Uzticamības pakalpojuma “eParaksts karte+” sniegšanas
POLITIKA

SAGATAVOJA: ePakalpojumu daļas vadītājs

NOSŪTĪTS: PUBLISKS

Saistītie dokumenti:

1. [CEN EN 419 211] Aizsardzības profili droša paraksta izveidošanas ierīcei
2. Elektronisko dokumentu likums
3. [ETSI TS 119 312] Elektroniskie paraksti un infrastruktūras (ESI); kriptogrāfijas kompleksi
4. Eiropas Komisijas 2015. gada 8.septembra Īstenošanas regula (ES) 2015/1502, 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
5. [eIDAS regula] Eiropas Parlamenta un Padomes 2014.gada 23.jūlija Regula (ES) Nr.910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK
6. [FPEIL] Fizisko personu elektroniskās identifikācijas likums
7. [MK not. 558] Ministru kabineta 2017.gada 19. septembra noteikumi Nr.558 "Noteikumi par kvalificēta vai kvalificēta paaugstinātas drošības elektroniskās identifikācijas pakalpojuma sniegšanas informācijas sistēmu, iekārtu un procedūru drošības aprakstā norādāmo informāciju"
8. [MK not. 560] Ministru kabineta 2017.gada 19. septembra noteikumi Nr.560 "Noteikumi par kvalificēta un kvalificēta paaugstinātas drošības elektroniskās identifikācijas pakalpojuma sniedzēja un tā sniegtā pakalpojuma tehniskajām un organizatoriskajām prasībām"
9. [ETSI EN 319 411-1] Politika un drošības prasības Uzticamības pakalpojumu sniedzējiem, kuri izdod sertifikātus. 1.daļa. Vispārējās prasības
10. [ETSI EN 319 411-2] Politika un drošības prasības Uzticamības pakalpojumu sniedzējiem, kuri izdod sertifikātus. 2.daļa. Prasības uzticamības pakalpojumu sniedzējiem, kuri izsniedz ES kvalificētus sertifikātus
11. Privātuma politika
12. Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu PROFILU APRAKSTS
13. [CPS] Latvijas Valsts radio un televīzijas centra Uzticamības pakalpojumu sniegšanas noteikumi
14. Uzticamības pakalpojumu vispārējie noteikumi

IZMAIŅU VĒSTURE:

Pārskatītā varianta nr.	**Spēkā stāšanās datums**	**Izmaiņu kopsavilkums**
01.0	17.05.2017.	Sākotnējā versija
01.1.	01.07.2017.	Veiktas izmaiņas detalizējot produktu un tā prasības
01.2	15.05.2018	Politika sasaistīta ar Fizisko personu elektroniskās identifikācijas likumu un saistītajiem Ministru Kabineta noteikumiem. Veiktas izmaiņas definīcijās. Precizēti 1.1.7. un 9.4. punkti. Papildināti 1.1.3., 1.5.1. un 4.9.6. punkti. Laboti 1.4.2.2., 3.2.3. un 4.1.3. punkti.
01.3	19.11.2019	Redakcionāli labojumi visā dokumentā

VĪZAS:

Amats	**Vārds, uzvārds**	**Paraksts**	**Datums**
Komercdepartamenta direktors	Mārcis Dzenis	Parakstīts ar drošu elektronisko parakstu	Laika zīmogs
Iekšējā audita un kvalitātes vadības daļas vadītāja	Irēna Dumpe	Parakstīts ar drošu elektronisko parakstu	Laika zīmogs
Cilvēkresursu attīstības daļas vadītāja	Jevgeņija Vološina	Parakstīts ar drošu elektronisko parakstu	Laika zīmogs

PARAKSTA:

Amats	**Vārds, uzvārds**	**Paraksts**	**Datums**
ePakalpojumu daļas vadītājs	Kārlis Siliņš	Parakstīts ar drošu elektronisko parakstu	Laika zīmogs

SATURS

1. Ievads

1.1. Pārskats

1.1.1. Šis dokuments “Uzticamības pakalpojuma “eParaksts karte+” sniegšanas politika” nosaka noteiktas procesuālās un darbības prasības, kādas valsts akciju sabiedrība “Latvijas Valsts radio un televīzijas centrs” ievēro un kuru ievērošanu prasa no institūcijām, izsniedzot un pārvaldot pakalpojuma “eParaksts karte+” saistītos sertifikātus.

1.1.2. Šie sertifikāti sekmē elektroniskā paraksta izmantošanu un elektronisko identifikāciju fiziskām personām. Sertifikāti tiek vienmēr izdoti pa pāriem – katra “eParaksts karte+” satur vienu autentifikācijas sertifikātu un vienu kvalificētu elektroniskā paraksta sertifikātu un to atbilstošās privātās atslēgas..

1.1.3. LVRTC darbību “eParaksts karte+” sertifikātu izsniegšanā regulē [eIDAS regula], [FPEIL], [MK not. 558], [MK not. 560] un saistītie standarti.

1.1.4. Šī politika kvalificētu elektronisko parakstu sertifikātiem balstās uz [ETSI EN 319 411-2] standartā noteikto QCP-n-qscd politiku un autentifikācijas sertifikātiem balstās uz [ETSI EN 319 411-1] standartā noteikto NCP+ politiku.

1.1.5. 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):

1.1.5.1. [ETSI EN 319 411-2];

1.1.5.2. [ETSI EN 319 411-1];

1.1.5.3. šī politika;

1.1.5.4. [CPS].

1.1.6. 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 vadošā.

1.1.7. Šajā politikā aprakstītajam pakalpojumam “eParaksts karte+”:

1.1.7.1. Elektroniskā paraksta sertifikāti tiek izsniegti kā kvalificēta elektroniskā paraksta sertifikāti [eIDAS regulas] kontekstā;

1.1.7.2. Autentifikācijas sertifikāti tiek izsniegti kā elektroniskās identifikācijas līdzeklis [FPEIL] kontekstā. Elektroniskā identifikācijas līdzekļa līmenis tiek noteikts Uzraudzības iestādes uzturētā sarakstā.

1.2. Dokumenta nosaukums un identifikācija

1.2.1. Šī dokumenta nosaukums ir “Uzticamības pakalpojuma “eParaksts karte+” sniegšanas politika”.

1.2.2. Šī politika ir identificēta ar OID: 1.3.6.1.4.1.32061.2.1.5.1.

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	1

Apakštips (eParaksts karte+)	5
Versija	1

1.2.3. “eParaksts karte+” kvalificēta elektroniskā paraksta sertifikāti, kas izsniegti saskaņā ar QCP-n-qscd politiku, satur šādus OID:
1.2.3.1. 0.4.0.194112.1.2 (QCP-n-qscd);
1.2.3.2. 1.3.6.1.4.1.32061.2.1.5.1 (šī politika).
1.2.4. “eParaksts karte+” autentifikācijas sertifikāti, kas izsniegti saskaņā ar NCP+ politiku, satur šādus OID:
1.2.4.1. 0.4.0.2042.1.2 (NCP+);
1.2.4.2. 1.3.6.1.4.1.32061.2.1.5.1 (šī politika).

1.3. Publiskās atslēgas infrastruktūras dalībnieki

1.3.1. Sertifikācijas institūcijas
1.3.1.1. Aprakstītas [CPS] 1.3.2.punktā.
1.3.2. Reģistrācijas institūcijas
1.3.2.1. Šīs politikas ietvaros reģistrācijas institūcija ir :
1.3.2.1.1. valsts akciju sabiedrība “Latvijas Valsts radio un televīzijas centrs” pakalpojuma “eParaksts karte+” un ar tām saistītu sertifikātu administrēšanai LVRTC personālam.
1.3.2.1.2. Rīgas Dome, kas rīkojas LVRTC reģistrācijas institūcijas vārdā, pakalpojuma “eParaksts karte+” un ar tām saistītu sertifikātu administrēšanai Rīgas domes personālam.
1.3.2.2. Reģistrācijas institūcija identificē pieteicējus un pārbauda dokumentāciju, kas garantē sertifikātos redzamo datu kvalitāti, un validē un apstiprina pieprasījumus par sertifikātu izsniegšanu, atsaukšanu un atjaunošanu.
1.3.3. Abonenti
1.3.3.1. Abonents saskaņā ar šo politiku ir izdotā sertifikāta subjekts.
1.3.3.2. Individuālais abonenta nosaukums ir sertifikāta lauks, kas precīzi identificē Abonentu.Abonenti var būt tikai fiziskas personas kas ir Valsts akciju sabiedrība “Latvijas Valsts radio un televīzijas centrs” vai Rīgas Dome darbinieki.
1.3.4. Atkarīgās puses
1.3.4.1. Atkarīgās puses ir juridiskas vai fiziskas personas, kuras pieņem lēmumus, pamatojoties uz pakalpojuma “eParaksts karte+” radītiem elektroniskajiem parakstiem vai saistītā autentifikācijas sertifikāta pielietojumu.

1.4. Sertifikātu pielietojums

1.4.1. Sertifikāta atbilstoša lietošana
1.4.1.1. Pakalpojuma “eParaksts karte+” kvalificēta elektroniskā paraksta sertifikāti tiek izmantoti kvalificēta elektroniskā paraksta radīšanai, pamatojoties uz kvalificēta elektroniskā paraksta sertifikātu, kas ir pievienots vai loģiski saistīts ar citiem datiem elektroniskā formā, lai nodrošinātu pēdējā no minētajiem izcelsmi un integritāti.
1.4.1.2. Pakalpojuma “eParaksts karte+” autentifikācijas sertifikāti tiek izmantoti abonenta autentifikācijai tīmeklī vai citās datu apstrādes sistēmās.
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 paraksta sertifikāta izmantošana dokumentu parakstīšanai, kas var radīt nevēlamas sekas (tai skaitā šādu dokumentu parakstīšanai sistēmu testēšanas laikā);
1.4.2.1.4. elektroniskā paraksta sertifikāta izmantošanu automatizētā veidā;
1.4.2.1.5. Abonenta privātās atslēgas nodošana trešajām pusēm.
1.4.2.2. Abonenta autentifikācijas sertifikāts nedrīkst tikt izmantots, lai radītu [eIDAS regulas] prasībām atbilstošus kvalificētus elektroniskos parakstus.

1.5. Politikas administrēšana

1.5.1. Šo politiku pārvalda valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs", kas darbojas kā uzticamības un elektroniskās identifikācijas pakalpojumu sniedzējs atbilstoši šai politikai.

1.5.2. Kontaktinformācija:

VAS "Latvijas Valsts radio un televīzijas centrs"	
Adrese	Ērgļu iela 14, Rīga, LV – 1012, Latvija
Uzticamības un elektroniskās identifikācijas pakalpojumu palīdzības dienests	
Tālrunis	+371 67 108 787
E-pasts	eparaksts@eparaksts.lv
Ofiss	
Tālrunis	+371 67 198 704
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 "Izmaiņu pārvaldība", 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 Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja mājaslapā www.eparaksts.lv.
1.5.3.3. Visus grozījumus un šīs politikas galīgo versiju apstiprina valsts akciju sabiedrības "Latvijas Valsts radio un televīzijas centrs" valde.

1.6. Termini un saīsinājumi

1.6.1. Termini

Termins	**Skaidrojums**
Atsaukšana	Izsniegto sertifikātu neatgriezeniska statusa maiņa, kas norāda, ka sertifikāti vairāk nav izmantojami. Atsaukšana

	šajā dokumentā iekļauj sevī arī elektroniskās identifikācijas līdzekļa (autentifikācijas sertifikāta) darbības izbeigšanu.
Autoritatīvs avots	Jebkura veida avots, uz kuru var paļauties, ka tas sniedz precīzus datus, informāciju un/vai pierādījumu, ko var izmantot identitātes pierādīšanai;
Pakalpojuma sniedzējs	Valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs", vienotais reģistrācijas Nr. 40003011203, Ērgļu iela 14, Rīga, Latvija, LV-1012, kas darbojās kā Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzējs
Politika	Šajā dokumentā – "Uzticamības pakalpojuma "eParaksts karte+" 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

Saīsinājums	**Skaidrojums**
CA	Sertifikācijas institūcija
CPS	Uzticamības pakalpojumu sniedzēja noteikumi
CRL	Atsaukto sertifikātu saraksts
eIDAS	Eiropas Parlamenta un padomes regula (ES) Nr. 910/2014 "par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK", 2014.gada 23.jūlijs
ES	Eiropas Savienība
ETSI	Eiropas Telekomunikācijas standartu institūts
LVRTC	Valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs", vienotais reģistrācijas Nr. 40003011203, Ērgļu iela 14, Rīga, Latvija, LV-1012
MK	Ministru kabinets
NCP+	Paplašināta normalizētā sertifikātu politika, kas noteikta [ETSI EN 319 411-1] Politika un drošības prasības Uzticamības pakalpojumu sniedzējiem, kuri izdod sertifikātus. 1.daļa. Vispārējās prasības
OCSP	Tiešsaistes sertifikātu statusa protokols
OID	Globālais objekta identifikators
PIN	Personas identifikācijas numurs
PKI	Publisko atslēgu infrastruktūra
PUK	PIN atbloķēšanas atslēga
RA	Sertifikātu reģistrēšanas institūcija
RD	Rīgas Dome
QCP-n-qscd	Politika fiziskai personai izsniegta ES kvalificēta sertifikāta jomā gadījumos, kad privātā atslēga un saistītais sertifikāts atrodas uz QSCD
QSCD	Kvalificēta elektroniskā paraksta/zīmoga radīšanas ierīce

2. Publicēšanas un repozitorija pienākumi

2.1. Repozitoriji

2.1.1. Atbilstoši aprakstam [CPS] 2.1.punktā.

2.2. Sertifikācijas informācijas publicēšana

2.2.1. Šī politika ir publicēta Pakalpojumu sniedzēja mājaslapā: www.eparaksts.lv.

2.3. Publicēšanas laiks vai biežums

2.3.1. Atbilstoši aprakstam [CPS] 2.3.punktā.

2.4. Piekļuves kontrole repozitorijiem

2.4.1. Atbilstoši aprakstam [CPS] 2.5.punktā.

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. Visām vērtībām sertifikāta turētāja (subject – angļu val.) laukā jābūt jēgpilnām.

3.1.3. Abonentu anonimitāte un pseidonimitāte:

3.1.3.1. Pakalpojuma sniedzējs šādu pakalpojumu nepiedāvā.

3.1.4. Nosaukumu unikalitāte:

3.1.4.1. Pakalpojuma sniedzējs 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. Atslēgas ģenerē reģistrācijas institūcija 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. Nav piemērojams.

3.2.3. Individuālās identitātes identifikācija un validācija

3.2.3.1. Individuālās identitātes validācija notiek:

3.2.3.1.1. fiziskās personas klātbūtnē kādā no Reģistrācijas institūcijām. Fiziska persona tiek identificēta pret Autoritatīvu avotu (piemēram, pase);

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

3.2.3.2. Identifikācijas laikā Pakalpojuma sniedzējam 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).

3.2.3.3. Fizisku personu identifikāciju veic Reģistrācijas institūcijas un tās personāls, kam piešķirtas Uzticamības lomas.

3.2.3.4. Individuālās identitātes autentifikāciju, kas attiecas uz pakalpojumu "eParaksts karte+" veic LVRTC.

3.3. Atslēgu atjaunošanas pieprasījumu identifikācija un validācija

3.3.1. Skat. šīs politikas 3.2.punktu.

3.4. Atsaukšanas pieprasījumu identifikācija un validācija

3.4.1. Abonenta sertifikāta atsaukšanu var pieprasīt šādas personas:
- 3.4.1.1. Abonents;
- 3.4.1.2. Pakalpojuma sniedzējs.

3.4.2. Pieteikumus atsaukšanas pieprasījumiem var iesniegt ar e-pasta starpniecību (parakstītus ar kvalificētu elektronisko parakstu) vai apmeklējot LVRTC vai RD.

3.4.3. LVRTC vai RD jāidentificē pieteicēju un viņa tiesības iesniegt pieteikumu. Pēc sekmīgas identifikācijas LVRTC vai RD jāreģistrē pieteikumu.

3.4.4. Pakalpojuma sniedzējam jāatsauc sertifikātu pēc tam, kad LVRTC vai RD 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. Identitātes validācija attiecas uz šīs politikas 3.2.punktu.

4.1.3. Pieteikšanās process "eParaksts karte+" pakalpojuma saņemšanai
- 4.1.3.1. Jāaizpilda pieteikums Pakalpojumu sniedzēja mājaslapā www.eparaksts.lv vai fiziskā klātbūtnē reģistrācijas institūcijā.
- 4.1.3.2. Pieteikuma veidošanas laikā Pakalpojumu sniedzējam jāveic šādas pārbaudes:
  - 4.1.3.2.1. personas datu pārbaude (Abonenta vārds, uzvārds, personas kods) pret autoritatīvu avotu fiziskas klātbūtnes gadījumā, vai pret kvalificēta paraksta atribūtiem gadījumos, ja pieteikums tiek parakstīts elektroniski;
  - 4.1.3.2.2. fiziskas klātbūtnes gadījumā uzrādītā personas apliecinošā dokumenta datus (dokumenta veids, numurs, derīguma termiņš, izdevējvalsts) jāpārbauda pret autoritatīvu avotu, piemēram, nederīgo dokumentu reģistru (dokumenta derīgums) vai Iedzīvotāju reģistru;
  - 4.1.3.2.3. saziņas kanāla verifikācija, primāri pārbaudot, vai pieteikumā norādītais mobilā telefona numurs ir pieteicēja pārvaldībā. Pārbaude tiek veikta ar vienreiz lietojama koda izsūtīšanu uz pieteikumā minēto numuru un saņemtā koda verifikāciju pieteikuma veidošanas brīdī.
- 4.1.3.3. Pakalpojumu sniedzējs var veikt papildus pārbaudes un iesniegto personas datu (Abonenta vārds, uzvārds, personas kods) izmaiņu uzraudzību pret autoritatīviem reģistriem.
- 4.1.3.4. Jāparaksta pieteikums.

4.2. Sertifikātu pieteikuma apstrāde:

4.2.1. Visus pieteikumus un pieteicējus jāpārbauda RA.
4.2.2. Visus pieteikumus apstrādā reģistrācijas operators un apstiprina reģistrācijas amatpersona.
4.2.3. Pakalpojumu sniedzējs neizsniedz sertifikātu, ja sertifikāta pieprasījums neatbilst piemērojamajos līgumos noteiktajām tehniskajām prasībām.
4.2.4. Ja Pakalpojumu sniedzējs atsakās izsniegt sertifikātu, par to tiek paziņots personai, kura to pieprasījusi.
4.2.5. Visus pieteikumus Pakalpojumu sniedzējs apstrādās saskaņā ar piemērojamiem tiesību aktiem un nolīgumiem.

4.3. Sertifikātu izsniegšana

4.3.1. Pakalpojumu sniedzējs veic pret sertifikātu viltošanu vērstus pasākumus un gadījumos, kad Pakalpojumu sniedzējs ģenerē Abonenta atslēgu pāri, 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 ir izsniegti saskaņā ar [Sertifikātu profiliem].
4.3.4. Pakalpojumu sniedzējs ģenerē Abonenta atslēgas QSCD, Abonenta privāto atslēgu saturošs QSCD tiek droši piegādāts reģistrētajam Abonentam.

4.4. Sertifikātu akceptēšana

4.4.1. Pirms līgumattiecību noslēgšanas Pakalpojumu sniedzējs informē Abonentu par Uzticamības pakalpojumu vispārējiem noteikumiem.
4.4.2. Pakalpojumu sniedzējs publicē Uzticamības pakalpojumu vispārējos noteikumus Pakalpojumu sniedzēja mājaslapā www.eparaksts.lv.
4.4.3. Pakalpojumu sniedzējs reģistrē parakstītu līgumu ar Abonentu.

4.5. Atslēgu pāra un sertifikātu lietošana

4.5.1. Galvenie sertifikāta lietošanas noteikumi 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 Pakalpojumu sniedzējs, 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. aktivizācijas datu (piem., PIN kods) 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

4.6.1. Pakalpojumu sniedzējam jāpārbauda atjaunojamā sertifikāta esamību un derīgumu, kā arī to, ka Abonenta identitāti un atribūtus apliecinošie dati joprojām ir derīgi.

4.6.2. Ja mainījušies kādi Uzticamības pakalpojumu vispārējie noteikumi un/vai citi nosacījumiem, par to tiek paziņots Abonentam un tiek parakstīts jauns līgums.
4.6.3. Pakalpojumu sniedzējs izsniedz jaunu sertifikātu, izmantojot Abonenta iepriekš sertificēto publisko atslēgu tikai tādā gadījumā, ja tās kriptogrāfiskā drošība joprojām ir pietiekama jaunā sertifikāta derīguma periodam un nav nekādu iemeslu uzskatīt, ka Abonenta privātās atslēgas drošums ticis apdraudēts, kā arī sertifikāts nav ticis atsaukts kāda drošības pārkāpuma dēļ.

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 atbilstoši [CPS] 3.2. punkta prasībām.
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. Pakalpojumu sniedzējam laikus jāatsauc sertifikātus, pamatojoties uz pilnvarotiem un apstiprinātiem sertifikātu atsaukšanas pieprasījumiem.
4.9.2. Pakalpojumu sniedzējam jāatsauc sertifikātus, ja notiek kāds no turpmāk minētajiem notikumiem:
- 4.9.2.1. saņemts un validēts atsaukšanas pieteikums;
- 4.9.2.2. abonenta vai Pakalpojumu sniedzēja 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. Notikušas izmaiņas datos, kas iesniegti sertifikāta iegūšanai, vai arī mainījušies apstākļi, kuru pārbaude bijusi pamatā sertifikāta izsniegšanai;
- 4.9.2.5. viena no pusēm nepilda savus pienākumus;
- 4.9.2.6. konstatēta kļūda sertifikāta izsniegšanas procedūrā, vai nav ticis izpildīts kāds no priekšnoteikumiem, vai arī sertifikāta izsniegšanas laikā radušos tehnisku problēmu dēļ;
- 4.9.2.7. tehniska kļūme sertifikātu vai saistītās dokumentācijas izsniegšanā un / vai izplatīšanā;
- 4.9.2.8. fiziskā persona ir sniegusi nepatiesas vai maldinošas ziņas par savu identitāti;
- 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, kad Pakalpojumu sniedzējs atsauc sertifikātu.

4.9.5. Visas atkarīgās puses var pārbaudīt sertifikāta statusu publicētajos CRL vai ar Pakalpojumu sniedzēja nodrošinātā OCSP pakalpojuma starpniecību.
4.9.6. Sertifikātu apturēšanas gadījumi ir aprakstīti [CPS] 4.9.6. punktā.

4.10. Sertifikātu statusa pakalpojumi

4.10.1. Pakalpojumu sniedzējs 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 publiska 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. Atslēgu nodošana glabāšanā trešajai pusei nav atļauta.

5. Operacionālās, fiziskās un pārvaldības kontroles

5.1. Fiziskās drošības kontroles

5.1.1. Aprakstīts [CPS] 5.1. punktā.

5.2. Procesuālas kontroles

5.2.1. Aprakstīts [CPS] 5.2. punktā.

5.3. Personāla kontroles

5.3.1. Aprakstīts [CPS] 5.3. punktā.

5.4. Audita reģistrācijas procedūras

5.4.1. Aprakstīts [CPS] 5.4. punktā.

5.5. Ierakstu arhīvs

5.5.1. Aprakstīts [CPS] 5.5. punktā.

5.6. Atslēgu aizvietošana

5.6.1. Aprakstīts [CPS] 5.6. punktā.

5.7. Kompromitējums un pēcavārijas atjaunošana

5.7.1. Aprakstīts [CPS] 5.7. punktā.

5.8. CA darbības izbeigšana

5.8.1. Aprakstīts [CPS] 5.8. punktā.

6. Tehniskās drošības kontroles

6.1. Atslēgu pāra ģenerēšana

6.1.1. Abonenta atslēgas ģenerējamas atbilstoši [ETSI TS 119 312] noteiktajām minimālajām algoritma un atslēgas garuma rekomendācijām.
6.1.2. Atslēgas kvalificēta elektroniskā paraksta sertifikātiem, kas izsniegtas saskaņā ar QCP-n-qscd, tiek ģenerētas tikai QSCD.
6.1.3. LVRTC ģenerētās atslēgas tiek nodotas Abonentam personīgi vai ar kurjeru, nogādājot tās slēgtā aploksnē.
6.1.4. Atļautos atslēgu pielietojumus nosaka atbilstoši [Sertifikāta profilā] aprakstītajam.

6.2. Privātās atslēgu aizsardzības un kriptogrāfijas moduļa tehniskie aizsargpasākumi:

6.2.1. QSCD ievietotie pakalpojuma “eParaksts karte+” kvalificēta elektroniskā paraksta sertifikāti izdoti saskaņā ar QCP-n-qscd politiku, atslēgas tiek ģenerētas ierīcē, kas sertificēta atbilstoši [eIDAS] un [CEN EN 419 211] standarta prasībām.

6.2.2. Abonents ir atbildīgs par savu privāto atslēgu drošības nodrošināšanu un pārvaldību.

6.2.3. Abonents ir atbildīgs par savu PIN kodu un viedkartes paturēšanu tikai savā kontrolē. Aizliegts nodot PIN kodus un/vai viedkarti trešajai personai.

6.2.4. Abonentam ir pienākums nekavējoties atsaukt savus sertifikātus, ja Abonenta PIN kodi un/vai viedkarte ir pazaudēta vai ir pamatotas aizdomas, ka sertifikāti ir tikuši izmantoti bez Abonenta ziņas un piekrišanas.

6.2.5. PIN kodu garumiem jābūt vismaz:

6.2.5.1. autentifikācijas atslēgai – 4 cipari;

6.2.5.2. paraksta atslēgai – 6 cipari.

6.2.6. PUK koda garumam jābūt vismaz 6 cipari.

6.3. Citi atslēgu pāra pārvaldības aspekti

6.3.1. Abonenta sertifikātu derīguma termiņš nepārsniegs piecus (5) gadus.

6.4. Aktivizēšanas dati

6.4.1. Abonenta atslēgas ģenerējis Pakalpojumu sniedzējs, aktivēšanas kodus (PIN and PUK) personīgi jānodod abonentam.

6.4.2. Abonentiem ir jānodrošina savu privāto atslēgu aktivēšanas datu aizsardzība.

6.5. Datu drošības kontroles

6.5.1. Pakalpojumu sniedzēja datora drošības pārbaudes aprakstītas [CPS] 6.5.punktā.

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

6.6. Dzīves cikla tehniskās kontroles

6.6.1. Pakalpojumu sniedzēja dzīves cikla tehniskās pārbaudes aprakstītas [CPS] 6.7.punktā.

6.6.2. Nav uz abonentiem attiecināmu noteikumu.

6.7. Tīkla drošības kontroles

6.7.1. Pakalpojumu sniedzēja tīkla drošības 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. Sertifikātu 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 izvērtējumi

8.1. Aprakstīts [CPS] 8.punktā.

9. Citi biznesa un juridiskie jautājumi

9.1. Maksājumi

9.1.1. Aprakstīts [CPS] 9.1.punktā.

9.2. Finansiālā atbildība

9.2.1. Aprakstīts [CPS] 9.2.punktā.

9.3. Biznesa informācijas konfidencialitāte

9.3.1. Aprakstīts [CPS] 9.3.punktā.

9.4. Fizisko personu datu informācijas privātums

9.4.1. Pakalpojuma sniedzējs nodrošina fizisko personu datu informācijas privātumu atbilstoši Privātuma politikā noteiktajam.

9.4.2. Privātuma politika ir publicēta Pakalpojuma sniedzēja mājaslapā www.eparaksts.lv.

9.5. Intelektuālā īpašuma tiesības

9.5.1. Aprakstīts [CPS] 9.5.punktā.

9.6. Pārstāvības un garantijas

9.6.1. Aprakstīts [CPS] 9.6.punktā.

9.7. Garantijas atrunas

9.7.1. Aprakstīts [CPS] 9.7.punktā.

9.8. Atbildības ierobežojumi

9.8.1. Aprakstīts [CPS] 9.8.punktā.

9.9. Atlīdzība

9.9.1. Aprakstīts [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. Aprakstīts [CPS] 9.11.punktā.

9.12. Grozījumi

9.12.1. Aprakstīts šīs politikas 1.5.3.punktā.

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

9.13. Domstarpību risināšanas kārtība

9.13.1. Aprakstīts [CPS] 9.13.punktā.

9.14. Piemērojamie normatīvie akti

9.14.1. Aprakstīts [CPS] 9.14.punktā.

9.15. Atbilstība piemērojamiem normatīvajiem aktiem

9.15.1. Aprakstīts [CPS] 9.15.punktā.

9.16. Dažādas prasības

9.16.1. Nav noteikumu.

9.17. Citas prasības

9.17.1. Nav citu noteikumu.