācijas pakalpojumu sniedzēja Sertifikātu politika.

1.3.8.3. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Sertifikātu politika nosaka pamata noteikumus eParaksts.lv Laika zīmogošanas institūcija darbībai.

1.3.8.4. eParaksts.lv Sertifikācijas pakalpojumu sniedzējs veic risku novērtēšanu, lai novērtētu draudus un noteiktu nepieciešamās drošības kontroles un darbības procedūras.

1.3.9. **Direktoriju pakalpojumi**

1.3.9.1. eParaksts.lv Sertifikācijas pakalpojumu sniedzējs sniedz direktoriju pakalpojumus, publicējot anulēto un apturēto sertifikātu sarakstus Direktoriju vieglpiekļuves protokola (angliski – *LDAP v3*) atbilstošā publiskā direktorijā.

1.3.9.2. eParaksts.lv Sertifikācijas pakalpojumu sniedzējs sniedz direktoriju pakalpojumu, publicējot sertifikātus Direktoriju vieglpiekļuves protokola atbilstošā publiskā direktorijā, ja pasūtītājs brīvprātīgi izvelējies un pašrocīgi parakstījis šādu opciju.

1.3.9.3. Šie eParaksts.lv SPS pakalpojumi ir pieejami tiešsaistē

https://www.eparaksts.lv/lv/repozitarijs/ldap/parbaudit-sertifikatu ;
ldap://eme.lv

1.3.10. **Sertifikātu pārbaudes pakalpojumi**

1.3.10.1. eParaksts.lv SPS sniedz pārbaudes pakalpojumus, kas ietver sertifikātu pārbaudi, izmantojot OCSP responderi.

1.3.10.2. Šie eParaksts.lv SPS pakalpojumi ir pieejami tiešsaistē

http://ocsp.eme.lv/responder.eme
https://ocsp.eme.lv/responder.eme

1.3.11. **Palīdzības dienests**

1.3.11.1. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja sastāvā ir Palīdzības dienests, kura darba pienākumi ietver:

1.3.11.1.1. konsultāciju pakalpojumu sniegšanu;

1.3.11.1.2. sertifikātu statusa informācijas noskaidrošanu;

1.3.11.1.3. gala lietotāju sertifikātu apturēšanas pieprasījumu pieņemšanu un apstrādi;

1.3.11.1.4. konkrētu pieprasījumu saistībā ar sertifikātu darbībām pāradresēšanu atbildīgajam eParaksts.lv Sertifikācijas pakalpojumu sniedzēja darbiniekam.

1.3.11.2. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Palīdzības dienesta kontaktinformācija ir šāda:

| | |
|---|---|
| **Tālrunis** | +371 67108787 |
| **E-pasts** | eparaksts@eparaksts.lv |

1.3.12. Tīmekļa vietne

1.3.12.1. eParaksts.lv Sertifikācijas pakalpojumu sniedzējs uztur tīmekļa vietni, kas nodrošina piekļuvi šādai informācijai un pakalpojumiem:

1.3.12.1.1. piekļuve sertifikātu pārbaudes pakalpojumiem (lai pārbaudītu sertifikātu derīgumu);

1.3.12.1.2. piekļuve direktoriju pakalpojumiem (lai meklētu un lejupielādētu sertifikātus);

1.3.12.1.3. piekļuve ar eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Sertificēšanas institūciju un Reģistrēšanas institūcijas darbību tieši saistītiem dokumentiem;

1.3.12.1.4. sertifikātu lietošanas programmatūras lejupielāde.

1.3.12.2. Piekļuve eParaksts.lv Sertifikācijas pakalpojumu sniedzēja tīmekļa vietnei nav ierobežota un tiek nodrošināta, izmantojot publisko datu komunikāciju tīklu. Šī tīmekļa vietne ir pieejama http://www.eparaksts.lv

1.3.12.3. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja tīmekļa vietne var arī ietvert eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Sertificēšanas institūciju un Reģistrēšanas institūcijas nodrošinātus papildus pakalpojumus. Šo pakalpojumu izmantošanai nepieciešama uz sertifikātu bāzēta personas autentifikācija.

## 1.4. Sertifikātu pielietojums

1.4.1. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Sertificēšanas institūcija ģenerē sertifikātus pakārtotām uzticamām Sertificēšanas institūcijām. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Saknes sertificēšanas institūcija arī izgatavo sertifikātus tās uzticamajam Tiešsaistes sertifikātu statusa protokola atbildētājam sertifikātu statusa pārbaudei (Tabula 1):

Tabula 1. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Saknes sertificēšanas institūcijas izsniegtie sertifikāti.

| Izsniedzējs | Sertifikāta nosaukums | Sertifikāta tips | Sertifikāta lietojums |
|---|---|---|---|
| eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Saknes sertificēšanas institūcija | eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Politikas sertificēšanas institūcijas sertifikāts | Publiskais Sertificēšanas institūcijas sertifikāts | Sertifikātu un Apturēto un anulēto sertifikātu saraksta parakstīšana |
| | Tiešsaistes sertifikātu statusa protokola atbildētāja sertifikāts | Publisko pakalpojumu sertifikāts | eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Sertifikātu pārbaudes pakalpojumu atbilžu parakstīšana |
| | Audita žurnāla paraksta sertifikāts | Nepublisks infrastruktūras sertifikāts | Koda parakstīšana sistēmas žurnāla pieprasījumiem |
| | Arhīva paraksta sertifikāts | Nepublisks infrastruktūras sertifikāts | Koda parakstīšana arhivēšanas pieprasījumiem |

1.4.2. Politikas SI sertifikātus izsniedz tikai eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Izsniegšanas sertificēšanas institūcijai, eParaksts.lv Sertifikācijas pakalpojumu sniedzēja uzticamajai Laika zīmogošanas institūcijai un laika zīmoga iekārtai (Tabula 2):

Tabula 2. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Politikas sertificēšanas institūcijas izsniegtie sertifikāti.

| Izsniedzējs | Sertifikāta nosaukums | Sertifikāta tips | Sertifikāta lietojums |
|---|---|---|---|
| eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Politikas sertificēšanas institūcija | eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Izsniegšanas sertificēšanas institūcijas sertifikāts | Publiskais sertificēšanas institūcijas sertifikāts | Sertifikātu un Apturēto un anulēto sertifikātu saraksta parakstīšana |
| | Uzticamās Laika zīmogošanas institūcijas sertifikāts | Publisko pakalpojumu sertifikāts | Laika zīmoga parakstīšana |
| | Laika zīmogošanas iekārtas sertifikāts | Infrastruktūras sertifikāts | Laika zīmoga parakstīšana |

1.4.3. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Izsniegšanas sertificēšanas institūcijas tiek izmantotas, lai gala lietotājiem izsniegtu kvalificētus un nekvalificētus sertifikātus, kā arī nepubliskus sertifikātus eParaksts.lv Sertifikācijas pakalpojumu sniedzēja infrastruktūras sistēmām un pakalpojumiem.

1.4.4. Turpmākajā tabulā (Tabula 3) ir nosaukti sertifikāti, kurus ir izsniegušas eParaksts.lv

Sertifikācijas pakalpojumu sniedzēja Izsniegšanas sertificēšanas institūcija un kuri ir publiski pieejami un pakļauti šiem Sertifikācijas noteikumiem.

1.4.5. Kopā ar šo nodaļu, šo Sertifikācijas noteikumu 2. un 9. nodaļas tiek piemērotas tikai gala lietotāju kvalificētiem elektroniskā paraksta, eZīmoga sertifikātiem un nekvalificētiem autentifikācijas sertifikātiem. Šo sertifikātu lietojamība atbilst kvalificēto sertifikātu prasībām, kas noteiktas LR Elektronisko dokumentu likumā [1]:

Tabula 3. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Izsniegšanas sertificēšanas institūcijas izsniegtie sertifikāti.

| **Sertificēšanas institūcija** | **Sertifikāta nosaukums** | **Sertifikāta tips** | **Sertifikāta lietojums** |
|---|---|---|---|
| Izsniegšanas sertificēšanas institūcija | Kvalificēts elektroniska paraksta sertifikāts | Gala lietotāja kvalificēts publiskais sertifikāts | Kvalificētu elektronisko parakstu izveidošanai un pārbaudei un parakstu nenoliegšanas atbalstam ar augstu paļāvības līmeni |
| | Autentifikācijas sertifikāts | Gala lietotāja nekvalificēts publiskais sertifikāts | Gala lietotāja autentifikācija ar augstu paļāvības līmeni |
| | Autentifikācijas sertifikāts ar viedkartes pieslēgšanās funkciju | Gala lietotāja nekvalificēts publiskais sertifikāts | Gala lietotāja autentifikācija ar augstu paļāvības līmeni |
| | HSM Kvalificēts elektroniska paraksta sertifikāts | Gala lietotāja kvalificēts publiskais sertifikāts | Kvalificētu elektronisko parakstu izveidošanai un pārbaudei un parakstu nenoliegšanas atbalstam ar augstu paļāvības līmeni, kas fiziski glabājas lietotāja kriptogrāfiski pārveidotā veidā, ar šifrēšanas (HSM) iekārtām šifrētā vidē. |
| | HSM Autentifikācijas sertifikāts | Gala lietotāja nekvalificēts publiskais sertifikāts | Gala lietotāja autentifikācija ar augstu paļāvības līmeni, kas fiziski glabājas lietotāja kriptogrāfiski pārveidotā veidā, ar šifrēšanas (HSM) iekārtām šifrētā vidē. |
| | WEB portāla kvalificētais elektroniskā paraksta sertifikāts | Gala lietotāja kvalificēts publiskais sertifikāts | Kvalificētu elektronisko parakstu izveidošanai un pārbaudei un parakstu nenoliegšanas atbalstam ar augstu paļāvības līmeni, kas fiziski glabājas lietotāja kriptogrāfiski pārveidotā veidā, ar šifrēšanas (HSM) iekārtām šifrētā vidē. |
| | WEB portāla autentifikācijas sertifikāts | Gala lietotāja nekvalificēts publiskais sertifikāts | Gala lietotāja autentifikācija ar augstu paļāvības līmeni, kas fiziski glabājas lietotāja kriptogrāfiski pārveidotā veidā, ar šifrēšanas (HSM) iekārtām šifrētā vidē. |
| | eZīmoga sertifikāts | Gala lietotāja publisks sertifikāts | Apliecina Organizācijas, kā eZīmoga radītāja, veidoto elektronisko dokumentu autentiskumu un nemainīgumu |
| | eZīmoga autentifikācijas sertifikāts | Gala lietotāja nekvalificēts publisks sertifikāts | Organizācijas, kā eZīmoga radītāja, autentifikācija ar augstu paļāvības līmeni |

1.4.6. Turpmākajā tabulā (Tabula 4) ir parādīti infrastruktūras sertifikāti, kurus ir izsniegušas eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Izsniegšanas sertificēšanas institūcija un kuri ir publiski pieejami un pakļauti šiem Sertifikācijas noteikumiem:

Tabula 4. eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Izsniegšanas sertificēšanas institūcijas izsniegtie infrastruktūras sertifikāti.

| **Sertificēšanas institūcija** | **Sertifikāta nosaukums** | **Sertifikāta tips** | **Sertifikāta lietojums** | **Laika zīmogošanas** |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| | | | | **institūcija** |
| Izsniegšanas sertificēšanas institūcija | Tīmekļa vietnes autentifikācijas sertifikāts | infrastruktūras sertifikāts | tīmekļa mājas lapām un vietnēm | atļauts |
| | eZīmoga sertifikāts | Infrastruktūras sertifikāts | Apliecina organizācijas, kā eZīmoga radītāja, veidoto elektronisko dokumentu autentiskumu un nemainīgumu, fiziski glabājas šifrēšanas (HSM) iekārtā pie organizācijas | atļauts |
| | eZīmoga autentifikācijas sertifikāts | Infrastruktūras sertifikāts | Organizācijas, kā eZīmoga radītāja, autentifikācija ar augstu paļāvības līmeni, fiziski glabājas HSM iekārtā pie organizācijas | atļauts |
| | Koda parakstīšanas sertifikāts | infrastruktūras sertifikāts | koda parakstīšanai | atļauts |
| | Domēna kontroliera sertifikāts | infrastruktūras sertifikāts | Domēna lietotāju identifikācija un autentifikācija | atļauts |
| | Autentifikācijas reģistrēšanās XP sertifikāts | infrastruktūras sertifikāts | eParaksts.lv Sertifikācijas pakalpojumu sniedzēja darbinieku autentifikācija | atļauts |
| | Autentifikācijas domēna kontroliera sertifikāts | Nepublisks infrastruktūras sertifikāts | Sertifikāts domēnu kontrolierim iekšējai autentifikācijai | atļauts |
| | Domēna kontroliera sertifikāts | Nepublisks infrastruktūras sertifikāts | | atļauts |

1.4.7. Vienam mērķim izsniegtu sertifikātu nav ieteicams izmantot citiem mērķiem.

1.4.8. **Sertifikātu lietojuma ierobežojumi**

1.4.8.1. Sertificēšanas institūciju sertifikātus nevar izmantot nekādām citām funkcijām, izņemot Sertificēšanas institūciju funkcijas. Turklāt gala lietotāju pasūtītāja sertifikātus nedrīkst izmantot kā Sertificēšanas institūciju sertifikātus.

## 1.5. Noteikumu pārvaldība

1.5.1. **Šo dokumentu administrējošā organizācija**

1.5.2. Šos Sertifikācijas noteikumus ir reģistrējusi VAS "Latvijas Valsts radio un televīzijas centrs" (Reģ. Nr.: 40003011203), Ērgļu ielā 7, LV-1012, Rīga, Latvijas Republika.

1.5.3. Atbildīgais par šo Sertifikācijas noteikumu administrēšanas pārvaldību ir Valsts akciju sabiedrības "Latvijas Valsts radio un televīzijas centrs" Informācijas sistēmu daļas vadītājs.

1.5.4. **Kontaktinformācija**

| | |
|---|---|
| **Adrese** | VAS Latvijas Valsts radio un televīzijas centrs, Ērgļu iela 7, Rīga, LV-1012 |
| **Tālrunis** | +371 67315300 |
| **Fakss** | +371 67315577 |
| **E-pasts** | eparaksts@eparaksts.lv |

1.5.5. **Sertifikācijas noteikumu apstiprināšanas procesi**

1.5.5.1. Sertificēšanas noteikumi jāapstiprina Valsts akciju sabiedrības "Latvijas Valsts radio un televīzijas centrs" valdei.

## 1.6. Definīcijas un saīsinājumi

1.6.1. Saīsinājumu un definīciju saraksts:

| Saīsinājums | Paskaidrojums |
|---|---|
| *AKK* | Šifrēšanas iekārtas administratora karšu komplekts |
| *CN* | Sugas vārds (*Common Name)* |
| *CRL* | Apturēto un anulēto sertifikātu saraksts (*Certificate Revocation List)* |
| *DN* | Atšķirīgais vārds *(Distinguished Name)* |
| *EDL* | Elektronisko dokumentu likums |
| *E-ME, EME* | Iepriekšējais LVRTC Sertifikācijas pakalpojumu sniedzēja identifikators |
| *eID* | Elektroniskā identifikācijas karte, personu apliecinošs dokuments |
| *eParaksts.lv* | Jaunais LVRTC Sertifikācijas pakalpojumu sniedzēja identifikators |
| *eZīmogs* | Elektroniski dati, kas pievienoti elektroniskajam dokumentam vai loģiski saistīti ar šo dokumentu lai apliecinātu elektroniska dokumenta autentiskumu un zīmoga radītāja identitāti |
| *FIPS* | ASV Federālās informācijas apstrādes standarti |
| *HSM* | Šifrēšanas iekārta *(Hardware security module)* |
| *I&A* | Identificēšana un autentifikācija |
| *IS* | Informācijas sistēma |
| *ISI* | Izsniegšanas sertificēšanas institūcija |
| *LDAP* | Direktoriju vieglpiekļuves protokols *(Lightweight Directory Access Protocol v3)* |
| *LR* | Latvijas Republika |
| *LZI* | Laika zīmogošanas institūcija |
| *LZIe* | Laika zīmogošanas iekārta (serveris) |
| *LZM* | Laika zīmogošanas marķieris |
| *LVRTC* | Valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs" |
| *nonce* | Gadījuma kods *(Arbitrary number)* |
| *O* | Organizācija |
| *OCSP* | Tiešsaistes sertifikātu statusa protokols *(Online Certificate Status Protocol)* |
| *OID* | Objekta identifikators |
| *OKK* | Šifrēšanas iekārtas operatora karšu komplekts |
| *OU* | Organizācijas vienība *(Organisational Unit)* |
| *Parakstītājs* | Parakstītājs ir fiziska persona, kuru autentificē privātā atslēga un kurš kontrolē tās izmantošanu. Pakalpojuma "eZīmogs" gadījumā parakstītājs var būt arī juridiska persona |
| *Pasūtītājs* | Juridiska perona, kas slēdz līgumu ar Sertificēšanas institūciju par sertifikātu izsniegšanu. Pasūtītājs ir atbildīgs pret SI ar publiskās atslēgas sertifikātu saistītās privātās atslēgas izmantošanu |
| *PD* | Palīdzības dienests |
| *Persona* | Fiziska persona, ja vien noteikumos nav minēts savādāk vai no konteksta neizriet, ka tiek saprasta juridiska persona vai fiziska un juridiska persona |
| *PIN* | Drošības kods *(Personal identification number)* |
| *PKCS* | Publiskās atslēgas infrastruktūras šifrēšanas standarts *(Public-key Cryptography Standard)* |
| *PKI* | Publiskās atslēgas infrastruktūra *(Public Key Infrastructure*) |
| *PMLP* | LR Pilsonības un migrācijas lietu pārvalde |
| *PSI* | Politikas SI |
| *PUK* | Drošības kods *(Personal unblocking code)* |
| *Repozitarijs* | Failu vai dokumentu vietne tīmeklī |
| *Responderis* | Atbildētājs, SPS iekārta vai serviss (*Responder)* |
| *RFC* | Komentāru pieprasījums *(Request for Comments)* |
| *RI* | Reģistrācijas institūcija |
| *RNG* | Īstu gadījumskaitļu ģeneratoru *(Random number generator)* |
| *RSA* | Noteikts publiskās atslēgas algoritms |
| *SI* | Sertificēšanas institūcija |
| *SN* | Sertifikācijas noteikumi |
| *SP* | Sertifikātu politika |
| *SPS* | Sertifikācijas pakalpojumu sniedzējs |
| *SSCD* | Droša elektroniskā paraksta radīšanas iekārta *(Secure signature creation device)* |
| *SSI* | Saknes SI |
| *URL* | Universālais resursu vietrādis *(Uniform Resource Locator)* |

| | |
|---|---|
| *UTC* | Universālais koordinētais laiks *(Coordinated Universal Time)* |
| *Web portāls* | SPS internēta vietne www.eparaksts.lv |

# 2. Publicēšanas un repozitorija pienākumi

## 2.1. Direktoriju un sertifikātu pārbaudes pakalpojumi

2.1.1. **Direktoriju pakalpojumi**

2.1.1.1. Direktoriju pakalpojumi ir tādi eParaksts.lv SPS pakalpojumi, kuri, izmantojot LDAP un HTTP, nodrošina tiešsaistes piekļuvi sekojošiem eParaksts.lv SPS publiskiem resursiem:

2.1.1.1.1. eParaksts.lv SPS Saknes SI izsniegtiem sertifikātiem;

2.1.1.1.2. eParaksts.lv SPS Saknes SI CRL;

2.1.1.1.3. eParaksts.lv SPS uzticamo SI izsniegtiem sertifikātiem;

2.1.1.1.4. eParaksts.lv SPS uzticamo SI CRL;

2.1.1.1.5. eParaksts.lv SPS Politikas SI sertifikātam un CRL;

2.1.1.1.6. publiskiem sertifikātiem, kurus izsniegusi eParaksts.lv SPS Saknes SI un pakārtota uzticama SI (tostarp Izsniegšanas SI, OCSP un LZI sertifikāts);

2.1.1.1.7. eParaksts.lv SPS Saknes SI un pakārtotu uzticamu SI, tostarp Izsniegšanas SI izsniegtiem CRL.

2.1.1.2. Piekļuve eParaksts.lv SPS publicētajiem sertifikātiem ir neierobežota un pieejama 24 stundas dienā 7 dienas nedēļā ar garantēto pieejamību 99,6% gadā, neskaitot plānotus pakalpojumu sniegšanas pārtraukumus.

2.1.2. **Sertifikātu glabāšanas ilgums**

2.1.2.1. Sertifikāti, ko izsniedz eParaksts.lv SPS SSI, eParaksts.lv SPS direktoriju pakalpojumi tiek glabāti 30 gadus pēc attiecīgā sertifikāta derīguma termiņa beigām.

2.1.2.2. Kvalificētos e-paraksta sertifikātus eParaksts.lv SPS direktoriju pakalpojumi glabās 30 gadus pēc sertifikāta derīguma termiņa beigām.

2.1.2.3. Tīmekļa vietnes autentifikācijas sertifikāts, koda parakstīšanas, laika zīmogošanas iekārtas un domēna kontroliera sertifikātus eParaksts.lv SPS glabās 10 gadus pēc sertifikāta derīguma termiņa beigām.

2.1.3. **CRL glabāšanas ilgums**

2.1.3.1. eParaksts.lv SPS SI CRL iekļauta informācija tiek glabāta 30 gadus pēc CRL derīguma termiņa beigām.

2.1.4. **Sertifikātu pārbaudes pakalpojumi**

2.1.4.1. eParaksts.lv SPS sertifikātu pārbaudes pakalpojumi, izmantojot OCSP responderi, nodrošina eParaksts.lv SPS Saknes SI un eParaksts.lv SPS uzticamo SI izsniegto sertifikātu statusa pārbaudi. Visi sertifikāti jebkurā laikā var tikt pārbaudīti, izmantojot sertifikātu pārbaudes pakalpojumus.

2.1.4.2. Šie eParaksts.lv SPS pakalpojumi ir pieejami tiešsaistē – URL http://ocsp.eme.lv/responder.eme

2.1.5. **eParaksts.lv SPS Saknes SI sertifikāta sākotnējā pārbaude**

2.1.5.1. eParaksts.lv SPS Saknes SI sertifikāts ir pašparakstīts un sertifikāta izvilkums ir publicēts eParaksts.lv SPS tīmekļa vietnē.

2.1.6. **Sertifikātu pārbaude**

2.1.6.1. Aktuālākā informācija par sertifikāta statusu ir pieejama, izmantojot OCSP.

2.1.6.2. Maksimālā aizkave starp apturēšanas vai anulēšanas pieprasījuma vai ziņojuma saņemšanu un visiem pārbaudītājiem pieejamo sertifikāta statusa informācijas izmaiņu ir atkarīga no sertifikātu pārbaudes metodes:

2.1.6.2.1. sertifikātu pārbaudei, izmantojot eParaksts.lv SPS uzticamu OCSP responderi, tā nepārsniegs 24 stundas;

2.1.6.2.2. sertifikātu pārbaudei, izmantojot visjaunāko CRL, tā nepārsniegs 48 stundas

## 2.2. Informācijas publicēšana

2.2.1. Lai nodrošinātu pieteicējus, pasūtītājus, parakstītājus un pārbaudītājus ar sertifikātu pieteikumu un aprites un eParaksts.lv SPS pakalpojumu informāciju, eParaksts.lv SPS uztur tīmekļa vietni.

2.2.2. eParaksts.lv SPS tīmekļa vietne ir pieejama tiešsaistē ar URL http://www.eparaksts.lv

2.2.3. Piekļuve eParaksts.lv SPS tīmekļa vietnei ir neierobežota, un tā ir pieejama 24 stundas dienā 7 dienas nedēļā ar garantēto pieejamību 99,6% gadā, neskaitot plānotus pakalpojumu sniegšanas pārtraukumus.

2.2.4. eParaksts.lv SPS uzturēs aktuālas šādu dokumentu pašreizējās versijas:

2.2.4.1. Sertifikācijas pakalpojumu sniegšanas noteikumi (EDL, 23. nod., § 9);

2.2.4.2. eParaksts.lv SPS informācijas sistēmu, iekārtu un procedūru drošības apraksts (EDL, 23. nod., § 9);

2.2.4.3. eParaksts.lv SPS SP;

2.2.4.4. eParaksts.lv SPS SI SN;

2.2.5. Turklāt eParaksts.lv SPS tīmekļa vietnē var iegūt šādu informāciju:

2.2.5.1. informāciju par sertifikātu lietošanu;

2.2.5.2. pasūtītāja līgumu paraugus;

2.2.5.3. sertifikāta pieteikuma formu;

2.2.5.4. eParaksts.lv SPS informāciju – nosaukums, reģistrācijas numurs, adrese, kontaktinformācija;

2.2.5.5. visu reģistrācijas institūciju sarakstu;

2.2.5.6. Saknes SI sertifikātu un tā izvilkumu, kas radīts izmantojot SHA1 jaucējfunkciju;

2.2.5.7. eParaksts.lv SPS SI un uzticamo pakalpojumu (LZI un OCSP respondera) sertifikātus.

## 2.3. Informācijas publicēšanas laiks vai biežums

2.3.1. Tiek piemērotas šādas laika vai biežuma vadlīnijas informācijas publicēšanai SPS vietnē eParaksts.lv:

| | |
|---|---|
| **Izsniegtie sertifikāti** | Tiek publicēti nekavējoties pēc ģenerēšanas un uzticamas SI veiktas akceptēšanas |
| **Saknes SI *CRL*** | Katrus 3 mēnešus ar vienas nedēļas pārklāšanās periodu un pēc izsniegta sertifikāta anulēšanas |
| **SPS PSI *CRL*** | Katrus 3 mēnešus ar vienas nedēļas pārklāšanās laiku |
| **Izsniegšanas SI *CRL*** | Vismaz vienu reizi 24h |

| | |
|---|---|
| **Politikas, vadlīnijas** | Politikas un vadlīnijas tiks publicētas pēc apstiprināšanas |

## 2.4. Piekļuves kontroles direktorijai

2.4.1. Informācija, ko publicējuši eParaksts.lv SPS direktoriju pakalpojumi, ir nepārtraukti un publiski pieejama informācija. eParaksts.lv SPS ir ieviesis loģiskas un fiziskas kontroles pasākumus, lai nepieļautu nepilnvarotām personām veikt repozitorija ierakstu pievienošanu, dzēšanu vai modificēšanu.

2.4.2. Sertifikātu integritāte tiek nodrošināta, ierobežojot tiesības veikt izmaiņas datu bāzē, kā arī ierobežotu piekļuvi sistēmai. Turklāt eParaksts.lv SPS direktoriju pakalpojumiem ir iekšējs integritātes mehānisms. eParaksts.lv SPS regulāri veic datu faila integritātes pārbaudi, ar mērķi konstatēt jebkuru zema līmeņa datu bāzes bojājumu.

# 3. Identificēšana un autentifikācija (I&A)

## 3.1. Vārda piešķiršana

3.1.1. **Vārdu tipi**

3.1.1.1. Visiem sertifikātiem, ko izsniegusi eParaksts.lv SPS SSI, laukā **Izsniedzējs** (angl. Issuer) ir atšķirīgi vārdi atbilstoši X.509. Tiks lietoti šādi atribūti:

| | |
|---|---|
| ***countryName (C)*** | LV |
| ***organisationalUnitName (OU)*** | Sertifikacijas pakalpojumu dala |
| ***commonName (CN)*** | E-ME SSI (RCA) |

3.1.1.2. Visiem sertifikātiem, ko izsniegusi Politikas SI, laukā **Izsniedzējs** (angl. Issuer) ir atšķirīgi vārdi atbilstoši X.509. Tiks lietoti šādi atribūti:

| | |
|---|---|
| ***countryName (C)*** | LV |
| ***organisationalUnitName (OU)*** | Sertifikacijas pakalpojumu dala |
| ***commonName (CN)*** | E-ME PSI (PCA) |

3.1.1.3. Visiem eParaksts.lv SPS ISI izsniegtiem sertifikātiem laukā **Izsniedzējs** (angl. Issuer) ir īpašie vārdi atbilstoši X.509. Tiks lietoti šādi atribūti:

| | |
|---|---|
| ***countryName (C)*** | LV |
| ***organisationalUnitName (OU)*** | Sertifikacijas pakalpojumu dala |
| ***commonName (CN)*** | E-ME SI(CA1) |

vai

| | |
|---|---|
| ***countryName (C)*** | LV |
| ***organisationName (O)*** | VAS Latvijas valsts radio un televīzijas centrs |
| ***commonName (CN)*** | eParaksts CA |

3.1.1.4. Visiem eParaksts.lv SPS ISI izsniegtiem publiskajiem sertifikātiem laukā Parakstītājs (angl. Subject) ir īpašie vārdi atbilstoši X.509. Tiks lietoti šādi atribūti:

| | |
|---|---|
| ***countryName (C)*** | <Parakstītāja valsts (ISO 3166 kods)> |
| ***organisationName (O)*** | Izvēles: <Parakstītāja organizācija> |
| ***OrganisationalUnitName (OU)*** | Izvēles: <Parakstītāja struktūrvienība> |
| ***commonName (CN)*** | <vārds> un <uzvārds><br>Alternatīva: <PN: pseidonīms>lieto tikai paraksta sertifikātā |
| ***surName (SN)*** | <uzvārds (kā rakstīts identifikācijas dokumentā)><br>Netiek lietots pseidonīma gadījumā |
| ***givenName (G)*** | <vārds (kā rakstīts identifikācijas dokumentā)><br>Netiek lietots pseidonīma gadījumā |
| ***Serial Number*** | <unikāls ID numurs (personas kods)> |

3.1.1.5. Kvalificētie paraksta sertifikāti paplašinājumā Signatory Alternative Name pēc parakstītāja pieprasījuma satur sertifikāta pieteikšanās laikā piešķirtu e-pasta adresi (Type RFC822Name).

3.1.1.6. Katram uzvārdam, vārdam, sērijas numuram, sugas vārdam, organizācijas vārdam un struktūrvienībai maksimālais rindas garums ir 64 rakstzīmes.

3.1.1.7. Atribūti 'commonName', 'givenName', 'surName', 'organisationName' un 'organisationalUnitName' tiek veidoti kā UTF8 virkne. Šajos atribūtos var būt īpašas rakstzīmes (UTF8 Unicode).

3.1.1.8. Kvalificētiem sertifikātiem parakstītājs drīkst izvēlēties pseidonīmus (sk. 3.1.3. Šajā 3.1.15.).

3.1.1.9. **Tīmekļa vietnes SSL sertifikātam:**

| | |
|---|---|
| ***countryName (C)*** | <Parakstītāja valsts (ISO 3166 kods)> |
| ***organisationName (O)*** | <Parakstītāja organizācijas nosaukums> |
| ***organisationalUnitName (OU)*** | Izvēles: <Parakstītāja struktūrvienība> |
| ***commonName (CN)*** | <Parakstītāja tīmekļa vietne> |
| ***Locality(L)*** | <Parakstītāja adrese> |
| ***State(S)*** | <Parakstītāja pilsēta> |
| ***e-mail (E)*** | Izvēles: <Parakstītāja organizācijas oficiālais e-pasts> |
| ***Serial Number*** | <unikāls ID numurs sertifikāta numurs> |

3.1.1.10. **Koda parakstīšanas sertifikātam:**

| | |
|---|---|
| ***countryName (C)*** | <Parakstītāja valsts (ISO 3166 kods)> |
| ***organisationName (O)*** | <Parakstītāja organizācijas nosaukums> |
| ***organisationalUnitName (OU)*** | Izvēles: <Parakstītāja struktūrvienība> |
| ***commonName (CN)*** | <Parakstītāja organizācijas īsais nosaukums> |
| ***Locality(L)*** | <Parakstītāja adrese> |
| ***State(S)*** | <Parakstītāja pilsēta> |
| ***e-mail (E)*** | Izvēles: <Parakstītāja organizācijas oficiālais e-pasts> |
| ***Serial Number*** | <unikāls ID numurs (sertifikāta numurs)> |

3.1.1.11. **Domēna kontroliera sertifikātam:**

| | |
|---|---|
| ***countryName (C)*** | <Parakstītāja valsts (ISO 3166 kods)> |
| ***organisationName (O)*** | <Parakstītāja organizācijas nosaukums> |
| ***organisationalUnitName (OU)*** | Izvēles: <Parakstītāja struktūrvienība> |
| ***commonName (CN)*** | < Parakstītāja domēns > |
| ***Locality(L)*** | <Parakstītāja adrese> |
| ***State(S)*** | <Parakstītāja pilsēta> |
| ***e-mail (E)*** | Izvēles: <Parakstītāja organizācijas oficiālais e-pasts> |
| ***Serial Number*** | <unikāls ID numurs (sertifikāta numurs)> |

3.1.1.12. **eZīmoga sertifikātam:**

| | |
|---|---|
| ***Common name (CN) : eZīmogs*** | <Organizācijas nosaukums> : eZīmogs |
| ***Serial number (SN)*** | <Organizācijas reģistrācijas numurs> |
| ***Organisation name (O)*** | <Organizācijas nosaukums> |
| ***OrggnisationalUnitName (OU)*** | Izvēles: <Parakstītāja struktūrvienība> |
| ***CountryName (C)*** | <Parakstītāja valsts (ISO 3166 kods)> |
| ***e-mail (E)*** | Izvēles: < Organizācijas vai kontaktpersonas e-pasts > |

3.1.2. **Prasības pret vārdu atbilstību**

3.1.2.1. Parakstītāja vārdam sertifikātā jābūt ar nozīmi no tāda viedokļa, lai eParaksts.lv SPS SI būtu atbilstoši pierādījumi par esošo saistību starp šiem vārdiem un vienumiem, kam tie pieder.

3.1.3. **Pasūtītāju pseidonimitāte**

3.1.3.1. Piesakoties sertifikātam, parakstītājs drīkst izvēlēties pseidonīmu. Ja kvalificētam sertifikātam vārda vietā parakstītājs vēlas lietot pseidonīmu, tad jānorāda, ka tas ir pseidonīms (no parakstītāja īstā personiskā vai organizācijas nosaukuma atšķirīgi vārdi), pievienojot sākumā „PN: ". Sertifikāts norādīs, ka identitāte ir autentificēta, bet tiek aizsargāta.

3.1.3.2. Pseidonīma lietošanas gadījumā izvēlētais pseidonīms tiks ievietots pasūtītāja DN atribūtā *'commonName'*. Tādā gadījumā netiks lietoti atribūti *'surName'* un *'givenName'*.

3.1.3.3. Nav atļauta pseidonīmu lietošana parakstītāja autentifikācijas sertifikātos.

3.1.3.4. Jebkurā gadījumā parakstītājam jāsniedz eParaksts.lv SPS savs vārds un kontaktinformācija. eParaksts.lv SPS ir atļauts sniegt personas vārdu pusei, kuru skaidri ir pilnvarojis parakstītājs vai pasūtītājs, vai pēc rakstiska pieprasījuma atbilstošai valsts pārvaldes institūcijai.

3.1.3.5. Vienīgi parakstītājs ir atbildīgs par izvēlēto pseidonīmu. eParaksts.lv SPS nav atbildīgs par pseidonīmu pareizrakstības pārbaudi un nozīmi. eParaksts.lv SPS ir tiesīgs atteikt vai apturēt jebkuru pieteikumu sertifikāta saņemšanai nenorādot atteikuma iemeslu.

3.1.4. **Dažādu vārdu formu interpretācijas noteikumi** – Nav nosacījumu

3.1.5. **Vārdu unikalitāte**

3.1.5.1. Parakstītāja (Subject) laukā jābūt atšķirīgam vārdam (DN) atbilstoši X.509. DN jābūt unikālam katram SI sertificētam parakstītājam atbilstoši definētajam izsniedzēja (Issuer) vārda laukam. SI var izsniegt vienam un tam pašam parakstītājam vairāk kā vienu sertifikātu ar to pašu DN.

3.1.5.2. Kā minimums, tiek pārbaudīts, vai piedāvātais atšķirīgais vārds jau nav lietots eParaksts.lv SPS SI citam vienumam izsniegtā sertifikātā. eParaksts.lv SPS SI noraidīs katru neunikālu elektroniskā sertifikāta pieprasījumu. Vārda ne unikalitātes dēļ SI noraidīti pasūtītāji tiks informēti tik drīz, cik tas ir praktiski iespējams.

3.1.6. **Preču zīmju pazīšana, pārbaude un loma**

3.1.6.1. **Publiskās un privātās atslēgas**

3.1.6.1.1. Visas ģenerēto publisko un privāto atslēgu intelektuālā īpašuma tiesības tiks piešķirtas vienībai, kura ir ģenerējusi šādas atslēgas vai kurai tās ir ģenerētas (piem., uzticama SI, gala lietotāji) vai tās norādītai vienībai. Pakārtotas PKI vienības vai gala lietotāji neiegūs jebkādas tiesības attiecībā uz sertifikātiem, to saturu, formātu vai struktūru.

3.1.6.2. **Sertifikāts**

3.1.6.3. Sertifikāta pieteicējiem aizliegts savos sertifikātu pieteikumos lietot vārdus, kuri aizskar citu personu intelektuālā īpašuma tiesības. Tomēr eParaksts.lv SPS nepārbauda, vai sertifikāta pieteicējam ir intelektuālā īpašuma tiesības uz sertifikāta pieteikumā minēto vārdu. eParaksts.lv SPS neizlemj arbitrāžā, nepilda starpnieka lomu vai citādi neizšķir jebkādas domstarpības par jebkura domēna vārda, tirdzniecības nosaukumu, tirdzniecības zīmes vai pakalpojuma apzīmējuma piederību.

3.1.6.4. eParaksts.lv SPS rezervē tiesības jebkurā laikā apturēt vai anulēt jebkuru sertifikātu saskaņā ar šajos Sertificēšanas noteikumos un atbilstošajā Sertifikātu politikā izklāstītajām procedūrām un politikām. Ar šo eParaksts.lv SPS piešķir visām pakārtotām PKI vienībām, gala lietotājiem, pārbaudītājiem un citām vienībām neekskluzīvu un atsaucamu licenci attēlot un izplatīt eParaksts.lv SPS

SI izsniegto sertifikātu kopijas ar mērķi saskaņā ar šo SN prasībām nodrošināt, lietot sertifikātus vai paļauties uz sertifikātiem un sertifikācijas pakalpojumiem.

## 3.2. Sākotnējās identitātes pārbaude

3.2.1. **Privātās atslēgas piederības pierādījuma metode**

3.2.1.1. Sertifikāta pieprasījums eParaksts.lv SPS SI tiek apstiprināts tikai kā eParaksts.lv SPS SI droši pārraidīts PKCS#10 sertifikāta pieprasījums. PKCS#10 pieprasījuma paraksta pārbaude ir pietiekams atbilstošās privātās atslēgas piederības pierādījums.

3.2.2. **Organizācijas identitātes autentifikācija**

3.2.2.1. Juridiskas personas drīkst kļūt par un darboties kā uzticama Sertificēšanas institūcija eParaksts.lv SPS uzticības ķēdē ar nosacījumu, ka ir pierādīta viņu identitāte un spēja sniegt sertificēšanas institūcijas pakalpojumus saskaņā ar eParaksts.lv SI SN.

3.2.2.2. Lai nodrošinātu darbības integritāti un uzticamību visā PKI hierarhijā, uzticamām sertificēšanas institūcijām jāapņemas pakļauties šajos SN aprakstītajām procedūrām un to pieņemtajiem SN kā daļai no sertifikāta pieteikšanas procesa. Šī nodaļa nosaka prasības eParaksts.lv SPS uzticamu Sertificēšanas institūciju pieteicēju identitātes pārbaudei. Prasības uzticamai SI pakārtotajām PKI vienībām ir noteiktas atbilstošajos uzticamu SI sertificēšanas noteikumos.

3.2.2.3. eParaksts.lv SPS SI vai RI, kas darbojas eParaksts.lv SPS SI vārdā, ir jānodrošina, ka pieteicēji tiek pareizi identificēti un autentificēti un pieteicēju sertifikātu pieprasījumi ir pilnībā aizpildīti, kā arī precīzi un pareizi apstiprināti.

3.2.2.4. Pieteicēja identitāte un spēja sniegt uzticamus SI pakalpojumus eParaksts.lv SPS PKI ietvaros tiek noteikta sarunu un uzticamas sertificēšanas institūcijas izveidošanas procesa laikā. Šāds process ietver:

3.2.2.4.1. augsta līmeņa vadības kontaktus starp eParaksts.lv SPS un pieteicēju;

3.2.2.4.2. eParaksts.lv SPS darbinieku pieteicēja telpu apmeklējumu;

3.2.2.4.3. juridiskas personas reģistrācijas numurs (Uzņēmumu reģistra uzturētajos reģistros);

3.2.2.4.4. publiskas personas gadījumā - oficiāla vēstule no augstākstāvošas institūcijas (ja tāda ir), kuras ietvaros pieteicējs darbojas, kurā ir norādīts tās atbalsts un pieteicēja tiesības sniegt uzticamus SI pakalpojumus;

3.2.2.5. Šādu faktu pārbaudi:

3.2.2.5.1. šīs institūcijas pilns juridiskais nosaukums un juridiskā adrese;

3.2.2.5.2. fiziskās(o) personas(u) identitāte un tiesības ar pilnvarojumu pārstāvēt pieteicēju saskaņā ar šo SN 3.2. nod.

3.2.2.6. Gadījumos, kad parakstītājs ir persona, kas ir identificēta kā juridiska persona vai cita organizatoriska vienība, identificētajai personai jāsniedz šādi pierādījumi:

3.2.2.6.1. pilns parakstītāja vārds (uzvārds un vārds);

3.2.2.6.2. valstiski atzīts identifikācijas numurs vai citi parakstītāja atribūti, kurus iespēju robežās būtu iespējams izmantot, lai atšķirtu vienu personu no citām ar to pašu vārdu;

3.2.2.6.3. saistītās juridiskās personas vai citas organizatoriskas vienības pilns nosaukums un juridiskais statuss;

3.2.2.6.4. piemērota saistītās juridiskās personas vai citas organizatoriskas struktūrvienības esošā reģistrācijas informācija (piem., uzņēmuma reģistrācija);

3.2.2.6.5. pierādījums, ka parakstītājs ir saistīts ar juridisko personu vai citu organizatorisko vienību.

3.2.2.7. Katru reizi, kad pieteicējs prasa iekļaut sertifikātā informāciju par noteiktu organizāciju, pieteicējam jānodrošina rakstiski pierādījumi, ka organizācija pilnā mērā apzinās šo faktu. Visos gadījumos, izmantojot citas piegādes metodes, jāuzrāda piemēroti juridiskie dokumenti, kas pierāda sertificējamos datus. Autentifikācija jāveic eParaksts.lv SPS ISI vai RI.

3.2.3. **Personas identitātes pārbaude**

3.2.3.1. Fiziskas personas identitātes autentifikācija pamatojas uz pieteicēja personīgu (fizisku) klātbūtni RI. Pieteicējam jāidentificē sevi ar derīgu personu apliecinošu dokumentu, saskaņā ar Personu apliecinošu dokumentu likumā noteikto.

3.2.3.2. WEB Portāla sertifikātu gadījumā personas identitāti var autentificēt arī Latvijā licenzētas bankas, ar kurām SI noslēdzis vienošanos, vai izmantojot LMT pakalpojumu „Mobilais kods".

3.2.3.3. Parakstītāja iesniegtā informācija tiek pārbaudīta LR Iedzīvotāju reģistrā. Pārbaudes rezultātu un visas sākotnējās identitātes pārbaudes procedūras pareizību pārbauda pilnvarotā eParaksts.lv SPS SI otrā uzticības loma.

3.2.4. **Nepārbaudītā informācija**

3.2.4.1. Parakstītāja e-pasta adrese sākotnējās reģistrācijas laikā netiek pārbaudīta un to sauc par "nepārbaudītu pasūtītāja informāciju".

3.2.5. **Tiesību pārbaude**

3.2.5.1. Katru reizi, kad pieteicējs pieprasa noteiktas organizācijas informācijas iekļaušanu sertifikātā, pieteicējam ir jānodrošina rakstiski pierādījumi, ka šī organizācija pilnā mērā apzinās šo faktu.

3.2.5.2. Ja sertifikāts ietver fiziskas personas kā organizācijas pilnvarota pārstāvja identificējošu informāciju, tad tiek pārbaudīta arī minētās personas nodarbinātība un tās tiesības rīkoties organizācijas vārdā.

3.2.5.3. eParaksts.lv SPS ISI sertifikāta pieteicējam jāiesniedz rakstiski pierādījumi, lai pārbaudītu iepriekš minēto informāciju.

3.2.6. **Savstarpējās sadarbības kritēriji un jaunizdošanas pieprasījumu I&A**

3.2.6.1. Šobrīd eParaksts.lv Sertifikācijas pakalpojumu sniedzējs nav definējis jebkādus savstarpējās sadarbības kritērijus integrācijas ar citiem SPS.

3.2.6.2. Sertifikātu jaunizdošana drīkst notikt pēc sazināšanās ar eParaksts.lv SPS amatpersonu, eParaksts.lv SPS drošības amatpersonu un uzticamas SI pārstāvi. Uzticamas SI sertifikātu jaunizdošanas pieprasījums jāveic rakstiski uz papīra.

3.2.6.3. Sertifikātu jaunizdošanas pieprasījumu identifikācijas un autentifikācijas procedūra seko sākotnējai identitātes pārbaudes procedūrām, kas noteiktas šajos SN (sk. 3.2. nodaļu).

3.2.6.4. WEB sertifikātu jaunizdošana notiek brīdī, kad ir beidzies WEB sertifikāta derīguma termiņš un parakstītājs autorizējas pie HSM caur WEB portālu.

3.2.6.5. Sertifikātu (viedkartē) attālinātas jaunizdošanas gadījumā, identifikācijas un autentifikācijas procedūra notiek izmantojot derīgu personas autentifikācijas sertifikātu ko izsniegusi eParaksts.lv ISI.

## 3.3. Apturēšanas, anulēšanas un atjaunošanas pieprasījumi

3.3.1. Sertifikātu anulēšanas pieprasījums jāveic rakstiski uz papīra vai ar elektroniski parakstīta dokumenta EDL izpratnē starpniecību.

3.3.2. Visiem anulēšanas pieprasījumiem ir jābūt derīgiem. eParaksts.lv SPS drošības amatpersonai ir jāautentificē, ka eParaksts.lv SPS PSI vai OCSP respondera sertifikāta anulēšanas pieprasījums ir pilnībā aizpildīts, precīzs un pienācīgi pilnvarots. Šādu derīgumu nosaka to atbilstība vai neatbilstība šo SN procedūrām (sk. 4.9), kuras ietver atsauces uz personas, kas drīkst veikt pieprasījumu, pilnvarām.

3.3.3. SI vai OCSP sertifikātu anulēšana tiks veikta pēc sazināšanās ar eParaksts.lv Sertifikācijas pakalpojumu vadītāju un eParaksts.lv SPS drošības amatpersonu.

3.3.4. eParaksts.lv ISI nodrošina sertifikātu apturēšanas, atjaunošanas un anulēšanas pakalpojumus.

3.3.5. Sertifikāta apturēšanas operācija ir sertifikāta atzīšana par uz laiku nederīgu. Apturēta sertifikāta darbība drīkst tikt atkārtoti aktivēta (atjaunošana). Sertifikāta anulēšana ir sertifikāta atzīšana par pastāvīgi nederīgu.

3.3.6. eParaksts.lv SPS izsniegtajiem sertifikātiem tiek nodrošināti šādi sertifikātu izsniegšanas pieprasījumi (Tabula 5):

Tabula 5. eParaksts.lv SPS sertifikātu izsniegšanas pieprasījumi

| Sertifikāta tips | Nodrošinātais pieprasījuma tips | | | |
|---|---|---|---|---|
| | Izsniegšana | Apturēšana | Atjaunošana | Anulēšana |
| Parakstīšanas, autentifikācijas un šifrēšanas sertifikāti viedkartē | ✓ | ✓ | ✓ | ✓ |
| SSL sertifikāts | ✓ | × | × | ✓ |
| Koda parakstīšanas sertifikāts | ✓ | × | × | ✓ |
| Domēna kontroliera sertifikāts | ✓ | × | × | ✓ |
| Laika zīmogošanas iekārtas sertifikāts | ✓ | × | × | ✓ |
| WEB portāla sertifikāti | ✓ | × | × | ✓ |
| eZīmoga sertifikāti | ✓ | ✓ | ✓ | ✓ |

3.3.7. **Gala lietotāja sertifikātu apturēšanas pieprasījums**

3.3.7.1. Personas vai organizācijas vienības, kas ir pilnvarotas (sk. **4.8.1** sadaļu) pieprasīt sertifikāta apturēšanu, drīkst iesniegt pieprasījumu šādi:

3.3.7.1.1. piezvanot eParaksts.lv SPS Palīdzības dienestam (PD) – Palīdzības dienests darbojas visu laiku (24 stundas dienā un 7 dienas nedēļā). eParaksts.lv SPS PD kontaktinformācija ir dota 1.4.7.3. sadaļā, vai to var atrast vietnē http://www.eparaksts.lv un https://www.eparaksts.lv/lv/viedkartes-eparaksts/atbalsts-viedkartes-lietotajiem/;

3.3.7.1.2. ar fizisku klātbūtni vienā no eParaksts.lv SPS Klientu apkalpošanas punktiem – eParaksts.lv SPS Klientu apkalpošanas punktu faktisko adresi var pieprasīt no eParaksts.lv SPS PD (1.4.7.3. nodaļa), vai to var atrast vietnē http://www.eparaksts.lv

3.3.7.2. Lai veiktu apturēšanu pa tālruni, ir nepieciešama sertifikāta apturēšanas parole. Apturēšanas paroli nosaka parakstītājs sertifikāta pieteikuma laikā.

3.3.7.3. Latvijas tiesai ir atļauts pieprasīt gala lietotāja kvalificēta paraksta sertifikāta apturēšanu. eParaksts.lv SPS nepieciešams rakstisks apstiprinājums, kurš deklarē ārvalstu tiesas lēmumu par izpildāmu Latvijā vai sabiedriskas iestādes lūgumu apturēt eParaksts.lv SPS izsniegtu sertifikātu.

3.3.7.4. WEB portāla sertifikātu apturēšana netiek veikta.

3.3.8. **Gala lietotāja sertifikātu anulēšanas pieprasījums**

3.3.8.1. Personas vai organizācijas vienības, kas ir pilnvarotas pieprasīt sertifikāta apturēšanu (sk. 4.8.1. sadaļu), drīkst iesniegt pieprasījumu personīgi eParaksts.lv SPS Klientu apkalpošanas punktā . eParaksts.lv SPS Klientu apkalpošanas punktu faktisko adresi var pieprasīt no eParaksts.lv SPS PD (1.4.7.3. sadaļa), vai to var atrast vietnē http://www.eparaksts.lv

3.3.8.2. Anulēšanas pieprasījumu gadījumā personai, kas veic pieprasīšanu, sevi jāidentificē, iesniedzot spēkā esošu identifikācijas dokumentu.

3.3.8.3. Turklāt pieprasītājam jānorāda šāda informācija:

3.3.8.3.1. pasūtītāja vārds un uzvārds;

3.3.8.3.2. pasūtītāja līguma numurs;

3.3.8.3.3. galvenā līguma numurs (ja tāds ir);

3.3.8.3.4. anulēšanas iemesls.

3.3.8.4. Latvijas tiesai ir atļauts pieprasīt gala lietotāja kvalificēta paraksta sertifikāta anulēšanu. eParaksts.lv SPS nepieciešams rakstisks apstiprinājums, kurš deklarē ārvalstu tiesas lēmumu par izpildāmu Latvijā vai sabiedriskas iestādes lūgumu anulēt eParaksts.lv SPS izsniegtu sertifikātu.

3.3.9. **Gala lietotāja sertifikāta atjaunošanas pieprasījums**

3.3.9.1. Personas vai organizācijas vienības, kas ir pilnvarotas pieprasīt sertifikāta atjaunošanu (sk. 4.8.1. nodaļu), drīkst iesniegt personīgi pieprasījumu eParaksts.lv SPS Klientu apkalpošanas punktā. eParaksts.lv SPS Klientu apkalpošanas punktu faktisko adresi var pieprasīt no eParaksts.lv SPS PD (1.4.7.3. nodaļa), vai to var atrast vietnē http://www.eparaksts.lv

3.3.9.2. Atjaunošanas pieprasījumu gadījumā personai, kas veic pieprasīšanu, sevi jāidentificē, iesniedzot spēkā esošu identifikācijas dokumentu.

3.3.9.3. Turklāt pieprasītājam jānorāda šāda informācija:

3.3.9.3.1. pasūtītāja vārds un uzvārds;

3.3.9.3.2. pasūtītāja līguma numurs;

3.3.9.3.3. galvenā līguma numurs (ja tāds ir);

3.3.9.3.4. sertifikāta sērijas numurs;

3.3.9.3.5. atjaunošanas iemesls.

3.3.10. **eParaksts.lv SPS ISI sertifikāta anulēšanas pieprasījums**

3.3.11. eParaksts.lv SPS ISI sertifikātus nedrīkst apturēt. Ja nepieciešams, eParaksts.lv SPS Izsniegšanas SI sertifikātus var anulēt pirms to derīguma termiņa beigām. Uzticamas SI sertifikātu anulēšanas pieprasījums jāiesniedz rakstveidā.

3.3.12. Nepieciešams, lai visi anulēšanas pieprasījumi būtu derīgi. eParaksts.lv SPS sistēmas amatpersonai jāautentificē, ka eParaksts.lv SPS ISI sertifikāta anulēšanas

pieprasījums ir pilnībā aizpildīts, precīzs un pareizi sankcionēts. Šāds derīgums jānosaka ar to atbilstību vai neatbilstību šo SN procedūrām (sk. 3.4.9), kuras ietver atsauces uz personas, kas drīkst veikt pieprasījumu, tiesībām.

3.3.13. SI sertifikātu anulēšana jāveic pēc sazināšanās ar eParaksts.lv Sertifikācijas pakalpojumu vadītāju un eParaksts.lv SPS drošības amatpersonu.

## 3.4. Laika zīmogošana

### 3.4.1. **Laika zīmoga marķieris**

3.4.1.1. eParaksts.lv SPS LZI elektroniski paraksta izdotos LZM ar privāto atslēgu, kas ir rezervēta tikai šim mērķim.

3.4.1.2. LZM nesatur nekādus citus parakstus kā tikai eParaksts.lv SPS LZI parakstu. eParaksts.lv SPS LZI sertifikāta identifikators kā atribūts tiek ietverts parakstīšanas sertifikātā.

3.4.1.3. Ja tiek atklāts, ka iekšējais pulkstenis ir ārpus noteiktās precizitātes, HSM pārtrauc LZM izdošanu. HSM nedarbosies, ja iekārta ir ārpus šīs noteiktās precizitātes.

3.4.1.4. Katrs LZM satur:

3.4.1.4.1. datu, kurus sniedz pieprasītājs un kuriem tiek uzlikts laika zīmogs, attēlojumu (piemēram, jaucējfunkcijas vērtību);

3.4.1.4.2. unikālu sērijas numuru, kas var tikt izmantots gan LZM pieprasīšanai, gan LZM identificēšanai;

3.4.1.4.3. Laika zīmoga politikas identifikators;

3.4.1.4.4. Laika vērtības, kuras LZIe izmanto LZM, ir izsekojamas līdz vismaz vienai no reālajām laika vērtībām, kuras izplata UTC(k) laboratorija;

3.4.1.4.5. LZM tiek parakstīts, izmantojot atslēgu, kas ir ģenerēta tikai šim mērķim (eParaksts.lv SPS LZI sertifikāts, sadaļā 4);

3.4.1.4.6. LZI un LZIe identifikators: TSA lauka (field) mērķis ir dot norādi, lai identificētu LZI vārdu. Tas atbilst vienam no parakstītāja (Signatory) vārdiem, kas ir iekļauti sertifikātā, ko izmanto, lai pārbaudītu LZM (skat 4. sadaļu); LZIe identificē laika zīmoga izsniedzošās iekārtas numuru;

3.4.1.4.7. neobligāto lauku “nonce”.

Tabula 6. LZM sertifikāta saturs

| **Lauka nosaukums** | **Vērtība vai vērtības robeža** | |
|---|---|---|
| *VersijasNr* | 1 | |
| *PolicyID* | 1.3.6.1.4.1.32061.1.1.1 | |
| *messageImprint* | jābūt tādai pašai vērtībai kā līdzīgā laukā *TimeStampReq*, ja jaucējfunkcijas vērtības izmērs sakrīt ar gaidāmo jaucējfunkcijas algoritma izmēru, kas identificēts *hashAlgorithm* | |
| *serialNumber* | Laika zīmogošanas lietotājiem JĀBŪT gataviem izmantot līdz 160 bitiem lielus skaitļus | |
| *genTime* | *GeneralizedTime* | |
| *Accuracy* | 1s | Izvēles |
| *ordering* | JĀBŪT norādītam, ja līdzīgs lauks bija norādīts *TimeStampReq*. Šajā gadījumā tai JĀBŪT tādai pašai vērtībai | Pēc noklusējuma nepatiess |
| *nonce* | | Izvēles |
| *TSA* | eParaksts.lv LZI(TSA) | eParaksts.lv SPS LZI nosaukums |
| TSU | nCipher DSE ESN:4911-62A6-9923 | LZ izsniedzošās iekārtas numurs |
| *extensions* | *[1] IMPLICIT extensions* | Izvēles |

3.4.2. **Pulksteņa sinhronizācija ar UTC**

3.4.2.1. eParaksts.lv SPS LZI nodrošina, ka tās pulkstenis ir sinhronizēts ar UTC deklarētās 1 sekundes precizitātes ietvaros.

3.4.2.2. It sevišķi:

3.4.2.2.1. LZIe pulksteņu kalibrēšana tiek uzturēta tā, ka pulksteņiem nevajadzētu pārkāpt deklarēto precizitāti;

3.4.2.2.2. LZIe pulksteņi ir aizsargāti pret apdraudējumiem, kuru rezultātā varētu rasties neatklāta pulksteņa pārmaiņa, kura to izvirzītu ārpus tā kalibrācijas;

3.4.2.2.3. atšķirības starp sistēmas pulksteni un UTC tiks atklātas. Laika kalkulācija atbilst BIPM un NTP ieteikumiem;

3.4.2.2.4. eParaksts.lv SPS LZI ir jānodrošina, ka pulksteņu sinhronizācija tiek uzturēta, kad parādās liekā sekunde, kad to ir paziņojusi atbilstošā organizācija. Divas reizes gadā – 30.jūnija un 31.decembra pēdējās minūtes laikā – automātiski tiek veikta noregulēšana, lai nodrošinātu to, ka kopējā atšķirība starp UTC un UT1 nepārsniegs 0,9 sekundes pirms nākamās paredzētās noregulēšanas. Ir jāsaglabā ieraksts par precīzo laiku (deklarētās precizitātes ietvaros), kad šī pārmaiņa ir notikusi.

3.4.3. **Laika zīmogošanas institūcijas ziņojumi**

3.4.3.1. eParaksts.lv SPS LZI ir pakalpojums, ko sniedz eParaksts.lv SPS, kas ir sertificēts kā Uzticams sertifikācijas pakalpojumu sniedzējs LR Elektronisko dokumentu likumā [3] paredzētajā kārtībā. eParaksts.lv SPS LZI ir pakļauta Latvijas Republikas normatīvajiem aktiem.

3.4.3.2. Katrs laika zīmoga marķieris, ko izsniegusi eParaksts.lv SPS LZI, satur politikas objekta identifikatoru - **OID 1.3.6.1.4.1.32061.1.1.1**

3.4.3.3. eParaksts.lv SPS LZI izmanto tādu kriptogrāfisko algoritmu un atslēgu garumu, kas atbilst ETSI TS 101 861 [8]

3.4.3.3.1. **Jaucējfunkcijas:** SHA-1, SHA 256, 384, 512

3.4.3.3.2. **Paraksts:** sha1WithRSAEncryption, 2048 bitu atslēga.

3.4.3.4. SPS paziņos savā tīmekļa vietnē, ja noskaidros, ka eParaksts.lv laika zīmogošanas institūcijas SPS PKI izmantotie kriptogrāfiskie algoritmi un atslēgu garumi vairs nav uzskatāmi par drošiem.

3.4.3.5. eParaksts.lv SPS LZI sertifikāta, kas izmantots LZM parakstīšanā, paredzētais darbības laiks ir 6 gadi.

3.4.3.6. eParaksts.lv SPS LZI nodrošina uzticama UTC laika avota precizitāti 1 sekunde un neizsniegs laika zīmogus ārpus šīs noteiktās laika precizitātes.

3.4.3.7. Pasūtītāju pienākumi ir noteikti sadaļā 1.3.6.3.

3.4.3.8. Pārbaudītāju pienākumi ir noteikti sadaļā 1.3.7.2.

3.4.3.9. Lai pārbaudītu laika zīmoga marķieri, pārbaudītājam saprātīgi paļaujoties uz LZM un uz jebkuru iespējamo derīguma perioda ierobežojumu, eParaksts.lv SPS LZI nodrošinās specifisku programmatūru LZM pārbaudei.

3.4.3.10. Bezmaksas programmatūra ir lejupielādējama URL: https://www.eparaksts.lv/lv/palidziba-1/lejupielades

3.4.3.11. Šī aplikācija veiks eParaksts.lv SPS LZI sertifikāta derīguma pārbaudi, pārliecinoties par eParaksts.lv SPS LZI paraksta nenoliedzamību. Tiešsaistes LZM pareizības pārbaude tiks nodrošināta vēl desmit gadus pēc tā izdošanas.

3.4.3.12. eParaksts.lv SPS uztur drošu auditācijas ierakstu un arhīva sistēmu. LZI notikumu ieraksti tiks saglabāti vismaz desmit gadus pēc LZI sertifikāta derīguma termiņa izbeigšanās. Pēc norādītā informācijas uzturēšanas laika izbeigšanās, dati tiks nogādāti valsts arhīvam.

3.4.3.13. eParaksts.lv SPS LZI atbildība pret gala lietotājiem ir jānorāda līgumos ar pasūtītājiem. Šie SN tiek pievienoti šajos līgumos kā to sastāvdaļa.

3.4.3.14. Ja puses nav īpaši vienojušās savādāk, atbildība pret parakstītājiem, pasūtītājiem, pārbaudītājiem un jebkurām citām personām attiecībā uz jebkura veida prasībām ir ierobežota un ir balstīta uz katru derīgu (sertifikāts nav apturēts vai anulēts) sertifikātu atsevišķi, neatkarīgi no transakciju un elektronisko parakstu skaita vai tādām darbībām, kuras izriet vai ir saistītas ar attiecīgo sertifikātu vai jebkādiem pakalpojumiem, kas sniegti saistībā ar attiecīgo sertifikātu.

3.4.3.15. Visas un jebkuras prasības eParaksts.lv SPS pakalpojumu ietvaros, kas saistītas ar sertifikātu (neatkarīgi no personas, kas radījusi zaudējumus vai personas, kas izsniedza sertifikātu vai sniedza sertifikācijas pakalpojumus), ir pakļautas ar konkrēto sertifikātu saistītiem atbildības ierobežojumiem saskaņā ar šiem SN.

3.4.3.16. Ņemot vērā augstākminētos ierobežojumus, eParaksts.lv SPS atbildība pret parakstītājiem, pasūtītājiem, pārbaudītājiem un jebkurām citām personām saistībā ar darbību, kas veikta ar eParaksts.lv SPS izsniegtu sertifikātu tā derīguma termiņa laikā, ja vien tas šīs darbības brīdī nav bijis anulēts vai apturēts, ir ierobežota eParaksts.lv SPS noteiktā apmērā.

3.4.3.17. Nekādā gadījumā eParaksts.lv SPS atbildība nedrīkst pārsniegt normatīvajos aktos noteiktos ierobežojumus.

3.4.3.18. Gadījumā, ja kāda daļa no šiem SN ar tiesas vai citas pilnvarotas institūcijas lēmumu ir atzīta par spēkā neesošu, pārējās šo SN daļas ir uzskatāmas par spēkā esošām.

3.4.3.19. Sūdzības, ierosinājumi un ziņojumi attiecībā uz eParaksts.lv SPS LZI darbību ir jāadresē personām, kas minētas šī dokumenta 1.5.3.punktā.

3.4.4.**eParaksts.lv SPS LZI pienākumi pret pasūtītājiem un parakstītājiem**

3.4.4.1. eParaksts.lv SPS uzņemas sekojošos pienākumus pret LZI pasūtītājiem un parakstītājiem:

3.4.4.1.1. nodrošināt, ka laika zīmogošanas iekārta (LZIe) uztur minimālo UTC laika precizitāti ne zemāku kā 1 (viena) sekunde;

3.4.4.1.2. veikt iekšējās un ārējās pārbaudes, lai nodrošinātu atbilstību attiecīgajiem normatīvajiem aktiem un iekšējām eParaksts.lv SPS politikām un procedūrām;

3.4.4.1.3. nodrošināt augstu pieejamību pie eParaksts.lv SPS LZI sistēmām, izņemot plānotu tehnisko pārtraukumu un laika sinhronizācijas zaudēšanas gadījumos.

# 4. Sertifikātu dzīves cikla darbības prasības

## 4.1. Sertifikātu pieteikums

4.1.1.**Sertifikātu pieteikuma pieteikšanas tiesības**

4.1.1.1. Jebkura reģistrēta organizācija vai juridiska persona drīkst pieteikties eParaksts.lv SPS SSI sertifikātiem.

4.1.1.2. eParaksts.lv SPS SI izsniegtu sertifikātu pieteikuma procedūra ir pakārtotas uzticamas sertificēšanas institūcijas izveidošanas neatņemama sastāvdaļa. Kā tāda, procedūra tiks iniciēta tikai tad, kad eParaksts.lv SPS SI uzskata, ka pieteicējs ir izpildījis vai var izpildīt visas SPS izvirzītās prasības, tajā skaitā, bet ne tikai tehniskās, finansiālās, infrastruktūras, prasmju, juridiskās un normatīvo aktu prasības.

4.1.1.3. eParaksts.lv SPS veiks pieteikumu apstrādi.

4.1.1.4. eParaksts.lv SPS Politikas SI izsniedz sertifikātus tikai eParaksts.lv SPS PKI ietvaros.

4.1.1.5. eParaksts.lv SPS Politikas sertificēšanas institūcija ir augsta līmeņa uzticama sertificēšanas institūcija, kurai sertifikātu ir izsniegusi eParaksts.lv SPS SSI. Tā izsniedz sertifikātus pakārtotajām SI (eParaksts.lv SPS Izsniegšanas SI) un eParaksts.lv SPS uzticamajiem pakalpojumiem

4.1.1.6. Visas LR Iedzīvotāju reģistrā reģistrētās personas var iesniegt pieteikumu sertifikātu saņemšanai. Pēc pieteikuma veidlapas akceptēšanas RI pieteicēja vārdā iesniedz eParaksts.lv SPS ISI pieteikumu sertifikātu saņemšanai.

4.1.2. **Sertifikātu pieteikuma iesniegšana**

4.1.2.1. Sertifikātu pieteikumā jābūt iekļautai visai sertifikātu pieteikumā definētajai informācijai.

4.1.2.2. Fiziskās personas nevar darboties kā uzticamas sertificēšanas institūcijas.

4.1.2.3. **Parakstītāja sertifikātu pieteikuma iesniegšana**

4.1.2.3.1. Šajā sadaļā ir aprakstīta parakstītāja sertifikātu pieteikuma apstrādes procedūra. eParaksts.lv SPS ISI un RI veic identifikācijas un autentifikācijas procedūras, lai pārbaudītu sertifikāta pieteikumu. Pēc tam SI vai RI sertifikāta pieteikumu vai nu apstiprinās, vai arī atteiks.

4.1.2.3.2. Visi nepieciešamie dati tiks uzglabāti eParaksts.lv SPS IS un arhivēti vai nu elektroniskā, vai arī papīra veidā saskaņā ar Fizisko personu datu aizsardzības likumu un Elektronisko dokumentu likuma 15.§. Nepieciešamie dati ir šādi (Tabula 7):

Tabula 7. Datu avoti un to uzglabāšana SPS IS.

| Dati | Avots | Mērķis |
|---|---|---|
| Vārds, uzvārds | Identifikācijas dokuments | Sertifikāts (ja netiek lietots pseidonīms) |
| Personas kods | Identifikācijas dokuments | Sertifikāts |
| Vārds uz kartes | Pieteikuma forma | Sertifikātu karte |
| Pseidonīms | Pieteikuma forma | Sertifikāts |
| Personas kods | Identifikācijas dokuments | Sertifikāts |
| Pasta adrese un kontaktinformācija | Pieteikuma forma | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| ID dokuments | Identifikācijas dokuments | Identifikācija un autentifikācija pieteikumam, anulēšanai un apturēšanai |
| ID dokumenta derīguma termiņš | Identifikācijas dokuments | ID dokumenta pārbaude |
| Sertifikāta veids (fiziskas vai juridiskas personas) | Pieteikuma forma | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Publicēt vai nepublicēt sertifikātus (jā/nē) | Pieteikuma forma | Publisks sertifikātu tiešsaistes reģistrs |
| Organizācijas nosaukums | Pieteikuma forma | Sertifikāts |
| Organizācijas struktūrvienība | Pieteikuma forma | Sertifikāts |
| Organizācijas reģistrācijas numurs | Pieteikuma forma | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Organizācijas pasta adrese un kontaktinformācija | Pieteikuma forma | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Iekļaut uzņēmuma informāciju sertifikātā (jā/nē) | Pieteikuma forma | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Parakstītāja norādītā e-pasta adrese, kas kalpo UPN viedkartes | Pieteikuma forma | Sertifikāts un Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |

| | | |
|---|---|---|
| pieslēgšanās sertifikātam | | |
| Iekļaut e-pastu sertifikātā vai nē (jā/nē) | Pieteikuma forma | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| PIN vēstules piegādes veids ierakstītā vēstulē | Pieteikuma forma | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Paziņojumu saņemšanas veids (pasts vai e-pasts) | Pieteikuma forma | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Apturēšanas drošības jautājums | Pieteikuma forma | Identifikācija apturēšanai, zvanot pa tālruni |
| Apturēšanas drošības frāze | Pieteikuma forma | Identifikācija apturēšanai, zvanot pa tālruni |
| Viedkaršu piegādes Klientu apkalpošanas punkts | Pieteikuma forma | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Viedkaršu derīguma termiņš | Pieteikuma forma | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Produkts un norēķinu informācija | Pieteikuma forma | Norēķiniem (konfidenciāla, SI datu bāze) |

4.1.2.3.3. RI veic sākotnējo identitātes pārbaudes procedūru, kā aprakstīts 3.2 nodaļā.

4.1.2.3.4. Pēc reģistrācijas un sākotnējās identitātes pārbaudes pieteikuma veidlapu paraksta parakstītājs un reģistrēšanas operators. Gadījumā, kad parakstītājs un pasūtītājs ir dažādas personas, Pasūtītāja līgums iepriekš ir jāparaksta pasūtītājam.

4.1.2.3.5. Sertifikātu publicēšanai direktorijas pakalpojumos ir nepieciešama pieteikuma procesa laikā skaidri pausta parakstītāja piekrišana.

4.1.2.3.6. Reģistrēšanas operators konsultē parakstītāju un izsniedz viņam rakstisku informāciju par sertifikātu un privāto atslēgu lietošanu, kā arī rīcību ar viedkartēm, kā noteikts šajos SN. Parakstītājs tiek informēts par kvalificētajiem parakstiem saistītajiem nepieciešamajiem drošības pasākumiem un parakstu tiesisko nozīmi.

4.1.2.3.7. WEB portāla sertifikātu pieteikums:

| **Dati** | **Avots** | **Mērķis** |
|---|---|---|
| Vārds, uzvārds | Sertifikāts uz viedkartes vai Bankas IS | Sertifikāts (ja netiek lietots pseidonīms) |
| Personas kods | Sertifikāts uz viedkartes vai Bankas IS | Sertifikāts |
| ID dokumenta numurs | Paša ievadīti dati no identifikācijas dokumenta | ID dokumenta pārbaude |
| ID dokumenta derīguma termiņš | Paša ievadīti dati no identifikācijas dokumenta | ID dokumenta pārbaude |

4.1.2.4. Pie reģistrācijas tiek pārbaudīti pieteikuma dati. Pēc pieteikuma aizpildīšanas, pieteikums ir jāapstiprina. To var izdarīt divējādi:

4.1.2.4.1. pieteikums ir jāizdrukā un personīgi jāiesniedz, kādā no speciāli šim mērķim paredzētiem klientu apkalpošanas centriem, līdzi ņemot personu apliecinošu dokumentu. Pieteikums ir jāparaksta. Speciālie klientu apkalpošanas centri, kuros var iesniegt pieteikumu, ir norādīti web portālā;

4.1.2.4.2. elektroniski apstiprināt pieteikumu izmantojot Latvijā akreditētās kredītiestādes - Akciju sabiedrība "SEB banka" sniegtās iespējas.

4.1.2.5. **Tīmekļa servera SSL sertifikāta pieteikums:**

| Dati | Avots | Mērķis |
|---|---|---|
| Pasūtītāja pilnvarotās personas vārds, uzvārds | Identifikācijas dokuments | Personas identifikācija |
| Pasūtītāja pilnvarotās personas kods | Identifikācijas dokuments | Personas identifikācija |
| Pasūtītāja organizācijas nosaukums vai privātpersonas vārds un uzvārds | Pieteikuma veidlapa | Sertifikāts<br>Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Pasūtītāja Organizācijas struktūrvienība vai tukšs privātpersonai | Pieteikuma veidlapa | Sertifikāts<br>Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Pasūtītāja Organizācijas reģistrācijas numurs vai privātpersonas personas kods | Pieteikuma veidlapa | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Pasūtītāja organizācijas vai privātpersonas pasta adrese un kontaktinformācija | Pieteikuma veidlapa | Sertifikāts<br>Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Pasūtītāja organizācijas vai privātpersonas e-pasta adrese | Pieteikuma veidlapa | Sertifikāts<br>Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Tīmekļa vietne | Pieteikuma veidlapa | Sertifikāts |
| Izvēlētā pakotne | Pieteikuma veidlapa | Sertifikāta pieteikuma pārbaudei un sertifikāta izsniegšanai<br>Norēķiniem |

4.1.2.6. **Laika zīmogošanas iekārtas sertifikāta pieteikums:**

| Dati | Avots | Mērķis |
|---|---|---|
| Pasūtītāja pilnvarotās personas vārds, uzvārds | Identifikācijas dokuments | Personas identifikācija |
| Pasūtītāja pilnvarotās personas kods | Identifikācijas dokuments | Personas identifikācija |
| Pasūtītāja organizācijas nosaukums vai privātpersonas vārds un uzvārds | Pieteikuma veidlapa | Sertifikāts<br>Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Pasūtītāja Organizācija struktūrvienība vai tukšs privātpersonai | Pieteikuma veidlapa | Sertifikāts<br>Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Pasūtītāja Organizācijas reģistrācijas numurs vai privātpersonas personas kods | Pieteikuma veidlapa | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Pasūtītāja organizācijas vai privātpersonas pasta adrese un kontaktinformācija | Pieteikuma veidlapa | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Pasūtītāja organizācijas vai privātpersonas e-pasta adrese | Pieteikuma veidlapa | Sertifikāts<br>Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |

4.1.2.7. **Koda parakstīšanas sertifikāta pieteikums:**

| Dati | Avots | Mērķis |
|---|---|---|
| Pasūtītāja pilnvarotās personas vārds, uzvārds | Identifikācijas dokuments | Personas identifikācija |
| Pasūtītāja pilnvarotās personas kods | Identifikācijas dokuments | Personas identifikācija |
| Pasūtītāja organizācijas nosaukums vai privātpersonas vārds un uzvārds | Pieteikuma veidlapa | Sertifikāts<br>Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Pasūtītāja Organizācijas struktūrvienība vai tukšs privātpersonai | Pieteikuma veidlapa | Sertifikāts<br>Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |

| | | |
|---|---|---|
| Pasūtītāja Organizācijas reģistrācijas numurs vai privātpersonas personas kods | Pieteikuma veidlapa | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Pasūtītāja organizācijas vai privātpersonas pasta adrese un kontaktinformācija | Pieteikuma veidlapa | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Pasūtītāja organizācijas vai privātpersonas e-pasta adrese | Pieteikuma veidlapa | Sertifikāts<br>Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Izvēlētā pakotne | Pieteikuma veidlapa | Sertifikāta pieteikuma pārbaudei un sertifikāta izsniegšanai Norēķiniem |

4.1.2.8. **Domēna kontroliera sertifikāta pieteikums:**

| **Dati** | **Avots** | **Mērķis** |
|---|---|---|
| Pasūtītāja pilnvarotās personas vārds, uzvārds | Identifikācijas dokuments | Personas identifikācija |
| Pasūtītāja pilnvarotās personas kods | Identifikācijas dokuments | Personas identifikācija |
| Pasūtītāja organizācijas nosaukums vai privātpersonas vārds un uzvārds | Pieteikuma veidlapa | Sertifikāts<br>Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Pasūtītāja Organizācijas struktūrvienība vai tukšs privātpersonai | Pieteikuma veidlapa | Sertifikāts<br>Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē |
| Pasūtītāja Organizācijas reģistrācijas numurs vai privātpersonas personas kods | Pieteikuma veidlapa | Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Pasūtītāja organizācijas vai privātpersonas pasta adrese un kontaktinformācija | Pieteikuma veidlapa | Sertifikāts<br>Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Pasūtītāja organizācijas vai privātpersonas e-pasta adrese | Pieteikuma veidlapa | Sertifikāts<br>Klientu attiecību pārvaldība (konfidenciāla, SI datu bāzē) |
| Domēns | Pieteikuma veidlapa | Sertifikāts |
| Izvēlētā pakotne | Pieteikuma veidlapa | Sertifikāta pieteikuma pārbaudei un sertifikāta izsniegšanai Norēķiniem |

4.1.2.9. **Elektroniskā zīmoga nodrošināšanai pieteikumā nepieciešamie dati:**

| Dati | Avots | Mērķis |
|---|---|---|
| Sertifikāta pamatvārds | Pieteikuma forma | Iekļaut sertifikātā, viedkartes un HSM nesējam |
| Organizācijas reģ. nr | Pieteikuma forma | Iekļaut sertifikātā, viedkartes un HSM nesējam |
| Organizācijas nosaukums | Pieteikuma forma | Iekļaut sertifikātā, viedkartes un HSM nesējam |
| Organizācijas struktūrvienība | Pieteikuma forma | Iekļaut sertifikātā, viedkartes un HSM nesējam |
| Valsts | Pieteikuma forma | Iekļaut sertifikātā, viedkartes un HSM nesējam |
| E-pasta adrese | Pieteikuma forma | Iekļaut sertifikātā, viedkartes un HSM nesējam |
| Nosaukums uz viedkartes | Pieteikuma forma | Norādīt uz sertifikātu viedkartes, tikai viedkartes nesējam |
| Organizācijas, nosaukums, pasta adrese un kontaktinformācija | Pieteikuma forma | Klientu attiecību pārvaldība, tikai viedkartes nesējam |

| | | |
|---|---|---|
| Viedkartes piegādes vieta | Pieteikuma forma | Klientu attiecību pārvaldība, tikai viedkartes nesējam |
| Informācijas par organizācijas pilnvaroto pārstāvi | Pieteikuma forma | Klientu attiecību pārvaldība, viedkartes un HSM nesējam |
| Apturēšanas drošības jautājums | Pieteikuma forma | Identifikācijai, sertifikātu apturēšanas nepieciešamības gadījumā, zvanot pa tālruni, viedkartes un HSM nesējam |
| Apturēšanas drošības frāze | Pieteikuma forma | Identifikācijai, sertifikātu apturēšanas nepieciešamības gadījumā, zvanot pa tālruni, viedkartes un HSM nesējam |
| Publicēt vai nepublicēt sertifikātus (jā/nē) | Pieteikuma forma | Publisks sertifikātu tiešsaistes reģistrs |

4.1.2.10. Sertifikātu (viedkartē) attālinātas jaunizdošanas gadījumā lietotājam pieteikums atsevišķi nav jāiesniedz, bet ir jāapstiprina sertifikātu jaunizdošana, ievadot nepieciešamos PIN.

## 4.2. Sertifikātu pieteikumu apstrādes process

### 4.2.1. **Sertifikātu pieteikuma apstiprināšana vai atteikšana**

4.2.1.1. Pēc tam, kad pabeigts sākotnējais pieteikums, lai kļūtu par eParaksts.lv SPS uzticamu SI, pieteikumu izvērtēšanas process ietver:

4.2.1.1.1. eParaksts.lv SPS darbinieku veiktu pilnīgu sertifikāta pieteikuma pārbaudi, lai noteiktu tā atbilstību eParaksts.lv SPS PKI prasībām un parametriem;

4.2.1.1.2. eParaksts.lv SPS pārstāvja apmeklējumu, lai pārbaudītu to tehniskās, finansiālās, infrastruktūras un prasmju spējas eParaksts.lv SPS PKI ietvaros nodrošināt sertifikācijas pakalpojumus;

4.2.1.1.3. īpašas eParaksts.lv SPS nozīmētas vienības veiktu pilnu sertificēšanas institūcijas auditu pieteicēja telpās saskaņā ar šo SN 8. nodaļu.

4.2.1.2. Jebkāda sertifikāta pieteikuma izvērtēšanas laikā atklāta neatbilstība tiks darīta zināma pieteicējam un tiks prasīta tās labošana iespējami īsā laikā. Ja neatbilstība ir būtiska, var būt nepieciešama jauna sertifikāta pieteikuma izvērtēšana.

### 4.2.2. **Parakstītāja sertifikātu pieteikuma apstiprināšana vai atteikšana**

4.2.2.1. Likumīgi pilnvarota reģistrācijas amatpersona akceptē vai atsaka pieteikumu, izmantojot SPS datu bāzi un LR Iedzīvotāju reģistru (sk. 3.2.3. apakšnodaļu), vadoties no šādiem apsvērumiem:

4.2.2.1.1. vai pieteicējs pieteikumā ir iesniedzis sertifikāta saņemšanai patiesu, pietiekamu un pilnu informāciju par savu personu;

4.2.2.1.2. vai pieteikuma procesa izpilde atbilst šiem SN.

4.2.2.2. eParaksts.lv SPS RI jāatsaka pieteikums sertifikāta saņemšanai, ja:

4.2.2.2.1. identifikācijas dokuments nav derīgs;

4.2.2.2.2. pieteicējs nav tiesīgs iesniegt pieteikumu sertifikāta izsniegšanai (sk. 4.1.1. nodaļu);

4.2.2.2.3. visas pieprasītās parakstītāja informācijas (3.2. nodaļas izpratnē) identifikācija un autentifikācija nevar tikt pabeigta;

4.2.2.2.4. LR Iedzīvotāju reģistrā nav atbilstošu datu ierakstu vai datu ieraksti neatbilst pieteikuma sertifikāta saņemšanai veidlapā norādītajiem;

4.2.2.2.5. pieteicējs vai organizācija nav parakstījusi pieteikuma veidlapu.

4.2.2.3. Pēc pieteikuma sekmīgas apstiprināšanas reģistrācijas amatpersona SPS IS identificē sevi ar savu autentifikācijas sertifikātu un nosūta kartes izgatavošanas pieprasījumu uz eParaksts.lv SPS karšu izgatavošanas uzņēmumu. Datu pārraide notiek drošā veidā pa VPN kanālu.

4.2.3. **WEB portāla sertifikātu pārbaudes**

4.2.3.1. WEB Portāls akceptē vai atsaka pieteikumu, izmantojot SPS datu bāzi un LR Iedzīvotāju reģistru, vadoties pēc šādiem apsvērumiem:

4.2.3.1.1. vai pieteicējs pieteikumā ir iesniedzis sertifikāta saņemšanai patiesu, pietiekamu un pilnu informāciju par savu personu;

4.2.3.1.2. vai pieteikuma procesa izpilde atbilst šiem SN.

4.2.3.2. WEB Portāls atsaka pieteikumu sertifikāta saņemšanai, ja:

4.2.3.2.1. identifikācijas dokuments nav derīgs;

4.2.3.2.2. visas pieprasītās parakstītāja informācijas identifikācija un autentifikācija nevar tikt pabeigta;

4.2.3.2.3. LR Iedzīvotāju reģistrā nav atbilstošu datu ierakstu vai datu ieraksti neatbilst pieteikuma sertifikāta saņemšanai veidlapā norādītajiem;

4.2.4. **Infrastruktūras sertifikātu pārbaudes**

4.2.4.1. **SSL sertifikātam:**

4.2.4.1.1. Tīmekļa vietnes piederība. Piederība tiek pārbaudīta izmantojot WHOIS, kur tiek noskaidrota domēna vārda kontaktpersona.

4.2.4.1.2. Lai pārliecinātos par domēna piederību pieprasītājam tiek veikts kontroles zvans uz WHOIS atrodamo telefona numuru vai pasta adresi un lūgts apstiprināt SSL pieprasījumu.

4.2.4.2. Koda parakstīšanas sertifikātam:

4.2.4.2.1. Pasūtītāja organizācijas dati tiek pārbaudīta pret uzņēmumu reģistrācijas apliecību;

4.2.4.2.2. Tiek pārbaudītas sertifikāta pieprasītāja pilnvaras rīkoties uzņēmuma vārdā;

4.2.4.2.3. Tiek pārbaudīta sertifikāta pieprasītāja identitāte pret uzrādīto personas apliecinošo dokumentu.

4.2.4.3. **Elektroniskā zīmoga sertifikātam:**

4.2.4.3.1. Pasūtītāja organizācijas dati tiek pārbaudīta pret uzņēmumu reģistrācijas apliecību;

4.2.4.3.2. Tiek pārbaudītas sertifikāta pieprasītāja pilnvaras rīkoties uzņēmuma vārdā;

4.2.4.3.3. Tiek pārbaudīta sertifikāta pieprasītāja identitāte pret uzrādīto personas apliecinošo dokumentu, vai, gadījumā ja pieteikums iesniegts elektroniski parakstīts ar drošu elektronisko parakstu – elektroniskā paraksta derīgums.

4.2.5. **Procedūra sertifikātu pieteikuma (sertifikāta pieprasījuma) apstrādei**

4.2.5.1. eParaksts.lv SPS izsniegtu sertifikātu pieteikuma procedūra ir pakārtotas uzticamas sertificēšanas institūcijas izveidošanas neatņemama sastāvdaļa. Kā tāda, procedūra tiks inicializēta tikai tad, kad eParaksts.lv SPS uzskata, ka pieteicējs ir izpildījis visas sertifikātu pieteikuma definētas prasības.

4.2.5.2. Sertifikāta pieprasījuma procedūra tiks dokumentēta un to apliecinās eParaksts.lv SPS drošības amatpersona un parakstītāja organizācijas pārstāvis. eParaksts.lv SPS drošības amatpersona īpaši nodrošina parakstītāja sertifikāta pieprasījuma drošu piegādi.

4.2.5.3. Sertifikāta pieprasījums eParaksts.lv SPS SI tiek apstiprināts tikai kā uz eParaksts.lv SPS SI droši pārraidīts PKCS#10 sertifikāta pieprasījums. PKCS#10 pieprasījuma paraksta pārbaude ir pietiekams atbilstošās privātās atslēgas piederības pierādījums.

4.2.5.4. Sertifikāta pieteikumi ietver pilnībā dokumentētu lietu, kurā ir atsauces uz atbilstību prasībām, lai kļūtu par eParaksts.lv SPS uzticamu SI, tostarp pilnu dokumentācijas komplektu, kas attiecas uz juridiskās vienības un fiziskās personas, kas ir pilnvarota to pārstāvēt, identitāti.

4.2.5.5. Pieteikumiem jābūt oriģinālā papīra formā un tādiem, kādus pieprasa eParaksts.lv SPS SI.

4.2.6. **Sertifikātu pieteikuma apstrādes laiks**

4.2.6.1. Sertifikāta pieteikuma apstrāde tiek veikta savlaicīgi pēc radīšanas un eParaksts.lv SPS SI veiktās akceptēšanas. Sertifikāta pieteikums ir aktīvs līdz brīdim, kad tas tiek atteikts.

## 4.3. Sertifikātu izsniegšana un publicēšana

4.3.1. Lai garantētu SI atslēgu pāra atbilstošu drošību, serveris, uz kura darbojas SSI un PSI pakalpojumi, nav savienots ar tīklu un atrodas nesaistē drošības objektā, kas atbilst 6.2.1. nodaļā izklāstītajiem kriptogrāfisko moduļu drošības standartiem. Ir ieviestas un apstiprinātas procedūras, lai nodrošinātu sertifikātu pieprasījumu, uzticamu SI publisko atslēgu sertificēšanas un sertifikātu izplatīšanas integritāti un nenoliegšanu. Piekļuve eParaksts.lv SPS SI līdzekļiem tiek piešķirta tikai pilnvarotam personālam. Turklāt vismaz divu personu autentifikācija tiek izmantota, lai nodrošinātu atbilstošu piekļuvi SI pakalpojumiem.

4.3.2. Sertifikāta izsniegšana eParaksts.lv SPS uzticamai SI ir saistīta ar šādām darbībām:

4.3.2.1. uzticama SI veic tās SI izveidošanas ceremoniju, kurai iepriekš piekritusi eParaksts.lv SPS un kuru apliecinās eParaksts.lv SPS darbinieki un eParaksts.lv SPS nozīmēts neatkarīgs auditors;

4.3.2.2. pieteicējs ģenerēs tā atslēgas pārus apstiprinātā kriptogrāfiskā modulī saskaņā ar šo SN 6.2.1. nodaļu un ģenerēs PKCS#10 sertifikāta pieprasījumu;

4.3.2.3. sertifikāta pieprasījums tiks droši transportēts datoram lasāmā vidē uz eParaksts.lv SPS SI, kur eParaksts.lv SPS darbinieki pārbaudīs pieprasījumu un tad ģenerēs SI sertifikātu un izveidos pakārtoto PKI vienību eParaksts.lv SPS loģiskajā infrastruktūrā;

4.3.2.4. uzticamas SI sertifikāts datoram lasāmā vidē tiks paņemts no SI, lai to iekļautu uzticamas SI sistēmā un izplatītu pēc vajadzības;

4.3.2.5. visi uzticamām sertificēšanas institūcijām izsniegtie derīgie sertifikāti tiks publicēti eParaksts.lv SPS tīmekļa vietnē.

4.3.3. Sertifikāta izsniegšanas procedūra ir eParaksts.lv SPS Sertificēšanas institūcijas vai eParaksts.lv SPS pakalpojumu izveidošanas neatņemama sastāvdaļa.

4.3.4. Sertifikāta izsniegšanas un publicēšanas procedūra tiks dokumentēta un to klātienē apliecinās eParaksts.lv SPS drošības amatpersona un parakstītāja organizācijas pārstāvis.

4.3.5. Sertifikātu izsniegšanas un publicēšanas procedūra ietver vismaz šādus darbību soļus:

4.3.5.1. sertifikācijas pieprasījuma apstiprināšana;

4.3.5.2. publiskajai atslēgai atbilstošu sertifikātu ģenerēšana;

4.3.5.3. sertifikātu parakstīšana;

4.3.5.4. izsniegto sertifikātu piegāde parakstītājam;

4.3.5.5. parakstītāja veikta sertifikāta akceptēšana;

4.3.5.6. izsniegtā sertifikāta publicēšana eParaksts.lv SPS tīmekļa vietnē un direktorijā.

4.3.6. **Parakstītāju sertifikātu izsniegšana un publicēšana**

4.3.7. **Sertifikāti uz viedkartes un sertifikāti HSM**

4.3.7.1. Pēc parakstītāja sertifikāta pieprasījuma apstiprināšanas eParaksts.lv SPS reģistrācijas amatpersonai veic pieprasījumu par HSM sertifikātu vai par viedkartes un tur iekļauto publiskās un privātās atslēgas ražošanu. Pēc kartes pieprasījuma saņemšanas eParaksts.lv SPS sāk sertifikāta izsniegšanas procesu drošā vidē, rīkojoties šādi:

4.3.7.1.1. izvēlētajai kartei vai HSM iekārtai ģenerē PIN un PUK kodus ;

4.3.7.1.2. ģenerē atslēgu pāri katram sertifikātam viedkartē vai HSM iekārtā, kas ir sertificēta kā droša elektroniskā paraksta radīšanas līdzeklis (SSCD);

4.3.7.1.3. ģenerē atbilstošu skaitu sertifikātu pieprasījumus un nosūta tos eParaksts.lv SPS ISI pa autentificētu un šifrētu sakaru kanālu. Šim nolūkam publiskā atslēga tiek nolasīta no SSCD un ievietota PKCS#10 pieprasījumā, kas iegults ar PKCS#7 parakstītā datu pakotnē;

4.3.7.2. eParaksts.lv SPS ISI pārbauda sertifikācijas pieprasījumu, veicot šādas darbības:

4.3.7.2.1. pārbaudot sertifikāta saņemšanas pieprasījuma parakstu;

4.3.7.2.2. pārbaudot sertifikāta pieprasījuma informācijas struktūras un satura derīgumu un tā pilnību;

4.3.7.2.3. nosakot sertifikāta pieprasījuma saskanību ar kartes pieprasījuma esamību;

4.3.7.2.4. nosakot sertifikāta pieprasījuma esošās informācijas saskanību ar apstiprināto sertifikāta pieteikumu;

4.3.7.2.5. ja pārbaudes rezultāti ir sekmīgi, eParaksts.lv SPS ISI ģenerē sertifikātu kā elektroniski parakstītu paziņojumu, kas sasaista parakstītāja informāciju ar viņa privāto atslēgu;

4.3.7.2.6. tiek izveidots ziņojums ar sertifikātiem un nosūtīts atbildes ziņojums pa autentificētu un šifrētu sakaru kanālu;

4.3.7.2.7. sertifikāti tiek ievietoti viedkartē, un tiek veikta fiziska kartes personalizācija;

4.3.7.2.8. HSM sertifikāti tiek ievietoti HSM iekārtā;

4.3.7.2.9. tiek ģenerēta PIN vēstule.

4.3.7.3. Pēc sekmīgas HSM sertifikātu izsniegšanas eParaksts.lv SPS SI informē Pasūtītāju ar pieņemšanas–nodošanas aktu. Pieņemšanas–nodošanas akts satur informāciju par sertifikāta derīguma termiņu un ieteikumu vērsties pēc jauna sertifikāta pirms sertifikāta derīguma termiņa beigām.

4.3.8. **WEB portāla sertifikāti:**

4.3.8.1. Pēc parakstītāja sertifikāta pieprasījuma apstiprināšanas, parakstītājam tiek pieprasīts apstiprināt distances līgumu, tikko tas ir apstiprināts, notiek pieprasījums par WEB portāla sertifikātu publiskās un privātās atslēgas ražošanu. Pēc pieprasījuma saņemšanas eParaksts.lv SPS sāk sertifikāta izsniegšanas procesu drošā vidē, rīkojoties šādi:

4.3.8.1.1. WEB portāla sertifikātiem tiek ģenerēts PIN pieprasījums (PIN ievada Parakstītājs);

4.3.8.1.2. ģenerē atslēgu pāri katram sertifikātam;

4.3.8.1.3. WEB portāla sertifikāti glabājas HSM iekārtā;

4.3.9. Infrastruktūras sertifikāti:

4.3.9.1. Gan tīmekļa vietnes SSL sertifikātam, gan koda parakstīšanas sertifikātam, gan domēna kontroliera sertifikātam, gan laika zīmogošanas iekārtas sertifikātam:

4.3.9.1.1. Sertifikātu programmatiskajam pieprasījumam SI izsniedz sertifikātu;

4.3.9.1.2. Sertifikāts kļūst pieejams reģistrācijas amatpersonai;

4.3.9.1.3. RA amatpersona pārbauda sertifikātu;

4.3.9.1.4. RA amatpersona apstiprina sertifikātu, kura laikā

4.3.9.1.5. Sertifikāts tiek nosūtīts pa e-pastu uz Pasūtītāja pilnvarotās personas pieteikumā norādīto e-pastu, cc tiek nosūtīts uz speciālu SI kontroles e-pastu;

4.3.9.1.6. Tiek izdrukāts pieņemšanas–nodošanas akts par sertifikāta nodošanu Pasūtītājam un Pasūtītāja un SI pienākumiem un atbildību.

4.3.9.2. Pēc sekmīgas infrastruktūras sertifikāta izsniegšanas eParaksts.lv SPS SI informē Pasūtītāju, nododot izsniegto infrastruktūras sertifikātu un parakstot pieņemšanas–nodošanas aktu. Pieņemšanas–nodošanas akts satur informāciju par sertifikāta derīguma termiņu un ieteikumu vērsties pēc jauna sertifikāta pirms sertifikāta derīguma termiņa beigām.

## 4.4. Sertifikātu akceptēšana

4.4.1. **Rīcība akceptējot sertifikātu**

4.4.1.1. Sertifikāta akceptēšana notiks kā daļa no uzticamas SI izveidošanas ceremonijas vai tās rezultātā tiks veikta brīdī, kad pieteicējs un eParaksts.lv SPS apstiprina ceremonijas atbilstību dokumentētajiem uzticamas SI izveidošanas noteikumiem. Pēc sava sertifikāta akceptēšanas pieteicējs kļūst par uzticamu sertificēšanas institūciju.

4.4.1.2. Pēc sertifikātu piegādes parakstītājam jāapstiprina eParaksts.lv SPS ISI sertifikāta saņemšana un pareizība. Sertifikāti netiek aktivēti, līdz šo apstiprinājumu nav saņēmusi eParaksts.lv SPS ISI.

4.4.1.3. Pēc infrastruktūras sertifikātu piegādes Pasūtītājam, tā pilnvarotai personai jāapstiprina eParaksts.lv SPS SI sertifikāta saņemšana un tā pareizība ar pieņemšanas-nodošanas aktu. Sertifikāti netiek aktivēti, līdz šo apstiprinājumu nav saņēmusi eParaksts.lv SPS SI.

4.4.1.4. Parakstītāja sertifikāta akceptēšanas procedūra:

4.4.1.4.1. nepieciešama parakstītāja personīga klātbūtne;

4.4.1.4.2. tiek veikta parakstītāja identifikācija (atbilstoši 3.2. nodaļai);

4.4.1.4.3. parakstītājs apliecina viedkartes, kas ietver sertifikātus ar atbilstošo saturu, saņemšanu;

4.4.1.4.4. parakstot Pasūtītāja līgumu, parakstītājs apliecina, ka ir saņēmis instrukcijas un izlasījis viedkaršu un atslēgu lietošanas informācijas materiālu;

4.4.1.4.5. RI izsniedz viedkarti un abu pušu parakstītu Pasūtītāja līguma oriģinālu. Pasūtītāja līgums ietver informāciju par sertifikāta izsniegšanu tieši parakstītājam;

4.4.1.4.6. visi dokumenti tiks pievienoti parakstītāja lietai un arhivēti.

4.4.1.5. HSM sertifikātiem Parakstītājs paraksta pieņemšanas – nodošanas aktu un nogādā atpakaļ SI

4.4.1.6. Pirms WEB portāla sertifikātu saņemšanas parakstītājs apstiprina distances līgumu. Distances līguma apstiprināšana notiek WEB portālā. Tikai pēc līguma apstiprināšanas tiek ražoti un izsniegti sertifikāti.

4.4.1.7. Infrastruktūras sertifikātiem Pasūtītāja pilnvarotā Persona paraksta pieņemšanas – nodošanas aktu un nogādā atpakaļ SI.

4.4.2. **SI veikta sertifikātu publicēšana**

4.4.2.1. Parakstītāja sertifikāti tiek publicēti brīdī, kad tiek aktivizēti eParaksts.lv SPS Direktoriju pakalpojumos. Parakstītājam jādod sava piekrišana viņa sertifikātu publicēšanai.

4.4.2.2. Pieeja eParaksts.lv SPS LZI publisko atslēgu saturošiem sertifikātiem ir iespējama ar:

4.4.2.2.1. LDAP publisko direktoriju (direktoriju pakalpojumi);

4.4.2.2.2. OCSP (derīguma pārbaude);

4.4.2.2.3. eParaksts.lv SPS tīmekļa vietni.

4.4.2.3. Infrastruktūras sertifikāti netiek publicēti.

## 4.5. Atslēgu pāra un sertifikātu lietošana

4.5.1. **Privāto atslēgu un sertifikātu lietošana Saknes SI**

4.5.1.1. Saknes SI privāto atslēgu lieto tikai:

4.5.1.1.1. sertifikātu izsniegšanai eParaksts.lv SPS Sertifikātu pārbaudes pakalpojumiem (OCSP respondera parakstīšanas sertifikāts);

4.5.1.1.2. sertifikātu izsniegšanai sertificēšanas institūcijām, kas ir apstiprinātas, lai kļūtu par eParaksts.lv SPS uzticamām sertificēšanas institūcijām;

4.5.1.1.3. eParaksts.lv SPS Saknes SI anulēto un apturēto sertifikātu sarakstu izsniegšanai;

4.5.1.1.4. savstarpējai sertificēšanai saskaņā ar eParaksts.lv SPS apstiprinājumu (pašlaik netiek plānots).

4.5.1.2. eParaksts.lv SPS uzticamas sertificēšanas institūcijas privātā atslēga un atbilstošais sertifikāts tiek izmantots mērķiem, kas minēti atbilstošajos sertificēšanas noteikumos. Ir jāpiemēro šādi vispārīgie pienākumi:

4.5.1.2.1. sertifikāts ir jāizmanto saskaņā ar uzticamas SI līgumu, šo SN noteikumiem un atbilstošo SP;

4.5.1.2.2. sertifikāta publiskai atslēgai atbilstošās privātās atslēgas izmantošana ir atļauta tikai tad, kad SI ir piekritusi uzticamas SI līgumam un ar apliecinājumu akceptējusi sertifikāta saturu.

4.5.2. **Pārbaudītāja publisko atslēgu un sertifikātu izmantošana Saknes SI**

4.5.2.1. Pirms jebkāda paļaušanās akta pārbaudītājiem:

4.5.2.1.1. kā norādīts atbilstošajā SP [2], ir jāievēro jebkādus sertifikātu izmantošanas un atbildības apjoma ierobežojumus;

4.5.2.1.2. drošā veidā jāiegūst eParaksts.lv SPS Saknes SI sertifikātu, uzticamu SI sertifikātu un jebkurus citus atbilstošajā sertifikātu hierarhijā esošos sertifikātus.

4.5.3. **Privātās atslēgas un sertifikātu lietošana Politikas SI**

4.5.3.1. eParaksts.lv SPS PSI izmanto savu privāto atslēgu, lai parakstītu Izsniegšanas SI un eParaksts.lv SPS LZI izsniegtos sertifikātus, OCSP respondera parakstīšanas sertifikātu un savus publicētos CRL.

4.5.3.2. Turpmāk apskatītie pienākumi ir jāiekļauj vienošanā starp eParaksts.lv SPS PSI un pakārtotajām SI:

4.5.3.2.1. sertifikāts ir jālieto likumīgi saskaņā ar vienošanos starp PSI un pakārtotajām SI, un šiem SN. Sertifikāta lietošanai jāatbilst sertifikātā iekļautajiem atslēgas lietojuma lauka paplašinājumiem (piem., ja nav atļauta elektroniska parakstīšana, tad sertifikātu nedrīkst izmantot parakstīšanai);

4.5.3.2.2. sertifikāta publiskajai atslēgai atbilstošās privātās atslēgas izmantošana ir atļauta tikai tad, kad pakārtotā Izsniegšanas SI ir piekritusi vienošanai starp PSI un pakārtoto SI un ar apliecinājumu akceptējusi sertifikāta saturu;

4.5.3.2.3. privātās atslēgas datu glabāšanas vide tiks personiski nodrošināta. Pakārtotajai Izsniegšanas SI ir jāaizsargā savu privāto atslēgu pret nesankcionētu izmantošanu un jāpārtrauc šīs privātās atslēgas lietošanu pēc sertifikāta derīguma termiņa beigām vai tā anulēšanas;

4.5.3.2.4. vienošanās starp PSI un pakārtoto SI nosaka, ka pakārtotajai Izsniegšanas SI nekavējoties jāinformē eParaksts.lv SPS par zināmu privātās atslēgas kompromitēšanu vai nepareizu lietošanu, vai kad par to ir aizdomas.

4.5.4. **Pārbaudītāja publisko atslēgu un sertifikātu lietošana Politikas SI**

4.5.4.1. Veicot jebkuras darbības ar eParaksts.lv SPS izsniegtajiem sertifikātiem, pārbaudītājiem neatkarīgi jānovērtē:

4.5.4.1.1. sertifikāta lietošanas atbilstība jebkuram norādītajam mērķim un jānosaka, ka sertifikāts faktiski tiek lietots atbilstošam mērķim, kuru neaizliedz vai savādāk neierobežo šie SN. eParaksts.lv SPS nav atbildīgs par sertifikāta lietošanas piemērotības novērtēšanu;

4.5.4.1.2. vai sertifikāts tiek izmantots atbilstoši sertifikātā iekļautajiem lauka KeyUsage paplašinājumiem (piem., ja nav atļauts elektroniskais paraksts, tad uz sertifikātu nedrīkst paļauties, lai pārbaudītu parakstītāja parakstu);

4.5.4.1.3. PSI sertifikāta statuss. Ja kāds no sertifikātiem sertifikātu hierarhijā ir anulēts, pārbaudītājs nedrīkst paļauties uz pakārtotās Izsniegšanas SI sertifikātu vai citu anulētu sertifikātu to hierarhijā.

4.5.5. **Pasūtītāja privāto atslēgu un sertifikātu lietošana**

4.5.5.1. eParaksts.lv SPS ISI kvalificētos sertifikātus saskaņā ar atbilstošo SP [2] drīkst lietot tikai drošu parakstu (nenoliegšanas izpratnē) izveidei.

4.5.5.2. Pasūtītāja līgumā ir iekļauti šādi pienākumi:

4.5.5.2.1. sertifikāts jāizmanto likumīgi saskaņā ar pasūtītāja līgumu, SP un šo SN noteikumiem. Sertifikāta izmantošanai jāatbilst sertifikātā iekļautajiem lauka KeyUsage paplašinājumiem (piem., ja nav atļauts elektroniskais paraksts, tad sertifikātu nedrīkst izmantot parakstīšanai);

4.5.5.2.2. sertifikāta publiskajai atslēgai atbilstošās privātās atslēgas izmantošana ir atļauta tikai tad, kad parakstītājs ir piekritis pasūtītāja līgumam un ar apliecinājumu ir apstiprinājis sertifikāta saturu;

4.5.5.2.3. privātās atslēgas datu nesējam ir jābūt nodrošinātam personīgi. Parakstītājiem jāaizsargā savas privātās atslēgas pret nesankcionētu lietošanu un jāpārtrauc savu privāto atslēgu izmantošana pēc sertifikāta derīguma termiņa izbeigšanās, tā apturēšanas vai anulēšanas;

4.5.5.2.4. parolēm (PIN, PUK), kas nepieciešamas identifikācijai attiecībā pret informācijas nesēju, kurā ir privātā atslēga, jāpaliek slepenām;

4.5.5.2.5. eParaksts.lv SPS ISI pasūtītāja līgums nosaka, ka parakstītājiem nekavējoties jāinformē eParaksts.lv SPS ISI vai nu par zināmu privātas atslēgas diskreditējumu vai aizdomām par to, vai arī par privātās atslēgas nepareizu izmantošanu.

4.5.6. **Pārbaudītāja publisko atslēgu un sertifikāta lietošana**

4.5.6.1. Pirms jebkāda paļaušanās akta pārbaudītājiem neatkarīgi jānovērtē:

4.5.6.1.1. sertifikāta lietošanas atbilstību jebkuram norādītajam nolūkam un jānosaka, vai sertifikāts tiks izmantots atbilstošam nolūkam, kuru neaizliedz vai citādi neierobežo šie SN. eParaksts.lv SPS ISI nav atbildīga par sertifikāta lietošanas piemērotības novērtēšanu;

4.5.6.1.2. vai sertifikāts tiek izmantots atbilstoši sertifikātā iekļautajiem lauka KeyUsage paplašinājumiem (piem., ja nav atļauts elektroniskais paraksts, tad uz sertifikātu nedrīkst paļauties, lai pārbaudītu parakstītāja parakstu);

4.5.6.1.3. statuss sertifikātam un visām hierarhijā esošajām SI, kas izsniedza šo sertifikātu. Ja atbilstošajā sertifikātu hierarhijā kāds no sertifikātiem ir ticis anulēts, pārbaudītājs nedrīkst paļauties uz parakstītāja sertifikātu vai citu anulētu sertifikātu hierarhijā.

## 4.6. Sertifikātu atkal izdošana

4.6.1. Sertifikāta atkal izdošana ir jauna sertifikāta izsniegšana uzticamai SI, nemainot publisko atslēgu vai jebkuru citu sertifikāta informāciju.

## 4.7. Sertifikātu jaunizdošana

4.7.1. Sertifikāta jaunizdošana nozīmē jauna atslēgu pāra ģenerēšanu un pieteikšanos jauna sertifikāta izsniegšanai, kas sertificē jauno publisko atslēgu.

4.7.2. Laika zīmogošanas iekārtas (LZIe) privātās parakstīšanas atslēgas tiek nomainītas pirms to derīguma termiņa iztecēšanas (t.i., kad to algoritms vai atslēgas garums vairs nav drošs).

4.7.3. Parakstītājs vai pasūtītājs tiks informēts 30 dienas pirms sertifikāta derīguma termiņa izbeigšanās ar pasta paziņojumu vai pa e-pastu. Ja sertifikāta derīguma termiņš ir beidzies, pasūtītājam jāpiesaka jauns sertifikāts saskaņā ar 4.1. nodaļu.

## 4.8. Sertifikātu modificēšana

4.8.1. eParaksts.lv SPS SSI neveic izmaiņas esošā sertifikātā, jo tas neļautu veikt jebkādu šī sertifikāta elektroniskā paraksta pārbaudi un padarītu šo sertifikātu par nederīgu. Gadījumā, kad informācija, kas ir iekļauta sertifikātā, ir mainījusies, vai tā ir jāmaina, eParaksts.lv SPS SSI izsniedz jaunu sertifikātu ar modificēto informāciju.

## 4.9. Sertifikātu apturēšana un anulēšana

4.9.1. **Apturēšana**

4.9.1.1. Sertifikātu, kurus ir izsniegusi eParaksts.lv SPS SSI, apturēšana netiek veikta.

4.9.1.2. Sertifikātu, kurus ir izsniegusi eParaksts.lv SPS PSI, apturēšana netiek veikta.

4.9.1.3. Visiem apturēšanas un anulēšanas pieprasījumiem ir jābūt derīgiem. Pieprasījuma derīgums tiek noteikts ar tā atbilstību vai neatbilstību šo SN procedūrām, kuras ietver atsauces uz personām, kas drīkst iesniegt pieprasījumu, pilnvarām.

4.9.1.4. Gala lietotāja sertifikātu apturēšanas procedūra ir aprakstīta 3.3.7 nodaļā un gala lietotāja sertifikātu anulēšanas procedūra ir aprakstīta 3.3.8 nodaļā.

4.9.2. **Apturēšanas apstākļi**

4.9.2.1. eParaksts.lv SPS ISI bez kavēšanās aptur sertifikātu šādos gadījumos:

4.9.2.1.1. ir saņemts pamatots pieprasījums;

4.9.2.1.2. izpildot tiesas lēmumu par sertifikāta apturēšanu;

4.9.2.1.3. SPS amatpersonām konstatējot neatbilstības vai drošības apdraudējumus sertifikātu lietojamībā.

4.9.2.2. eParaksts.lv SPS ISI izsniegto sertifikātu apturēšana notiek nekavējoties pēc apturēšanas pieprasījuma apstiprināšanas.

4.9.3. **Anulēšanas vai apturēšanas pieprasīšanas tiesības**

4.9.3.1. Saskaņā ar šo SN noteikumiem un nosacījumiem uzsākt izsniegto sertifikātu apturēšanu vai anulēšanu ir pilnvarotas šādas personas un organizācijas vienības:

4.9.3.1.1. parakstītājs;

4.9.3.1.2. pasūtītājs (proti, fiziska vai juridiska persona, kas parakstīja Pasūtītāja līgumu, saskaņā ar kuru parakstītājam tika izsniegts sertifikāts);

4.9.3.1.3. Latvijas tiesa;

4.9.3.1.4. eParaksts.lv SPS (veic sertifikātu apturēšanu vai anulēšanu, pamatojoties uz 4.9.2.1.3 punktā noteiktajiem apstākļiem).

4.9.3.2. Anulēšanu pēc likumīga un pilnvarota pieprasījuma saņemšanas veic anulēšanas amatpersona.

4.9.4. **Apturēšanas pieprasījuma procedūra**

4.9.4.1. Klientu servisā sertifikāta apturēšanas pieprasījumi tiek apstrādāti šādi:

4.9.4.1.1. pieprasošā persona iesniedz apturēšanas pieprasījumu apturēšanas operatoram;

4.9.4.1.2. apturēšanas operators pārliecinās, vai apturēšanas pieprasījums ir pareizi noformēts;

4.9.4.1.3. apturēšanas operators pārliecinās, ka pieprasošā persona ir pareizi identificēta, autentificēta un pilnvarota;

4.9.4.1.4. apturēšanas operators autentificē sevi (izmantojot autentifikācijas sertifikātu);

4.9.4.1.5. apturēšanas operators apstrādā apturēšanas pieprasījumu;

4.9.4.1.6. apturēšanas amatpersona autentificē sevi (izmantojot autentifikācijas sertifikātu);

4.9.4.1.7. apturēšanas amatpersona apstiprina apturēšanu;

4.9.4.1.8. eParaksts.lv SPS IS ar vēstuli vai pa e-pastu informē parakstītāju un pasūtītāju.

4.9.4.2. **Palīdzības Dienestā pa telefonu +371 67108989:**

4.9.4.2.1. Pieprasītājs pieprasa sertifikātu apturēšanu;

4.9.4.2.2. Operators prasa slepeno jautājumu no pieteikuma;

4.9.4.2.3. Apturēšanas pieprasītājs pasaka slepeno atbildi;

4.9.4.2.4. Apturēšanas operators aptur sertifikātu.

4.9.5. **Laiks, kādā SI jāapstrādā apturēšanas pieprasījums**

4.9.5.1. Maksimālā aizkave starp apturēšanas pieprasījuma saņemšanu un visiem pārbaudītājiem pieejamo sertifikātu statusa informācijas izmaiņu ir atkarīga no sertifikātu pārbaudes metodes:

4.9.5.1.1. sertifikātu pārbaudei, izmantojot eParaksts.lv SPS uzticamo OCSP responderi, tā nepārsniegs 1 dienu (24 stundas);

4.9.5.1.2. sertifikātu pārbaudei, izmantojot visjaunāko CRL, tā nepārsniegs 1 dienu (24 stundas).

4.9.5.2. Šaubu gadījumā pārbaudītājiem jāiegūst visjaunākā statusa informācija no eParaksts.lv SPS uzticama OCSP respondera.

4.9.6. Apturēšanas laika ierobežojums

4.9.6.1. Apturēšanas laiks netiek ierobežots.

4.9.7. **Atjaunošana**

4.9.7.1. Kad sertifikāts ir ticis apturēts, ar to rīkojas vienā no šādiem trim veidiem:

4.9.7.1.1. apturētā sertifikāta ieraksts paliek CRL līdz sertifikāta derīguma termiņa beigām bez turpmākas rīcības (OCSP-R dos noliedzošu atbildi uz sertifikāta derīguma pieprasījumu);

4.9.7.1.2. apturētā sertifikāta CRL ierakstu aizstāj ar tā paša sertifikāta anulēšanas ierakstu, un tiek izsniegts atjaunots CRL (OCSP-R sniegs noliedzošu atbildi uz sertifikāta derīguma pieprasījumu);

4.9.7.1.3. sertifikāts tiek atjaunots, ieraksts tiek izņemts no CRL un tiek izdots jauns CRL (uz sertifikāta derīguma pieprasījumu OCSP-R sniegs apstiprinošu atbildi).

4.9.7.2. Atjaunošanas pieprasījums tiks pieņemts tikai rakstiskā veidā ar parakstītāja parakstu, kurā parakstītājs apstiprina, ka privātā atslēga un aktivizācijas kodi apturēšanas laikā ir bijuši viņa ekskluzīvā pārvaldībā.

4.9.8. Laiks, kādā SI jāapstrādā atjaunošanas pieprasījums

4.9.8.1. Ir nepieciešams nogaidīt līdz 48 stundām, lai nodrošinātu, ka apturētais sertifikāts ir vismaz vienā CRL izmaiņu sarakstā.

4.9.9. **Sertifikātu anulēšana**

4.9.9.1. Sertifikāta anulēšana ir process sertifikāta statusa maiņai no "derīgs" uz "anulēts". Sertifikāta statuss „anulēts” nozīmē, ka uz to nevienam vairs nekādā nolūkā nevajadzētu paļauties.

4.9.9.2. eParaksts.lv SPS SI sniedz uzticamas SI sertifikātu anulēšanas pakalpojumus.

4.9.10. Anulēšanas apstākļi

4.9.10.1. eParaksts.lv SPS SI bez kavēšanās anulē sertifikātu šādos apstākļos:

4.9.10.1.1. ir saņemts derīgs sertifikāta anulēšanas pieprasījums;

4.9.10.1.2. sertifikāta publiskajai atslēgai atbilstošā privātā atslēga ir pazaudēta, bez sankcionēšanas izpausta, nozagta vai jebkādā veidā kompromitēta;

4.9.10.1.3. sertifikāta pasūtītājs nepilda SI vienošanās ar eParaksts.lv SPS būtiskas saistības;

4.9.10.1.4. sertifikāta pasūtītājs pārtrauc darboties kā uzticama sertificēšanas institūcija;

4.9.10.1.5. izpildot tiesas lēmumu attiecībā par sertifikāta anulēšanu;

4.9.10.1.6. gadījumā, ja eksistē pamatotas aizdomas, ka privāto atslēgu radīšanai un lietošanai izmantotie algoritmi, parametri un līdzekļi vairs negarantē radīto parakstu pret viltošanas drošību.

4.9.11. **Anulēšanas apstākļi ISI**

4.9.11.1. Sertifikātu anulēšana notiek nekavējoties pēc tam, kad, saskaņā ar šo SN 4.8.1.nodaļu, derīgu sertifikātu anulēšanas pieprasījumu saņem eParaksts.lv SPS ISI. Nekavējoša anulēšana notiks 24 stundu laikā no derīga anulēšanas pieprasījuma saņemšanas viena vai vairāku šādu apstākļu gadījumā:

4.9.11.1.1. sertifikāta publiskajai atslēgai atbilstošā privātā atslēga ir pazaudēta, nesankcionēti izpausta, nozagta vai ir konstatēta tās kompromitēšana;

4.9.11.1.2. ir beigušās līguma saistības starp eParaksts.lv SPS ISI un parakstītāju (pasūtītāju);

4.9.11.1.3. sertifikāta pasūtītājs nepilda būtiskas līguma ar eParaksts.lv SPS prasības, jebkuru atbilstošu SN vai šo SN uzliktās saistības;

4.9.11.1.4. eParaksts.lv SPS ISI saņem oficiālu informāciju par sertifikāta izmaiņās iekļautas jebkādas nozīmīgas informācijas izmaiņām;

4.9.11.1.5. eParaksts.lv SPS saņem oficiālu informāciju, ka parakstītājs vai pasūtītājs ir sniedzis eParaksts.lv SPS nepatiesu vai maldinošu informāciju, lai saņemtu sertifikātu;

4.9.11.1.6. izpildot tiesas lēmumu attiecībā uz sertifikāta anulēšanu;

4.9.11.1.7. gadījumā, ja pastāv pamatotas aizdomas, ka privāto atslēgu izgatavošanai un izmantošanai lietotie algoritmi, parametri un līdzekļi vairs negarantē izveidoto parakstu pret viltošanas drošību;

4.9.11.1.8. eParaksts.lv SPS ISI darbības izbeigšanas gadījumā (sk. 5.8. nodaļu);

4.9.11.1.9. jebkuru citu nozīmīgu apstākļu gadījumā, kad nepieciešams veikt izmeklēšanu, lai nodrošinātu eParaksts.lv SPS sertifikācijas pakalpojumu drošību, integritāti vai uzticamību.

4.9.12. **Anulēšanas pieprasījuma procedūra**

4.9.12.1. Anulēšanu pēc likumīga un pilnvarota pieprasījuma veic sankcionēta eParaksts.lv SPS drošības amatpersona:

4.9.12.1.1. eParaksts.lv SPS SSI saņem anulēšanas pieprasījumu;

4.9.12.1.2. drošības amatpersona nodrošina, ka anulēšanas pieprasījums ir pareizi noformēts;

4.9.12.1.3. drošības amatpersona nodrošina, ka pieprasošais pārstāvis tiek pareizi identificēts, autentificēts un pilnvarots;

4.9.12.1.4. drošības amatpersona autentificē pati sevi eParaksts.lv SPS IS;

4.9.12.1.5. drošības amatpersona veic anulēšanu (atjauninot OCSP statusa informāciju un publicējot jaunu CRL);

4.9.12.1.6. ar vēstuli vai e-pastu eParaksts.lv SPS informē pasūtītāju.

4.9.13. **Lietotāju anulēšanas pieprasījuma procedūra**

4.9.13.1. Personai, kas pieprasa anulēšanu, nepieciešams šo pieprasījumu paziņot eParaksts.lv SPS, kas savukārt nekavējoties sāks sertifikāta anulēšanu:

4.9.13.1.1. pieprasošā personā iesniedz anulēšanas pieprasījumu;

4.9.13.1.2. anulēšanas operators garantē, ka anulēšanas pieprasījums ir pareizi noformēts;

4.9.13.1.3. anulēšanas amatpersona garantē, ka pieprasošā persona ir pareizi identificēta, autentificēta un pilnvarota;

4.9.13.1.4. anulēšanas operators autentificē sevi (izmantojot sertifikātu);

4.9.13.1.5. anulēšanas operators veic anulēšanu;

4.9.13.1.6. anulēšanas amatpersona autentificē sevi (izmantojot sertifikātu);

4.9.13.1.7. anulēšanas amatpersona apstiprina anulēšanu; un

4.9.13.1.8. eParaksts.lv SPS ISI ar vēstuli vai pa e-pastu informē parakstītāju (pasūtītāju).

4.9.14. Laiks, kādā SI jāapstrādā anulēšanas pieprasījums

4.9.14.1. Maksimālā aizkave starp anulēšanas pieprasījuma vai ziņojuma saņemšanu un visiem pārbaudītājiem pieejamo sertifikāta statusa informācijas izmaiņu ir atkarīga no sertifikātu pārbaudes metodes:

4.9.14.1.1. sertifikātu pārbaudei, izmantojot eParaksts.lv SPS uzticamu OCSP responderi, tā nepārsniegs 24 stundas;

4.9.14.1.2. sertifikātu pārbaudei, izmantojot visjaunāko CRL, tā nepārsniegs 1 dienas (24 stundas).

4.9.14.2. Šaubu gadījumā pārbaudītājiem jāiegūst visjaunākā statusa informācija no eParaksts.lv SPS uzticama OCSP respondera.

4.9.15. **Anulēšanas pārbaudes prasības pārbaudītājiem**

4.9.15.1. Veicot jebkādas darbības ar eParaksts.lv SPS izsniegtajiem sertifikātiem, pārbaudītājiem ir jāpārbauda sertifikāta derīgumu, izmantojot pašreizējo anulēšanas statusa informāciju un ņemot vērā sertifikāta statusa informācijas izplatīšanas aizkavēšanos. Vērā ņemamie aspekti iekļauj, vai:

4.9.15.1.1. elektroniskais paraksts ir izveidots šī sertifikāta derīguma termiņa laikā;

4.9.15.1.2. visi atbilstošajā sertifikātu hierarhijā atrodošos sertifikātu publisko atslēgu jaucējsummas rezultāti (izvilkumi) ir sekmīgi pārbaudīti;

4.9.15.1.3. sertifikātiem sertifikātu hierarhijā nav beidzies derīguma termiņš;

4.9.15.1.4. sertifikāts un sertifikāta hierarhija ir sekmīgi pārbaudīta.

4.9.15.2. Viena no metodēm, ar kuru pārbaudītāji var pārbaudīt sertifikāta statusu, ir vēršanās pie visjaunākā CRL, izmantojot eParaksts.lv SPS direktorijas pakalpojumus. Apturēts vai anulēts sertifikāts var parādīties publicētā CRL tikai pēc 24 stundām.

4.9.15.3. OCSP atbildes pamatojas uz sertifikāta statusu eParaksts.lv SPS iekšējā sertifikātu datu bāzē un tādējādi tās pēc sertifikāta statusa izmaiņām jau ir nekavējoties aktualizētas. eParaksts.lv SPS iesaka, ka pārbaudītājiem, izmantojot SPS eParaksts.lv uzticamu OCSP responderi, jāpārbauda visjaunākais sertifikātu statuss.

4.9.16. CRL iemeslu kodu nozīme

4.9.16.1. Kad sertifikāts ir anulēts, eParaksts.lv SPS SI precizē, kāpēc šī darbība tika veikta. Šim nolūkam tiek precizēts anulēšanas iemesls. Šie iemesli ir definēti RFC 3280 [6] un ietver:

| ***CRL* iemesla kods** | **Nozīme** |
|---|---|
| Nav norādīts | Sertifikāts tika anulēts bez konkrēta iemesla koda vai ar iemeslu, kas atšķiras no norādītā. |
| Atslēgas kompromitējums | Parakstītāja privātā atslēga, kas ir saistīta ar šo sertifikātu, ir kompromitēta. Tas nozīmē, ka viedkarte vai tās parole atrodas nesankcionēta personas īpašumā. Tas var ietver gadījumu, kad viedkarte ir pazaudēta. |
| SI kompromitējums | Kriptogrāfiskais modulis (*HSM*), kurā tiek glabāta SI privātā atslēga, ir kompromitēts, un tas atrodas nepilnvarotas personas valdījumā. |
| Izmainīta saistība | Šis iemesla kods tiks izmantots gadījumā, kad:<br>vai nu ir mainīta būtiska informācija parakstītāja sertifikāta informācijā,<br>vai arī parakstītājs ir izbeidzis savas attiecības ar organizāciju, kas ir norādīta sertifikāta īpašā vārda atribūtā. |
| Aizstāts | Parakstītājam ir izsniegts aizstājēj sertifikāts, un iemesls nav neviens no iepriekšējiem iemesliem. Šo anulēšanas iemeslu parasti izmanto viedkartes atteices gadījumā vai kad parakstītājs ir mainījis savu juridisko vārdu. |
| Darbības izbeigšana | Parakstītāja vai pasūtītāja saistības ar eParaksts.lv SPS ir beigušās jebkura iemesla dēļ. |
| Sertifikāts apturēts | Sertifikāts ir apturēts. Tā apturēšanas laikā eParaksts.lv SPS neuzskatīs sertifikātu par derīgu. |
| Noņemt no *CRL* | Ja sertifikāts ir apturēts ar iemesla kodu *CertificateHold*, ir iespējams šo sertifikātu "aktivēt no jauna". Kad sertifikāts tiek atjaunots, tas joprojām atrodas *CRL*, bet ar iemesla kodu *RemoveFromCRL*.<br>Piezīme: tas ir specifiski iemesla kodam *CertificateHold* un tiek izmantots tikai izmaiņu *CRL*. |

4.9.17. CRL izdošanas biežums

4.9.17.1. CRL tiks publicēti bieži, kā parādīts turpmākajā tabulā

| **Ģenerēts un parakstīts** | **Veids** | **Saturs** | **Derīgums (iesk. pārklāšanās laiku)** | **Pārklāšanās laiks** |
|---|---|---|---|---|
| eParaksts.lv SPS Saknes SI | Kopējs / pabeigts | eParaksts.lv SPS Saknes SI izsniegtie anulētie sertifikāti | 3 mēneši un 1 nedēļa (un pēc anulēšanas) | 1 nedēļa |
| eParaksts.lv SPS Politikas SI | Kopējs / pabeigts | eParaksts.lv SPS Politikas SI izsniegtie anulētie sertifikāti | 3 mēneši un 1 nedēļa (un pēc anulēšanas) | 1 nedēļa |
| eParaksts.lv SPS Izsniegšanas SI | Kopējs / pabeigts | eParaksts.lv SPS Izsniegšanas SI izsniegtie anulētie sertifikāti | 24 stundas | 12 stundas |

4.9.17.2. Laiks starp Effective date un Next update norāda CRL derīguma termiņu. Tehnisku iemeslu dēļ (laiks, kurš nepieciešams CRL izveidošanai) nākamais CRL parasti tiks izdots pirms norādītā laika (pārklāšanās laikā), bet ne vēlāk.

4.9.17.3. Ja CRL iekļauta sertifikāta derīguma termiņš beidzas, tas tiks izņemts no vēlāk publicētiem CRL. CRL, kuru derīguma termiņš ir beidzies, tiks arhivēti.

4.9.18. **CRL maksimālais latentums**

4.9.18.1. CRL tiek nosūtīti uz repozitoriju komerciāli saprātīgā laikā pēc ģenerēšanas, kas parasti notiek dažu minūšu laikā.

4.9.19. **Tiešsaistes anulēšanas un statusa pārbaudes pieejamība**

4.9.19.1. eParaksts.lv SPS Sertifikātu pārbaudes pakalpojumi, izmantojot OCSP responderi, nodrošina eParaksts.lv SPS Saknes SI un eParaksts.lv SPS uzticamo SI izsniegto sertifikātu statusa pārbaudi tiešsaistē. Visi sertifikāti jebkurā laikā var tikt pārbaudīti, izmantojot sertifikātu pārbaudes pakalpojumus bez plānotiem pārtraukumiem. eParaksts.lv SPS uzticamā OCSP respondera slodze ir līdzsvarota un tiek rezervēta, lai nodrošinātu augstu pieejamību.

4.9.20. **Anulēšanas tiešsaistes pārbaudes prasības**

4.9.20.1. OCSP atbildes pamatojas uz sertifikāta statusu eParaksts.lv SPS iekšējā sertifikātu datu bāzē, un tādējādi tās pēc sertifikāta statusa izmaiņām tiek nekavējoties aktualizētas. eParaksts.lv SPS iesaka pārbaudītājiem izmantot eParaksts.lv SPS uzticamu OCSP responderi, lai pārbaudītu aktuālo sertifikātu statusu.

4.9.20.2. Cits nodrošinātais mehānisms ir sertifikāta statusa pārbaude nesaistē, izmantojot CRL, ko var lejupielādēt eParaksts.lv SPS direktoriju pakalpojumos.

4.9.21. **Speciālas prasības attiecībā uz atslēgu kompromitējumu**

4.9.21.1. eParaksts.lv SPS drošības amatpersona uzsāk atbilstošu izmeklēšanu, ja pastāv aizdomas, ka privāto atslēgu ģenerēšanai un lietošanai izmantotie algoritmi, parametri vai līdzekļi vairs nav droši.

## 4.10. Sertifikātu statusa pakalpojumi

4.10.1. **Darbības raksturojums**

4.10.1.1. eParaksts.lv SPS Sertifikātu pārbaudes pakalpojumi, izmantojot OCSP responderi, nodrošina tiešsaistes eParaksts.lv SPS Saknes SI un eParaksts.lv SPS uzticamo SI izsniegto sertifikātu statusa pārbaudi saskaņā ar RFC 2560 [7].

4.10.1.2. OCSP responderis ir pieejams URL http://ocsp.eme.lv/responder.eme un https://ocsp.eme.lv/responder.eme

4.10.1.3. Piekļuve OCSP responderim kvalificēta e-paraksta sertifikāta statusa pārbaudei nav ierobežota, un šī piekļuve netiek autentificēta. Lai pārbaudītu citus sertifikātus, kas nav kvalificēti, eParaksts.lv SPS uzticams OCSP responderis pieņem arī autentificētus pieprasījumus.

4.10.1.4. eParaksts.lv SPS uzticams OCSP responderis:

4.10.1.4.1. autentificē lietotāja pieprasījumu, ja pieprasītājs piekļuvei OCSP izmanto autentificētu kanālu;

4.10.1.4.2. pārbauda sertifikāta statusa pieprasījumu šādiem RFC noteiktajiem apstākļiem:

4.10.1.4.3. vai pieprasījuma ziņojums ir pareizi sastādīts;

4.10.1.4.4. vai responderis ir konfigurēts tā, lai varētu sniegt pieprasīto pakalpojumu;

4.10.1.4.5. vai pieprasījumā ir responderim nepieciešamā informācija;

4.10.1.4.6. ja pārbaude neizdodas, tiek sagatavots un nosūtīts atpakaļ kļūdas ziņojums;

4.10.1.4.7. ja sertifikāta statusa pieprasījums ir derīgs (saskaņā ar RFC), OCSP responderis vēršas pie sertifikātu datu bāzes, lai iegūtu sertifikāta statusa informāciju;

4.10.1.4.8. sagatavo atbildes ziņojumu un to paraksta, izmantojot privātu atslēgu, kas ir saistīta ar nozīmētā uzticama respondera sertifikātu (eParaksts.lv SPS OCSP sertifikātu);

4.10.1.4.9. nosūta atbildi pieprasītājam;

4.10.1.4.10. reģistrē sertifikāta statusa pieprasījuma apstrādes pabeigšanu audita žurnālā kopā ar operācijas statusu.

4.10.1.5. OCSP paraksta atbildes, izmantojot uzticama respondera sertifikātu, kas atbalsta SHA1 jaucējsummas algoritmu un nonce paplašinājumu. Ja uzticamā

respondera sertifikāta derīguma termiņš ir beidzies vai tas ir anulēts, OCSP responderis aptur darbību.

4.10.1.6. Jāatzīmē, ka kļūdu ziņojumi nav jāparaksta.

4.10.2. **Atbilžu nozīme**

4.10.2.1. OCSP responderis tiek izmantots, lai atbildētu uz sertifikātu statusa pieprasījumiem, un tas var izsniegt vienu no trijām atbildēm: “derīgs”, “anulēts” un “nezināms”.

| ***OCSP* atbilde** | **Nozīme** |
|---|---|
| Derīgs | "Derīgs" statuss norāda, ka atbilde uz statusa pieprasījumu ir pozitīva.<br>Šī pozitīvā atbilde norāda, ka sertifikāts nav apturēts vai anulēts, bet tas noteikti nenozīmē, ka laiks, kurā šī atbilde tika sastādīta, atbilst šī sertifikāta derīguma intervālam. |
| Anulēts | Statuss "anulēts" norāda, ka sertifikāts ir anulēts (vai nu pastāvīgi, vai arī uz laiku (apturēts)). |
| Nezināms | Sertifikāts datu bāzē nav atrasts!<br>Šis statusa pieprasījums attiecas uz sertifikāta statusu, kuru nav izsniedzis eParaksts.lv SPS. |

4.10.3. **Sertifikātu derīguma pārbaude**

eParaksts.lv SPS izsniegto sertifikātu pārbaude jāveic pēc sekojošas kārtības:

4.10.3.1. Ja izmantojat interneta pieslēgumu, tad pārbaudiet sertifikātu ar OCSP responderi, izmantojot sertifikāta statusa pakalpojumus (skat.4.10.). Sertifikāta statusa pārbaudi ar OCSP var veikt eParaksts.lv SPS mājas lapā www.eparaksts.lv

4.10.3.2. Ja nav iespējas pārbaudīt sertifikātu ar OCSP responderi, tad paļaujieties uz CRL. Ceļš uz sertifikāta izsniedzēja CRL ir norādīts sertifikātā (skat. 7. nodaļu). Ja sertifikāts ir CRL, tad tas ir nederīgs uz CRL publicēšanas brīdi.

4.10.3.3. Ja nav pieejams ne OCSP responderis, ne derīgi CRLi, tad sertifikāta derīgumu nevar pārbaudīt.

4.10.3.4. eParaksts.lv SPS rekomendācijas konkrētajiem pārbaudes situācijām:

| **Situācija** | **Rekomendēta pārbaudes metode** |
|---|---|
| Nesen anulēts sertifikāts | CRL informācija var būt nokavēta, rekomendētā pārbaudes metode ir OCSP responderis |
| Nesen apturēts sertifikāts | CRL informācija var būt nokavēta, rekomendētā pārbaudes metode ir OCSP responderis |
| Nesen atjaunots sertifikāts | CRL informācija var būt nokavēta, rekomendētā pārbaudes metode ir OCSP responderis<br>Lai pārbaudītu sertifikātu apturēšanas laikā, ir lietojama saglabāta CRL vēsture |
| Sertifikāta derīguma termiņš ir beidzies | Rekomendētā pārbaudes metode ir saglabāta CRL vēsture |

## 4.11. Sertifikāta izmantošanas beigas

4.11.1. Pasūtītājs var izbeigt eParaksts.lv SPS ISI sertifikāta izmantošanu:

4.11.1.1. ļaujot beigties sertifikāta derīguma termiņam un neaizstājot šo sertifikātu;

4.11.1.2. anulējot sertifikātu pirms derīguma termiņam beigām, neaizstājot šo sertifikātu.

## 4.12. Atslēgu nodošana glabāšanā trešajai pusei un atjaunošana

4.12.1. Atslēgu nodošana glabāšanā trešajai pusei netiek atļauta.

# 5. Objekta, pārvaldības un darbības kontroles

## 5.1. Fiziskās drošības kontroles

5.1.1. eParaksts.lv SPS lieto uzticamas sistēmas un produktus, kas ir aizsargāti pret modificēšanu, un nodrošina to uzturēto procesu tehnisko un kriptogrāfisko drošību.

5.1.2. eParaksts.lv SPS ir ieviesis Fiziskās drošības noteikumus un procedūras, kas atbalsta šo SN drošības prasības. Fiziskās drošības noteikumi un procedūras ietver jutīgu drošības informāciju un ir pieejamas tikai vienojoties ar eParaksts.lv SPS. Prasību pārskats ir aprakstīts zemāk.

5.1.3. **Objekta novietojuma apsvērumi un izbūve**

5.1.3.1. eParaksts.lv SPS pakalpojumi tiek sniegti fiziski aizsargātā vidē, kura attur, aizsargā un atklāj nesankcionētu jutīgas informācijas un sistēmu lietošanu, piekļuvi vai izpaušanu gan slēptā, gan atklātā veidā.

5.1.3.2. eParaksts.lv SPS savām SI darbībām uztur pēcavārijas atjaunošanas telpas un iekārtas. eParaksts.lv SPS pēcavārijas atjaunošanas telpas un iekārtas ir aizsargātas ar vairākiem fiziskās drošības līmeņiem, kas ir salīdzināmi ar eParaksts.lv SPS primārajām telpām un iekārtām.

5.1.4. **Fiziskā piekļuve**

5.1.4.1. eParaksts.lv SPS SI sistēmas ir aizsargātas ar vismaz trīs fiziskās drošības līmeņiem, turklāt tiek prasīta piekļuve zemākam drošības līmenim pirms var piekļūt augstākam līmenim. Progresējoši ierobežojošas fiziskās piekļuves tiesības kontrolē piekļuvi katram līmenim.

5.1.4.2. Nodrošinātā aizsardzība ir samērāma ar identificētajiem riskiem. eParaksts.lv SPS nodrošina, ka fiziska piekļuve kritiskajiem pakalpojumiem tiek kontrolēta, un fiziskie riski tās resursiem ir samazināti.

5.1.4.3. Ir pieejams skaidrs eParaksts.lv SPS fiziskās vides apraksts. Tas ietver:

5.1.4.3.1. ieviestās drošības zonas un to aizsardzības īpašības (profilaktiska, represīva, atklājoša un koriģējoša);

5.1.4.3.2. saistību ar drošībai kritiskiem resursiem;

5.1.4.3.3. dokumentāciju par to, kuriem eParaksts.lv SPS darbiniekiem ir piekļuve kurām zonām;

5.1.4.3.4. pamatojoties uz dokumentētu riska analīzi, ieviestu adekvātu aizsardzību (profilaktiska, atklājoša un koriģējoša) pret ugunsgrēku un dūmiem, enerģijas padeves bojājumiem, plūdiem, vētru utt.;

5.1.4.3.5. uzstādītās piekļuves kontroles sistēmas;

5.1.4.3.6. procedūras regulārai augsta riska zonu piekļuves kodu maiņai;

5.1.4.3.7. ieviestie līdzekļi un procedūras, lai nodrošinātu, ka jebkuru personu, kura ieiet fiziski drošā zonā, vienmēr pavada pilnvarota persona;

5.1.4.3.8. iepriekš minētā apraksta, riska analīzes un inventāra uzturēšanas atbildība ir uzticēta eParaksts.lv SPS drošības amatpersonai. Vadības uzdevums ir periodiski pārskatīt iepriekšminēto aprakstu.

5.1.5. **Energoapgāde un gaisa kondicionēšana**

5.1.5.1. eParaksts.lv SPS drošie objekti ir apgādāti ar primārajām un rezerves:

5.1.5.1.1. energoapgādes sistēmām, lai nodrošinātu pastāvīgu un nepārtrauktu elektroenerģijas padevi;

5.1.5.1.2. apkures, ventilācijas un gaisa kondicionēšanas sistēmām, lai kontrolētu temperatūru un relatīvo mitrumu.

5.1.6. **Pakļaušana ūdens iedarbībai**

5.1.6.1. eParaksts.lv SPS ir veikusi saprātīgus drošības pasākumus, lai samazinātu ūdens iedarbību uz informācijas sistēmām.

5.1.7. **Ugunsgrēka riska novēršana un ugunsdrošība**

5.1.7.1. eParaksts.lv SPS ir veikusi saprātīgus drošības pasākumus, lai aizkavētu un nodzēstu ugunsgrēkus vai novērstu citu kaitējošu liesmu vai dūmu iedarbību. eParaksts.lv SPS ugunsdrošības pasākumi atbilst vietējiem ugunsdrošības noteikumiem.

5.1.8. **Datu nesēju glabāšana**

5.1.8.1. Visi datu nesēji, kuros ir produkcijas programmatūra un dati, audita, arhīva vai rezerves kopiju informācija, tiek glabāta eParaksts.lv SPS objektos vai drošā ārpus objekta vietas izvietotā glabāšanas objektā. Šiem objektiem ir pienācīgas fiziskās un loģiskās pieejas kontroles, paredzētas, lai ierobežotu piekļuvi tikai pilnvarotam personālam un aizsargātu šos datu nesējus no iespējama postījuma (piem., no ūdens, uguns un elektromagnētiskās iedarbības).

5.1.9. **Atkritumu likvidēšana**

5.1.9.1. Pirms likvidēšanas jutīgie dokumenti un materiāli tiek sasmalcināti. Jutīgās informācijas vākšanai vai pārraidei izmantotie datu nesēji pirms likvidēšanas tiek padarīti nelasāmi. Kriptogrāfiskie līdzekļi pirms likvidēšanas tiek fiziski iznīcināti vai tiek izdzēsta to atmiņa saskaņā ar ražotāja instrukcijām.

5.1.10. **Ārpus objekta izvietota rezerves kopija**

5.1.10.1. eParaksts.lv SPS veic kritisku sistēmas datu, audita žurnāla datu un citas jutīgas informācijas regulāru rezerves kopiju izveidi. Ārpus objekta vietas izvietotie datu nesēji tiek glabāti fiziski drošā veidā, izmantojot saistītu trešās puses datu glabātavu vai eParaksts.lv SPS pēcavārijas atjaunošanas līdzekļus.

## 5.2. Procedurālas kontroles

5.2.1. **Uzticības lomas**

5.2.1.1. Visas eParaksts.lv SPS kritiskās un jutīgās aktivitātes tiek apvienotas lomās. Saskaņā ar ETSI 101456 [6] uzticības lomas ietver lomas ar šādām atbildībām:

5.2.1.1.1. drošības amatpersona: vispārēja atbildība par drošības procedūru ieviešanas administrēšanu;

5.2.1.1.2. sistēmas amatpersona: atbildīga par ikdienas darbu ar SI uzticamajām sistēmām. Pilnvarota veikt sistēmas rezerves kopiju izveidi un atjaunošanu;

5.2.1.1.3. sistēmas administrators: pilnvarots instalēt, konfigurēt un uzturēt SI uzticamās sistēmas reģistrācijas, sertifikātu ģenerēšanas, parakstītāju ierīču nodrošināšanas un anulēšanas pārvaldībai;

5.2.1.1.4. sistēmas operators; pilnvarots veikt operētājsistēmas un SI datu bāzes rezerves kopiju izveidi un atjaunošanu;

5.2.1.1.5. sistēmas auditors: pilnvarots skatīt ar SI uzticamām sistēmām saistītos arhīvus un audita žurnālus.

5.2.1.2. eParaksts.lv SPS uzskata šajā nodaļā identificētās personāla kategorijas kā uzticamās personas, kam ir uzticības lomas.

5.2.1.3. Uzticības lomas un atbildības ietver prasību:

5.2.1.3.1. ieviest un darboties saskaņā ar organizācijas informācijas drošības politikām;

5.2.1.3.2. aizsargāt resursus no nesankcionētas piekļuves, izpaušanas, modificēšanas, iznīcināšanas vai uzlaušanas;

5.2.1.3.3. izpildīt īpašus drošības procesus un aktivitātes;

5.2.1.3.4. nodrošināt, ka personai par veiktajām darbībām tiek noteikta atbildība;

5.2.1.3.5. ziņot par esošiem vai iespējamiem drošības pārkāpumiem vai citiem drošības draudiem organizācijai.

5.2.2. Uzdevumam nepieciešamo darbinieku skaits

5.2.2.1. eParaksts.lv SPS ir ieviesusi, uztur un nodrošina stingras kontroles procedūras, lai nodrošinātu atbildības pienākumu atdalīšanu un to, ka jutīgu uzdevumu veikšanai ir nepieciešamas vairākas uzticamas personas.

5.2.2.2. Turpmāk uzskaitītajām aktivitātēm nepieciešama vismaz divu uzticamu personu fiziska vai loģiska piekļuve ierīcei vai vietai:

5.2.2.2.1. loģiska vai fiziska piekļuve HSM;

5.2.2.2.2. fiziska piekļuve datu arhīvam;

5.2.2.2.3. loģiska piekļuve eParaksts.lv SPS SI centrālajām, jutīgajām vai kritiskajām sistēmām un to dublējošajām sistēmām.

5.2.3. **Katras lomas identifikācija un autentifikācija**

5.2.3.1. Personu identifikācija un autentifikācija tiek veikta, sniedzot piekļuvi drošībai svarīgām zonām un ar viedkartēm piekļūstot kritiskajām sistēmām. Vadības sistēmās lietotāju pilnvarošana notiek atbilstoši lomām.

## 5.3. Personāla kontroles

5.3.1. Visa personāla, kas vēlas kļūt par uzticamām personām, identitātes pārbaude notiek šī personāla personīgā (fiziskā) klātbūtnē pret personu apliecinošu dokumentu. Kā aprakstīts šajos SN, turpmāka identitātes apstiprināšana notiek, veicot personas datu pārbaudes procedūras. eParaksts.lv SPS nodrošina, ka personāls ir sasniedzis uzticamu statusu, un tiek sniegts struktūrvienības apstiprinājums, pirms šim personālam tiek:

5.3.1.1. izsniegtas nepieciešamās piekļuves ierīces un piešķirtas piekļuves tiesības nepieciešamajiem līdzekļiem;

5.3.1.2. izsniegtas elektroniskās pilnvaras, lai piekļūtu un veiktu eParaksts.lv SPS SI specifiskos pienākumus.

5.3.2. **Kvalifikācijas, pieredzes un atļaujas izsniegšanas prasības**

5.3.2.1. Lai dokumentētu drošības un citas uzticības lomas un pienākumus, tiek izmantoti skaidri izklāstīti amata apraksti, un darbā pieņemšanas procesā tie tiek skaidri paziņoti darba kandidātiem.

5.3.2.2. Visu darba pretendentu (līgumdarbinieku un ārējo lietotāju) datu pārbaude tiek veikta saskaņā ar atbilstošiem normatīviem aktiem, noteikumiem un ētikas prasībām, kā arī atbilstoši biznesa prasībām, piekļuves informācijas slepenībai un novērtētajam riska līmenim.

5.3.3. **Personāla datu pārbaudes procedūras**

5.3.3.1. eParaksts.lv SPS veiks atbilstošu visa personāla, kas darbojas uzticības lomās, izpēti (pirms nodarbinātības uzsākšanas un pēc tam periodiski pēc vajadzības), lai apliecinātu viņu uzticamību un kompetenci saskaņā ar šo SN prasībām un eParaksts.lv SPS SI personāla vadības procedūrām vai līdzīgiem

noteikumiem. Viss personāls, kurš neiztur sākotnējo vai periodisko pārbaudi, nedarbosies vai neturpinās darboties uzticības lomā.

5.3.4. **Apmācības prasības**

5.3.4.1. eParaksts.lv SPS SI nodrošina, ka viss personāls, kas pilda vadības pienākumus attiecībā uz SI darbību, saņem visaptverošu apmācību šādās jomās:

5.3.4.1.1. SI drošības principi un mehānismi;

5.3.4.1.2. drošības jautājumu izpratne;

5.3.4.1.3. eParaksts.lv SPS IS visas lietotās SPS programmatūras versijas;

5.3.4.1.4. visi veicamie darba pienākumi;

5.3.4.1.5. pēcavārijas atjaunošanas un biznesa nepārtrauktības procesi.

5.3.5. **Kvalifikācijas celšanas apmācību biežums un prasības**

5.3.5.1. 5.3.4. nodaļas prasības ir regulāri jāatjauno, un tajās ir jāiestrādā eParaksts.lv SPS IS izmaiņas. Pēc vajadzības jāveic kvalifikācijas celšanas apmācības, un eParaksts.lv SPS vismaz reizi gadā jāpārskata šīs prasības.

5.3.6. Darbu rotācijas biežums un secība

5.3.6.1. Šie SN neparedz ierobežojumus darbu rotācijas biežumam un secībai. Individuālas politikas, kuras uzliek šāda veida prasības, nodrošinās eParaksts.lv SPS pakalpojumu pastāvību un integritāti.

5.3.7. **Sankcijas par nesankcionētu darbību veikšanu**

5.3.7.1. eParaksts.lv SPS izveido, uztur un īsteno nodarbinātības politiku personāla disciplīnai pēc nesankcionētu darbību veikšanas. Disciplinārie sodi ietver pasākumus līdz pat darba attiecību pārtraukšanai, un tiem jābūt samērojamiem ar nesankcionēto darbību biežumu un nopietnību.

5.3.8. **Prasības līgumdarbiniekiem**

5.3.8.1. eParaksts.lv SPS ļauj neatkarīgiem līgumdarbiniekiem vai konsultantiem kļūt par uzticamām personām tikai tādā mērā, kā tas ir nepieciešams, lai noregulētu skaidri definētas ārpakalpojumu attiecības, un tikai šādos apstākļos:

5.3.8.1.1. organizācijai, kas kā uzticamas personas izmanto neatkarīgus līgumdarbiniekus vai konsultantus, nav piemērotu darbinieku, kas varētu pildīt uzticamu personu lomas;

5.3.8.1.2. organizācija uzticas līgumdarbiniekiem un konsultantiem tādā pašā apjomā kā saviem darbiniekiem.

5.3.8.2. Pretējā gadījumā neatkarīgi līgumdarbinieki un konsultanti varēs piekļūt eParaksts.lv SPS drošam objektam tikai uzticamu personu pavadībā un tiešā uzraudzībā.

5.3.9. **Personālam izsniedzamā dokumentācija**

5.3.9.1. eParaksts.lv SI sniegs savam personālam (tostarp uzticamajām personām) nepieciešamo apmācību un citu dokumentāciju, kas nepieciešama, lai savus darba pienākumus tas veiktu kompetenti un apmierinoši.

## 5.4. Audita reģistrācijas procedūras

5.4.1. Visi žurnāla ieraksti ietver šādus elementus:

5.4.1.1. ieraksta datums un laiks;

5.4.1.2. ieraksta sērijas vai kārtas numurs (automātiskiem žurnāla ierakstiem);

5.4.1.3. ieraksta veids;

5.4.1.4. ieraksta avots (piem., terminālis, ports, atrašanās vieta, klients, u.t.t);

5.4.1.5. žurnāla ieraksta veicēja identitāte.

5.4.2. **Reģistrējamo notikumu tipi**

5.4.2.1. **SI darbības procedūras**

5.4.2.2. Visi notikumi, kas ir saistīti ar darbībām ar eParaksts.lv SPS SI, tiks reģistrēti:

5.4.2.2.1. sistēmas darbības sākšana un beigšana;

5.4.2.2.2. SI lietojumprogrammu sākšana un beigšana;

5.4.2.2.3. mēģinājumi izveidot, atcelt, noteikt paroles vai mainīt pilnvarotu lietotāju (uzticības lomu) sistēmas pilnvaras;

5.4.2.2.4. sertifikātu izveidošanas politiku, piem., derīguma termiņa, izmaiņas;

5.4.2.2.5. pieteikšanās un atteikšanās mēģinājumi;

5.4.2.2.6. ar sertifikāta dzīves cikla pārvaldību saistīti notikumi (piem., sertifikātu pieteikumi, izsniegšana, anulēšana un atjaunošana);

5.4.2.2.7. ar kriptogrāfiskā moduļa dzīves cikla pārvaldību saistīti notikumi (piem., saņemšana, lietošana, demontāža, un lietošanas pārtraukšana);

5.4.2.2.8. sistēmas konfigurācijas izmaiņas un uzturēšana;

5.4.2.2.9. izmaiņas, kas skar SI parametrus vai atslēgu;

5.4.2.2.10. pakārtoto SI atslēgu ģenerēšana.

5.4.2.3. **HSM un sistēmas karšu dzīves cikla notikumi**

5.4.2.3.1. AKK, OKK inicializēšana;

5.4.2.3.2. HSM inicializēšana;

5.4.2.3.3. HSM konfigurācijas izmaiņas;

5.4.2.3.4. pieteikšanās HSM un atteikšanās no tā;

5.4.2.3.5. atslēgu ģenerēšana HSM ar AKK;

5.4.2.3.6. atslēgu atkārtota ģenerēšana jaunā HSM ar AKK;

5.4.2.3.7. privāto atslēgu deaktivēšana.

5.4.2.4. **Reģistrācijas dati**

5.4.2.5. Visi katra sertifikāta reģistrācijas procesā iesaistītie dati tiks rūpīgi reģistrēti iespējamām uzziņām nākotnē. SI ir jānodrošina, ka tiek reģistrēta visa reģistrācijas informācija, tostarp:

5.4.2.5.1. pieteicēja reģistrāciju atbalstošie iesniegtie dokumenta(u) tipi;

5.4.2.5.2. ja piemērojami, unikālu identifikācijas datu, skaitļu vai to apvienojuma identifikācijas dokumentos ieraksts;

5.4.2.5.3. pieteikumu un identifikācijas dokumentu, tostarp parakstīta Pasūtītāja līguma, kopiju glabāšanās vieta;

5.4.2.5.4. pasūtītāja līguma konkrētas izvēles (piem., piekrišana sertifikāta publikācijai);

5.4.2.5.5. pieteikuma akceptēšanas struktūrvienības identitāte;

5.4.2.5.6. saņemošās SI vai iesniedzošās Reģistrācijas institūcijas nosaukums.

5.4.2.6. **Sertifikātu ģenerēšana**

5.4.2.7. Visi dati un procedūras, kas ir saistītas ar sertificēšanu un sertifikātu izplatīšanu, tiks reģistrētas. Tas ietver tādu informāciju kā:

5.4.2.7.1. sertifikātu pieprasījums;

5.4.2.7.2. sertifikātu izsniegšana;

5.4.2.7.3. sertifikātu akceptēšana;

5.4.2.7.4. sertifikātu publicēšana.

5.4.2.8. **Sertifikātu un CRL publicēšana**

5.4.2.8.1. Tiks reģistrēti visi dati, kas saistīti ar eParaksts.lv SPS SI sertifikātu un CRL publicēšanu LDAP serverī.

5.4.2.9. **Sertifikātu anulēšana**

5.4.2.10. Tiks reģistrētas visas sertifikāta anulēšanas pieprasījuma detaļas, tostarp:

5.4.2.10.1. anulēšanas amatpersonas vārds;

5.4.2.10.2. datums, laiks un pieprasījumu iniciējošās personas identitāte;

5.4.2.10.3. anulēšanas iemesls.

5.4.2.11. **Sistēmas uzturēšana un kļūdu atklāšana**

5.4.2.11.1. Tā kā eParaksts.lv SPS vide ietvers nozīmētu eParaksts.lv SPS SI administratoru veiktu uzturēšanu, visa uz aparatūras veiktās uzturēšanas detalizētā informācija tiks reģistrēta. eParaksts.lv SPS SI administratori reģistrēs jebkuras noteiktās aparatūras atklātos kritiskos kļūdu ziņojumus.

5.4.3. **Reģistrācijas žurnāla apstrādes biežums**

5.4.3.1. eParaksts.lv SPS SI nodrošina, ka tās audita žurnālus regulāri pārskata nozīmēts personāls un visi aizdomīgie notikumi tiek reģistrēti un analizēti. Šāda analīze ietver pārbaudi, vai audita žurnāls nav labots, attiecīgo žurnāla ierakstu pārskatīšanu un trauksmju vai atkāpju no normas rūpīgāku izpēti. Atbalstošie SI manuālie un elektroniskie reģistri jāsalīdzina, ja kāda darbība tiek uzskatīta par aizdomīgu. Jādokumentē darbības, kas tiek veiktas pēc šiem pārskatiem.

5.4.4. **Audita žurnāla uzglabāšanas ilgums**

5.4.4.1. Audita žurnāli vismaz divus mēnešus pēc apstrādes jāuzglabā objektā un tad jāarhivē saskaņā ar 5.5. nodaļu.

5.4.5. **Audita žurnāla aizsardzība**

5.4.5.1. Audita žurnāli tiks aizsargāti ar elektroniskā audita žurnāla sistēmu, kas ietver mehānismus, lai aizsargātu žurnāla failus pret nesankcionētu skatīšanos, modificēšanu, dzēšanu, vai citādu bojāšanu. Elektroniskajai audita žurnāla sistēmai jāiekļauj ierakstu laika zīmogošanas mehānismi. Neelektroniskai audita informācijai jābūt aizsargātai pret nesankcionētu skatīšanos, modifikāciju un iznīcināšanu.

5.4.6. **Audita žurnāla rezerves kopiju izveides procedūras**

5.4.6.1. Audita žurnālu inkrementālas rezerves kopijas tiek veidotas katru nedēļu, un pilna rezerves kopēšana tiek veikta reizi mēnesī.

5.4.7. **Audita veidošanas sistēma (iekšējā, salīdzinot ar ārējo)**

5.4.7.1. Automatizēti audita dati tiek ģenerēti un ierakstīti lietojumprogrammu un operētājsistēmas līmenī. Neelektroniski ģenerētus audita datus ieraksta eParaksts.lv SPS personāls, kam piešķirtas uzticības lomas.

## 5.5. Ierakstu arhīvs

5.5.1. **Arhivējamo ierakstu tipi**

5.5.1.1. eParaksts.lv SPS SI ieraksti, kas attiecas uz tās sertificēšanas pakalpojumu darbību, tiek arhivēti un uzglabāti vismaz tik ilgi, cik norādīts 5.5.2. nodaļā. Visi fiziskie ieraksti un identifikācijas informācija jāarhivē vienībai, kas pasūtītājam tieši sniedz sertifikācijas pakalpojumus (t.i., eParaksts.lv SPS klientu apkalpošanas punktiem). Visos gadījumos šie ieraksti jāarhivē papīra vai elektroniskā formā.

5.5.1.2. Rakstīti dokumenti tiks arhivēti klientu apkalpošanas punktos vai eParaksts.lv SPS centralizētā arhīvā saskaņā ar Latvijas Valsts arhīva noteikumiem.

5.5.2. **Arhīva glabāšanas ilgums**

5.5.2.1. Arhīva ieraksti tiks uzglabāti vismaz desmit (10) gadus bez jebkāda datu zuduma. Šo laiku var pagarināt konkrētiem ierakstiem un informācijai pēc speciālu arhivēšanas pakalpojumu pieprasījuma.

5.5.3. **Arhīva aizsardzība**

5.5.3.1. Arhīvu jāaizsargā pret nesankcionētu skatīšanos, modificēšanu, dzēšanu, vai citu uzticamas sistēmas datu glabāšanas bojāšanu. Datu nesēji, kuros ir arhīva dati un arhīva datu apstrādei nepieciešamās lietojumprogrammas, jāuztur, lai nodrošinātu, ka arhīva datiem var piekļūt 5.5.2. nodaļā noteiktajā laikā.

5.5.4. **Arhīva rezerves kopijas izveides procedūras**

5.5.4.1. Primāro arhīvu zuduma vai iznīcināšanas gadījumā darbojas adekvātas rezerves kopiju izveides procedūras, kas nodrošina, ka īsā laikā ir pieejams pilns rezerves kopiju komplekts.

5.5.5. **Prasības ierakstu laika zīmogošanai**

5.5.5.1. Sertifikātos, CRL un citos anulēšanas datu bāzes ierakstos jābūt laika un datuma informācijai. Šādai laika informācijai nav jābūt kriptogrāfiskai.

5.5.6. **Arhīva veidošanas sistēma (iekšēja vai ārēja)**

5.5.6.1. eParaksts.lv SPS arhīva veidošanas sistēmai jābūt iekšējai.

5.5.7. **Procedūras arhīva informācijas iegūšanai un pārbaudei**

5.5.7.1. Tikai pilnvarotas uzticības personas var iegūt piekļuves tiesības arhīvam. Informācijas integritāte tiek pārbaudīta, to atjaunojot.

## 5.6. Atslēgu aizvietošana

5.6.1. Atslēgu aizvietošana nav automātiska. Atslēgu derīguma termiņš beidzas tajā pašā laikā kā ar tām saistītiem sertifikātiem. eParaksts.lv SPS SSI ierosina atslēgas aizvietošanu 9 (deviņus) gadus pirms beidzas tās sertifikātu derīguma termiņš (izsniegšanas pārtraukšanas datums). Gala lietotāja sertifikātu uzticības hierarhijas citi izsniegšanas pārtraukšanas datumi ir parādīti turpmākajā tabulā

| **SI** | **Derīguma termiņš** | **Darbības laiks (Izsniegšanas pārtraukšanas datums)** |
|---|---|---|
| eParaksts.lv SPS SI | 18 gadi | 9 gadi |
| eParaksts.lv SPS Politikas SI | 12 gadi | 6 gadi |
| eParaksts.lv SPS Izsniegšanas SI | 6 gadi | 3 gadi |

5.6.2. Izsniegšanas pārtraukšanas datumā SI pārtrauc sertifikātu izsniegšanu ar veco atslēgu un sāk jaunu atslēgu ģenerēšanu. SI atslēgas aizvietošana jāapstiprina eParaksts.lv Sertifikācijas pakalpojumu vadītājam un tā jāapliecina eParaksts.lv SPS drošības amatpersonai. Jaunās publiskās atslēgas jauno sertifikātu publicē eParaksts.lv SPS direktoriju pakalpojumi. Sertifikātu pieprasījumi, kas saņemti pēc izsniegšanas pārtraukšanas datuma, tiks parakstīti ar jauno SI privāto atslēgu.

5.6.3. eParaksts.lv SPS SSI samazina darbības pārtraukumus, ko izraisa SI atslēgas aizvietošana, gala lietotājiem un pārbaudītājiem viņu uzticības hierarhijā. Ņemot to vērā, eParaksts.lv SPS Saknes SI turpina izdot CRL, kas parakstīti ar sākotnējo privāto atslēgu, līdz sākotnējā atslēgu pāra derīguma termiņa beigām. Tas nozīmē, ka pēc izsniegšanas pārtraukšanas datuma būs pieejami divi CRL ar vienu, no kuriem pirmais CRL būs parakstīts ar veco atslēgu, bet otrais CRL - ar jauno atslēgu.

## 5.7. Kompromitējums un pēcavārijas atjaunošana

5.7.1. **Incidentu un kompromitējumu apstrādes procedūras**

5.7.1.1. Turpmāk uzskaitītās SI informācijas rezerves kopijas jātur ārpus objekta vietā, un tām jābūt pieejamām kompromitējuma vai avārijas gadījumā: sertifikātu pieteikumu dati, audita dati un datu bāzes ieraksti visiem izsniegtajiem sertifikātiem. SI privāto atslēgu rezerves kopijas jāģenerē un jāuztur saskaņā ar 6.2.5. nodaļu.

5.7.1.2. Procedūras informācijas drošības incidentu un eParaksts.lv SPS sertificēšanas institūciju privāto atslēgu kompromitējumu apstrādei ir dokumentētas eParaksts.lv SPS iekšējā avārijas atjaunošanas plānā. eParaksts.lv SPS iekšējais avārijas atjaunošanas plāns apraksta procedūras un atbildības, rīkojoties šādu incidentu gadījumos. Avārijas atjaunošanas plāna mērķis ir tūlītēja sertifikācijas pakalpojumu pieejamības un pastāvīgas nodrošināšanas atjaunošana. Šo procedūru pamati ir precizēti turpmākajās nodaļās.

5.7.2. **Atjaunošana pēc datu apstrādes resursu bojājuma**

5.7.2.1. Pēc iedomātas vai patiesas resursu, programmatūras vai datu kompromitēšanas tiks piemērotas avārijas atjaunošanas procedūras (saskaņā ar 5.7.4. nodaļu).

5.7.3. **Vienības privātās atslēgas kompromitējuma procedūras**

5.7.3.1. Ja ir kompromitēta eParaksts.lv SPS SI privātā atslēga vai ir aizdomas par šādu kompromitējumu, eParaksts.lv SPS SI veiks vismaz šādas darbības:

5.7.3.1.1. informēs parakstītājus, savstarpēji sertificējošos SI un pārbaudītājus;

5.7.3.1.2. izbeigs sertifikātu un CRL, kas ir izsniegti ar kompromitēto privāto atslēgu, izplatīšanas pakalpojumus;

5.7.3.1.3. pieprasīs SI sertifikāta anulēšanu.

5.7.4. **Darbības nepārtrauktības iespējas pēc avārijas**

5.7.4.1. eParaksts.lv SPS sniegto sertifikācijas pakalpojumu augsto pieejamību garantē ar informācijas sistēmas ātru instalāciju.

5.7.4.2. Skaitļošanas resursu, programmatūras vai datu bojājumu vai zudumu gadījumam eParaksts.lv SPS ir sagatavots atbilstošs avārijas atjaunošanas un darbības nepārtrauktības plāns. Šis plāns prasa izveidot un iedarbināt telpas un iekārtas, kas atrodas citā ģeogrāfiskā vietā un var sniegt SI pakalpojumus saskaņā ar šiem SN.

5.7.4.3. Kritisku pakalpojumu, tādu kā sertifikātu apturēšana un anulēšana, sertifikātu pārbaude un CRL publicēšana tiks veikta maks. 4 stundu laikā. Pilna funkcionalitāte tiks nodrošināta septiņdesmit divu (72) stundu laikā. Šis plāns ietver šāda objekta gatavības pilnīgu un periodisku pārbaudi. Uz šo plānu būs atsauce atbilstošā dokumentācijā, un tas būs pieejams izskatīšanai pilnvarotām pusēm.

## 5.8. SI darbības izbeigšana

5.8.1. Gadījumā, ja eParaksts.lv SPS SI ir nepieciešams pārtraukt darbību, pirms SI darbības izbeigšanas eParaksts.lv SPS veic komerciāli pamatotus pasākumus, lai informētu uzticamas SI, pārbaudītājus un citus šādas darbības izbeigšanas dēļ ietekmētas vienības. Sekojošam darbības izbeigšanas plānam ir jāsamazina darbības pārtraukumus ar klientiem, uzticamām SI un pārbaudītājiem:

5.8.1.1. ziņojuma publicēšana par darbības izbeigšanu skartajām pusēm, tādām kā pasūtītāji un pārbaudītāji;

5.8.1.2. eParaksts.lv SPS uzticamām SI izsniegto sertifikātu anulēšana;

5.8.1.3. SI arhīvu un ierakstu saglabāšana uz laiku, kas ir prasīts šajos SN;

5.8.1.4. klientu atbalsta un Palīdzības dienesta pakalpojumu turpināšana;

5.8.1.5. anulēšanas pakalpojumu turpināšana, tādu kā CRL izdošana vai tiešsaistes statusa pārbaudes pakalpojumu uzturēšana;

5.8.1.6. Saknes SI privātās atslēgas iznīcināšana;

5.8.1.7. pasākumi, kas nepieciešami pārejai no eParaksts.lv SPS Saknes SI pakalpojumiem uz pārņēmēju Saknes SI;

5.8.1.8. fizisko personu datu konfidencialitātes nodrošināšana.

# 6. Tehniskās drošības kontroles

## 6.1. Atslēgu pāra ģenerēšana un instalēšana

6.1.1. **Atslēgu pāra ģenerēšana**

6.1.1.1. eParaksts.lv SPS SI atslēgu pāra ģenerēšanu veic apmācīts un uzticams personāls, izmantojot uzticamas sistēmas, kas ģenerētajām atslēgām nodrošina drošību un nepieciešamo kriptogrāfisko spēku. Atslēgu pāra ģenerēšana notiek saskaņā ar dokumentētu SI atslēgas ceremoniju, ko apliecina neatkarīgs auditors.

6.1.1.2. eParaksts.lv SPS SI atslēgas tiks ģenerētas un glabātas aparatūras drošības modulī (HSM), kurš ir sertificēts FIPS 140-2 3.līmenī atslēgu ģenerēšanai un glabāšanai, kas aizsargā atslēgu no ārējas kompromitēšanas. SSI privātā atslēga nekad nedrīkst nokļūt ārpus HSM nolasāmā formā.

6.1.1.3. HSM FIPS atbilstības režīmā ir nepieciešami divi HSM sistēmas karšu komplekti: viens administratīviem, un otrs ekspluatācijas nolūkiem. Šie komplekti nav savstarpēji aizstājami.

6.1.1.4. eParaksts.lv SPS ISI veic parakstītāja atslēgu pāru ģenerēšanu viedkartē (SSCD 3. tips saskaņā ar ISO/IEC 15408 novērtēto EAL4+), garantējot, ka privātā paraksta atslēga vienmēr paliek viedkartē.

6.1.1.5. eParaksts.lv SPS ISI veic HSM parakstītāja atslēgu pāru ģenerēšanu HSM iekārtā (SSCD 3. tips saskaņā ar ISO/IEC 15408 novērtēto EAL4+), garantējot, ka privātā paraksta atslēga vienmēr paliek HSM iekārtā.

6.1.1.6. Infrastruktūras sertifikātu (gan tīmekļa vietnes SSL, gan koda parakstīšanas, gan domēna kontroliera, gan laika zīmogošanas iekārtas

sertifikātu) privātās un publiskās atslēgas ģenerē Pasūtītājs drošā vidē un drošos apstākļos.

6.1.2. **LZI atslēgu ģenerēšana**

6.1.2.1. eParaksts.lv SPS LZI atslēgu pāri tiek ģenerēti LZI HSM ietvaros. To izpilda uzticams personāls ar noteiktām uzticības lomām (skat. eParaksts.lv SPS Izsniegšanas SN). HSM, ko lieto eParaksts.lv SPS LZI, atbilst FIPS PUB 140-2 Level 3 [5].

6.1.2.2. HSM izmanto īstu gadījumskaitļu ģeneratoru (RNG), lai ģenerētu atslēgas. Lai nodrošinātu atbilstošu atslēgu ģenerēšanu HSM ietvaros, modulis veic statistiskos testus.

6.1.2.3. Atslēgu un sertifikātu ģenerēšana tiek veikta drošā fiziskā vidē un vismaz ar duālu kontroli. Tā kā Politikas SI nav saistīta ar datortīklu, datu pārvietošana starp eParaksts.lv SPS LZI un Politikas SI un uz attiecīgajām eParaksts.lv SPS IS datubāzēm tiek izpildīta manuāli. Attiecīgajiem procesiem ir jāatbilst drošības procedūrām un vismaz duālai kontrolei.

6.1.2.4. HSM nodrošina divus karšu komplektus, lai piekļūtu atslēgām: AKK un OKK.

6.1.3. **Publiskās atslēgas piegāde SI**

6.1.3.1. Kad uzticamas SI publisko atslēgu nodod sertificēšanai eParaksts.lv SPS SI, tā tiks piegādāta, izmantojot drošu mehānismu, kas nodrošina, ka publiskā atslēga pārsūtīšanas laikā nav mainīta un uzticamajai SI pieder privātā atslēga, kas atbilst pārsūtītajai publiskajai atslēgai.

6.1.3.2. Privātās atslēgas (t.i. viedkartes) tiek izplatītas RI, izmantojot komerciālus piegādes pakalpojumus un iesaiņojumā, kas ļauj atklāt mēģinājumus to atvērt. Karšu izplatīšanu reģistrē eParaksts.lv SPS ISI. Privātās atslēgas (t.i. viedkartes) RI jāizsniedz parakstītājam tā personīgā klātbūtnē.

6.1.3.3. HSM privātās atslēgas tiek uzglabātas pie eParaksts.lv SPS un tām parakstītājs var piekļūt attālināti veicot drošu autentifikāciju un lietojot sev zināmo PIN.

6.1.3.4. Viedkartes vai HSM iekārtas aizsargā privātās atslēgas pret nepareizu lietošanu un kompromitēšanu, un privātā paraksta atslēga vienmēr paliek viedkartē vai HSM iekārtā. Privātās atslēgas izmantošanai nepieciešama PIN koda ievade, kas parakstītājam ir piegādāts atsevišķi pa pastu aizzīmogotā PIN vēstulē.

6.1.3.5. Infrastruktūras sertifikātiem (gan tīmekļa vietnes SSL, gan koda parakstīšanas, gan domēna kontroliera, laika zīmogošanas iekārtas) sertifikācijas nolūkiem pasūtītāja publiskā atslēga jātransportē uz eParaksts.lv SPS ISI kā PKCS#10 sertifikāta pieprasījums drošā veidā.

6.1.4. **Parakstītāja publiskās atslēgas piegāde sertifikāta izsniedzējam**

6.1.4.1. Publiskās atslēgas karšu ražošanas uzņēmumā tiek ģenerētas viedkartē (sk. 6.1.1.). Sertifikācijas nolūkiem parakstītāja publiskā atslēga jāeksportē no SSCD un jātransportē uz eParaksts.lv SPS ISI kā PKCS#10 sertifikāta pieprasījums, izmantojot tiešsaistes SSL sesiju. PKCS#10 sertifikāta pieprasījuma paraksta apliecinājums sastāda atbilstošās privātās atslēgas piederības pietiekamu pierādījumu.

6.1.4.2. Izmantotais publiskās atslēgas piegādes mehānisms garantē, ka:

6.1.4.2.1. pārraides laikā publiskā atslēga nav mainīta;

6.1.4.2.2. sertifikāta pieteicējam pieder pārraidītajai publiskajai atslēgai atbilstošā privātā atslēga.

6.1.4.3. Tīmekļa vietnes SSL sertifikātiem, koda parakstīšanas sertifikātiem un laika zīmogošanas iekārtas sertifikātiem publiskās atslēgas ir pieejamas Pasūtītāju sertifikātu pielietošanas interneta vietnēs vai publiskos servisos. Domēna kontroliera sertifikātiem publiskās atslēgas ir pieejamas Pasūtītāja iekšējā IT infrastruktūrā.

6.1.5. **Publiskās atslēgas piegāde lietotājiem un pārbaudītājiem**

6.1.5.1. Visas eParaksts.lv SPS ISI publiskās atslēgas ir pieejamas eParaksts.lv SPS direktoriju pakalpojumos. Turklāt pašparakstīta saknes SI sertifikāta jaucējsummas vērtība (sertifikāta nospiedums) sākotnējai pārbaudei ir pieejama, kā aprakstīts 2.1. nodaļā.

6.1.5.2. Parakstītāja publiskā atslēga tiek piegādāta, piegādājot parakstītāja atslēgu pāra glabāšanai izmantoto viedkarti. Sertifikāta ģenerēšanas laikā SI sistēma pārbauda, vai parakstītāja sertifikātu var pārbaudīt, izmantojot eParaksts.lv SPS ISI publisko atslēgu. Ja parakstītājs ir piekritis sava sertifikāta publicēšanai eParaksts.lv SPS sertifikātu repozitorijā, tad sertifikāts ir arī pieejams lejupielādei.

6.1.6. **Atslēgu izmēri**

| **Atslēga** | **Izmērs** |
|---|---|
| Saknes SI | 4096 biti |
| Politikas SI | 2048 biti |
| LZI | 2048 biti |
| Izsniegšanas SI | 2048 biti |
| Parakstītāja paraksta atslēga | 2048 biti |
| Parakstītāja autentifikācijas atslēga | 2048 biti |
| Tīmekļa vietnes SSL atslēga | 2048 biti |
| Koda parakstīšanas atslēga | 2048 biti |
| Domēna kontroliera sertifikāts | 2048 biti |
| Laika zīmogošanas iekārtas sertifikāts | 2048 biti |
| eZīmoga sertifikāts | 2048 biti |
| eZīmoga autentifikācijas sertifikāts | 2048 biti |

6.1.6.1. Izmantotais kriptogrāfiskais algoritms ir RSA 2048 biti / 4096 biti (PKCS#1).

6.1.7. **Publiskās atslēgas parametru ģenerēšana un kvalitātes pārbaude**

6.1.7.1. Nav piemērojams.

6.1.8. Atslēgu lietošanas mērķi

6.1.8.1. Parakstītāja privātā atslēga jālieto saskaņā ar 4.4.5 nodaļu.

6.1.8.2. SI privātā parakstīšanas atslēga tiks izmantota tikai gala lietotāju sertifikātu sertificēšanai un tiešā apturēto un anulēto sertifikātu saraksta parakstīšanai saskaņā ar eParaksts.lv SPS noteikto X.509 v3 atslēgas lietošanas lauku (sk. arī 7.1. nodaļu).

## 6.2. Privāto atslēgu aizsardzība

6.2.1. Kriptogrāfiskā moduļa standarti

6.2.1.1. eParaksts.lv SPS SI lietotais HSM atbilst FIPS 140-2, 3. līmeņa noteiktajām prasībām.

6.2.1.2. Viedkartes, kas tiek izmantotas kā SSCD un informācijas nesējs parakstītāja privāto atslēgu pārnešanai, ir novērtētas saskaņā ar Vienotajiem kritērijiem (ISO/IEC 15408) ar novērtējuma līmeni EAL4+.

6.2.1.3. HSM iekārtas, kas tiek izmantotas kā SSCD un informācijas nesējs parakstītāja privāto atslēgu pārnešanai, ir novērtētas saskaņā ar Vienotajiem kritērijiem (ISO/IEC 15408) ar novērtējuma līmeni EAL4+.

6.2.1.4. eParaksts.lv SPS LZI nodrošina LZM parakstošās kriptogrāfiskās HSM aparatūras drošību visā tās dzīvescikla laikā, radot un ieviešot dokumentētas procedūras, ar kurām tiek veiktas darbības ar šo aparatūru. Konkrēti, eParaksts.lv SPS LZI ir jānodrošina, ka:

6.2.1.4.1. kriptogrāfiskā aparatūra, kas paraksta LZM, netiek bojāta piegādes laikā;

6.2.1.4.2. kriptogrāfiskā aparatūra, kas paraksta LZM, netiek bojāta uzglabāšanas laikā;

6.2.1.4.3. LZIe parakstīšanas atslēgu instalēšana, aktivizēšana un kopijas izgatavošana kriptogrāfiskajā iekārtā HSM jāveic tikai personālam ar uzticības lomām, izmantojot vismaz duālo kontroli fiziski drošā vidē;

6.2.1.4.4. HSM, kas paraksta LZM, funkcionē pareizi;

6.2.1.4.5. LZIe privātās atslēgas, kas tiek glabātas uz LZIe HSM, tiek izdzēstas pēc ierīces lietošanas pārtraukšanas.

6.2.1.5. Katra darbība, kas attiecas uz HSM, ir jādokumentē (piemēram, strādājošā personāla darbību reģistrēšana), un tā var tikt izpildīta tikai saskaņā ar definētu procesu un zem duālās kontroles.

6.2.1.6. Visi notikumi, kas iesaistīti eParaksts.lv SPS LZI atslēgu pāru ģenerācijā, tiks reģistrēti. Tas ietver visus konfigurācijas datus, kas tiek izmantoti procesā, tāpat kā ar HSM dzīvescikla pārvaldību saistītie notikumi (piemēram, saņemšana, izmantošana, demontāža un lietošanas pārtraukšana).

6.2.1.7. HSM un atbilstošo sistēmas karšu dzīvescikla notikumi ir:

6.2.1.7.1. HSM aktivizēšana:

6.2.1.7.2. eParaksts.lv SPS LZI iepriekš sagatavoto sistēmas karšu inicializēšana;

6.2.1.7.3. HSM inicializēšana;

6.2.1.7.4. izmaiņas HSM konfigurācijā;

6.2.1.7.5. iereģistrēšanās un izreģistrēšanās no HSM;

6.2.1.7.6. atslēgu ģenerēšana HSM izmantojot sistēmas kartes;

6.2.1.7.7. atslēgu pārģenerēšana jaunā HSM ar sistēmas kartēm;

6.2.1.7.8. atslēgu izdzēšana no HSM

6.2.2. **Privātās atslēgas vairāku personu kontrole**

6.2.2.1. eParaksts.lv SPS ir ieviesis tehniskus un procedurālus mehānismus, kas prasa vairāku uzticamu personu klātbūtni, lai veiktu jutīgās SI kriptogrāfiskas darbības. Lai iegūtu piekļuvi privātajām atslēgām, ir nepieciešamas 2 personas no 6 personām. Nevienai atsevišķai personai nav visu aktivēšanas datu, kas nepieciešami piekļuvei jebkurai no SI privātajām atslēgām.

6.2.3. **LZI privātās atslēgas aizsardzība**

6.2.3.1. HSM, kas tiek izmantots kā LZIe, ir tīklā ieslēgta ierīce, kas kriptogrāfiski apzīmogo dokumentus, pielietojot elektronisko parakstu un neatkarīgi pievienojot auditējamu laika zīmogu.

6.2.3.2. HSM izmanto iekšēju kriptogrāfisko moduli (iekārtu), kurš iekšēji ģenerē kriptogrāfiskās atslēgas. Kriptogrāfiskā moduļa ģenerētās kriptogrāfiskās atslēgas apstiprinātā algoritma vai drošības funkcijas izmantošanai ir jāreģenerē, izmantojot apstiprinātu atslēgu ģenerēšanas metodi.

6.2.3.3. eParaksts.lv SPS LZI ir ieviesusi tehniskos un procedurālos mehānismus, kas prasa vairāku droša personāla pārstāvju līdzdalību, lai veiktu jutīgas kriptogrāfiskās darbības. Pieeja privātajām atslēgām prasa autentifikāciju ar paroli un sistēmas karti, kas ir specifiska katram HSM (AKK, OKK), pielietojot duālo kontroli.

6.2.3.4. eParaksts.lv SPS LZI privātajai atslēgai tiks veikta rezerves kopēšana un droša uzglabāšana mazvarbūtīgajam gadījumam, ja atslēga tiks zaudēta negaidītas strāvas atslēgšanās vai aparatūras atteikuma dēļ. Atslēgu rezerves kopēšana ir SI atslēgu ģenerēšanas procedūras sastāvdaļa. SI privātās atslēgas rezerves kopija ir slepena, un tiek nodrošināta tās integritāte un autentiskums.

6.2.3.5. Privātās atslēgas var tikt pārģenerētas, izmantojot atslēgu pārģenerēšanas kartes. Atslēgu pārģenerēšanas procedūra ir dokumentēta, un tai ir jānotiek ar duālo kontroli fiziski drošā vietā.

6.2.4. Privātās atslēgas nodošana glabāšanā trešajai pusei

6.2.4.1. SI privāto atslēgu nodošana glabāšanā trešajai pusei nav atļauta.

6.2.5. **Privātās atslēgas rezerves kopijas izveide**

6.2.5.1. Tiks nodrošināta eParaksts.lv SPS SSI privātās atslēgas rezerves kopija, un tā tiks droši uzglabāta mazticamam atslēgas zaudējuma gadījumam negaidīta barošanas pārtraukuma vai aparatūras bojājuma dēļ. Atslēgas rezerves kopijas izveide notiek kā daļa no SI atslēgas ģenerēšanas ceremonijas. Rezerves SI privātajai atslēgai ir jāsaglabā slepenību, un ir jāsaglabā tās integritāte un autentiskums.

6.2.5.2. Privātās atslēgas tiks ģenerētas no jauna, izmantojot atslēgas atkārtotas ģenerēšanas karšu komplektu. Atslēgas atkārtotas ģenerēšanas procedūra ir dokumentēta, un tā ir jāveic ar divkāršu kontroli fiziski drošā vietā.

6.2.5.3. Parakstītāja privātās atslēgas drošiem e-parakstiem tiek ģenerētas un saglabātas uz viedkartes vai HSM iekārtas. Tā kā tās no viedkartes vai HSM iekārtas nevar izdabūt, tām netiek izveidota rezerves kopija.

6.2.6. **Privātās atslēgas arhivēšana**

6.2.6.1. eParaksts.lv SPS SI atslēgu pārim beidzoties to derīguma termiņam, tas saskaņā ar šiem SN tiks droši iznīcināts.

6.2.7. **Privātās atslēgas pārnešana uz kriptogrāfisko moduli**

6.2.7.1. eParaksts.lv SPS ģenerē SI atslēgu pārus HSM moduļos, kuros šīs atslēgas tiks izmantotas.

6.2.8. **Privātās atslēgas glabāšana kriptogrāfiskajā modulī**

6.2.8.1. eParaksts.lv SPS SI privātā atslēga tiek glabāta HSM moduļos šifrētā formā.

6.2.9. **Privātās atslēgas aktivēšanas metode**

6.2.9.1. SI privātā atslēga var tikt aktivēta, ievadot HSM operatoru karšu iepriekš definētu skaitu. SI privātās atslēgas aktivēšanai nepieciešams ievadīt un apstiprināt PIN saskaņā ar norādītajiem drošības parametriem.

6.2.10. **Privātās atslēgas deaktivēšanas metode**

6.2.10.1. Pēc izmantošanas tās jādeaktivē, izņemot no HSM operatoru kartes.

6.2.11. **Privātās atslēgas iznīcināšanas metode**

6.2.11.1. Privātās atslēgas jāiznīcina, ja tās vairs nav nepieciešamas vai tām atbilstošo sertifikātu derīguma termiņš ir beidzies, vai arī tie ir anulēti. Privātās atslēgas ir jāiznīcina tādā veidā, kas novērš to pazušanu, zādzību, modificēšanu, nesankcionētu izpaušanu vai nesankcionētu lietošanu.

6.2.11.2. SI privātā atslēga ir jāuzskata par iznīcinātu, ja visas tās aktivēšanai nepieciešamās operatoru kartes ir iznīcinātas.

## 6.3. Citi atslēgu pāra pārvaldības aspekti

6.3.1. **Publiskās atslēgas arhivēšana**

6.3.1.1. Kā daļa no eParaksts.lv SPS regulārajām rezerves kopiju izveides procedūrām tiek veikta eParaksts.lv SPS SI publisko atslēgu rezerves kopiju izveide un arhivēšana.

6.3.2. **Sertifikāta darbības laiki un atslēgu pāra lietošanas laiki**

6.3.2.1. Sertifikāta darbības laiks beidzas līdz ar tā derīguma termiņu vai anulēšanu. Atslēgas pāru darbības laiks ir tāds pats kā ar tiem saistīto sertifikātu darbības laiks, izņemot to, ka tos drīkst turpināt izmantot paraksta pārbaudei. Maksimālais sertifikātu darbības laiks, kas izsniegti šo SN darbības laikā, tiek noteikts turpmākajā tabulā.

6.3.2.2. Turklāt eParaksts.lv SPS ISI pārtrauc izsniegt jaunus sertifikātus noteiktā datumā pirms SI sertifikāta derīguma termiņa beigām tādā veidā, lai neviena pakārtotas SI izsniegta sertifikāta derīguma termiņš nebeigtos pēc jebkura svarīgāka SI sertifikāta derīguma termiņa beigām.

| Sertifikāts | Derīguma laiks |
|---|---|
| eParaksts.lv Saknes SI sertifikāts (pašparakstīts) | Līdz 18 gadiem |
| eParaksts.lv Politikas SI sertifikāts | Līdz 12 gadiem |
| eParaksts.lv Izsniegšanas SI sertifikāts | Līdz 6 gadiem |
| LZI | Līdz 6 gadiem |
| Gala lietotāja kvalificēts paraksta sertifikāts | Līdz 5 gadiem |
| Gala lietotāja autentifikācijas sertifikāts | Līdz 5 gadiem |
| OCSP SI respondera sertifikāts | Līdz 2 gadiem |
| OCSP Politikas SI respondera sertifikāts | Līdz 6 gadiem |
| OCSP Saknes SI respondera sertifikāts | Līdz 6 gadiem |
| Tīmekļa vietnes SSL atslēga | Līdz 2 gadiem |
| Koda parakstīšanas atslēga | Līdz 2 gadiem |
| Domēna kontroliera sertifikāts | Līdz 2 gadiem |
| WEB portāla sertifikāti | Līdz 2 dienām |
| Laika zīmogošanas iekārtas sertifikāts | Līdz 2 gadiem |
| eZīmoga sertifikāts | Līdz 2 gadiem |
| eZīmoga autentifikācijas sertifikāts | Līdz 2 gadiem |

6.3.2.3. Vadība pastāvīgi pārrauga kriptogrāfisko algoritmu un parametru piemērojamību. Ja algoritms vai atbilstošais atslēgas garums negarantē pietiekamu drošību sertifikāta derīguma laikā, šis sertifikāts tiks anulēts un tiks iniciēts jauna sertifikāta pieteikums.

## 6.4. Aktivēšanas dati

6.4.1. Aktivēšanas datu aizsardzība atbilst FIPS 140-2, 3. līmenim.

6.4.2. **Aktivēšanas datu ģenerēšana un instalēšana**

6.4.2.1. Lai aizsargātu piekļuvi privātai atslēgai, jāizmanto PIN vai paroles frāze. Ja šī informācija jāpārraida parakstītājam, tam jānotiek pa atbilstoši drošu kanālu, kura laiks un vieta atšķiras no saistītā kriptogrāfiskā moduļa (viedkartes) laika un vietas. Ja tas nenotiek manuāli, parakstītājs jāinformē par sūtīšanas datumu, metodi un gaidāmo aktivēšanas datu piegādes datumu. Kā daļa no piegādes metodes parakstītājam jāapstiprina viedkaršu un aktivēšanas datu saņemšana. Turklāt parakstītājiem jāsaņem informācija (un jāapstiprina tās saņemšana) par kriptogrāfiskā moduļa izmantošanu un kontroli.

6.4.3. **Aktivēšanas datu aizsardzība**

6.4.3.1. Aktivēšanas dati jāatceras, nevis jāpieraksta. Ja tos pieraksta, tie jāaizsargā tādā pašā līmenī kā dati, kuru aizsardzībai izmanto saistīto kriptogrāfisko moduli. Aktivēšanas datus nedrīkst koplietot.

6.4.3.2. Parakstītājiem jāaizsargā savu privāto atslēgu aktivēšanas dati, ja tādi ir, tādā mērā, kā tas ir nepieciešams, lai novērstu šo privāto atslēgu zudumu, zādzību, modifikāciju, nesankcionētu izpaušanu vai nesankcionētu izmantošanu.

6.4.4. **Citi aktivēšanas datu aspekti**

6.4.4.1. **Aktivēšanas datu pārraide**

6.4.4.1.1. Tādā apjomā, kādā tiek pārraidīti parakstītāju privāto atslēgu aktivēšanas dati, parakstītājiem jāaizsargā viņu privāto atslēgu aktivēšanas datu pārraidīšana, izmantojot metodes, kas novērš šo privāto atslēgu zudumu, zādzību, modifikāciju, nesankcionētu izpaušanu vai nesankcionētu izmantošanu.

6.4.4.2. Aktivēšanas datu iznīcināšana

6.4.4.2.1. eParaksts.lv SPS ISI privāto atslēgu aktivēšanas dati jāiznīcina, izmantojot metodes, kas novērš šo aktivēšanas datu aizsargāto privāto atslēgu zudumu, zādzību, modifikāciju, nesankcionētu izpaušanu vai nesankcionētu izmantošanu. Pēc ierakstu saglabāšanas laika, kā aprakstīts 5.5.2. nodaļā, beigām apstiprinošajai ir SI jāiznīcina aktivēšanas dati, tos pārrakstot vai fiziski iznīcinot.

## 6.5. Datoru drošības kontroles

6.5.1. eParaksts.lv SPS ir definējusi un dokumentējusi visas datoru tehniskās kontroles, kas ir ieviestas eParaksts.lv SPS SI un sertifikātu pārbaudes pakalpojumiem saskaņā ar ISO 17799:2005 prasībām.

## 6.6. Dzīves cikla tehniskās kontroles

6.6.1. Nav nosacījumu

## 6.7. Tīkla drošības kontroles

6.7.1. Lai nodrošinātu eParaksts.lv SPS SSI un PSI atslēgu pāra atbilstošu drošību, gan SSI un PSI, gan pamatā esošais HSM ir nesaistes režīma komponenti, kuriem var piekļūt tikai pilnvarots personāls, kam ir fiziska piekļuve aparatūras platformai, kas nodrošina Saknes SI un Politikas SI pakalpojumus. Turklāt tiek izmantota vismaz divu personu autentifikācija, lai nodrošinātu atbilstošu piekļuvi eParaksts.lv SPS PSI pakalpojumiem.

6.7.2. Turklāt šie serveri nav pieslēgti tīklam un atrodas nesaistes drošības objektā.

# 7. eParaksts.lv SPS sertifikāta profili

Visi eParaksts.lv SPS izsniegti elektroniskie sertifikāti atbilst RFC 3280 [4] aprakstītajiem elektroniskā sertifikāta un CRL profiliem.

## 7.1. eParaksts.lv Saknes SI sertifikāta profils

| eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Saknes SI Saknes SI pašparakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Versija | | | *V3* |
| Sērijas numurs | | | Automātiski piešķir Saknes SI |
| Paraksta algoritms | | | *sha1RSA* |
| Izsniedzējs | | | *CN=E-ME SSI(RCA)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + 18 gadi |
| Parakstītājs | | | *CN= E-ME SSI(RCA)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Publiskā atslēga | | | RSA (4096 biti) |
| **X.509 V3 paplašinājumi** | | | |
| Parakstītāja atslēgas identifikators | Nē | | Saknes SI publiskās atslēgas *Sha1* izvilkums |
| SI versija | Nē | | *V0.0* |
| Sertifikātu politikas | Nē | Politikas identifikators | *1.3.6.1.4.1.32061.1.1.1* |
| | | | |
| | | SN | *http://www.eme.lv/repository* |
| Atslēgas lietošana | Jā | | Sertifikātu parakstīšana, Nesaistes *CRL* parakstīšana, *CRL* parakstīšana |
| Pamata ierobežojumi | Jā | | *Signatory Type=CA*<br>*Path Length Constraint=None* |
| **Īpašības** | | | |
| Izvilkuma algoritms | | | *Sha1* |
| Izvilkums | | | Saknes SI sertifikāta izvilkums |

## 7.2. eParaksts.lv SPS Politikas SI sertifikāta profils

| Sertifikācijas pakalpojumu sniedzēja eParaksts.lv Politikas SI Saknes SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Versija | | | *V3* |
| Sērijas numurs | | | Automātiski piešķir Saknes SI |
| Paraksta algoritms | | | *sha1RSA* |
| Izsniedzējs | | | *CN= E-ME SSI(RCA)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + 12 gadi |
| Parakstītājs | | | *CN= E-ME PSI(PCA)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 paplašinājumi** | | | |
| Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | Politikas SI publiskās atslēgas *sha1* izvilkums |
| | | | |
| SI versija | Nē | | *Versijas numurs* |
| Sertifikātu politikas | Nē | Politikas identifikators | *1.3.6.1.4.1.32061.1.1.1* |
| | | | |

| Sertifikācijas pakalpojumu sniedzēja eParaksts.lv Politikas SI Saknes SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| | | SN | *http://www.eme.lv/repository* |
| Sertifikātu šablona nosaukums | Nē | | *SubCA* |
| Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Saknes SI publiskās atslēgas *sha1* izvilkums |
| *CRL* izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *http://www.eme.lv/cdp/E-ME%20SSI%20(RCA).crl*<br><br>*ldap://eme.lv/cn=E-ME%20SSI%20(RCA),OU=Sertifikacijas%20pakalpojumu%20dala,O=E-ME,C=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/CN=E-ME%20SSI%20(RCA),OU=sertifikacijas%20pakalpojumu%20dala,O=E-ME,C=lv?cacertifcate?base?objectclass=certificationauthority* |
| | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *http://ocsp.eme.lv/responder.eme* |
| | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *http://www.eme.lv/aia/E-ME%20SSI%20(RCA).crt* |
| Pamata ierobežojumi | Jā | | *Signatory Type=CA*<br>*Path Length Constraint=None* |
| Atslēgas lietošana | Jā | | *Certificate Signing, Off-line CRL Signing, CRL Signing (06)* |
| **Īpašības** | | | |
| Izvilkuma algoritms | | | *sha1* |
| Izvilkums | | | Politikas SI sertifikāta izvilkums |

## 7.3. eParaksts.lv SPS OCSP RCA respondera sertifikāta profils

| eParaksts.lv Sertifikācijas pakalpojumu sniedzēja *OCSP* responderis Saknes SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Versija | | | *V3* |
| Sērijas numurs | | | Automātiski piešķir Saknes SI |
| Paraksta algoritms | | | *sha1RSA* |
| Izsniedzējs | | | *CN= E-ME SSI(RCA)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + 6 gadi |
| Parakstītājs | | | *CN = E-ME SI (OCSP RCA)* |
| Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 paplašinājumi** | | | |
| Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | *OCSP* respondera publiskās atslēgas *Sha1* izvilkums |
| Uzlabotā atslēgas lietošana | Nē | | *OCSP Signing (1.3.6.1.5.5.7.3.9)* |
| Atslēgas lietošana | Nē | | *Digital Signature Non-repudiation (c0)* |

| **eParaksts.lv Sertifikācijas pakalpojumu sniedzēja *OCSP* responderis Saknes SI parakstīts** | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Saknes SI publiskās atslēgas *Sha1* izvilkums |
| *CRL* izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *ldap://eme.lv/cn=E-ME%20SSI%20(RCA),OU=Sertifikacijas%20pakalpojumu%20dala,O=E-ME,C=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/CN=E-ME%20SSI%20(RCA),OU=sertifikacijas%20pakalpojumu%20dala,O=E-ME,C=lv?cacertificate?base?objectclass=certificationauthority* |
| | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *http://ocsp.eme.lv/responder.eme* |
| | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *http://www.eme.lv/aia/E-ME%20SSI%20(RCA).crt* |
| **Īpašības** | | | |
| Izvilkuma algoritms | | | *sha1* |
| Izvilkums | | | *OCSP* sertifikāta izvilkums |

## 7.4. eParaksts.lv SPS Izsniegšanas SI sertifikāta profils

| **Sertifikācijas pakalpojumu sniedzēja eParaksts.lv Izsniegšanas SI Politikas SI parakstīts** | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Versija | | | *V3* |
| Sērijas numurs | | | Automātiski piešķir Politikas SI |
| Paraksta algoritms | | | *sha1RSA* |
| Izsniedzējs | | | *CN = E-ME PSI(PCA)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + 6 gadi |
| Parakstītājs | | | *CN = E-ME SI(CA1)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV*<br><br>*----------Vai----------*<br><br>*CN = eParaksts CA*<br>*O = VAS Latvijas valsts radio un televīzijas centrs*<br>*C = LV* |
| Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 paplašinājumi** | | | |
| Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | Izsniegšanas SI 1 publiskās atslēgas *sha1* izvilkums |
| | | | |
| SI versija | Nē | | *Versijas numurs* |
| Sertifikātu politikas | Nē | Politikas identifikators | *1.3.6.1.4.1.32061.1.1.1* |

| Sertifikācijas pakalpojumu sniedzēja eParaksts.lv Izsniegšanas SI Politikas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| | | | |
| | | SN | *http://www.eme.lv/repository* |
| Sertifikātu šablona nosaukums | Nē | | *SubCA* |
| Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Saknes SI publiskās atslēgas *sha1* izvilkums |
| *CRL* izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *http://www.eme.lv/cdp/E-ME%20PSI%20(PCA).crl*<br><br>*ldap://eme.lv/cn=E-ME%20PSI%20(PCA),OU=Sertifikacijas%20pakalpojumu%20dala,O=E-ME,C=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/cn=E-ME%20PSI%20(PCA),OU=Sertifikacijas%20pakalpojumu%20dala,O=E-ME,C=lv?cacertificate?base?objectclass=certificationauthority* |
| | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *http://ocsp.eme.lv/responder.eme* |
| | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *http://www.eme.lv/aia/E-ME%20PSI%20(PCA).crt* |
| Pamata ierobežojumi | Jā | | *Signatory Type=CA*<br>*Path Length Constraint=None* |
| Atslēgas lietošana | Jā | | *Certificate Signing, Off-line CRL Signing, CRL Signing (06)* |
| **Īpašības** | | | |
| Izvilkuma algoritms | | | *sha1* |
| Izvilkums | | | Izsniegšanas SI 1 sertifikāta izvilkums |

## 7.5. eParaksts.lv SPS OCSP PCA respondera sertifikāta profils

| eParaksts.lv Sertifikācijas pakalpojumu sniedzēja *OCSP* responderis Saknes SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Satur** |
| Versija | | | *V3* |
| Sērijas numurs | | | Automātiski piešķir Saknes SI |
| Paraksta algoritms | | | *sha1RSA* |
| Izsniedzējs | | | *CN = E-ME PSI (PCA)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + 6 gadi |
| Parakstītājs | | | *CN = E-ME SI (OCSP PCA)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 paplašinājumi** | | | |
| Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | *OCSP* respondera publiskās atslēgas *Sha1* izvilkums |

| **eParaksts.lv Sertifikācijas pakalpojumu sniedzēja *OCSP* responderis Saknes SI parakstīts** | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Satur** |
| Uzlabotā atslēgas lietošana | Nē | | *OCSP Signing (1.3.6.1.5.5.7.3.9)* |
| Atslēgas lietošana | Nē | | *Digital Signature, Non-Repudiation (c0)* |
| Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Politikas SI publiskās atslēgas *Sha1* izvilkums |
| *CRL* izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *http://www.eme.lv/cdp/E-ME%20PSI%20(PCA).crl*<br><br>*ldap://eme.lv/cn=E-ME%20PSI%20(PCA),OU=Sertifikacijas%20pakalpojumu%20dala,O=E-ME,C=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas isniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/cn=E-ME%20PSI%20(PCA),OU=Sertifikacijas%20pakalpojumu%20dala,O=E-ME,C=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *http://ocsp.eme.lv/responder.eme* |
| | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *http://www.eme.lv/aia/E-ME%20PSI%20(PCA).crt* |
| **Īpašības** | | | |
| Izvilkuma algoritms | | | *sha1* |
| Izvilkums | | | *OCSP* sertifikāta izvilkums |

## 7.6. eParaksts.lv SPS Laika zīmogošanas institūcijas sertifikāta profils

| **Sertifikācijas pakalpojumu sniedzēja eParaksts.lv Laika zīmogošanas institūcija Politikas SI parakstīts** | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Versija | | | *V3* |
| Sērijas numurs | | | Automātiski piešķīra Politikas SI |
| Paraksta algoritms | | | sha1RSA |
| Izsniedzējs | | | *CN = E-ME PSI(PCA)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + 6 gadi |
| Parakstītājs | | | *CN = eParaksts LZI1 (TSA1)*<br>*OU = nCipher DSE ESN:E59C-7140-BF94*<br>*OU = ISD*<br>*O = LVRTC*<br>*L = Riga*<br>*C = LV*<br><br>vai<br><br>*CN = EME LZI2 (TSA2)*<br>*OU = nCipher DSE ESN:E1A7-712B-15D9*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*O = EME*<br>*C = LV* |

| | | | |
|---|---|---|---|
| Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 paplašinājumi** | | | |
| Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | Politikas SI publiskās atslēgas *sha1* izvilkums |
| Institūcijas atslēgas identifikators | Nē | Atslēga s identifikators | LZI1 publiskās atslēgas *sha1* izvilkums |
| *CRL* izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *http://www.eme.lv/cdp/E-ME%20PSI%20(PCA).crl*<br><br>*ldap://eme.lv/cn=E-ME%20PSI%20(PCA),OU=Sertifikacijas%20pakalpojumu%20dala,O=E-ME,c=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/CN=E-ME%20PSI%20(PCA),OU=sertifikacijas%20pakalpojumu%20dala,O=E-ME,C=lv?cacertificate?base?objectclass=certificationauthority* |
| | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *http://ocsp.eme.lv/responder.eme* |
| | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *http://www.eme.lv/aia/E-ME%20PSI%20(PCA).crt* |
| Paplašinātā atslēgas lietošana | Nē | | *Time Stamping (1.3.6.1.5.5.7.3.8)* |
| Sertifikātu politikas | Nē | Politikas identifikators | *1.3.6.1.4.1.32061.1.1.1* |
| | | SN | *http://www.eme.lv/repository* |
| Atslēgas lietošana | Jā | | *Digital Signature, Non-Repudiation (c0)* |
| **Īpašības** | | | |
| Izvilkuma algoritms | | | *sha1* |
| Izvilkums | | | LZI1 sertifikāta izvilkums |

## 7.7. eParaksts.lv SPS OCSP CA respondera sertifikāta profils

| **eParaksts.lv Sertifikācijas pakalpojumu sniedzēja *OCSP* responderis Saknes SI parakstīts** | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritis** | **Atribūts** | **Saturs** |
| Versija | | | *V3* |
| Sērijas numurs | | | Automātiski piešķir Saknes SI |
| Paraksta algoritms | | | *sha1RSA* |
| Izsniedzējs | | | *CN = E-ME SI (CA1)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + 14 dienas |
| Parakstītājs | | | *CN = E-ME SI (CA1)(OCSP)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 paplašinājumi** | | | |

| **eParaksts.lv Sertifikācijas pakalpojumu sniedzēja *OCSP* responderis Saknes SI parakstīts** | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritis** | **Atribūts** | **Saturs** |
| Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | *OCSP* respondera publiskās atslēgas *Sha1* izvilkums |
| OCSP No Revocation Checking (1.3.6.1.5.5.7.48.1.5) | Nē | | *NULL* |
| Uzlabotā atslēgas lietošana | Nē | | *OCSP Signing (1.3.6.1.5.5.7.3.9)* |
| Atslēgas lietošana | Nē | | *Digital Signature, Non-Repudiation (c0)* |
| Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Izsniegšanas SI publiskās atslēgas *Sha1* izvilkums |
| *CRL* izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *http://www.eme.lv/cdp/E-ME%20SI%20(CA1).crl*<br><br>*ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| Pieeja institūcijas informācija | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/cn=E-ME%20SI%20(CA1)(4),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?cacertificate?base?objectclass=certificationauthority* |
| | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *https://ocsp.eme.lv/responder.eme* |
| | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *http://www.eme.lv/aia/E-ME%20SI%20(CA1).crt* |
| **Īpašības** | | | |
| Izvilkuma algoritms | | | *sha1* |
| Izvilkums | | | *OCSP* sertifikāta izvilkums |

## 7.8. eParaksts.lv Izsniegšanas SI izsniegta kvalificētā paraksta sertifikāta profils

| **eParaksts.lv kvalificētā paraksta sertifikāts Izsniegšanas SI parakstīts** | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Versija | | | *V3* |
| Sērijas numurs | | | Automātiski piešķir Izsniegšanas SI |
| Paraksta algoritms | | | *sha1RSA* |
| Izsniedzējs | | | *CN = E-ME SI(CA1)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + līdz 5 gadi |
| Parakstītājs | fCR | Sērijas numurs | Unikāls ID numurs (personas kods) |
| | | *G* | Vārds (kā rakstīts identifikācijas dokumentā)<br>Netiek lietots pseidonīma gadījumā |

| **eParaksts.lv kvalificētā paraksta sertifikāts Izsniegšanas SI parakstīts** | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| | | *SN* | Uzvārds (kā rakstīts identifikācijas dokumentā)<br>Netiek lietots pseidonīma gadījumā |
| | | *CN* | Sugas vārds: vārds un uzvārds<br>Alternatīva: PN: pseidonīms, lieto tikai paraksta sertifikātā |
| | | *O* | Izvēles: Parakstītāja organizācija |
| | | *OU* | Izvēles: Parakstītāja struktūrvienība |
| | | *C* | Parakstītāja valsts (*ISO* 3166 kods) |
| Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 paplašinājumi** | | | |
| Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | Parakstītāja publiskās atslēgas *sha1* izvilkums |
| Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Izsniegšanas SI publiskās atslēgas *sha1* izvilkums |
| *CRL* izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *http://www.eme.lv/cdp/E-ME%20SI%20(CA1).crl*<br><br>*ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?cacertificate?base?objectclass=certificationauthority* |
| | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *https://ocsp.eme.lv/responder.eme* |
| | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *http://www.eme.lv/aia/E-ME%20SI%20(CA1).crt* |
| Uzlabotā atslēgas lietošana | Nē | | *Document Signing (1.3.6.1.4.1.311.10.3.12)*<br>*Secure Email (1.3.6.1.5.5.7.3.4)* |
| Sertifikātu politikas | Nē | Politikas identifikators | *1.3.6.1.4.1.32061.1.1.1* |
| | | Lietotāja norāde | *Sis ir sertifikats, ko izdevis VAS Latvijas Valsts radio un televizijas centrs (reg.Nr.40003011203), nodrosinot atbilstibu Elektronisko dokumentu likumam un Eiropas Parlamenta direktivai 1999/93/EK* |
| | | SN | *http://www.eme.lv/repository* |
| Pielietojumu politikas | Nē | Pielietojumu sertifikātu politika | *Policy Identifier=Document Signing*<br>*Policy Identifier=Secure Email* |
| Kvalificēta sertifikāta paziņojums | Nē | Paziņojuma ID | Id-etsi-pcs-QcCompliance (0.4.0.1862.1.1) |
| Atslēgas lietošana | Jā | | *Digital Signature, Non-Repudiation (c0)* |
| Parakstītāja alternatīvais vārds | Jā | RFC822 vārds | Parakstītāja e-pasts |

| eParaksts.lv kvalificētā paraksta sertifikāts Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Pamata ierobežojumi | Jā | | *Signatory Type=End Entity*<br>*Path Length Constraint=None* |
| **Īpašības** | | | |
| Izvilkuma algoritms | | | *Sha1* |
| Izvilkums | | | Parakstītāja sertifikāta izvilkums |

## 7.9. Izsniegšanas SI izsniegta parakstītāja autentifikācijas sertifikāta profils

| eParaksts.lv autentifikācijas sertifikāts Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Versija | | | *V3* |
| Sērijas numurs | | | Automātiski piešķir Izsniegšanas SI |
| Paraksta algoritms | | | *sha1RSA* |
| Izsniedzējs | | | *CN = E-ME SI(CA1)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + līdz 5 gadi |
| Parakstītājs | | | SERIALNUMBER = Personas kods<br>G = Vārds<br>SN = Uzvārds<br>CN = Vārds Uzvārds<br>O = Izvēles: Parakstītāja organizācija<br>OU = Izvēles: Parakstītāja struktūrvienība<br>C = Parakstītāja valsts (*ISO* 3166 kods) |
| Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 paplašinājumi** | | | |
| Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | Parakstītāja publiskās atslēgas *sha1* izvilkums |
| Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Izsniegšanas SI publiskās atslēgas *sha1* izvilkums |
| *CRL* izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *http://www.eme.lv/cdp/E-ME%20SI%20(CA1).crl*<br><br>*ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?cacertificate?base?objectclass=certificationauthority* |
| | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *https://ocsp.eme.lv/responder.eme* |
| | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *http://www.eme.lv/aia/E-ME%20SI%20(CA1).crt* |

| eParaksts.lv autentifikācijas sertifikāts Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Uzlabotā atslēgas lietošana | Nē | | *Client Authentication (1.3.6.1.5.5.7.3.2)* |
| Sertifikātu politikas | Nē | Politikas identifikators | *1.3.6.1.4.1.32061.1.1.1* |
| | | Lietotāja norāde | *Sis ir sertifikats, ko izdevis Sertifikacijas pakalpojumu sniedzejs E-ME* |
| | | SN | *http://www.eme.lv/repository* |
| Pielietojumu politikas | Nē | Pielietojumu sertifikātu politika | *Policy Identifier=Client Authentication* |
| Atslēgas lietošana | Jā | | *Digital Signature (80)* |
| Signatory Alternative Name | Jā | RFC822 vārds | Parakstītāja e-pasts |
| Pamata ierobežojumi | Jā | | *Signatory Type=End Entity*<br>*Path Length Constraint=None* |
| **Īpašības** | | | |
| Izvilkuma algoritms | | | *sha1* |
| Izvilkums | | | Parakstītāja sertifikāta izvilkums |

## 7.10. Izsniegšanas SI izsniegta parakstītāja autentifikācijas sertifikāta ar viedkartes pieslēgšanās funkciju profils

| eParaksts.lv autentifikācijas sertifikāts ar viedkartes pieslēgšanos Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Versija | | | *V3* |
| Sērijas numurs | | | Automātiski piešķir Izsniegšanas SI |
| Paraksta algoritms | | | *sha1RSA* |
| Izsniedzējs | | | *CN = E-ME SI(CA1)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + līdz 5 gadi |
| Parakstītājs | | | Sērijas numurs = Personas kods<br>G = Vārds<br>SN = Uzvārds<br>CN = Vārds Uzvārds<br>O = Izvēles: Parakstītāja organizācijas<br>C = Parakstītāja valsts (*ISO* 3166 kods) |
| Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 paplašinājumi** | | | |
| Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | Parakstītāja publiskās atslēgas *sha1* izvilkums |
| Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Izsniegšanas SI publiskās atslēgas *sha1* izvilkums |
| *CRL* izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *http://www.eme.lv/cdp/E-ME%20SI%20(CA1).crl*<br><br>*ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs | *ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-* |

| eParaksts.lv autentifikācijas sertifikāts ar viedkartes pieslēgšanos Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| | | (1.3.6.1.5.5.7.48.2) | *ME,c=lv?cacertificate?base?objectclass=certificationauthority* |
| | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *https://ocsp.e-me.lv/responder.eme* |
| | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *URL=http://www.eme.lv/aia/E-ME%20SI%20(CA1).crt* |
| Uzlabotā atslēgas lietošana | Nē | | *Smart Card Logon (1.3.6.1.4.1.311.20.2.2)*<br>*Client Authentication (1.3.6.1.5.5.7.3.2)* |
| Sertifikātu politikas | Nē | Politikas identifikators | *1.3.6.1.4.1.32061.1.1.2* |
| | | Lietotāja norāde | *Sis ir sertifikats, ko izdevis Sertifikacijas pakalpojumu sniedzejs E-ME* |
| | | SN | *https://www.eparaksts.lv/lv/repozitarijs* |
| Pielietojumu politikas | Nē | Pielietojumu sertifikātu politika | *Policy Identifier=Client Authentication*<br>*Policy Identifier=Smart Card Logon* |
| Atslēgas lietošana | Jā | | *Digital Signature (80), Key Encipherment (a0)* |
| Signatory Alternative Name | Jā | RFC822 vārds un User Principa vārds | Parakstītāja e-pasts un lietotāja vārds domēnā |
| Pamata ierobežojumi | Jā | | *Signatory Type=End Entity*<br>*Path Length Constraint=None* |
| **Īpašības** | | | |
| Izvilkuma algoritms | | | *sha1* |
| Izvilkum | | | Parakstītāja sertifikāta izvilkums |

## 7.11. eParaksts.lv izsniegšanas SI izsniegta eID kvalificētā paraksta sertifikāta profils

| eParaksts.lv Izsniegšanas SI izsniegta eID kvalificētā PARAKSTA sertifikāts | | | | |
|---|---|---|---|---|
| **Standarts X.509 V1 angliski** | **Standarts X.509 V1 latviski** | **Kritisks** | **Atribūts** | **Saturs** |
| Version | Versija | | | V3 |
| Serial number | Sērijas numurs | | | Automātiski piešķir Izsniegšanas SI |
| Signature algorithm | Paraksta algoritms | | | sha1RSA |
| Issuer | Izsniedzējs | | | CN = E-ME SI(CA1)<br>OU = Sertifikacijas pakalpojumu dala<br>C = LV |
| Valid from | Derīgs no | | | Izsniegšanas datums |
| Valid to | Derīgs līdz | | | līdz 5 gadiem kopš izsniegšanas datuma |
| Subject | Parakstītājs | | Sērijas numurs | Unikāls ID numurs (personas kods) |
| | | | G | Vārds (kā rakstīts identifikācijas dokumentā) |

| eParaksts.lv Izsniegšanas SI izsniegta eID kvalificētā PARAKSTA sertifikāts | | | | |
|---|---|---|---|---|
| **Standarts X.509 V1 angliski** | **Standarts X.509 V1 latviski** | **Kritisks** | **Atribūts** | **Saturs** |
| | | | SN | Uzvārds (kā rakstīts identifikācijas dokumentā) |
| | | | CN | Sugas vārds: vārds un uzvārds |
| | | | C | Parakstītāja valsts (ISO 3166 kods) |
| Public key | Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 Extensions** | **X.509 V3 paplašinājumi** | | | |
| Subject Key Identifier | Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | Parakstītāja publiskās atslēgas sha1 izvilkums |
| Authority Key Identifier | Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Izsniegšanas SI publiskās atslēgas sha1 izvilkums |
| CRL Distribution Points | CRL izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *http://www.eme.lv/cdp/E-ME%20SI%20(CA1).crl*<br><br>*ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| Authority Information Access | Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?cacertificate?base?objectclass=certificationauthority* |
| | | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *https://ocsp.eme.lv/responder.eme* |
| | | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *http://www.eme.lv/aia/E-ME%20SI%20(CA1).crt* |
| Enhanced Key Usage | Uzlabotā atslēgas lietošana | Nē | | Document Signing (1.3.6.1.4.1.311.10.3.12)<br>Secure Email (1.3.6.1.5.5.7.3.4) |
| Certificate Policies | Sertifikātu politikas | Nē | Politikas identifikators | 1.3.6.1.4.1.32061.1.1.1 |
| | | | Lietotāja norāde | Šis sertifikāts ir iekļauts Latvijas Republikas izsniegtā personu apliecinošā dokumentā. Sertifikātu izdevis VAS Latvijas Valsts radio un televīzijas centrs (reģ.Nr.40003011203), nodrošinot atbilstību Elektronisko dokumentu likumam un Eiropas Parlamenta direktīvai 1999/93/EK. |

| eParaksts.lv Izsniegšanas SI izsniegta eID kvalificētā PARAKSTA sertifikāts | | | | |
|---|---|---|---|---|
| **Standarts X.509 V1 angliski** | **Standarts X.509 V1 latviski** | **Kritisks** | **Atribūts** | **Saturs** |
| | | | SN | *http://www.eme.lv/repository* |
| Application Policies | Pielietojumu politikas | Nē | Pielietojumu sertifikātu politika | Policy Identifier=Document Signing<br>Policy Identifier=Secure Email |
| Qualified Certificate Statement | Kvalificēta sertifikāta paziņojums | Nē | Paziņojuma ID | Id-etsi-pcs-QcCompliance (0.4.0.1862.1.1) |
| Key Usage | Atslēgas lietošana | Jā | | Digital Signature, Non-Repudiation (c0) |
| Basic Constraints | Pamata ierobežojumi | Jā | | Signatory Type=End Entity<br>Path Length Constraint=None |
| **Properties** | **Īpašības** | | | |
| Thumbprint algorithm | Izvilkuma algoritms | | | Sha1 |
| Thumbprint | Izvilkums | | | Parakstītāja sertifikāta izvilkums |

## 7.12. eParaksts.lv izsniegšanas SI izsniegta eID kvalificētā autentifikācijas sertifikāta profils

| eParaksts.lv Izsniegšanas SI izsniegta eID kvalificēts AUTENTIFIKĀCIJAS sertifikāts | | | | |
|---|---|---|---|---|
| **Standarts X.509 V1 angliski** | **Standarts X.509 V1 latviski** | **Kritisks** | **Atribūts** | **Saturs** |
| Version | Versija | | | V3 |
| Serial number | Sērijas numurs | | | Automātiski piešķir Izsniegšanas SI |
| Signature algorithm | Paraksta algoritms | | | sha1RSA |
| Issuer | Izsniedzējs | | | CN = E-ME SI(CA1)<br>OU = Sertifikcijas pakalpojumu dala<br>C = LV |
| Valid from | Derīgs no | | | Izsniegšanas datums |
| Valid to | Derīgs līdz | | | līdz 5 gadiem kopš izsniegšanas datuma |
| Subject | Parakstītājs | | | Sērijas numurs = Personas kods<br>G = Vārds<br>SN = Uzvārds<br>CN = Vārds Uzvārds<br>C = Parakstītāja valsts (ISO 3166 kods) |
| Public key | Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 Extensions** | **X.509 V3 paplašinājumi** | | | |
| Signatory Key Identifier | Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | Parakstītāja publiskās atslēgas sha1 izvilkums |
| Authority Key Identifier | Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Izsniegšanas SI publiskās atslēgas sha1 izvilkums |
| CRL Distribution Points | CRL izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *http://www.eme.lv/cdp/E-ME%20SI%20(CA1).crl*<br><br>*ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikcijas%20pakalpojumu%20dala,o=E-ME,c=lv?certificaterevocationlist?ba* |

| eParaksts.lv Izsniegšanas SI izsniegta eID kvalificēts AUTENTIFIKĀCIJAS sertifikāts | | | | |
|---|---|---|---|---|
| **Standarts X.509 V1 angliski** | **Standarts X.509 V1 latviski** | **Kritisks** | **Atribūts** | **Saturs** |
| | | | | *se?objectclass=certificationauthority* |
| Authority Information Access | Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?cacertificate?base?objectclass=certificationauthority* |
| | | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *https://ocsp.eme.lv/responder.eme* |
| | | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *URL=http://www.eme.lv/aia/E-ME%20SI%20(CA1).crt* |
| Enhanced Key Usage | Uzlabotā atslēgas lietošana | Nē | | Client Authentication (1.3.6.1.5.5.7.3.2) |
| Certificate Policies | Sertifikātu politikas | Nē | Politikas identifikators | 1.3.6.1.4.1.32061.1.1.1 |
| | | | Lietotāja norāde | Šis sertifikāts ir iekļauts Latvijas Republikas izsniegtā personu apliecinošā dokumentā. |
| | | | SN | *http://www.eme.lv/repository* |
| Application Policies | Pielietjumu politikas | Nē | Pielietojumu sertifikātu politika | Policy Identifier=Client Authentication |
| Key Usage | Atslēgas lietošana | Jā | | Digital Signature (80) |
| Basic Constraints | Pamata ierobežojumi | Jā | | Signatory Type=End Entity<br>Path Length Constraint=None |
| **Properties** | **Īpašības** | | | |
| Thumbprint algorithm | Izvilkuma algoritms | | | sha1 |
| Thumbprint | Izvilkums | | | Parakstītāja sertifikāta izvilkums |

## 7.13. eParaksts.lv Izsniegšanas SI izsniegta šifrēšanas sertifikāta profils

| E-ME Izsniegšanas SI izsniegts ŠIFRĒŠANAS sertifikāts | | | | |
|---|---|---|---|---|
| **Standarts X.509 V1 angliski** | **Standarts X.509 V1 latviski** | **Kritisks** | **Atribūts** | **Saturs** |
| Version | Versija | | | V3 |
| Serial number | Sērijas numurs | | | Automātiski piešķir Izsniegšanas SI |
| Signature algorithm | Paraksta algoritms | | | sha1RSA |
| Issuer | Izsniedzējs | | | CN = E-ME SI(CA1) |

| E-ME Izsniegšanas SI izsniegts ŠIFRĒŠANAS sertifikāts | | | | |
|---|---|---|---|---|
| **Standarts X.509 V1 angliski** | **Standarts X.509 V1 latviski** | **Kritisks** | **Atribūts** | **Saturs** |
| | | | | OU = Sertifikacijas pakalpojumu dala<br>C = LV |
| Valid from | Derīgs no | | | Izsniegšanas datums |
| Valid to | Derīgs līdz | | | līdz 5 gadiem kopš izsniegšanas datuma |
| Signatory | Parakstītājs | | | Sērijas numurs = Personas kods<br>G = Vārds<br>SN = Uzvārds<br>CN = Vārds Uzvārds<br>O = Izvēles: Parakstītāja organizācija<br>OU = Izvēles: Parakstītāja struktūrvienība<br>C = Parakstītāja valsts (ISO 3166 kods) |
| Public key | Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 Extensions** | **X.509 V3 paplašinājumi** | | | |
| Signatory Key Identifier | Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | Parakstītāja publiskās atslēgas sha1 izvilkums |
| Authority Key Identifier | Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Izsniegšanas SI publiskās atslēgas sha1 izvilkums |
| CRL Distribution Points | CRL izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *http://www.eme.lv/cdp/E-ME%20SI%20(CA1).crl*<br><br>*ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikcijas%20pakalpojumu%20dala,o=E-ME,c=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| Authority Information Access | Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?cacertificate?base?objectclass=certificationauthority* |
| | | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *https://ocsp.eme.lv/responder.eme* |
| | | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *http://www.eme.lv/aia/E-ME%20SI%20(CA1).crt* |
| Enhanced Key Usage | Uzlabotā atslēgas lietošana | Nē | | Secure Email (1.3.6.1.5.5.7.3.4)<br>Encrypting File System (1.3.6.1.4.1.311.10.3.4) |
| Certificate Policies | Sertifikātu politikas | Nē | Politikas identifikators | 1.3.6.1.4.1. 32061.1.1.2 |
| | | | Lietotāja norāde | |

| E-ME Izsniegšanas SI izsniegts ŠIFRĒŠANAS sertifikāts | | | | |
|---|---|---|---|---|
| **Standarts X.509 V1 angliski** | **Standarts X.509 V1 latviski** | **Kritisks** | **Atribūts** | **Saturs** |
| | | | SN | *http://www.eme.lv/repository* |
| Application Policies | Pielietjumu politikas | Nē | Pielietojumu sertifikātu politika | [1]Application Certificate Policy: Policy Identifier=Secure Email |
| | | | | [2]Application Certificate Policy: Policy Identifier=Encrypting File System |
| Key Usage | Atslēgas lietošana | Jā | | Key Encipherment (20) |
| Basic Constraints | Pamata ierobežojumi | Jā | | Signatory Type=End Entity<br>Path Length Constraint=None |
| **Properties** | **Īpašības** | | | |
| Thumbprint algorithm | Izvilkuma algoritms | | | sha1 |
| Thumbprint | Izvilkums | | | Parakstītāja sertifikāta izvilkums |

## 7.14. Izsniegšanas SI izsniegta tīmekļa vietnes SSL sertifikāta profils

| eParaksts.lv SSL sertifikāts Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Versija | | | *V2* |
| Sērijas numurs | | | Automātiski piešķir Izsniegšanas SI |
| Paraksta algoritms | | | *sha1RSA* |
| Izsniedzējs | | | *CN = E-ME SI(CA1)*<br>*OU = Sertifikacijas pakalpojumi dala*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + 1 gads vai 2 gadi |
| Parakstītājs | | *CN* | Sugas vārds: tīmekļa vietnes web adrese |
| | | *O* | Parakstītāja organizācija |
| | | *OU* | Parakstītāja struktūrvienība |
| | | *L* | Izvēles: Parakstītāja adrese |
| | | *S* | Izvēles: Parakstītāja pilsēta |
| | | *E* | Parakstītāja e-pasts |
| | | *C* | Parakstītāja valsts (*ISO* 3166 kods) |
| Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 paplašinājumi** | | | |
| Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | Parakstītāja publiskās atslēgas *sha1* izvilkums |
| Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Izsniegšanas SI publiskās atslēgas *sha1* izvilkums |
| *CRL* izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?cacertificate?base?objectclass=certificationauthority* |
| | | Tiešsaistes sertifikātu statusa | *https://ocsp.eme.lv/responder.eme* |

| eParaksts.lv SSL sertifikāts Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| | | protokols (1.3.6.1.5.5.7.48.1) | |
| | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *http://www.eme.lv/aia/E-ME%20SI%20(CA1).crt* |
| Uzlabotā atslēgas lietošana | Nē | | Server Authentication (1.3.6.1.5.5.7.3.1) |
| Sertifikātu politikas | Nē | Politikas identifikators | 1.3.6.1.4.1.32061.1.1.1 |
| | | SN | *http://www.eme.lv/repository* |
| Pielietojumu politikas | Nē | Pielietojumu sertifikātu politika | *Policy Identifier= Server Authentication* |
| Atslēgas lietošana | Jā | | *Digital Signature, Key Encipherment (a0)* |
| Pamata ierobežojumi | Jā | | *Signatory Type=End Entity*<br>*Path Length Constraint=None* |
| **Īpašības** | | | |
| Izvilkuma algoritms | | | *Sha1* |
| Izvilkums | | | Parakstītāja sertifikāta izvilkums |

## 7.15. Izsniegšanas SI izsniegta koda parakstīšanas sertifikāta profils

| eParaksts.lv koda parakstīšanas sertifikāts Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Versija | | | *V3* |
| Sērijas numurs | | | Automātiski piešķir Izsniegšanas SI |
| Paraksta algoritms | | | *sha1RSA* |
| Izsniedzējs | | | *CN = E-ME SI(CA1)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + 1 gads vai 2 gadi |
| Parakstītājs | | *CN* | Sugas vārds: Parakstītāja nosaukums |
| | | *O* | Parakstītāja organizācija |
| | | *OU* | Parakstītāja struktūrvienība |
| | | *L* | Izvēles: Parakstītāja adrese |
| | | *S* | Izvēles: Parakstītāja pilsēta |
| | | *E* | Parakstītāja e-pasts |
| | | *C* | Parakstītāja valsts (*ISO* 3166 kods) |
| Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 paplašinājumi** | | | |
| Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | Parakstītāja publiskās atslēgas *sha1* izvilkums |
| Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Izsniegšanas SI publiskās atslēgas *sha1* izvilkums |
| *CRL* izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?certificaterevocationlist?base?objectclass* |

| eParaksts.lv koda parakstīšanas sertifikāts Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| | | | *=certificationauthorityhttp://www.eme.lv/cdp/e-me%20si(ca1).crl*<br><br>*http://www.eme.lv/cdp/E-ME%20SI%20(CA1).crl* |
| Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?cacertificate?base?objectclass=certificationauthority* |
| | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *https://ocsp.eme.lv/responder.eme* |
| | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *http://www.eme.lv/aia/E-ME%20SI%20(CA1).crt* |
| Uzlabotā atslēgas lietošana | Nē | | *Code Signing (1.3.6.1.5.5.7.3.3)* |
| Sertifikātu politikas | Nē | Politikas identifikators | 1.3.6.1.4.1.32061.1.1.1 |
| | | SN | *http://www.eme.lv/repository* |
| Pielietojuma politikas | Nē | Pielietojumu sertifikātu politika | *Policy Identifier= Code signing* |
| Atslēgas lietošana | Jā | | *Digital Signature (80)* |
| Pamata ierobežojumi | Jā | | *Signatory Type=End Entity*<br>*Path Length Constraint=None* |
| **Īpašības** | | | |
| Izvilkuma algoritms | | | *Sha1* |
| Izvilk ums | | | Parakstītāja sertifikāta izvilkums |

## 7.16. Izsniegšanas SI izsniegta domēna kontroliera sertifikāta profils

| eParaksts.lv domeina kontroliera sertifikāts Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Versija | | | *V3* |
| Sērijas numurs | | | Automātiski piešķir Izsniegšanas SI |
| Paraksta algoritms | | | *sha1RSA* |
| Izsniedzējs | | | *CN = E-ME SI(CA1)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*O = E-ME*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + 1 gads vai 2 gadi |
| Parakstītājs | | *N* | Sugas vārds: Parakstītājs |
| | | *O* | Parakstītāja organizācija |
| | | *OU* | Parakstītāja struktūrvienība |
| | | *L* | Izvēles: Parakstītāja adrese |
| | | *S* | Izvēles: Parakstītāja pilsēta |
| | | *E* | Parakstītāja e-pasts |
| | | *C* | Parakstītāja valsts (*ISO* 3166 kods) |

| eParaksts.lv domeina kontroliera sertifikāts Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 paplašinājumi** | | | |
| Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | Parakstītāja publiskās atslēgas *sha1* izvilkums |
| Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Izsniegšanas SI publiskās atslēgas *sha1* izvilkums |
| *CRL* izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?certificaterevocationlist?base?objectclass=certificationauthorityhttp://www.eme.lv/cdp/e-me%20si(ca1).crl*<br><br>*http://www.eme.lv/cdp/E-ME%20SI%20(CA1).crl* |
| Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?cacertificate?base?objectclass=certificationauthority* |
| | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *https://ocsp.eme.lv/responder.eme* |
| | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *http://www.eme.lv/aia/E-ME%20SI%20(CA1).crt* |
| Uzlabotā atslēgas lietošana | Nē | | Client Authentication (1.3.6.1.5.5.7.3.2)<br>Server Authentication (1.3.6.1.5.5.7.3.1)<br>Smart Card Logon (1.3.6.1.4.1.311.20.2.2) |
| Sertifikātu politikas | Nē | Politikas identifikators | 1.3.6.1.4.1.32061.1.1.1 |
| | | SN | *https://www.eparaksts.lv/lv/repozitarijs* |
| Pielietojumu politikas | Nē | Pielietojumu sertifikātu politika | *Policy Identifier=Server Authentication*<br>*Policy Identifier=Client Authentification*<br>*Policy Identifier=Smart Card Logon* |
| Atslēgas lietošana | Jā | | *Digital Signature, Key Encipherment (a0)* |
| Pamata ierobežojumi | Jā | | *Signatory Type=End Entity*<br>*Path Length Constraint=None* |
| Subjekta alternatīvais vārds | Jā | DNS Name | *Domeina nosaukums* |
| **Īpašības** | | | |
| Izvilkuma algoritms | | | *Sha1* |
| Izvilkums | | | Parakstītāja sertifikāta izvilkums |

## 7.17. Izsniegšanas SI izsniegta elektroniskā zīmoga sertifikāta profils

| eParaksts.lv eZīmoga sertifikāts Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Versija | | | *V3* |

| **eParaksts.lv eZīmoga sertifikāts Izsniegšanas SI parakstīts** | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Sērijas numurs | | | Automātiski piešķir Izsniegšanas SI |
| Paraksta algoritms | | | *sha1RSA* |
| Izsniedzējs | | | *CN = E-ME SI(CA1)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + 2 gadi |
| Parakstītājs | | *CN* | <Organizācijas nosaukums> : eZīmogs |
| | | Serialnumber | <Organizācijas reģistrācijas numurs> |
| | | *O* | <Organizācijas nosaukums> |
| | | *OU* | Izvēles: <Parakstītāja struktūrvienība> |
| | | *C* | Parakstītāja valsts (*ISO* 3166 kods) |
| | | *E* | Izvēles: Organizācijas vai kontaktpersonas e-pasts |
| Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 paplašinājumi** | | | |
| Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | Parakstītāja publiskās atslēgas *sha1* izvilkums |
| Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Izsniegšanas SI publiskās atslēgas *sha1* izvilkums |
| *CRL* izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *http://www.eme.lv/cdp/E-ME%20SI%20(CA1).crl*<br><br>*ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?cacertificate?base?objectclass=certificationauthority* |
| | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *https://ocsp.eme.lv/responder.eme* |
| | | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *http://www.eme.lv/aia/E-ME%20SI%20(CA1).crt* |
| Uzlabotā atslēgas lietošana | Nē | | *Document Signing (1.3.6.1.4.1.311.10.3.12)*<br>*Secure Email (1.3.6.1.5.5.7.3.4)* |
| Sertifikātu politikas | Nē | Politikas identifikators | *1.3.6.1.4.1.32061.1.1.1* |
| | | Lietotāja norāde | *So sertifikatu ir izsniedzis VAS Latvijas Valsts radio un televizijas centrs, reg.Nr.40003011203, pamatojoties uz savstarpeji noslegtu ligumu* |
| | | SN | *http://www.eme.lv/repository* |
| Pielietojumu politikas | Nē | Pielietojumu sertifikātu politika | *Policy Identifier=Document Signing*<br>*Policy Identifier=Secure Email* |

| eParaksts.lv eZīmoga sertifikāts Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Atslēgas lietošana | Jā | | *Digital Signature, Non-Repudiation (c0)* |
| Pamata ierobežojumi | Jā | | *Signatory Type=End Entity*<br>*Path Length Constraint=None* |
| **Īpašības** | | | |
| Izvilkuma algoritms | | | *Sha1* |
| Izvilkums | | | Parakstītāja sertifikāta izvilkums |

## 7.18. Izsniegšanas SI izsniegta elektroniskā zīmoga autentifikācijas sertifikāta profils

| eParaksts.lv eZīmoga autentifikācijas sertifikāts Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| Versija | | | *V3* |
| Sērijas numurs | | | Automātiski piešķir Izsniegšanas SI |
| Paraksta algoritms | | | *sha1RSA* |
| Izsniedzējs | | | *CN = E-ME SI(CA1)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Derīgs no | | | Izsniegšanas datums |
| Derīgs līdz | | | Izsniegšanas datums + 2 gadi |
| Parakstītājs | | *CN* | <Organizācijas nosaukums> : eZīmogs |
| | | Serialnumber | <Organizācijas reģistrācijas numurs> |
| | | *O* | <Organizācijas nosaukums> |
| | | *OU* | Izvēles: <Parakstītāja struktūrvienība> |
| | | *C* | Parakstītāja valsts (*ISO* 3166 kods) |
| | | *E* | Izvēles: Organizācijas vai kontaktpersonas e-pasts |
| Publiskā atslēga | | | RSA (2048 biti) |
| **X.509 V3 paplašinājumi** | | | |
| Parakstītāja atslēgas identifikators | Nē | Atslēgas identifikators | Parakstītāja publiskās atslēgas *sha1* izvilkums |
| Institūcijas atslēgas identifikators | Nē | Atslēgas identifikators | Izsniegšanas SI publiskās atslēgas *sha1* izvilkums |
| *CRL* izplatīšanas vietas | Nē | Izplatīšanas vietas vārds | *http://www.eme.lv/cdp/E-ME%20SI%20(CA1).crl*<br><br>*ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?certificaterevocationlist?base?objectclass=certificationauthority* |
| Pieeja institūcijas informācijai | Nē | Sertificēšanas institūcijas izsniedzējs (1.3.6.1.5.5.7.48.2) | *ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?cacertificate?base?objectclass=certificationauthority* |
| | | Tiešsaistes sertifikātu statusa protokols (1.3.6.1.5.5.7.48.1) | *https://ocsp.eme.lv/responder.eme* |
| | | Sertificēšanas institūcijas izsniedzējs | *http://www.eme.lv/aia/E-ME%20SI%20(CA1).crt* |

| eParaksts.lv eZīmoga autentifikācijas sertifikāts Izsniegšanas SI parakstīts | | | |
|---|---|---|---|
| **Standarts X.509 V1** | **Kritisks** | **Atribūts** | **Saturs** |
| | | (1.3.6.1.5.5.7.48.2) | |
| Informācija par sertifikātu šablonu | Nē | Šablons | *Template=1.3.6.1.4.1.311.21.8.5179758.1349991.6178693.1269097.5245921.164.11111213.14174680*<br>*Major Version Number=100*<br>*Minor Version Number=5* |
| Uzlabotā atslēgas lietošana | Nē | | *Client Authentication (1.3.6.1.5.5.7.3.2)* |
| Sertifikātu politikas | Nē | Politikas identifikators | *1.3.6.1.4.1.32061.1.1.1* |
| | | Lietotāja norāde | *So sertifikatu ir izsniedzis VAS Latvijas Valsts radio un televizijas centrs, reg.Nr.40003011203, pamatojoties uz savstarpeji noslegtu ligumu* |
| | | SN | *http://www.eme.lv/repository* |
| Pielietojumu politikas | Nē | Pielietojumu sertifikātu politika | *Policy Identifier= Client Authentication* |
| Atslēgas lietošana | Jā | | *Digital Signature (80)* |
| Pamata ierobežojumi | Jā | | *Signatory Type=End Entity*<br>*Path Length Constraint=None* |
| **Īpašības** | | | |
| Izvilkuma algori tms | | | *Sha1* |
| Izvilkums | | | Parakstītāja sertifikāta izvilkums |

## 7.19. CRL profili

7.19.1. Root CA CRL profils

| Saknes SI parakstīts Sertifikācijas pakalpojumu sniedzēja eParaksts.lv Saknes SI *CRL* | | |
|---|---|---|
| ***CRL* standarts** | **Atribūts** | **Saturs** |
| Versija | | *V2* |
| Izsniedzējs | | *CN= E-ME SSI(RCA)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Spēkā stāšanās datums | | Izsniegšanas datums un laiks |
| Nākamais papildinājums | | Nākamā papildinājuma datums un laiks |
| Paraksta algoritms | | *sha1RSA* |
| Institūcijas atslēgas identifikators | Atslēgas identifikators | Saknes SI publiskās atslēgas *Sha1* izvilkums |
| SI versija | | *V0.0* |
| *CRL* numurs | | Automātiski piešķir Saknes SI |
| Nākamā *CRL* publicēšana | | Izsniegšanas datums + 3 mēneši |

7.19.2. Politikas SI CRL profils

| Politikas SI parakstīts Sertifikācijas pakalpojumu sniedzēja eParaksts.lv *CRL* Politikas SI | | |
|---|---|---|
| ***CRL* standarts** | **Atribūts** | **saturs** |
| Versija | | *V2* |
| Izsniedzējs | | *CN = E-ME PSI(PCA)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |

| | | |
|---|---|---|
| Spēkā stāšanās datums | | Izsniegšanas datums un laiks |
| Nākamais papildinājums | | Nākamā papildinājuma datums un laiks |
| Paraksta algoritms | | *sha1RSA* |
| Institūcijas atslēgas identifikators | Atslēgas identifikators | Politikas SI publiskās atslēgas *Sha1* izvilkums |
| SI versija | | *V0.0* |
| *CRL* numurs | | Automātiski piešķir Politikas SI |
| Nākamā *CRL* publicēšana | | Izsniegšanas datums + 3 mēneši |

7.19.3. eParaksts.lv izsniegšanas SI CRL profils

| | | **eParaksts.lv Sertifikācijas pakalpojumu sniedzēja Izsniegšanas SI *CRL* Izsniegšanas SI parakstīts** |
|---|---|---|
| ***CRL* standarts** | **Atribūts** | **Saturs** |
| Versija | | *V2* |
| Izsniedzēj | | *CN = E-ME SI(CA1)*<br>*OU = Sertifikacijas pakalpojumu dala*<br>*C = LV* |
| Spēkā stāšanās datums | | Izsniegšanas datums un laiks |
| Nākamais papildinājums | | Nākamā papildinājuma datums un laiks |
| Paraksta algoritms | | *sha1RSA* |
| **Anulētie sertifikāti** | | |
| Sērijas numurs | | Apturētā vai anulētā sertifikāta numurs |
| Anulēšanas datums | | Apturēšanas vai anulēšanas datums un laiks |
| ***CRL* paplašinājumi** | | |
| Institūcijas atslēgas identifikators | Atslēgas identifikators | Izsniegšanas SI publiskās atslēgas *Sha1* izvilkums |
| SI versija | | *V0.0* |
| *CRL* numurs | | Automātiski piešķir Izsniegšanas SI 1 |
| Nākamā *CRL* publicēšana | | Izsniegšanas datums + 12 stundas |
| Jaunākais *CRL* | Izplatīšanas punkta nosaukums | *http://www.eme.lv/cdp/E-ME%20SI%20(CA1).crl*<br><br>*ldap://eme.lv/cn=E-ME%20SI%20(CA1),ou=Sertifikacijas%20pakalpojumu%20dala,o=E-ME,c=lv?certificaterevocationlist?base?objectclass=certificationauthority* |

# 8. Atbilstības audits un citi vērtējumi

## 8.1. Atbilstības audita biežums un apstākļi

8.1.1. SI atbilstība šiem Sertificēšanas noteikumiem tiek pārbaudīta katru gadu.

8.1.2. Atbilstības audits tiek veikts ārpus ikgadējā atbilstības audita, gadījumos, ja UPSP veic būtiskas izmaiņas USPS pārvaldībā vai informācijas sistēmā.

## 8.2. Prasības Auditoriem

8.2.1. Prasības pret ekspertiem, kas ir tiesīgi veikt USPS atbilstības auditu nosaka Elektronisko dokumentu likums.

## 8.3. Auditoru attiecības ar LVRTC

8.3.1. Auditors drīkst būt no eParaksts.lv SPS iekšējas organizācijas, bet viņam nevar būt nekādas hierarhiskas saistības ar daļu, kas pārvalda eParaksts.lv SPS SI.

## 8.4. Ikgadējā atbilstības novērtējuma temati

8.4.1. Ikgadējo atbilstības auditu tematiem jāietver:

8.4.1.1. fiziskā drošība;

8.4.1.2. tehnoloģiju novērtējums;

8.4.1.3. SI un RI pakalpojumu administrēšana (tostarp SI vides kontroles, atslēgu pārvaldības darbības un infrastruktūras / administratīvās SI uzraudzības pasākumi, sertifikātu dzīves cikla pārvaldība);

8.4.1.4. personāla pārbaude;

8.4.1.5. attiecīgie SN un SP;

8.4.1.6. līgumi;

8.4.1.7. datu aizsardzības un privātuma apsvērumi;

8.4.1.8. avārijas atjaunošanās plānošanas dokumenti.

8.4.2. Gadskārtējā audita apjomā ir SI vides kontroles, atslēgu pārvaldības darbības, infrastruktūras un administratīvās SI kontroles, sertifikāta dzīves cikla pārvaldība un SI biznesa procedūru izziņošana.

## 8.5. Reakcija uz atbilstības auditā atklātajiem trūkumiem

8.5.1. Atbilstības audita laikā identificēti nozīmīgi iebildumi vai trūkumi noteiks nepieciešamās veicamās darbības. Lēmumu pieņem eParaksts.lv SPS vadība, ievērojot auditora pausto viedokli. eParaksts.lv SPS vadība ir atbildīga par koriģējoša darbības plāna izveidošanu un ieviešanu.

## 8.6. Rezultātu paziņošana

8.6.1. Pārbaudes veikšanas un rezultātu paziņošana ir noteikta MK 2003.gada 1.jūlija noteikumos Nr.358 „Sertifikācijas pakalpojumu sniegšanas informācijas sistēmu, iekārtu un procedūru drošības pārbaudes kārtība un termiņi".

# 9. Citi biznesa un juridiskie jautājumi

## 9.1. Maksājumi

9.1.1. Sertifikātu pārvaldības maksa

9.1.1.1. Sertifikātu pieteikšanas process un sertifikātu izsniegšana, anulēšana vai atjaunošana drīkst būt maksas pakalpojums. Gadījumos, kad ir piemērojama maksa, eParaksts.lv SPS sertificēšanas institūcijām nodrošinās cenrāžu jaunāko versiju (pieejams vietnē www.eparaksts.lv), pamatojoties uz ar tām panāktām konkrētām biznesa vienošanām uzticamas SI līgumā.

9.1.2. Sertifikātu pārbaudes maksa

9.1.2.1. eParaksts.lv SPS sertifikātu pārbaudes pakalpojumi, lai pārbaudītu kvalificētos parakstītāju sertifikātus, ir bezmaksas. eParaksts.lv SPS var prasīt maksu par sertifikātu pārbaudes pakalpojumiem gadījumos, kurus neaizliedz EDL.

9.1.3. Kompensācijas politika

9.1.3.1. eParaksts.lv SPS Saknes SI vai pakārtota sertificēšanas institūcija var ieviest kompensācijas politiku. Kad kompensācijas politika attiecas uz gala

lietotājiem, tiem tiks nodrošināta tās jaunākā versija, kuru iespējams publicēt interneta vietnē www.eparaksts.lv.

## 9.2. Finansiālā atbildība

9.2.1. eParaksts.lv SPS atbildības ierobežojumi attiecībā uz pakārtotām izsniegšanas sertificēšanas institūcijām tiek noteikti uzticamo SI savstarpējos līgumos. Šie SN ir iekļauti šādos līgumos kā to sastāvdaļa.

9.2.2. Ja nav tieši norunāts savādāk vai skaidri noteikts eParaksts.lv SPS apstiprinātā Sertifikātu politikā, eParaksts.lv SPS atbildība pret pakārtotām SI, pārbaudītājiem un jebkurām citām vienībām, kas nav pakārtotās SI, ir ierobežota attiecībā uz visu veidu prasībām, gan līgumiskām, gan ārpuslīgumiskām, pamatojoties uz katru sertifikātu atsevišķi neatkarīgi no transakciju vai elektronisko parakstu skaita, vai arī no sertifikātiem vai jebkādu attiecībā uz šiem sertifikātiem nodrošinātu pakalpojumu izrietošiem darbību iemesliem, kā arī uz kumulatīva pamata.

9.2.3. Jebkādas un visas prasības, kas saistītas ar eParaksts.lv SPS pakalpojumiem attiecībā uz sertifikātu (neatkarīgi no kaitējuma radošās vienības vai sertifikātus izsniedzošās un sertifikācijas pakalpojumus nodrošinošās vienības), tiks pakļautas saskaņā ar šo SN piemērojamiem atbildības ierobežojumiem.

9.2.4. Kvalificētam sertifikātam norādītais darījuma summas ierobežojums ir tikai ar mērķi noteikt LVRTC atbildības ierobežojumu, kaitējuma rašanās gadījumā parakstītājam, ja par iemeslu šo zaudējumu rašanai ir USPS normatīvajos aktos noteikto prasību neievērošana vai pārkāpšana.

9.2.5. Saskaņā ar Elektronisko dokumentu likumu, LVRTC noteiktais summas ierobežojums darījumiem, kuru veikšanai var izmantot kvalificētu sertifikātu, ir 150 000,00 EUR par katru darījumu.

9.2.6. Gadījumā, ja parakstītājs izmanto kvalificētu sertifikātu darījumu veikšanai, kuru summa pārsniedz Summas ierobežojumu darījumiem, LVRTC atbild par zaudējumiem, kas radušies no USPS neatbilstības normatīvajos aktos noteiktajām prasībām, tikai tādā apmērā, kas nepārsniedz 150 000,00 EUR.

9.2.7. USPS neuzņemas atbildību par darījumu, kura veikšanai tiek izmantots kvalificēts sertifikāts, saturu, apjomu un izpildi. Parakstītājs vai Pasūtītājs var ierobežot sertifikāta lietošanu to apturot vai anulējot.

9.2.8. Nekādos apstākļos eParaksts.lv SPS atbildība nepārsniedz iepriekš minētos ierobežojumus.

## 9.3. Biznesa informācijas konfidencialitāte

9.3.1. **Konfidenciāli glabājamas informācijas tipi**

9.3.1.1. **Personas informācijas vākšana un lietošana**

9.3.1.1.1. Visa eParaksts.lv SPS SI savāktā vai lietotā fizisko personu informācija tiek apstrādāta saskaņā ar normatīvajiem aktiem fizisko personu datu aizsardzības jomā un šajos SN noteikto. Uzticamu sertificēšanas institūciju apstrādātie fizisko personu dati tiks apstrādāti saskaņā ar normatīvajiem aktiem fizisko personu datu aizsardzības jomā.

9.3.1.1.2. Gadījumos, kad uzticama sertificēšanas institūcija pārstāj sniegt sertifikācijas pakalpojumus, kā daļu no darbības izbeigšanas procedūras tai jānodod sertifikācijas pakalpojumu nodrošināšanai atbilstošie personas un citi dati citai vietējai pakārtotai sertificēšanas institūcijai vai citai eParaksts.lv SPS vai kompetentas iestādes nozīmētai vienībai. Jebkurā gadījumā tiks prasīta šādu datu glabāšana un pieejamība sertifikācijas pakalpojumu nodrošināšanai gala lietotājiem.

9.3.1.2. **Reģistrācijas informācija**

9.3.1.2.1. Reģistrācijas informācija nav vispārpieejama informācija, izņemot, ja vien ir saņemta tieša tās vienības, uz kuru šī informācija attiecas, piekrišana.

9.3.1.3. **Sertifikāta un sertifikāta statusa informācija**

9.3.1.3.1. Sertifikāta un sertifikāta statusa informācija ir jāatklāj visiem nolūkiem, kas var būt saistīti ar šādas informācijas izmantošanu un sertifikāta statusu saskaņā ar gala lietotāja pasūtītāja līgumā vai citās vienošanās pausto piekrišanu. Ja vien Sertifikātu politikā vai Sertificēšanas noteikumos nav tieši noteikts savādāk, pēc sertifikāta pieņemšanas gala lietotājiem ir jāpilnvaro eParaksts.lv SPS Saknes SI un pakārtotās SI publicēt informāciju, kā parakstītāja norādīta izsniegtajā sertifikātā, un citu informāciju, kas nepieciešama sertifikācijas pakalpojumu nodrošināšanai.

9.3.1.4. **Ekspluatācijas un konfigurācijas dokumentācija**

9.3.1.4.1. eParaksts.lv SPS uztur virkni iekšēju dokumentu, kas detalizēti aprakstīs eParaksts.lv SPS SI un tās sertifikācijas pārbaudes pakalpojumu darbību un konfigurāciju. Šie dokumenti tiek uzskatīti par konfidenciāliem un netiek izpausti ārpus eParaksts.lv SPS, izņemot konsultēšanas un audita nolūkiem.

9.3.1.5. **Audita informācija**

9.3.1.5.1. Visa eParaksts.lv SPS saņemtā audita informācija, kas attiecas uz eParaksts.lv SPS SI, tās sertifikātu pārbaudes pakalpojumiem vai jebkuru citu pakārtotu SI, tiks uzskatīta par konfidenciālu informāciju, izņemot apjomā ierobežotus šādu auditu kopsavilkumus, kurus eParaksts.lv SPS var publicēt pēc savas neierobežotas izvēles vai saskaņā ar piemērojamiem normatīvajiem aktiem.

9.3.1.5.2. Ja to prasa normatīvie akti un ir iegūtas vai izpildītas atbilstošas procedūras, rīkojumi vai citas juridiskas prasības, pilnus audita datus var izpaust saskaņā ar 9.3.4 un 9.3.5. nodaļu.

9.3.2. **Par konfidenciālu neuzskatāmas informācijas tipi**

9.3.2.1. **Sertifikātu un sertifikātu statusa informācija**

9.3.2.1.1. Visi eParaksts.lv SPS SI publiskai lietošanai izsniegtie sertifikāti būs publiski pieejami. Rīcību ar uzticamo SI izsniegtajiem sertifikātiem noteiks atbilstošie SN un sertifikātu politikas. Visos gadījumos visu eParaksts.lv SPS pakalpojumu ietvaros izsniegto sertifikātu statusa informācija būs pieejama ikvienam, kurš saskaņā ar šiem SN, uzticamas SI SN, sertifikātu politikām un jebkurām citām atbilstošajām vienošanām, izmanto sertifikātu pārbaudes pakalpojumus.

9.3.2.2. **PKI dokumentācija**

9.3.2.2.1. apstiprinātas publiskas sertifikātu politikas un sertificēšanas noteikumi;

9.3.2.2.2. šie SI SN;

9.3.2.2.3. citi eParaksts.lv SPS publikācijai apstiprināti dokumenti.

9.3.3. **Sertifikātu anulēšanas informācijas atklāšana**

9.3.3.1. Uzticamas SI sertifikāta anulēšanas iemeslam ir jābūt publiski pieejamam saskaņā ar piemērojamajām normatīvo aktu prasībām vai pēc anulēto sertifikātu izsniegušās uzticamās SI vai eParaksts.lv SPS savas neierobežotas izvēles.

9.3.3.2. Informācija par sertifikātu anulēšanu vai derīgumu tiek atklāta, izmantojot OCSP protokolu un anulēto un apturēto sertifikātu sarakstus (CRL). eParaksts.lv SPS sertifikātu pārbaudes pakalpojumi atklāj, vai pieprasītais sertifikāts ir

derīgs, anulēts vai apturēts, kā arī, vai sertifikāta pārbaudes pakalpojumiem nav ziņu par sertifikāta statusu. Cita informācija netiek atklāta.

9.3.4. **Informācijas sniegšana tiesībsargājošām iestādēm**

9.3.4.1. Neviens eParaksts.lv SPS glabāts dokuments vai ieraksts netiek atklāts tiesībsargājošām iestādēm vai to pārstāvjiem, izņemot gadījumus, kad:

9.3.4.1.1. tiek uzrādīts pareizi sastādīts orderis vai pieprasījums;

9.3.4.1.2. tiesībsargājošās iestādes darbinieks tiek pareizi identificēts;

9.3.4.1.3. tiek ievērotas citas piemērojamas tiesiskās procedūras.

9.3.4.2. Uzticamo SI paturētiem dokumentiem tiks piemērotas līdzīgas prasības, bet saskaņā ar atbilstošajiem SN un piemērojamiem likumiem.

9.3.5. **Informācijas sniegšana civilprocesa pierādījumu vai atklāšanas nolūkiem**

9.3.5.1. Vispārīgi neviens eParaksts.lv SPS glabāts konfidenciāls dokuments vai ieraksts netiek atklāts nevienai personai, izņemot gadījumus, kad:

9.3.5.1.1. tiek uzrādīts informācijas sniegšanai pareizi sastādīts pieprasījums (t.i. tāds, kurš atbilst visām normatīvajos aktos noteiktajām prasībām);

9.3.5.1.2. persona, kas prasa informācijas uzrādīšanu, ir persona, kura ir pilnvarota to darīt un ir pareizi identificēta.

9.3.5.2. Uzticamās SI tiks lūgtas sniegt informāciju no ikvienas eParaksts.lv SPS pakalpojumu daļas civilprocesa pierādījumu vai atklāšanas nolūkiem katrā jurisdikcijā, kur ir ievērotas atbilstošās likumīgās procedūras. Šiem nolūkiem eParaksts.lv SPS pakalpojumu ietvaros var tikt iedibināta iekšēja procedūra, saskaņota ar piemērojamiem likumiem un atbilstošo kompetento iestāžu apstiprinājumu.

## 9.4. Personas informācijas privātums

9.4.1.1. Visi eParaksts.lv SPS SSI apstrādātie fizisko personu dati tiek aizsargāti saskaņā ar Fizisko personu datu aizsardzības likumu. Fizisko personas dati tiek atklāti trešajām personām normatīvajos aktos noteiktajos gadījumos, kārtībā un termiņos.

9.4.2. **Par konfidenciālu uzskatāma informācija**

9.4.2.1. Visa eParaksts.lv SPS SI apstrādātie personas dati tiek apstrādāti saskaņā ar spēkā esošiem normatīvajiem aktiem.

9.4.2.2. Reģistrācijas informācija tiek uzskatīta par konfidenciālu (neizpaužamu) informāciju. Konfidenciālas informācijas izpaušana notiek vienīgi ar informācijas sniedzēja tiešu piekrišanu šīs informācijas publiskošanai.

9.4.2.3. Gadījumos, kad SI pārstāj sniegt sertifikācijas pakalpojumus, kā daļu no darbības izbeigšanas procedūras tai jānodod sertifikācijas pakalpojumu nodrošināšanai atbilstošie personas un pārējie dati citai sertificēšanas institūcijai vai uzraugošās iestādes nozīmētai vienībai.

9.4.3. **Par konfidenciālu neuzskatāma informācija**

9.4.3.1. Sertifikātu un sertifikātu statusa informācija tiek atklāta visiem nolūkiem, kas var būt nozīmīgi šādas informācijas un sertifikātu statusa izmantošanai saskaņā ar uzticamas SI atbilstošajos līgumos sniegto piekrišanu, izņemot gadījumos, kas noteikti saistošajos normatīvajos aktos. Pēc sertifikātu apstiprināšanas pakārtotās SI pilnvaro eParaksts.lv SPS publicēt informāciju, kas norādīta izsniegtajā sertifikātā, un citu informāciju, kas nepieciešama sertifikācijas pakalpojumu nodrošināšanai.

9.4.4. **Pienākums aizsargāt privātu informāciju**

9.4.4.1. Visas eParaksts.lv SPS vienības, kas apstrādā fizisko personu datus ievēro Fizisko personu datu aizsardzības likuma prasības.

9.4.5. **Pieteikums un piekrišana privātas informācijas lietošanai**

9.4.5.1. Informācija, kura nav publiski pieejama, tiek izmantota tikai tiem mērķiem, kas saistīti ar sertifikācijas pakalpojumu sniegšanu. Citiem mērķiem minēto informāciju izmanto tikai saskaņā ar spēkā esošajiem normatīvajiem aktiem un ievērojot to prasības.

9.4.6. **Atklāšana atbilstoši tiesiskam vai administratīvam procesam**

9.4.6.1. eParaksts.lv SPS ir tiesīga atklāt fizisko personu datus gadījumos, kas noteikti spēkā esošajos normatīvajos aktos.

9.4.7. **Citi informācijas atklāšanas apstākļi**

9.4.7.1. Nav nosacījumu

## 9.5. Intelektuālā īpašuma tiesības

9.5.1. Visas ar intelektuālo īpašumu saistītās tiesības, tostarp visu sertifikātu, anulēto un apturēto sertifikātu sarakstu, OCSP sertifikāta statusa ziņojumu, sertifikātu direktoriju un, ja vien netiek īpaši paredzēts citādi, visu procedūru, politikas, eParaksts.lv SPS PKI ekspluatācijas un drošības dokumentu (elektronisku un citādu), kā arī līgumu autortiesības un / vai mantiskās tiesības pieder eParaksts.lv SPS un turpinās būt tā īpašums.

## 9.6. Pārstāvības un garantijas

9.6.1. Nav nosacījumu.

## 9.7. Atbildības ierobežošana un atrunas

9.7.1. eParaksts.lv SPS ir jānodrošina eParaksts.lv SPS SI sertifikācijas pakalpojumus saskaņā ar šiem SN. Šo SN 1.4. nodaļā ir uzskaitīti lietojuma ierobežojumi, ko sniedz eParaksts.lv SPS, darbojoties kā eParaksts.lv SPS SI. Visas citas garantijas tiek izslēgtas, tostarp jebkuras šādas garantijas:

9.7.1.1. attiecībā pret tādas informācijas precizitāti vai uzticamību, kas iekļauta sertifikātos, ko nav izsniedzis vai pārbaudījis eParaksts.lv SPS vai uzticama SI;

9.7.1.2. kuras atkāpjas no šiem SN vai ir pretrunā tiem;

9.7.1.3. attiecībā uz ārpus eParaksts.lv SPS saprātīgas kontroles esošiem jautājumiem.

9.7.2. eParaksts.lv SPS neatbild par jebkādu kaitējumu (tostarp īpaša, izrietoša, nejauša, netieša vai sodāma) un jebkādiem zaudējumiem, neatkarīgi no tā, vai ir par tiem (vai to iespējām) informēts un vai tie ir bijuši saprātīgi paredzami, kas izriet no:

9.7.2.1. veiktajām transakcijām starp gala lietotājiem un pārbaudītājiem;

9.7.2.2. sertifikātu, kriptogrāfisko atslēgu, elektronisko parakstu un sertifikācijas pakalpojumu tādu lietošanu vai paļaušanos uz tiem, kas nav atbilstoša šiem SN vai mērķiem, kas nav atļauti šajos SN;

9.7.2.3. trešo pušu produktiem vai pakalpojumiem (ieskaitot aparatūru un programmatūru);

9.7.2.4. sertifikāta neatjaunošanu dēļ neatbilstības šajos SN norādītajām sertifikāta atjaunošanas prasībām;

9.7.2.5. jebkura netieša vai izrietoša zuduma vai kaitējuma, tai skaitā, bet ne tikai, peļņas zaudējuma, paredzamo ietaupījumu zuduma, ieņēmumu zuduma, biznesa zaudējuma, biznesa pārtraukuma vai informācijas zuduma.

9.7.3. Nekādos apstākļos eParaksts.lv SPS nebūs atbildīgs par jebkuru kaitējumu veidu par summu, kas lielāka par paļaušanās apjomu, kas minēts šo SN 9.2 nodaļā.

## 9.8. Tiesības saņemt atlīdzību par kaitējumu

9.8.1. **eParaksts.lv SPS SSI atbildības nodošana pasūtītājiem**

9.8.1.1. Tādā apmērā, kādā to atļauj piemērojamais likums, pakārtotajām sertificēšanas institūcijām ir jāuzņemas atbildību attiecībā pret eParaksts.lv SPS SI par:

9.8.1.1.1. uzticamas SI sertifikāta pieteikuma faktu nepatiesumu vai to nepareizu interpretēšanu;

9.8.1.1.2. uzticamas SI neveiktu būtisku faktu atklāšanu sertifikātu pieteikumā, ja nepareiza interpretēšana vai izlaidums ir veikti nevērības dēļ vai ar mērķi maldināt kādu pusi;

9.8.1.1.3. uzticamas SI nespēju aizsargāt uzticamas SI privāto atslēgu, lietot uzticamu sistēmu vai citādi ievērot uzticamas SI privātās atslēgas kompromitējuma, zuduma, atklāšanas, modificēšanas vai nesankcionētas lietošanas novēršanai nepieciešamo piesardzību;

9.8.1.1.4. uzticamas SI nosaukuma lietošanu (tostarp bez ierobežojumiem sugas vārdos, domēna nosaukumos, e-pasta adresēs), kas aizskar trešās puses intelektuālā īpašuma tiesības.

9.8.1.1.5. Atbilstošais uzticamas SI līgums var iekļaut papildu saistības attiecībā uz tiesībām saņemt atlīdzību par kaitējumu.

9.8.2. **eParaksts.lv SPS atbildības nodošana pārbaudītājiem**

9.8.2.1. Tādā apmērā, kādā to atļauj normatīvie akti, pārbaudītāja līgumiem jānosaka, ka eParaksts SPS ir tiesības prasīt (piemēram, ar regresa prasību) un pārbaudītājam ir jākompensē eParaksts.lv SPS par:

9.8.2.1.1. pārbaudītāja neveiktiem pārbaudītāja pienākumiem;

9.8.2.1.2. pārbaudītāja paļaušanos uz sertifikātu, ja tas noteiktajos apstākļos nav saprātīgi;

9.8.2.1.3. pārbaudītāja neveiktu šāda sertifikāta statusa pārbaudi, lai noteiktu, vai sertifikāta derīguma termiņš nav beidzies vai tas nav anulēts.

9.8.2.2. Atbilstošais pārbaudītāja līgums var iekļaut papildu saistības attiecībā uz tiesībām saņemt atlīdzību par kaitējumu.

## 9.9. Termiņi un darbības izbeigšana

9.9.1. Termiņi

9.9.1.1. Šie SN stājas spēkā 30 dienas pēc to publicēšanas eParaksts.lv SPS repozitārijā vietnē www.eparaksts.lv/lv/repozitarijs

9.9.2. Darbības izbeigšana

9.9.2.1. Šie SN tiek regulāri pārskatīti un pēc nepieciešamības laboti un ir spēkā, līdz tiek aizstāti ar jaunu versiju.

## 9.10. Individuāli paziņojumi un saziņa ar dalībniekiem

9.10.1. Nav nosacījumu.

## 9.11. Grozījumi

9.11.1. Procedūra SN grozījumu ieviešanai

9.11.1.1. SN uzturēšanai un apstiprināšanai ir definēts iekšējs process ar piemērotām vadības līmeņa lomām.

9.11.1.2. Grozījumi, kas nemaina SN būtību vai nozīmi, piemēram, pareizrakstības kļūdu labojumi, kontaktinformācijas atjaunošana utml., tiek dokumentētas izmaiņu vēsturē šajā dokumenta un dokumenta versijas apakšnumurs tiek palielināts.

9.11.1.3. Attiecībā uz būtiskām izmaiņām tiek palielināta SN versija.

9.11.2. **Informēšanas mehānisms un termiņš**

9.11.2.1. SN aktualizācija tiek sniegta eParaksts.lv SPS tīmekļa vietnes www.eparaksts.lv repozitārijā. Grozījumi SN stājās spēkā 30 kalendārās dienās pēc SN jaunās versijas publicēšanas eParaksts.lv repozitārijā.

## 9.12. Domstarpību atrisināšanas kārtība

9.12.1. Sertificēšanas noteikumu hierarhija

9.12.1.1. Gadījumos, kad šie SN nonāk konfliktā vai pretrunā ar citām politikām, plāniem, vienošanām, līgumiem vai procedūrām, kad konflikts vai pretruna ir starp SN un:

9.12.1.2. uzticamas SI vienošanos, dominēs šie SN;

9.12.1.3. jebkuru vienošanos starp pakārtotām uzticamām SI, dominēs šie SN;

9.12.1.4. gala lietotāja vienošanos vai pārbaudītāja vienošanos, dominēs šie SN;

9.12.1.5. jebkuru politiku (izņemot SP), plānu, procedūrām vai jebkādu citu darbības vai procesu dokumentāciju, dominēs šie SN.

9.12.2. Atrisināšanas kārtība

9.12.2.1. Ja izceļas strīds, kas izriet vai ir saistīts ar šīm procedūrām vai saistītajiem līgumiem, pirms sākt tiesvedību, strīdā iesaistītajām pusēm ir jāmēģina atrisināt strīdu vai uzskatu atšķirības labticīgi ar pārrunām starp pusēm.

9.12.2.2. Ja puses nespēj atrisināt strīdu pārrunu ceļā viena (1) mēneša laikā kopš strīda rašanās, tad puses piekrīt vērsties tiesā saskaņā ar normatīvajiem aktiem. Strīdi netiek izskatīti šķīrējtiesā.

## 9.13. Piemērojamie likumi

9.13.1. Šie SN tiks pārvaldīti un interpretēti saskaņā ar Latvijas Republikas normatīvajiem aktiem.

## 9.14. Dažādas prasības

9.14.1. Nav nosacījumu.

## 9.15. Citas prasības

9.15.1. Nav nosacījumu.