Uzticamības pakalpojuma “eParaksts” sniegšanas POLITIKA

SAGATAVOJA: ePakalpojumu daļas vadītājs

NOSŪTĪTS: Publisks

SAISTĪTIE DOKUMENTI:

1. [ETSI EN 419 211] Aizsardzības profili droša paraksta izveidošanas ierīcei
2. [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
3. Elektronisko dokumentu likums
4. [ETSI TS 119 312] Elektroniskie paraksti un infrastruktūras (ESI); kriptogrāfijas kompleksi
5. [FPEIL] Fizisko personu elektroniskās identifikācijas likums
6. 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
7. [Sertifikāta profils] Latvijas Valsts radio un televīzijas centra Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu apraksts
8. [CPS] Latvijas Valsts radio un televīzijas centra Uzticamības pakalpojumu sniegšanas noteikumi
9. [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"
10. [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"
11. [ETSI EN 319 411-1] Politika un drošības prasības Uzticamības pakalpojumu sniedzējiem, kuri izdod sertifikātus. 1.daļa. Vispārējās prasības
12. [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
13. Privātuma politika
14. Uzticamības pakalpojumu vispārējie noteikumi

IZMAIŅU VĒSTURE:

Pārskatītā varianta nr.	**Spēkā stāšanās datums**	**Izmaiņu kopsavilkums**
01.0	17.05.2017.	Sākotnējā versija
01.1	01.08.2017.	Veiktas izmaiņas detalizējot produktu un tā prasības
01.2	01.05.2018	Politika sasaistīta ar Fizisko personu elektroniskās identifikācijas likuma un saistītajiem Ministru Kabineta noteikumiem. Veiktas izmaiņas definīcijās. Precizēti 1.1.7. un 9.4. punkti. Papildināts ar 4.9.6. punktu.
01.3.	01.11.2019	Papildināts ar 1.1.8.punktu.
2.1	30.06.2020	Veiktas izmaiņas sakarā ar kvalificēta paraksta ieviešanu. Veikta OID versijas nomaiņa un šīs politikas versijas paaugstināšana. Precizēti un papildināti sekojoši punkti, 1.1.4, 1.2.2, 1.2.3, 1.2.4, 1.4.1.1, 1.6.2, 4.6. un 6.1.3.
2.2	11.01.2021	Papildināts 1.3.2.1. punkts ievērojot reģistrācijas institūciju tīkla paplašināšanu, iekļaujot Latvijas Zvērinātu notāru padomi un zvērinātus notārus, kas rīkojas LVRTC reģistrācijas institūcijas vārdā. Papildināts punkts 6.5.3 ar atsauci uz ISO 15408. Redakcionāli precizēti 3.2.3., 3.4.1, 3.4.2., 4.1.3.3., 9.4.1. punkti.

SATURS

1. Ievads

1.1. Pārskats:

1.1.1. Šis dokuments “Uzticamības pakalpojuma “eParaksts” 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” saistītos sertifikātus.

1.1.2. Šie sertifikāti sekmē elektroniskā paraksta izmantošanu un elektronisko identifikāciju fiziskām personām. Sertifikāti tiek vienmēr izdoti pa pāriem – katrs pakalpojums “eParaksts” satur vienu autentifikācijas sertifikātu “eParaksts mobile” mobilās ierīces atslēgu pārvaldības aplikācijā un vienu kvalificētu elektroniskā paraksta sertifikātu “eParakstsTX” risinājumā un to atbilstošās privātās atslēgas. Katra privātā atslēga tiek aizsargāta ar atsevišķiem aktivizēšanas datiem – PIN kodu.

1.1.3. LVRTC darbību “eParaksts” 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”:

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.

1.1.8. Autentifikācijas sertifikāta saistīto atslēgu pāra atbilstība Eiropas Savienības elektroniskās identifikācijas shēmu uzticamības līmeņiem:

1.1.8.1. “Augsts uzticamības līmenis”.

1.1.8.1.1. atslēgas tiek ģenerētas un pārvaldītas “trusted execution environment (TEE)” Android ierīču un “Secure Enclave (SE)” iOS ierīču drošajās vidēs (Atslēgas pēc noklusējuma tiek ģenerētas minētajās drošības vidēs ja mobila ierīce satur minētos aparatūras elementus) un

1.1.8.1.2. atslēgta biometriskā autentifikācija (tiek izmantots PIN kods).

1.1.8.2. “Būtisks uzticamības līmenis”.
1.1.8.2.1. atslēgas tiek ģenerētas un pārvaldītas speciālos Android vai iOS programmatūras konteineros (pēc noklusējuma visām mobilām ierīcēm, kurās nav TEE vai SE drošības vides), un/vai
1.1.8.2.2. ieslēgta biometriskā autentifikācija.

1.2. Dokumenta nosaukums un identifikācija

1.2.1. Šī dokumenta nosaukums ir “Uzticamības pakalpojuma “eParaksts” sniegšanas politika”.
1.2.2. Šī politika ir identificēta ar OID: 1.3.6.1.4.1.32061.2.1.3.2.

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”)	3
Versija	2

1.2.3. “eParaksts” kvalificēta elektroniskā paraksta sertifikāti, kas izsniegti saskaņā ar QCP-n-qscd politiku, satur šādus OID:
1.2.3.1. 0.4.0.194112.1.0 (QCP-n-qscd OID);
1.2.3.2. 1.3.6.1.4.1.32061.2.1.3.2 (šī politika).
1.2.4. “eParaksts” autentifikācijas sertifikāti, kas izsniegti saskaņā ar NCP politiku, satur šādus OID:
1.2.4.1. 0.4.0.2042.1.1 (NCP);
1.2.4.2. 1.3.6.1.4.1.32061.2.1.3.1 (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 RA ir:
1.3.2.1.1. Valsts akciju sabiedrība “Latvijas Valsts radio un televīzijas centrs” pakalpojuma “eParaksts” un ar to saistītu sertifikātu administrēšanai;
1.3.2.1.2. SIA “DPD Latvija”, kas rīkojas LVRTC reģistrācijas institūcijas vārdā;
1.3.2.1.3. Latvijas Zvērināto notāru padome un zvērināti notāri, kas rīkojas LVRTC reģistrācijas institūcijas vārdā;
1.3.2.1.4. Uzticamības pakalpojumu sniedzēja mājas lapa www.eparaksts.lv:
1.3.2.1.4.1. pakalpojuma “eParaksts” pieteikumu, kas parakstīti ar kvalificētu elektronisko parakstu, iesniegšana;

1.3.2.1.4.2. pakalpojuma “eParaksts” saistīto sertifikātu administrēšana.

1.3.2.2. RA 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. Abonenti saskaņā ar šo politiku var būt tikai fiziskas personas.

1.3.4. Atkarīgās puses:

1.3.4.1. Atkarīgās puses ir juridiskas vai fiziskas personas, kuras pieņem lēmumus, pamatojoties uz “eParaksts” radītiem elektroniskajiem parakstiem vai saistītā autentifikācijas sertifikāta pielietojumu.

1.4. Sertifikātu pielietojums

1.4.1. Sertifikāta atbilstoša lietošana:

1.4.1.1. “eParaksts” elektroniskā paraksta sertifikāti tiek izmantoti attālināta kvalificēta elektroniskā paraksta radīšanai. Kvalificēta elektroniskā paraksta ģenerēšanas un radīšanas vidi pārvalda uzticamības pakalpojumu sniedzējs un parakstītājs ir vienīgais, kurš pārvalda sava elektroniskā paraksta izveides vidi.

1.4.1.2. “eParaksts” 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. 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 vēsture", 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 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	Atsaukšana ir 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.
eParaksts	Pakalpojuma sniedzēja sniegts uzticamības pakalpojums kas satur elektroniskās identifikācijas līdzekli – autentifikācijas sertifikātu "eParaksts mobile" mobilās ierīces atslēgu pārvaldības aplikācijā un kvalificētu elektroniskā paraksta sertifikātu "eParakstsTX" risinājumā.
eParaksts mobile	Mobilā lietotne, ko izmanto identitātes apliecināšanai ar eParakstu digitālajā vidē autentificējoties portālos e-pakalpojumu izmantošanai.
eParakstsTX risinājums	Abonenta valdījumā esošs elektroniskā paraksta risinājums, kur elektroniskais paraksts parakstītāja vārdā tiek izveidots vidē, ko nodrošina uzticamības pakalpojumu sniedzējs un parakstītājs ir vienīgais, kurš *pilnībā* kontrolē sava elektroniskā paraksta izveides vidi.
eParakstsTX sertifikāts	Abonenta valdījumā esošs, pakalpojuma "eParaksts" kvalificēts elektroniskā paraksta sertifikāts, kas tiek izmantots eParakstsTX risinājumā elektroniskā paraksta radīšanai.
Pakalpojuma sniedzējs	LVRTC, kas darbojās kā Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzējs
Politika	Šajā dokumentā – "Uzticamības pakalpojuma "eParaksts" 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
HSM	Šifrēšanas šaurlietojumu ierīce (aparatūra), kas nodrošina šifrēšanas atslēgu aizsardzību
LVRTC	Valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs", vienotais reģistrācijas Nr. 40003011203, Ērgļu iela 14, Rīga, Latvija, LV-1012
NCP	Normalizēta sertifikātu politika
OCSP	Tiešsaistes sertifikātu statusa protokols
OID	Globālais objekta identifikators
PIN	Personas identifikācijas numurs
PKI	Publisko atslēgu infrastruktūra
RA	Sertifikātu reģistrēšanas institūcija
QCP-n-qscd	Politika fiziskai personai izsniegta ES kvalificēta sertifikāta jomā
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 Pakalpojuma 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. kad atslēgu pāri ir ģenerējis mobilās ierīces atslēgas konteiners, privātās atslēgas valdījumu demonstrē uzticama atslēgu pāra ģenerēšanas procedūra un sertifikāta izsniegšana. Procedūra sevī iekļauj vismaz šādas kontroles:

3.2.1.1.1. lietotāja izveidots autentifikācijas atslēgu aizsardzības PIN;

3.2.1.1.2. unikālo reģistrācijas kodu var iegūt tikai pēc fiziskas vai arī elektroniskas identifikācijas;

3.2.1.1.3. reģistrācijas vienreiz lietojamo kodu var saņemt tikai uz pieteikumā norādīto, verificēto mobilā tālruņa numuru vai e-pastu.

3.2.1.2. kad atslēgu pāri ģenerē reģistrācijas iestāde un atslēgas tiek saglabātas HSM (QSCD) iekārtā ko pārvalda Pakalpojuma sniedzējs, privātās atslēgas valdījumu demonstrē pamatojoties uz uzticamu HSM (QSCD) pārvaldību un uzticamu procedūru, kas garantē elektroniskā paraksta izveides vides uzticamību un to, ka parakstītājs ir vienīgais, kurš kontrolē sava elektroniskā paraksta izveides vidi. Procedūra sevī iekļauj vismaz šādas kontroles:

3.2.1.2.1. lietotājam ir jābūt elektroniski identificētam Pakalpojuma sniedzēja mājaslapā www.eparaksts.lv ar “eParaksts mobile” autentifikācijas rīku vai arī kādu no Pakalpojuma sniedzēja izsniegtām viedkartēm (QSCD);

3.2.1.2.2. lietotājam pašam ir jāiniciē eParakstsTX sertifikāta pieprasīšana;

3.2.1.2.3. pirms sertifikātu izsniegšanas Abonentam ir jāizveido savs eParakstaTX atslēgu aizsardzības PIN kods;

3.2.1.2.4. Abonents jebkurā laikā Pakalpojuma sniedzēja mājaslapā www.eparaksts.lv var iniciēt eParakstsTX atslēgu pārģenerēšanu un PIN koda nomaiņu.

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 validācijai jānotiek:

3.2.3.1.1. fiziskā klātbūtnē kādā no RA. Fiziska persona tiek identificēta pret Autoritatīvu avotu (personu apliecinošs dokuments);

3.2.3.1.2. izmantojot elektroniskos saziņas līdzekļus – 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 (sērija, numurs, izdevējs, izdevējvalsts).

3.2.3.3. Fizisku personu identifikāciju veic RA un tās personāls, kam piešķirtas Uzticamības lomas.
3.2.3.4. “eParaksts” izsniegšanu un ar tām saistītu sertifikātu administrēšanu veic LVRTC;.
3.2.3.5. Individuālās identitātes autentifikāciju, kas attiecas “eParaksts” 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;
3.4.2. Pieteikumus atsaukšanas pieprasījumiem var iesniegt ar e-pasta starpniecību (parakstītus ar kvalificētu elektronisko parakstu), apmeklējot LVRTC, RA vai Pakalpojuma sniedzēja mājaslapā www.eparaksts.lv savā profilā.
3.4.3. Pakalpojuma sniedzējam jāidentificē pieteicēju un viņa tiesības iesniegt pieteikumu. Pēc sekmīgas identifikācijas RA jāreģistrē pieteikumu.
3.4.4. Pakalpojuma sniedzējam jāatsauc sertifikātu pēc tam, kad Pakalpojuma sniedzējs 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 pakalpojuma “eParaksts” saņemšanai
4.1.3.1. Jāaizpilda pieteikums Pakalpojuma sniedzēja mājaslapā www.eparaksts.lv vai fiziskā klātbūtnē RA.
4.1.3.2. Pieteikuma veidošanas laikā Pakalpojuma 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. Pakalpojuma sniedzējs var veikt papildus pārbaudes un veic iesniegto personas datu (Abonenta vārds, uzvārds, personas kods) izmaiņu monitoringu pret autoritatīviem reģistriem.

4.1.3.4. Jānorāda pieteikuma parakstīšanas veids – klātienē, ar DPD kurjeru vai elektroniski ar kvalificētu elektronisko parakstu.
4.1.3.5. Abonentam jāiesniedz pašrocīgi parakstīts 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. Pakalpojuma sniedzējs neizsniedz sertifikātu, ja sertifikāta pieprasījums neatbilst piemērojamajos līgumos noteiktajām tehniskajām prasībām.
4.2.4. Ja Pakalpojuma sniedzējs atsakās izsniegt sertifikātu, par to tiek paziņots personai, kura pieprasīja sertifikāciju.
4.2.5. Visus pieteikumus Pakalpojuma sniedzējs apstrādās saskaņā ar piemērojamiem tiesību aktiem.

4.3. Sertifikātu izsniegšana

4.3.1. Pakalpojuma sniedzējs veic pret sertifikātu viltošanu vērstus pasākumus un gadījumos, kad Pakalpojuma 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. "eParaksts mobile" autentifikācijas sertifikāta izsniegšanas process:
4.3.4.1. Abonentam jālejupielādē un savā mobilā ierīcē jāuzstāda "eParaksts mobile" atslēgu pārvaldības aplikācija;
4.3.4.2. pēc pieteikuma pārbaudes un apstiprināšanas, abonents saņem uzģenerētu QR kodu, kas satur unikālu reģistrācijas kodu un lietotājvārdu, kā arī atsevišķi unikālo reģistrācijas kodu un lietotājvārdu gadījumiem, ja lietotājam ar mobilo ierīci nav iespējams noskenēt QR kodu:
4.3.4.2.1. fiziskas klātbūtnes gadījumā – Reģistrācijas institūcijas darbinieki uzrādīs Abonentam uzģenerēto QR kodu un unikālo reģistrācijas kodu ar Abonenta lietotājvārdu,
4.3.4.2.2. Pakalpojuma sniedzēja mājaslapā – Abonentam tiks atrādīts uzģenerētais QR kodu un unikālais reģistrācijas kods ar Abonenta lietotājvārdu;
4.3.4.3. Abonents atver "eParaksts mobile" mobilās ierīces atslēgu pārvaldības aplikāciju, izveido savu PIN kodu;
4.3.4.4. pēc PIN koda ievades, noskenē uzģenerēto QR kodu vai ievada saņemto unikālo reģistrācijas kodu un savu lietotājvārdu;
4.3.4.5. pēc QR koda vai unikālā reģistrācijas koda un lietotājvārda ievades, uz pieteikumā minēto un verificēto telefona numuru (saziņas kanālu) tiek nosūtīts reģistrācijas vienreiz lietojams kods;
4.3.4.6. saņemtais reģistrācijas vienreiz lietojamais kods jāievada "eParaksts mobile" mobilās ierīces atslēgu pārvaldības aplikācijā;
4.3.4.7. pēc reģistrācijas vienreiz lietojamā koda pārbaudes (pie sekmīga rezultāta) tiek ģenerēts atslēgu pāris un izsniegts atbilstošs sertifikāts;

4.3.4.8. Abonentam “eParaksts mobile” mobilās ierīces atslēgu pārvaldības aplikācijas aktivizēšana jāveic 5 (piecu) minūšu laikā pēc unikālā reģistrācijas koda saņemšanas.

4.3.5. Pieteikšanās process eParakstsTX sertifikāta saņemšanai;

4.3.5.1. Abonents pēc “eParaksts mobile” autentifikācijas sertifikāta saņemšanas autentificējas Pakalpojuma sniedzēja mājaslapā, izmantojot “eParaksts mobile” autentifikācijas rīku vai arī kādu no Pakalpojuma sniedzēja izsniegtām viedkartēm (QSCD);

4.3.5.2. Abonents izvēlas veikt eParakstsTX sertifikāta ģenerēšanu;

4.3.5.3. pēc izvēles izdarīšanas, Abonents izveido jaunu PIN kodu eParakstsTX atslēgām, pēc kā tiek uzģenerētas eParakstsTX atslēgas un izsniegts jauns sertifikāts.

4.4. Sertifikātu akceptēšana

4.4.1. Pirms līguma noslēgšanas ar Abonentu Pakalpojuma sniedzējs informē abonentu par Uzticamības pakalpojumu vispārējiem noteikumiem.

4.4.2. Pakalpojuma sniedzējs publicē Uzticamības pakalpojumu vispārējos noteikumus Pakalpojuma sniedzēja mājaslapā www.eparaksts.lv.

4.4.3. Pakalpojuma sniedzējs reģistrē Abonenta parakstīto līgumu.

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 Pakalpojuma 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. Sertifikātu atjaunošana nav atļauta.

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.

4.7.3. Sertifikātu, kas tiek izsniegti “eParaksts mobile” mobilās ierīces atslēgas konteinerī un eParakstsTX risinājumā sertifikātu jaunizdošanu var veikt tikai pats abonents autentificējoties Pakalpojuma sniedzēja mājaslapā ar augsta līmeņa autentifikācijas līdzekli.

4.7.4. Pakalpojuma “eParaksts” saistīto sertifikātu jaunizdošanas process ir identisks šī dokumenta 4.3.4. un 4.3.5. punktā minētajam procesam.

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. Pakalpojuma sniedzējam laikus jāatsauc sertifikātus, pamatojoties uz pilnvarotiem un apstiprinātiem sertifikātu atsaukšanas pieprasījumiem.

4.9.2. Pakalpojuma 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 Pakalpojuma 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 personas 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 Pakalpojuma sniedzējs atsauc sertifikātu.

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

4.9.6. Sertifikātu apturēšanas nav atļauta.

4.10. Sertifikātu statusa pakalpojumi

4.10.1. Pakalpojuma 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. Kad abonents ģenerē atslēgas "eParaksts mobile" autentifikācijas sertifikātam, tās jāģenerē Abonenta valdījumā esošā mobilās ierīces atslēgas konteinerī.
6.1.3. Elektroniskā paraksta sertifikāti tiek izdoti tikai saskaņā ar QCP-n-qscd politiku.
6.1.4. eParakstsTX 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.
6.1.5. eParakstsTX atslēgas tiek glabātas HSM iekārtā, kas konfigurēta atbilstoši droša paraksta radīšanas ierīces vadlīnijām.
6.1.6. Atļautos atslēgu pielietojumus nosaka atbilstoši [Sertifikāta profilā] aprakstītajam.
6.2. Privātās atslēgu aizsardzības un kriptogrāfijas moduļa tehniskie aizsargpasākumi
6.2.1. Abonents ir atbildīgs par savu privāto atslēgu drošības nodrošināšanu un pārvaldību.
6.2.2. Privātās atslēgas aktivēšana tiek veikta ar PIN. "eParaksts mobile" mobilās ierīces atslēgu pārvaldības aplikācijā lietotājs var izvēlēties iespējot pirkstu nospiedumu salīdzināšanu PIN ievades vietā.
6.2.3. Abonents ir atbildīgs par savu PIN kodu un mobilās ierīces paturēšanu tikai savā kontrolē. Aizliegts nodot PIN kodus un/vai mobilās ierīces lietošanu trešajai personai.
6.2.4. Abonentam ir pienākums nekavējoties atsaukt savus sertifikātus, ja Abonenta PIN kodi un/vai mobilā ierīce ir pazaudēta vai ir pamatotas aizdomas, ka sertifikāti ir tikti 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.
6.3. Citi atslēgu pāra pārvaldības aspekti

6.3.1. Abonenta sertifikātu derīguma termiņš nepārsniegs trīs (3) gadus.

6.4. Aktivizēšanas dati

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

6.5. Datu drošības kontroles

6.5.1. Pakalpojuma sniedzēja datora 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. Pakalpojuma sniedzēja 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. Pakalpojuma 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 apstrādi atbilstoši LVRTC Privātuma politikā noteiktajam.

9.4.2. LVRTC 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.