Uzticamības pakalpojumu “eZīmogs+ mākonī” sniegšanas POLITIKA

SAGATAVOJA: ePakalpojumu daļa

NOSŪTĪTS: Publisks

SAISTĪTIE DOKUMENTI:

1. [CEN EN 419 211] Aizsardzības profili drošai paraksta radīšanas ierīcei
2. [eIDAS regula] Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK
3. [ETSI TS 119 312] Elektroniskie paraksti un infrastruktūras (ESI); Kriptogrāfijas virknes
4. [ETSI EN 319 401] Elektroniskie paraksti un infrastruktūras (ESI); Vispārīgās politikas prasības Uzticamības pakalpojumu sniedzējiem
5. [ETSI EN 319 411-1] Politikas un drošības prasības Uzticamības pakalpojumu sniedzējiem, kas izsniedz sertifikātus. 1.daļa. Vispārīgas prasības
6. [ETSI EN 319 411-2] Politikas un drošības prasības Uzticamības pakalpojumu sniedzējiem, kas izsniedz sertifikātus. 2.daļa. Prasības Uzticamības pakalpojumu sniedzējiem, kas izsniedz ES kvalificētus sertifikātus
7. [FPEIL] Latvijas Republikas Fizisko personu elektroniskās identifikācijas likums
8. [Sertifikāta profils] Latvijas Valsts Radio un televīzijas centra Uzticamības pakalpojumu sniedzēja izsniegto sertifikātu profilu apraksts
9. [CPS] Latvijas Valsts Radio un televīzijas centra Uzticamības pakalpojumu sniegšanas noteikumi
10. Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja vispārējie noteikumi
11. Procesa “Pakalpojumu pārdošana” apakšprocesa “Pakalpojumu pārdošana fiziskām personām” apraksts
12. Procesa “pakalpojumu piegāde” apakšprocesa “Pakalpojumu piegāde fiziskām personām” apraksts

VĒSTURE:

Pārskatītā varianta nr.	Spēkā stāšanās datums	Izmaiņu kopsavilkums
01.0	16.02.2023.	Sākotnējā versija

Saturs

1. Ievads

1.1. Pārskats

1.1.1. Šis dokuments „Uzticamības pakalpojumu “eZīmogs+ mākonī” sniegšanas politika” nosaka procesuālās un darbības prasības, ko Latvijas Valsts radio un televīzijas centrs (turpmāk - LVRTC) ievēro un kuru ievērošanu pieprasa no institūcijām, izsniedzot un pārvaldot elektronisko zīmogu sertifikātus un “eZīmogs+ mākonī” pakalpojumos.

1.1.2. LVRTC darbību kvalificētu elektronisko zīmogu un saistītu autentifikācijas sertifikātu izsniegšanā regulē [eIDAS Regula] un saistītie standarti.

1.1.4. Šī politika pakalpojumam “eZīmogs+ mākonī” balstās uz [ETSI EN 319 411-2] standartā noteikto „QCP-l-qscd” politiku un [ETSI EN 319 411-1] standartā noteikto NCP+ politiku.

1.1.6. Ja kāda no šajā politikā minētajām prasībām atšķiras no prasībām, kas minētas saistītajos standartos vai [CPS], tad dokumenti un tajos minētās prasības jāpiemēro šādā hierarhiskā secībā (augstāks spēks ir pirmajam minētajam):

1.1.6.1. [ETSI EN 319 411-2];

1.1.6.2. [ETSI EN 319 411-1];

1.1.6.3. šī politika;

1.1.6.4. [CPS].

1.1.7. Šī politika ir sagatavota latviešu valodā. Šī politika var tikt tulkota un var būt pieejama arī citās valodās. Politikas tulkojumu nesakritību gadījumā politikas versija latviešu valodā vienmēr ir vadoša.

1.1.8. Šajā politikā aprakstītajiem “eZīmogs+ mākonī” pakalpojumam tiek piešķirts kvalificēts statuss.

1.2. Dokumenta nosaukums un identifikācija

1.2.1. Šī dokumenta nosaukums ir „Uzticamības pakalpojumu “eZīmogs+ mākonī” sniegšanas politika”.

1.2.2. Šīs politikas identifikators ir: OID: 1.3.6.1.4.1.32061.2.2.2.1.

1.2.3. OID veidots atbilstoši tabulā norādītajam saturam:

Parametrs	*OID reference*
ISO	1
Identificētā organizācija	3
DoD	6
Internets	1

Privātuzņēmums	4
IANA reģistrēts privātuzņēmums	1
IANA numurs (LVRTC)	32061
Sertifikācijas pakalpojuma atribūts	2
Politikas veids (elektroniskā zīmoga)	2
Apakštips (eZīmogs+ mākonī)	2
Versija	1

1.2.6. "eZīmogs+ mākonī" pakalpojuma kvalificēta elektroniskā zīmoga sertifikāts atbilstoši QCP-l-qscd politikai satur šādus OID:

1.2.6.1. 0.4.0.194112.1.3 (QCP-l-qscd);

1.2.6.2. 1.3.6.1.4.1.32061.2.2.2.1. (šī politika).

1.3. **Publiskās atslēgas infrastruktūras dalībnieki:**

1.3.1. **Sertifikācijas institūcijas**

1.3.1.1. Aprakstītas šis [CPS]1.3.2. punktā.

1.3.2. **Reģistrācijas institūcijas**

1.3.2.1. Šīs politikas ietvaros reģistrācijas institūcija:

1.3.2.1.1. pakalpojumu "eZīmogs+ mākonī" un ar to saistītu sertifikātu pārvaldībai ir: valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs";

1.3.2.2. Uzticamības pakalpojumu sniedzēja mājas lapa www.eparaksts.lv:

1.3.2.1.2.1. pakalpojuma "eZīmogs+ mākonī" pieteikumu, kas parakstīti ar kvalificētu elektronisko parakstu, iesniegšana;

1.3.2.1.2.2. pakalpojuma "eZīmogs+ mākonī" saistīto sertifikātu administrēšana;

1.3.2.2. RA identificē pieteicējus un pārbauda dokumentāciju, kas garantē sertifikātos redzamo datu kvalitāti, kā arī validē un apstiprina pieprasījumus par sertifikātu izsniegšanu, atsaukšanu un atjaunošanu.

1.3.3. **Abonenti**

1.3.3.1. Abonents ir atbilstoši šai politikai izsniegtā sertifikāta turētājs.

1.3.3.2. Par abonentu var būt tikai juridiska persona, kas atrodama Eiropas Uzņēmējdarbības reģistrā, Latvijas Uzņēmumu reģistrā, Latvijas valsts iestāžu vai Latvijas bezpeļņas organizāciju reģistrā.

1.3.4. **Atkarīgās puses**

1.3.4.1. Atkarīgās puses ir juridiskās vai fiziskās personas, kas pieņem lēmumus, paļaujoties elektroniskā zīmoga vai saistīto autentifikācijas sertifikātu.

1.4. **Sertifikātu pielietojums**

1.4.1. **Sertifikāta atbilstoša lietošana**:

1.4.1.1. kvalificēti elektronisko zīmogu sertifikāti tiek lietoti tādu elektronisko zīmogu izveidei, kas tiek pievienoti vai loģiski sasaistīti ar citiem datiem elektroniskā formā, lai nodrošinātu šo datu izcelsmi un integritāti;

1.4.2. **Aizliegti sertifikāta lietojumi:**

1.4.2.1. Atbilstoši šai politikai izsniegtu sertifikātu lietošana ir aizliegta visiem tālāk uzskaitītajiem mērķiem:

1.4.2.1.1. prettiesiska darbība (tai skaitā kiberuzbrukumi un mēģinājumi sabojāt sertifikātu);

1.4.2.1.2. jaunu sertifikātu un informācijas par sertifikātu derīgumu izsniegšana;

1.4.2.1.3. elektroniskā zīmoga sertifikāta izmantošana dokumentu parakstīšanai, kas var radīt nevēlamas sekas (tai skaitā šādu dokumentu parakstīšanai sistēmu testēšanas laikā).

1.5. **Politikas pārvaldība**

1.5.1. **Dokumenta pārvaldības organizācija**

1.5.1.1. Šo politiku pārvalda valsts akciju sabiedrība „Latvijas Valsts radio un televīzijas centrs”, kas darbojas kā Uzticamības pakalpojumu sniedzējs atbilstoši šai politikai.

1.5.2. **Kontaktinformācija**

Valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs"	
Adrese	Zemitāna iela 9 k-3, Rīga, Latvija, LV-1012
Uzticamības pakalpojumu palīdzības dienests	
Tālrunis	+371 67108787
e-pasts	eparaksts@eparaksts.lv
Birojs	
Tālrunis	+371 67198704
e-pasts	lvrtc@lvrtc.lv

1.5.3. **Politikas apstiprināšanas procedūras**

1.5.3.1. Grozījumi, kas nemaina politikas nozīmi, piemēram, pārrakstīšanās, tulkojuma kļūdu un kontaktinformācijas atjaunošana, tiek norādīti šī dokumenta sadaļā „Versijas un izmaiņas”, kā arī tiek palielināta dokumenta versijas numura daļskaitļa daļa.

1.5.3.2. Būtisku izmaiņu gadījumā politikas jaunā versija tiek skaidri nošķirta no iepriekšējām. Jaunajai versijai tiek piešķirts par vienu veselu vienību palielināts kārtas numurs. Grozītā politika līdz ar spēkā stāšanās datumu, kas nedrīkst būt agrāk par 30 dienām pēc publikācijas, tiek elektroniski publicēta UPS mājaslapā www.eparaksts.lv.

1.5.3.3. Visus grozījumus un šīs politikas galīgo versiju apstiprina LVRTC valde.

1.6. **Termini un saīsinājumi**

1.6.1. **Termini**

Autoritatīvs avots	Jebkura veida avots, uz kuru var paļauties, ka tas sniedz precīzus datus, informāciju un/vai pierādījumu, ko var izmantot identitātes pierādīšanai (saskaņā ar CIR 2015/1502)
Droša šifrēšanas ierīce	Kvalificēta elektroniskā paraksta/zīmoga radīšanas ierīce, kas satur lietotāja privāto atslēgu, aizsargā šo atslēgu no drošības apdraudējumiem un veic parakstīšanas vai šifrēšanas funkcijas lietotāja vārdā
"eZīmogs+ mākonī"	Abonenta valdījumā esošs elektroniskā zīmoga risinājums, kur elektroniskais zīmogs parakstītāja vārdā tiek izveidots vidē, ko nodrošina uzticamības pakalpojumu sniedzējs un parakstītājs ir vienīgais, kurš pilnībā kontrolē sava elektroniskā zīmoga izveides vidi
Lietotājs	Abonenta darbinieks, kuram Abonents piešķir tiesības lietot pakalpojumu "eZīmogs+ mākonī".
Pārvaldnieks	Fiziska persona, kurai piešķirtas tiesības pārvaldīt Abonenta Lietotājus, kas izmanto pakalpojumu "eZīmogs+ mākonī".
Politika	Šajā dokumentā – Uzticamības pakalpojumu ar kvalificētu elektroniskā zīmoga sertifikātu sniegšanas politika
Sertifikāta turētājs	Persona, kas norādīta sertifikātā kā privātās atslēgas turētāja, kas saistīta ar sertifikātā esošo publisko atslēgu
Sertifikāts	Lietotāja publiska atslēga kopā ar citu informāciju, kas aizsargāta pret viltošanu, izmantojot šifrēšanu ar tādas sertifikācijas iestādes privātu atslēgu, kas to izsniegusi.

1.6.2. **Saīsinājumi**

CA	Sertifikātu izsniegšanas institūcija
CPS	Uzticamības pakalpojumu sniedzēja noteikumi
CRL	Atsaukto sertifikātu saraksts
NCP+	Paplašināta normalizētā sertifikātu politika, kas noteikta [ETSI EN 319 4111] Politika un drošības prasības Uzticamības pakalpojumu sniedzējiem, kuri izdod sertifikātus. 1.daļa. Vispārējās prasības
OCSP	Tiešsaistes sertifikātu statusa protokols
OID	Globālais objekta identifikators
Parole	Privāto atslēgu aktivēšanas dati (burtu un/vai ciparu kombinācija), kas nepieciešami, lai veiktu zīmogošanas darbību ar eZīmogs+ mākonī Sertifikātu un kas nodrošina iespēju lietot Sertifikātu tikai personai, kurai zināma Parole
PKI	Publisko atslēgu infrastruktūra
RA	Reģistrācijas institūcija
QCP-l	Politika juridiskai personai izsniegta ES kvalificēta sertifikāta jomā
QCP-l-qscd	Politika juridiskai personai izsniegta ES kvalificēta sertifikāta jomā gadījumos, kad privātā atslēga un saistītais sertifikāts atrodas uz QSCD
QSCD	Kvalificēta elektroniskā paraksta/zīmoga radīšanas ierīce

UPS	Fiziska vai juridiska persona, kas sniedz vienu vai vairākus uzticamības pakalpojumus vai nu kā kvalificēts, vai kā nekvalificēts uzticamības pakalpojumu sniedzējs

2. Publicēšanas un reģistrēšanas atbildība

2.1. **Repozitoriji**

2.1.1. Atbilstoši [CPS] 2.1. punktā aprakstītajam.

2.2. **Sertifikācijas informācijas publicēšana**

2.2.1. Šī Politika ir publicēta UPS mājaslapā: www.eparaksts.lv.

2.3. **Publicēšanas laiks vai biežums**

2.3.1. Atbilstoši [CPS] 2.3. punktā aprakstītajam.

2.4. **Piekļuves kontrole repozitorijiem**

2.4.1. Atbilstoši [CPS] 2.5. punktā aprakstītajam.

3. Identifikācija un autentifikācija

3.1. **Vārda piešķiršana**

3.1.1. **Nosaukumu veidi**

3.1.1.1. Jebkura atbilstoši šai politikai izsniegta sertifikāta nosaukums jāveido saskaņā ar sertifikāta profilu.

3.1.2. **Prasība pēc jēgpilniem nosaukumiem**

3.1.2.1. Šādām vērtībām sertifikāta turētāja (subject – angļu val.) laukā jābūt jēgpilnām:

3.1.2.1.1. organizācija (O);

3.1.2.1.2. parastais nosaukums (CN);

3.1.2.1.3. organizācijas identifikators.

3.1.3. **Abonentu anonimitāte vai pseidonīma piešķiršana**

3.1.3.1. Nav atļauta.

3.1.4. **Nosaukumu unikalitāte**

3.1.4.1. UPS dažādiem Abonentiem sertifikātus ar identisku abonenta individuālo nosaukumu neizsniedz.

3.2. **Sākotnējās identitātes validācija**

3.2.1. **Metode privātās atslēgas valdījuma pierādīšanai**

3.2.1.1. “eZīmogs+ mākonī”: atslēgu pāri ģenerē reģistrācijas iestāde un atslēgas ir noglabātas QSCD, privātās atslēgas valdījuma pierādījums ir atkarīgs no QSCD un tajā noglabātā atbilstošā sertifikāta un atslēgu pāra piegādes un pieņemšanas uzticamības procedūras.

3.2.2. **Organizācijas identitātes identifikācija un validācija**

3.2.2.1. UPS var izmantot jebkādus likumīgus saziņas vai izmeklēšanas līdzekļus, lai noskaidrotu fizisko vai juridisko personu identitāti.

3.2.2.2. UPS darbojas saskaņā ar Komisijas Īstenošanas regulu (ES) 2015/1502 (2015. gada 8. septembris), kas saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 8. panta 3. punktu nosaka elektroniskās identifikācijas līdzekļu uzticamības līmeņu minimālās tehniskās specifikācijas un procedūras.

3.2.2.3. UPS obligāti pārbauda abonentu atbilstošajā šīs politikas 1.3.3. punktā minētajā reģistrā.

3.2.2.4. UPS pēc saviem ieskatiem drīkst atteikties izsniegt sertifikātu.

3.2.3. **Individuālās identitātes identifikācija un validācija**

3.2.3.1. UPS pārliecinās par pakalpojuma “eZīmogs+ mākonī” pieteicēja tiesībām pieteikties un saņemt elektroniskā zīmoga sertifikātu.

3.2.3.2. “eZīmogs+ mākonī” pakalpojumu pieteicējam jābūt tiesīgam darboties organizācijas vārdā.

3.2.3.3. Individuālās identitātes validācija notiek:

3.2.3.3.1. fiziskās personas vai juridiskās personas pilnvarotā pārstāvja fiziskā klātbūtnē kādā no Reģistrācijas institūcijām. Fiziska persona tiek identificēta pret autoritatīvu avotu (piemēram, pase);

3.2.3.3.2. izmantojot kvalificētu elektronisko parakstu – identitāte tiek apliecināta ar datiem kvalificētā elektroniskajā parakstā, kas satur laika zīmogu.

3.2.3.3.3. izmantojot [FPEIL] noteikto kvalificētu paaugstinātas drošības elektroniskās identifikācijas līdzekli.

3.2.3.4. Identifikācijas laikā UPS jāsavāc nepieciešamos pierādījumus, kas sevī iekļauj vismaz identificējamās personas vārdu, uzvārdu, personas kodu un uzrādītā personas apliecinošā dokumenta datus (piemēram, pases sērija, numurs, izdevējs, izdevējvalsts).

3.2.3.5. Fizisku personu identifikāciju veic Reģistrācijas institūcijas un tās personāls, kam piešķirtas Uzticamās lomas.

3.2.3.6. Individuālās identitātes validāciju, kas attiecas uz pakalpojumu “eZīmogs+ mākonī” veic LVRTC.

3.3. **Atslēgu atjaunošanas pieprasījumu identifikācija un validācija**

3.3.1. Skatīt šīs politikas 3.2. punktu.

3.4. **Atsaukšanas pieprasījumu identifikācija un validācija**

3.4.1. Pakalpojuma “eZīmogs+ mākonī” sertifikāta atsaukšanu var pieprasīt šādas personas:

3.4.1.1. sertifikāta pieteikumā norādītais abonenta autorizētais pārstāvis vai pilnvarotā persona;

3.4.1.2. Uzraudzības iestādes vai datu aizsardzības uzraudzības iestādes pilnvarots pārstāvis;

3.4.1.3. pilnvarots valsts ierēdnis nolūkā veikt pirmstiesas kriminālo izmeklēšanu un novērst tālākus noziegumus;

3.4.1.4. UPS.

3.4.2. Atsaukšanas pieprasījuma pieteikumu iespējams iesniegt pašapkalpošanās portālā www.eparaksts.lv vai nosūtot e-pastā (parakstot ar kvalificētu elektronisko parakstu), vai apmeklējot reģistrācijas institūciju.

3.4.3. RA jāidentificē pieteicēju un viņa tiesības iesniegt pieteikumu. Pēc sekmīgas identifikācijas RA jāreģistrē pieteikumu.

3.4.4. UPS jāatsauc sertifikātu pēc tam, kad RA ir reģistrējis atsaukšanas pieteikumu.

3.4.5. Laiks starp sertifikāta atsaukšanas reģistrāciju un lēmuma par tā statusa izmaiņu paziņošanu visām atkarīgajām pusēm nedrīkst pārsniegt 24 stundas.

4. Sertifikāta dzīves cikla darbības prasības

4.1. **Sertifikātu pieteikums**

4.1.1. Tiek pieņemti tikai parakstīti pieteikumi.

4.1.2. Pieteikšanās process “eZīmogs+ mākonī” pakalpojuma saņemšanai:

4.1.2.1. jāaizpilda pieteikums UPS mājaslapā www.eparaksts.lv vai fiziskā klātbūtnē reģistrācijas institūcijā. Pieteikumā jānorāda organizācijas, kas piesākās pakalpojumam “eZīmogs+ mākonī” rekvizīti.

4.1.2.2. Organizācijas un pilnvarotā pārstāvja identifikācijas pārbaudes jāveic atbilstoši šīs politikas 3.2. punktā noteiktajam.

4.1.2.3. Jāpārbauda pieteicēja tiesības pieteikties un saņemt elektroniskā zīmoga sertifikātu.

4.1.2.4. UPS var veikt papildus pārbaudes un iesniegto datu izmaiņu monitoringu pret autoritatīviem reģistriem.

4.1.2.5. Jānorāda pieteikuma parakstīšanas veids – klātienē RA vai elektroniski ar kvalificētu elektronisko parakstu.

4.1.2.6. Jāparaksta pieteikums. Pieteikumu paraksta uzņēmuma paraksttiesīgā persona vai persona ar atbilstošu pilnvarojumu.

4.2. **Sertifikātu pieteikuma apstrāde**

4.2.1. Visus “eZīmogs+ mākonī” pakalpojumu pieteikumus un pieteicējus jāpārbauda reģistrācijas institūcijai.

4.2.2. Visus “eZīmogs+ mākonī” pakalpojumu pieteikumus apstrādā reģistrācijas operators un apstiprina reģistrācijas amatpersona.

4.2.3. UPS neizsniedz sertifikātu, ja sertifikāta pieprasījums neatbilst piemērojamajos līgumos noteiktajām tehniskajām prasībām.

4.2.4. Ja UPS atsakās izsniegt sertifikātu, par to tiek paziņots personai, kura pieprasīja sertifikātu.

4.2.5. Visus pieteikumus UPS apstrādā 5 (piecu) darba dienu laikā.

4.3. **Sertifikātu izsniegšana**

4.3.1. UPS veic pret sertifikātu viltošanu vērstus pasākumus un gadījumos, kad UPS ģenerē abonenta atslēgu, šādu datu ģenerēšanas procesa laikā garantē to konfidencialitāti.

4.3.2. Sertifikāta izsniegšanas procedūra tiek droši sasaistīta ar saistīto reģistrāciju, sertifikāta atjaunošanu vai atslēgas maiņu, ieskaitot visu abonentam ģenerētu publisku atslēgu nodrošināšanu.

4.3.3. Visi sertifikāti tiek izsniegti atbilstoši sertifikātu profiliem.

4.3.4. Pieteikšanās process “eZīmogs+ mākonī” sertifikāta saņemšanai;

4.3.4.1. Abonents pēc pieteikuma apstiprināšanas autentificējas Pakalpojuma sniedzēja mājaslapā, izmantojot kvalificētu paaugstinātas drošības elektroniskās identifikācijas līdzekli;

4.3.4.2. Abonents pievieno Lietotājus, kas ir tiesīgi veikt sertifikāta “eZīmogs+ mākonī” pieprasījuma ģenerēšanu;

4.3.4.3. Lietotājs autentificējoties Pakalpojumu sniedzēja mājaslapā ar kvalificētu paaugstinātas drošības elektroniskās identifikācijas līdzekli izveido Paroli atslēgām, pēc kā tiek uzģenerētas eZīmogs+ mākonī” sertifikāta atslēgas un izsniegts jauns sertifikāts.

4.4. **Sertifikātu akceptēšana**

4.4.1. Pirms līgumattiecību uzsākšanas ar abonentu UPS informē abonentu par Uzticamības pakalpojumu vispārējiem noteikumiem.

4.4.2. UPS publicē Uzticamības pakalpojumu vispārējos noteikumus UPS mājaslapā www.eparaksts.lv.

4.4.3. UPS reģistrē parakstīto līgumu ar abonentu.

4.5. **Atslēgu un sertifikātu lietošana**

4.5.1. Galvenie sertifikāta lietošanas nosacījumi aprakstīti šīs politikas 1.4. punktā.

4.5.2. Abonentam jāievēro līgumā, Uzticamības pakalpojumu vispārējos noteikumos, šajā politikā un [CPS] noteiktos abonenta pienākumus.

4.5.3. Visas abonenta atslēgas jāģenerē, izmantojot [ETSI TS 119 312] standartā noteikto atslēgu garumu un algoritmu.

4.5.4. Abonentam nekavējoties jāinformē UPS, ja līdz sertifikātā norādītā derīguma termiņa beigām iestājas kāds no minētajiem apstākļiem:

4.5.4.1. Abonenta privātā atslēga tiek pazaudēta, nozagta, vai arī pastāv varbūtība, ka apdraudēts atslēgas drošums;

4.5.4.2. aktivācijas datu (piem., Parole) drošuma apdraudējuma vai citu iemeslu dēļ zudusi kontrole pār abonenta privāto atslēgu;

4.5.4.3. pastāv neprecizitātes vai izmaiņas sertifikāta saturā, par ko ziņots abonentam.

4.6. **Sertifikātu atjaunošana**

4.6.4. UPS nenodrošina sertifikāta atjaunošanu “eZīmogs+ mākonī” pakalpojuma sertifikātiem, kuru atslēgas ģenerētas QSCD.

4.7. **Sertifikātu jaunizdošana**

4.7.1. Sertifikātu jaunizdošanas process tiek veikts atbilstoši [CPS] 3.2., 4.1., 4.2., 4.3., 4.4. un 4.7. punktu prasībām.

4.7.2. Sertifikātu jaunizdošanas gadījumā, vecie sertifikāti tiek atsaukti.

4.8. **Sertifikātu modificēšana**

4.8.1. Sertifikātu modificēšana var tikt veikta tikai pēc veiksmīgas Abonenta personas identifikācijas, izmantojot fizisku identitātes pārbaudi vai digitālu autentifikācijas metodi.

4.8.2. Ja tiek mainīti kādi sertifikātā iekļautie nosaukumi vai atribūti vai arī tajos ir kļūdas, nepareizie sertifikāti tiek atsaukti, reģistrācijas informācija tiek pārbaudīta, reģistrēta, saskaņota ar abonentu šīs politikas noteiktajā kārtībā.

4.9. **Sertifikātu atsaukšana un apturēšana**

4.9.1. UPS laikus jāatsauc sertifikātus, pamatojoties uz pilnvarotiem un apstiprinātiem sertifikātu atsaukšanas pieprasījumiem.

4.9.2. UPS jāatsauc sertifikātus, ja pastāv kāds no tālāk minētajiem apstākļiem:

4.9.2.1. saņemts un apstiprināts atsaukšanas pieteikums;

4.9.2.2. Abonenta vai UPS CA privātās atslēgas drošums ir apdraudēts vai abonents vai trešā puse pārkāpusi datu lietošanas noteikumus;

4.9.2.3. izdots likumīgs vai administratīvs rīkojums atsaukt sertifikātu;

4.9.2.4. juridiskās personas likvidācija;

4.9.2.5. notikušas izmaiņas datos, kas iesniegti sertifikāta iegūšanai, vai arī mainījušies apstākļi, kuru pārbaude bijusi pamatā sertifikāta izsniegšanai;

4.9.2.6. viena no pusēm nepilda savus pienākumus;

4.9.2.7. konstatēta kļūda sertifikāta izsniegšanas procedūrā, vai nu nav ticis

izpildīts kāds no priekšnoteikumiem, vai arī sertifikāta izsniegšanas laikā radušos tehnisku problēmu dēļ;

4.9.2.8. tehniska kļūme sertifikātu vai saistītās dokumentācijas izsniegšanā un vai izplatīšanā;

4.9.2.9. no sertifikāta pieprasīšanas līdz tā saņemšanai pagājuši vismaz trīs mēneši.

4.9.3. Informāciju par atsaukšanas pieprasītājiem un pieejamajiem atsaukšanas pieteikumu apstrādes kanāliem skatīt šīs politikas 3.4. punktā.

4.9.4. Paziņojumi par sertifikāta atsaukšanu jānosūta abonentam.

4.9.5. Visas atkarīgās puses var pārbaudīt sertifikāta statusu publicētajos CRL vai ar UPS nodrošinātā OCSP pakalpojuma starpniecību.

4.10. **Sertifikātu statusa pakalpojumi**

4.10.1. UPS nodrošina atsaukšanas statusa informāciju ar publicēto CRL vai OCSP pakalpojuma starpniecību atbilstoši [CPS] 2.1. punktā noteiktajam pieejamības režīmam.

4.10.2. Atsaukšanas statusa informācija ir publiski un starptautiski pieejama.

4.11. **Sertifikātu izmantošanas beigas**

4.11.1. Kad beidzas sertifikāta derīguma termiņš vai sertifikāts ticis atsaukts, tas vairs nav derīgs lietošanai.

4.12. **Atslēgu nodošana glabāšanā trešajai pusei un atjaunošana**

4.12.1. Nav atļauta.

5. Infrastruktūras, vadības un darbības kontroles

5.1. **Fiziskās drošības kontroles**

5.1.1. Aprakstītas [CPS] 5.1. punktā.

5.2. **Procesuālās kontroles**

5.2.1. Aprakstītas [CPS] 5.2. punktā.

5.3. **Personāla kontroles**

5.3.1. Aprakstītas [CPS] 5.3. punktā.

5.4. **Audita reģistrācijas procedūras**

5.4.1. Aprakstītas [CPS] 5.44. punktā.

5.5. **Ierakstu arhīvs**

5.5.1. Aprakstītas [CPS] 5.5. punktā.

5.6. **Atslēgu aizvietošana**

5.6.1. Aprakstītas [CPS] 5.6. punktā.

5.7. **Kompromitējums un pēcavārijas atjaunošana**

5.7.1. Aprakstītas [CPS] 5.7. punktā.

5.8. **CA darbības izbeigšana**

5.8.1. Aprakstītas [CPS] 5.8. punktā.

6. Tehniskās drošības kontroles

6.1. **Atslēgu pāra ģenerēšana**

6.1.1. Pakalpojumu “eZīmogs+ mākonī” abonenta atslēgas ģenerējamas atbilstoši [ETSI TS 119 312] noteiktajām minimālajām algoritma un atslēgas garuma rekomendācijām.

6.1.2. Atslēgas pakalpojuma “eZīmogs+ mākonī” sertifikātiem, kas izsniegti saskaņā ar QCPl-qscd, tiek ģenerētas tikai QSCD.

6.1.3. “eZīmogs+ mākonī” sertifikāta atslēgas ģenerē LVRTC, atslēgas tiek ģenerētas vidē, ko nodrošina uzticamības pakalpojumu sniedzējs un parakstītājs ir vienīgais, kurš pilnībā kontrolē sava elektroniskā paraksta un ar to saistītā sertifikāta izveides vidi.

6.1.4. “eZīmogs+ mākonī” atslēgas tiek glabātas HSM iekārtā, kas konfigurēta atbilstoši droša paraksta radīšanas ierīces vadlīnijām.

6.1.5. Atļautos atslēgu pielietojumus nosaka atbilstoši [Sertifikāta profilā] aprakstītajam.

6.2. **Privātās atslēgu aizsardzības un kriptogrāfijas moduļa tehniskie aizsargpasākumi**

6.2.1. Atslēgas tiek ģenerētas ierīcē, kas sertificēta atbilstoši [eIDAS regulai] un [CEN EN 419 211].

6.2.2. Abonents ir atbildīgs par savu privāto atslēgu drošības nodrošināšanu un pārvaldību tiktāl, cik tas ir Abonenta kontrolē.

6.3. **Citi atslēgu pārvaldības aspekti**

6.3.1. Abonenta sertifikātu derīguma termiņš nepārsniegs divus (2) gadus.

6.4. **Aktivizēšanas dati**

6.4.1. UPS nedrīkst glabāt aktivizēšanas datu kopijas.

6.4.3. Abonentiem ir jānodrošina savu privāto atslēgu aktivēšanas datu (Paroles) aizsardzība.

6.4.4. Paroles garumam jābūt vismaz: 6 ciparu vai burtu kombinācija .

6.5. **Datoru drošības kontroles**

6.5.1. UPS datoru drošības kontroles aprakstītas [CPS] 6.5. punktā.

6.5.2. Abonents ir atbildīgs par savā pārvaldībā esošo ierīču un iekārtu pienācīgu aizsardzību.

6.5.3. Pakalpojuma sniedzēja uzticamas elektronisko parakstu sertifikātu pārvaldības IT sistēmas ir sertificētas atbilstoši standarta ISO 15408 prasībām.

6.6. **Dzīves cikla tehniskās kontroles**

6.6.1. UPS dzīves cikla tehniskās kontroles aprakstītas [CPS] 6.6. punktā.

6.6.2. Nav uz abonentiem attiecināmu noteikumu.

6.7. **Tīkla drošības kontroles**

6.7.1. UPS dzīves cikla tehniskās kontroles aprakstītas [CPS] 6.7. punktā.

6.7.2. Nav uz abonentiem attiecināmu noteikumu.

6.8. **Laika zīmogošana**

6.8.1. Neattiecas uz šī dokumenta darbības jomu.

7. Sertifikātu, CRL un OCSP profili

7.1. **Sertifikāta profils**

7.1.1. Sertifikātam jāatbilst [Sertifikāta profilā] definētajam profilam.

7.2. **CRL profils**

7.2.1. CRL jāatbilst [Sertifikāta profilā] definētajam profilam.

7.3. **OCSP profils**

7.3.1. OCSP atbildēm jāatbilst [Sertifikāta profilā] definētajam profilam.

8. Atbilstības audits un citi novērtējumi

8.1. Aprakstīts [CPS] 8. punktā.

9. Citi uzņēmuma darbības un likumdošanas jautājumi

9.1. **Maksājumi**

9.1.1. Aprakstīta [CPS] 9.1. punktā.

9.2. **Finansiālā atbildība**

9.2.1. Aprakstīta [CPS] 9.2. punktā.

9.3. **Biznesa informācijas konfidencialitāte**

9.3.1. Aprakstīta [CPS] 9.3. punktā.

9.4. **Fizisko personu datu informācijas privātums**

9.4.1. Aprakstīts [CPS] 9.4. punktā.

9.5. **Intelektuālā īpašuma tiesības**

9.5.1. Aprakstītas [CPS] 9.5. punktā.

9.6. **Pārstāvības un garantijas**

9.6.1. Aprakstīti [CPS] 9.6. punktā.

9.7. **Garantijas atrunas**

9.7.1. Aprakstītas [CPS] 9.7. punktā.

9.8. **Atbildības ierobežojumi**

9.8.1. Aprakstīti [CPS] 9.8. punktā.

9.9. **Atlīdzība**

9.9.1. Aprakstīta [CPS] 9.9. punktā.

9.10. **Termiņi un darbības izbeigšana**

9.10.1. Šī politika ir spēkā līdz brīdim, kad tā tiek aizvietota ar jaunu versiju vai tās darbība tiek izbeigta CA likvidācijas dēļ, vai pakalpojumu sniegšana tiek izbeigta un visi sertifikāti kļūst nederīgi.

9.10.2. Darbības izbeigšanas gadījumā LVRTC nodrošinās klientu un iesaistīto pušu informētību.

9.11. **Individuāli paziņojumi un saziņa ar dalībniekiem**

9.11.1. Aprakstīti [CPS] 9.11. punktā.

9.12. **Grozījumi**

9.12.1. Aprakstīti šīs politikas 1.5.3. punktā;

9.12.2. OID mainās, kad mainās šīs politikas darbības joma vai tiek ieviests jauns sertifikāts.

9.13. **Domstarpību risināšanas kārtība**

9.13.1. Aprakstīti [CPS] 9.13. punktā.

9.14. **Piemērojamie normatīvie akti**

9.14.1. Aprakstīta [CPS] 9.14. punktā.

9.15. **Atbilstība piemērojamiem normatīvajiem aktiem**

9.15.1. Aprakstīta [CPS] 9.15. punktā.

9.16. **Dažādas prasības**

9.16.1. Nav noteikumu.

9.17. Citas prasības

9.17.1. Citu noteikumu nav.

10. Noslēguma noteikumi

10.1. “Uzticamības pakalpojumu “eZīmogs+ mākonī” sniegšanas politikā” tiek veikti grozījumi, mainoties saistošajiem normatīvajiem aktiem, kā arī, pilnveidojot LVRTC kvalitātes pārvaldības sistēmu.

10.2. “Uzticamības pakalpojumu “eZīmogs+ mākonī” sniegšanas politikas” izmaiņu vadību nodrošina ePakalpojumu daļa.

10.3. “Uzticamības pakalpojumu “eZīmogs+ mākonī” sniegšanas politika” stājas spēkā ar tā apstiprināšanu LVRTC Valdes sēdē Valdes lēmumā noteiktajā kārtībā.

10.4. “Uzticamības pakalpojumu “eZīmogs+ mākonī” sniegšanas politikas” spēkā esošā versija tiek uzturēta DVS