Pakalpojuma Zaļais sertifikāts sniegšanas NOTEIKUMI

SAGATAVOJA: Atbilstības vadītājs

NOSŪTĪTS: Publisks

SAISTĪTIE DOKUMENTI:

1. [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”
2. [ETSI EN 319 102-1] Elektroniskie paraksti un infrastruktūras (ESI); AdES digitālo parakstu izveides un apstiprināšanas procedūras; 1. daļa: Izveide un apstiprināšana
3. [ETSI TS 119 312] Šifrēšanas komplekti
4. Fizisko personu datu aizsardzības likums
5. Fizisko personu elektroniskās identifikācijas likums un saistītie Ministru kabineta noteikumi.
6. Tehniskās specifikācijas digitālajiem zaļajiem sertifikātiem 1, V1.0.5 — E-veselības tīkls
7. Veselības sertifikātu savietojamība — Uzticības sistēma — v. 1.0
8. Privātuma politika
9. [Sertifikātu profili] Latvijas Valsts radio un televīzijas centra Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu apraksts

SATURS

1. Dokumenta mērķis un auditorija

Valsts akciju sabiedrība “Latvijas Valsts radio un televīzijas centrs” (turpmāk – Pakalpojumu sniedzējs) ir dibināta 1924 gadā. 2009. gadā valsts akciju sabiedrība “Latvijas Valsts radio un televīzijas centrs” pārņēma uzticamības pakalpojuma sniedzēja infrastruktūru no valsts akciju sabiedrības “Latvijas Pasts” un uzsāka uzticamības pakalpojumu sniegšanu, bet vēlāk uzsāka arī elektroniskās identifikācijas pakalpojumu sniegšanu.

1.1. Dokumenta mērķis

1.1.1. Dokuments nosaka Pakalpojuma sniedzēja nodrošinātā pakalpojuma “Zaļais sertifikāts” sniegšanas procedūras.

1.1.2. Dokuments attiecas tikai uz elektroniskajiem sertifikātiem, ko izsniedz “Digital Green Certificate CSCA” sertifikācijas institūcija.

1.1.3. “Zaļais sertifikāts” pakalpojums sastāv no:

1.1.3.1. sertifikātu izsniegšanas pakalpojuma;

1.1.3.2. sertifikātu statusa maiņas pakalpojuma;

1.1.3.3. atsaukto sertifikātu saraksta publicēšanas;

1.1.3.4. LVRTC saistīto dokumentu publicēšanas.

1.1.4. Pakalpojumu “Zaļais sertifikāts” sniedz saskaņā ar dokumentos *Veselības sertifikātu savietojamība — Uzticības sistēma — v. 1.0 un Tehniskās specifikācijas digitālajiem zaļajiem sertifikātiem 1, V1.0.5 — E-veselības tīkls* noteiktajām prasībām.

1.2. Dokumenta nosaukums un identifikācija

1.2.1. Dokumenta nosaukums ir “Zaļais sertifikāts pakalpojumu sniegšanas noteikumi”.

1.3. Publiskās atslēgas infrastruktūras dalībnieki

1.3.1. Pakalpojuma sniedzēja publisko atslēgu infrastruktūras pārvaldībā un lietošanā ir iesaistīti šādi dalībnieki:

1.3.1.1. Sertifikācijas institūcijas (CA);

1.3.1.2. Reģistrācijas institūcijas (RA);

1.3.1.3. Partneri;

1.3.1.4. Partneru nodrošināto pakalpojumu gala lietotāji (turpmāk - Gala lietotāji);

1.3.1.5. Atkarīgās puses.

1.3.2. **Sertifikācijas institūcijas**

1.3.2.1. Pakalpojuma sniedzējs šo noteikumu ietvaros pārvalda šādas Sertifikācijas institūcijas:

1.3.2.1.1. Saknes sertifikācijas institūcija (saknes CA).

1.3.2.1.2. Pakārtotās izsniegšanas sertifikācijas institūcijas (izsniegšanas CA).

1.3.2.2. Saknes sertifikācijas institūcija izsniedz sertifikātus:

1.3.2.2.1. Izsniegšanas sertifikācijas institūcijām.

1.3.2.3. Saknes sertifikāta izvilkums

X.509 V1	Content
Version	*V3*
Serial number	5e 17 28 9f 18 c1 73 00 58 78 8f 5e 69 db 06 8e
Signature Algorithm	SHA384RSA
Signature Hash algorithm	SHA384
Issuer	CN = eParaksts Root CA 2.5.4.97 = NTRLV-40003011203 O = VAS Latvijas Valsts radio un televīzijas centrs C = LV
Valid From	piektdiena, 2017. gada 13. janvārī 10:27:10
Valid To	sestdiena, 2035. gada 13. janvārī 10:27:10
Subject	CN = eParaksts Root CA 2.5.4.97 = NTRLV-40003011203 O = VAS Latvijas Valsts radio un televīzijas centrs C = LV
Public Key	RSA (4096 biti) 30 82 02 0a 02 82 02 01 00 c0 a8 9e d2 db 3c fd c9 05 d6 7e 98 dd 14 04 23 e6 7c a3 71 58 2c 49 9f bc 4a 88 5a 6b 43 af d0 5c 08 c8 f7 b6 68 11 36 71 07 d4 31 87 10 35 e2 e7 e3 96 83 30 c3 90 cb 59 9f 7f 8b 90 c3 d4 92 79 99 18 e1 05 98 21 c8 d6 3b 1d 15 3c 48 7c 71 87 83 55 10 af 71 35 10 e7 17 05 78 2c e4 d3 47 83 6e 56 a1 62 5d b9 34 08 95 6d 1b a6 a0 16 c1 e2 c0 37 2a ad 59 44 3a bd 79 b8 d5 c3 e4 71 bd 4d f1 1f 82 0f 22 9c fe 15 59 7b 82 8c 0e 32 30 67 21 37 cb 9d a4 5d d8 36 bb 49 8d 96 ca 1a dc e4 f5 04 6d 12 75 3f 5d 7c 28 12 6b cc fd 32 01 83 6a 68 1f ff 23 36 05 a3 20 1b 5a 65 29 4a 6b 6d 4b 6e f4 09 2f f8 f4 7e e1 ae 5f ae 64 f1 51 d8 d7 1e 10 6b 2a 83 76 5f 94 67 fc bd 8d 80 d2 fc 75 55 9f 24 98 57 b5 52 f2 4b ef 60 88 3c 89 fc 3d 5d 81 06 1e ba 0b 97 7b bf 17 85 0e f4 0d c0 db fc ac 90 bc 5e 44 a1 8d 72 24 80 db da a8 5b e1 fb 47 20 e9 28 6a a3 23 6d d1 71 34 c3 7a 4f 9f 0a 63 77 17 5e 2e d0 84 b3 d5 17 9e de 26 45 5e 17 3a 53 59 bf dc 1b 3e 28 d5 76 1a 2b 2b a1 53 81 82 94 dd d0 28 88 eb 8d 12 4a a6 50 e6 0f bf 35 12 e3 82 72 65 05 1e d9 13 c2 6b 0a 6b 33 9f 4c f8 c5 76 e7 10 1d 8b 62 ef 84 a0 ae 37 92 eb 35 bc bc d1 96 1a c7 5d 97 dd 63 39 7e 0b d9 8b 67 3e dc 22 bd 6a 84 68 0f 0b 69 9a 3e f7 33 ce 5f ad b5 f3 e3 45 ce 3f 69 09 14 79 52 d2 95 98 9c 8a b6 96 e9 62 45 af 0b 58 36 d3 b5 8f 18 df

X.509 V1	Content	
	1e 6f 27 77 e6 d6 3c f0 60 e7 43 17 86 5c 0b 4a 34 18 a0 e6 84 d9 dc 7d 27 12 3a b6 77 79 42 36 9d 56 f9 ad 7c 44 4c 26 bc de b0 46 67 60 a8 b3 35 8d 76 45 e1 45 85 03 8e 7e 14 23 dd 87 2b 51 e9 8d ab 61 97 ed 42 36 38 83 af ab fc 79 02 03 01 00 01	
X.509 V3 Extensions	**Critical**	**Content**
Subject key identifier	No	0e ff 89 3e 7f 5e 6d eb b5 67 a2 0a e7 b3 78 5c fb 93 bc e9
Key Usage	Yes	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constrants	Yes	Subject Type=CA Path Length Constraint=None
Properties	**Content**	
Thumbprint algorithm	sha1	
Thumbprint	3d a4 4d ee 88 da 1b bd 74 d3 49 33 e6 20 e2 86 43 a6 27 d1	

1.3.2.4. “Zaļais sertifikāts” pakalpojuma ietvaros Pakalpojuma sniedzējs pārvalda šādu nekvalificētas izsniegšanas sertifikācijas institūciju (CA):

X.509 V1	Content
Version	*V3*
Serial number	525a5f516d0aff3a60a7ab40c232f3e0
Signature Algorithm	SHA384RSA
Signature Hash algorithm	SHA384
Issuer	CN = eParaksts Root CA 2.5.4.97 = NTRLV-40003011203 O = VAS Latvijas Valsts radio un televīzijas centrs C = LV
Valid From	piektdiena, 2021. gada 21. maijs 14:44:48
Valid To	trešdiena, 2025. gada 21. maijs 14:44:48
Subject	CN = Digital Green Certificate CSCA 2.5.4.97 = NTRLV-40003011203 O = VAS Latvijas Valsts radio un televīzijas centrs C = LV
Public Key	RSA (4096 biti)

X.509 V1	Content	
X.509 V3 Extensions	**Critical**	**Content**
Subject key identifier	No	e4936a801ede23dc3d42f14682137c23bdaf3d1c
Authority Key Identifier	No	KeyID=0eff893e7f5e6debb567a20ae7b3785cfb93bce9
Authority Information Access	No	[1]Authority Information Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.eparaksts.lv/cert/eParaksts_Root_CA.crt
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.2042.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.32061.2.4.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_Root_CA.crl
Key Usage	Yes	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constrants	Yes	Subject Type=CA Path Length Constraint=0
Properties	**Content**	
Thumbprint	907f5e460863faea2b10bb1cb66951cc9662ac06	

1.3.3. **Reģistrācijas institūcija**

1.3.3.1. Noteikumi attiecas uz visām reģistrācijas institūcijām, arī kuras nodrošina Partneris.

1.3.3.2. Reģistrācijas institūcija identificē pieteicējus un apstiprina sertifikātu izsniegšanas, apturēšanas, anulēšanas un atjaunošanas pieprasījumus.

1.3.4. **Partneri**

1.3.4.1. Partneri nodrošina savu pakalpojumu sniegšanu gala lietotājiem.

1.3.5. **Gala lietotāji**

1.3.5.1. Gala lietotāji ir definēti atbilstošos Partnera sniegtā pakalpojuma noteikumos.

1.3.6. **Atkarīgās puses**

1.3.6.1. Atkarīgās puses definē Partneris.

1.4. Sertifikātu pielietojums

1.4.1. Pakalpojuma sniedzēja izsniegto sertifikātu veidi un pielietojums ir definēts atbilstošos Partnera sniegtā pakalpojuma noteikumos, saskaņā ar dokumentos *Veselības sertifikātu savietojamība — Uzticības sistēma — v. 1.0 un Tehniskās specifikācijas digitālajiem zaļajiem sertifikātiem 1, V1.0.5 — E-veselības tīkls* noteiktajām prasībām.

1.5. Noteikumu pārvaldība

1.5.1. Atbildīgais par šo "Zaļais sertifikāts pakalpojuma sniegšanas noteikumu" pārvaldību ir valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs" (reģ. nr. 40003011203), kas darbojas kā Pakalpojumu sniedzējs atbilstoši šiem noteikumiem.

1.5.2. **Kontaktinformācija**

Valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs"	
Adrese	Ērgļu iela 14, Rīga, LV-1012, Latvija
Uzticamības un elektroniskās identifikācijas pakalpojumu sniegšanas palīdzības dienests	
Tālrunis	+371 67108787
e-pasts	eparaksts@eparaksts.lv
Birojs	
Tālrunis	+371 67198704
e-pasts	lvrtc@lvrtc.lv

1.5.3. **Pakalpojumu sniedzēja noteikumu apstiprināšanas procesi**

1.5.3.1. "Zaļais sertifikāts pakalpojumu sniegšanas noteikumus" apstiprina Pakalpojumu sniedzēja valde.

1.5.3.2. Noteikumos veic grozījumus, mainoties Latvijas Republikā spēkā esošajiem normatīvajiem aktiem, kā arī pilnveidojot Uzticamības un elektroniskās identifikācijas sniedzēja sistēmu darbību vai biznesa procesus.

1.6. Termini un saīsinājumi

Termins, saīsinājums	**Skaidrojums**
Atkarīgā puse	Fiziska vai juridiska persona, kas paļaujas uz elektronisku identifikāciju vai uzticamības pakalpojumu

Termins, saīsinājums	Skaidrojums
CA	Sertificēšanas iestāde
Cenrādis	Pakalpojumu sniedzēja apstiprinātais pakalpojumu cenrādis
CRL	Atsaukto sertifikātu saraksts
eIDAS	Eiropas Parlamenta un Padomes 2014. gada 23. jūlija regula (ES) Nr. 910/2014 “Par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK”
IDS	Ielaušanās atklāšanas sistēma
IPS	Pretielaušanās sistēma
ES	Eiropas Savienība
FIPS	Federālais informācijas apstrādes standarts
CPS	Pakalpojumu sniegšanas noteikumi
Gala lietotājs	Partnera nodrošinātā pakalpojuma lietotājs.
HSM	Šifrēšanas šaurlietojumu ierīce (aparatūra), kas nodrošina šifrēšanas atslēgu aizsardzību
Latvijas Republikā spēkā esošie normatīvie akti	Ietver visus Latvijas Republikā spēkā esošos normatīvos aktus. Atsauce uz Latvijas Republikā spēkā esošajiem normatīvajiem aktiem ietver arī Latvijas Republikai saistošos starptautiskos līgumus un Eiropas Savienības tiesību normas. Ja attiecīgo tiesību jautājumu regulē Eiropas Savienības tiesību normas, kas ir tieši piemērojamas Latvijā, Latvijas likumu piemēro, ciktāl to pieļauj Eiropas Savienības tiesību normas.
LVRTC jeb Pakalpojumu sniedzējs	Valsts akciju sabiedrība “Latvijas Valsts radio un televīzijas centrs”, vienotais reģistrācijas Nr. 40003011203, Ērgļu iela 14, Rīga, Latvija, LV-1012, kas darbojas kā Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzējs
NTP	Tīkla laika protokols
Objekts	Fiziska vide, kurā atrodas ar pakalpojumu sniegšanu saistīti Pakalpojuma sniedzēja resursi
OCSP	Tiešsaistes sertifikātu statusa protokols
OID	Globālais objekta identifikators
Pakalpojuma sniedzēja mājas lapa	www.eparaksts.lv
PKI	Publisko atslēgu infrastruktūra
RA	Sertifikātu reģistrēšanas institūcija
SIEM	Drošības informācijas un notikumu pārvaldība
Partneris	Šī dokumenta kontekstā juridiska vai fiziska persona, kas noslēgusi Līgumu ar LVRTC par “Zaļais sertifikāts” pakalpojuma izmantošanu un nodrošina savu pakalpojumu sniegšanu gala lietotājiem.
X.509	Publiskās atslēgas infrastruktūras sertifikātu formāts

2. Publicēšanas un repozitorija pienākumi

2.1. **Repozitoriji**

2.1.1. Pakalpojuma sniedzējs uztur 24 stundas diennaktī 7 dienas nedēļā publiski pieejamu repozitoriju Pakalpojuma sniedzēja mājaslapā http://www.eparaksts.lv, tam nodrošinot vismaz 99,6% pieejamību mēnesī.

2.2. **Sertifikācijas informācijas publicēšana**

2.2.1. Pakalpojuma sniedzējs publicē šādu informāciju:

2.2.1.1. Izsniegto Saknes un izsniegšanas CA sertifikātus;

2.2.1.2. Ar Pakalpojumu sniegšanu saistītos sertifikātus;

2.2.1.3. Visus atsaukto sertifikātu sarakstus (CRL);

2.2.2. Pakalpojuma sniedzējs publicē vismaz šādus dokumentus:

2.2.2.1. Privātuma politiku;

2.2.2.2. Zaļais sertifikāts pakalpojuma sniegšanas noteikumus;

2.3. **Publicēšanas laiks vai biežums**

2.3.1. Izsniegtie sertifikāti tiek publicēti tiklīdz tie tiek uzģenerēti;

2.3.2. Pakalpojuma sniedzēja publicējamā dokumentācija tiek publicēta ne vēlāk kā 30 kalendārās dienas pirms tās spēkā stāšanās;

2.3.3. CRL publicē atbilstoši 2.1.1.punktā noteiktajam pieejamības līmenim.

2.4. **Publicēšanas un apziņošanas nosacījumi**

2.4.1. Pakalpojuma sniedzējs, izmantojot Pakalpojuma sniedzēja mājaslapu https://www.eparaksts.lv , informēs visas iesaistītās puses par:

2.4.1.1. Izmaiņām, kas veiktas saistītajā Pakalpojuma sniedzēja publicējamajā dokumentācijā;

2.4.1.2. Izmaiņām, kas veiktas Zaļais sertifikāts pakalpojuma sniegšanas noteikumos;

2.4.1.3. Izmaiņām, kas saistītas ar pakalpojumu Cenrādi.

2.4.2. Pakalpojuma sniedzējs apziņo par konkrētiem grozījumiem vismaz 30 kalendāra dienas pirms grozījumu, Pakalpojuma sniedzēja publicējamā dokumentācijā, stāšanās spēkā.

2.5. **Piekļuves kontrole repozitorijiem**

2.5.1. Pakalpojuma sniedzēja mājaslapā www.eparaksts.lv uzturētais repozitorijs tiek nodrošināts ar publisku pieeju. Visa repozitorijā publicētā informācija ir publiska un pieejama lietotājiem lasīšanas režīmā.

2.5.2. Tiesības veikt publicējamās informācijas izmaiņas ir tikai Pakalpojuma sniedzējam.

3. Partneru identifikācija un autentifikācija

3.1. **Vārda piešķiršana**

3.1.1. Visi Pakalpojuma sniedzēja izsniegtie Partneru sertifikāti sertifikāta turētāja laukā (Subject - *angļu val.*) satur Partnera identificētus sertifikāta turētāja datus.

3.1.2. Gadījumā, ja Pakalpojuma sniedzēja izsniegtie sertifikāti satur Sertifikāta turētāja alternatīvā vārda paplašinājumu, tas satur informāciju, kas identificē privātās atslēgas turētāju, un minētā vērtība var atšķirties no vērtības, kas ir iekļauta sertifikāta turētāja laukā. Minētajam paplašinājumam, atkarībā no sertifikāta veida, var tikt izmantoti dažādi atribūti.

3.1.3. Detalizēti nosacījumi un prasības ir definētas atbilstošos Partnera sniegtā pakalpojuma noteikumos.

3.2. **Sākotnējās identitātes validācija**

3.2.1. **Metode privātās atslēgas valdījuma pierādīšanai**

3.2.1.1. Pakalpojuma sniedzējs saknes CA un izsniegšanas CA institūciju privātās atslēgas valdījumu pierāda ar atslēgu ģenerēšanas procedūru.

3.2.1.2. Partnera sertifikāta privātās atslēgas valdījuma pierādīšanai ir definēta atbilstošos Partnera sniegtā pakalpojuma noteikumos.

3.2.2. **Organizācijas identitātes identifikācija un validācija**

3.2.2.1. Pakalpojuma sniedzējs var izmantot jebkādus likumīgus saziņas vai informācijas ieguves līdzekļus un avotus, lai noskaidrotu fizisko vai juridisko personu identitāti.

3.2.2.2. Juridiskās personas tiek identificētas pret autoritatīvu avotu.

3.2.2.3. Juridiskās personas identifikācijas laikā Pakalpojuma sniedzējs savāc nepieciešamos pierādījumus, kas iekļauj vismaz:

3.2.2.3.1. Pilns juridiskās personas nosaukums un juridiskā forma;

3.2.2.3.2. Juridiskās personas reģistrācijas numurs (identifikators);

3.2.2.3.3. Cita informācija, ja tā nepieciešama pakalpojuma nodrošināšanai.

3.2.2.4. Pakalpojuma sniedzējs pēc saviem ieskatiem, nepaskaidrojot iemeslus, drīkst atteikties izsniegt sertifikātu.

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

3.3.1. Atbilstoši šī CPS 3.2. punkta prasībām.

3.4. **Atsaukšanas pieprasījumu identifikācija un validācija**

3.4.1. Partneri nosūtīs pakalpojuma sniedzējam pašrocīgi parakstītu sertifikāta atsaukšanas pieteikumu.

3.4.2. Pakalpojuma sniedzējs identificēs Partneri un atsauks sertifikātu pēc Partnera atsaukšanas pieteikuma reģistrācijas.

3.4.3. Laiks starp sertifikāta atsaukšanas reģistrāciju un lēmuma par tā statusa izmaiņu paziņošanu visām atkarīgajām pusēm nepārsniegs 24 stundas.

4. Sertifikātu dzīves cikla darbības prasības

4.1. **Sertifikātu pieteikums**

4.1.1. Partneris iesniegs sertifikātu pieteikumus Pakalpojumu sniedzējam pēc Līguma parakstīšanas.

4.1.2. Pakalpojumu sniedzējs pārbaudīs iesniegtos pieteikuma datus un reģistrēs pieteikumu.

4.2. **Sertifikātu pieteikuma apstrāde**

4.2.1. Pakalpojuma sniedzējs neizsniegs sertifikātu, ja sertifikāta pieprasījums neatbilst piemērojamajos līgumos vai normatīvajos aktos noteiktajām tehniskajām prasībām.

4.2.2. Ja Pakalpojuma sniedzējs atsaka izsniegt sertifikātu, par to tiks paziņots Partnerim.

4.2.3. Visus pieteikumus Pakalpojuma sniedzējs apstrādās saskaņā ar noslēgtajiem līgumiem.

4.3. **Sertifikātu izsniegšana**

4.3.1. Pakalpojuma sniedzējs veic pasākumus pret sertifikātu viltošanu.

4.3.2. Partnerim Partnera sniegtā pakalpojuma noteikumos droši jāsasaista sertifikāta atjaunošana vai atslēgas maiņa, ieskaitot ģenerēto publisko atslēgu nodrošināšanu.

4.3.3. Pakalpojumu sniedzējs izsniedz sertifikātus tikai pēc sertifikāta pieprasījuma saņemšanas no Partnera.

4.4. **Sertifikātu akceptēšana**

4.4.1. Pirms partnera pakalpojuma sniegšanas, Partnera pienākums ir informēt gala lietotāju par Partnera sniegtā pakalpojuma noteikumiem.

4.4.2. Partneris nosaka kārtību saskaņā ar piemērojamajiem normatīvajiem aktiem, kādā tas informē gala lietotājus ar sniegtā pakalpojuma noteikumiem.

4.5. **Atslēgu pāra un sertifikātu lietošana**

4.5.1. Visas Partnera sertifikātu atslēgas jāģenerē, izmantojot [ETSI TS 119 312] standartā noteikto atslēgu garumu un algoritmu.

4.5.2. Partneris sertifikātus izmanto tikai Partnera sniegtā pakalpojuma noteikumos minētajiem mērķiem.

4.6. **Sertifikātu jaunizdošana**

4.6.1. Sertifikātu jaunizdošanas process ir definēts atbilstošos Partnera sniegtā pakalpojuma noteikumos.

4.6.2. Sertifikātu jaunizdošanas process tiek veikts atbilstoši šī dokumenta 3.2., 4.1., 4.2., 4.3. un 4.4. punktu prasībām.

4.7. **Sertifikātu modificēšana**

4.7.1. Gadījumā ja tiek mainīti Partnera sertifikātā iekļautie nosaukumi vai atribūti vai arī tajos ir kļūdas, nepareizie sertifikāti tiek atsaukti, reģistrācijas informācija tiek pārbaudīta, reģistrēta un saskaņota ar Pakalpojumu sniedzēju.

4.8. **Sertifikātu atsaukšana un apturēšana**

4.8.1. Pakalpojuma sniedzējs laikus, nepārsniedzot 3.4.3. punktā minēto laiku, atsauc sertifikātus, pamatojoties uz pilnvarotiem un apstiprinātiem sertifikātu atsaukšanas pieprasījumiem.

4.8.2. Visas atkarīgās puses var pārbaudīt sertifikāta statusu publicētajos CRL.

4.8.3. Pakalpojuma sniedzējs veic sertifikātu apturēšanu šādos gadījumos:

4.8.3.1. Izpildot tiesas nolēmumu;

4.8.3.2. Pamatojoties uz Partnera pieprasījuma;

4.8.3.3. Ar Partneri noslēgtajā līgumā noteiktajos gadījumos.

4.9. **Sertifikātu statusa pakalpojumi**

4.9.1. Pakalpojuma sniedzējs nodrošina atsaukšanas statusa informāciju ar publicēto CRL starpniecību atbilstoši šī dokumenta 2.1. punktā noteiktajam pieejamības režīmam.

4.9.2. Atsaukšanas statusa informācija ir publiska un starptautiski pieejama.

4.10. **Sertifikātu izmantošanas beigas**

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

5. Operacionālās, fiziskās un pārvaldības kontroles

5.1. **Fiziskās drošības kontroles**

5.1.1. Pakalpojuma sniedzējs lieto uzticamas sistēmas un produktus, kas ir aizsargāti pret modificēšanu, un nodrošina minēto sistēmu un produktu uzturēto procesu tehnisko un kriptogrāfisko drošību.

5.1.2. Pakalpojuma sniedzējs ir ieviesis fiziskās drošības noteikumus un procedūras, kas atbalsta šī dokumenta drošības prasības. Fiziskās drošības noteikumi un procedūras ietver iekšējai lietošanai paredzētu drošības informāciju un ir pieejamas tikai vienojoties ar Pakalpojuma sniedzēju. Prasību pārskats ir aprakstīts zemāk.

5.1.3. **Objekta novietojuma apsvērumi un izbūve**

5.1.3.1. Pakalpojuma sniedzēja Pakalpojumi tiek sniegti fiziski aizsargātā vidē, kura attur, aizsargā un atklāj nesankcionētu sensitīvas informācijas un sistēmu lietošanu, piekļuvi vai izpaušanu gan slēptā, gan atklātā veidā.

5.1.3.2. Pakalpojuma sniedzējs savām CA darbībām uztur pēcavārijas atjaunošanas telpas un iekārtas. Pakalpojuma sniedzēja pēcavārijas atjaunošanas telpas un iekārtas ir aizsargātas ar vairākiem fiziskās drošības līmeņiem, kas ir salīdzināmi ar Pakalpojuma sniedzēja primārajām telpām un iekārtām.

5.1.4. **Fiziskā piekļuve**

5.1.4.1. Pakalpojuma sniedzēja CA 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. Pakalpojuma sniedzējs nodrošina, ka fiziska piekļuve drošības zonām, kurās atrodas ar Pakalpojumu sniegšanu saistītie resursi, tiek kontrolēta un potenciālie riski tās resursiem ir minimizēti.

5.1.4.3. Ir pieejams skaidrs Pakalpojuma sniedzēja 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 Pakalpojuma sniedzēja 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 u.t.t.;

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;

5.1.4.4. Iepriekš minētā apraksta, riska analīzes un inventāra uzturēšanas atbildība ir uzticēta Pakalpojuma sniedzēja drošības pārvaldniekam.

Pakalpojuma sniedzēja vadības uzdevums ir periodiski pārskatīt iepriekšminēto aprakstu.

5.1.5. **Energoapgāde un gaisa kondicionēšana**

5.1.5.1. Pakalpojuma sniedzēja objekti, kuros atrodas ar Pakalpojumu sniegšanu saistītie resursi, 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. **Ūdens radītie riski**

5.1.6.1. Pakalpojuma sniedzējs ir veicis saprātīgus drošības pasākumus, lai samazinātu ūdens iedarbību uz informācijas sistēmām.

5.1.7. **Ugunsgrēka riska novēršana un ugunsdrošība**

5.1.7.1. Pakalpojuma sniedzējs ir veicis saprātīgus drošības pasākumus, lai atklātu, aizkavētu un nodzēstu ugunsgrēkus vai novērstu citu kaitējošu liesmu vai dūmu iedarbību. Pakalpojuma sniedzējs ugunsdrošības pasākumi atbilst spēkā esošajiem normatīvajiem aktiem ugunsdrošības jomā.

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 Pakalpojuma sniedzēja objektā vai alternatīvā identiskas drošības 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 nesankcionētas piekļuves).

5.1.8.2. Pakalpojuma sniedzējs ir definējis resursu klasifikācijas procesu, noteicis resursu piederību un atbilstošas prasības informācijas glabāšanai, apstrādei un arhivēšanai.

5.1.9. **Atkritumu likvidēšana**

5.1.9.1. Sensitīvie dokumenti un materiāli pirms likvidēšanas tiek sasmalcināti.

5.1.9.2. Sensitīvas informācijas vākšanai vai pārraidei izmantotie datu nesēji pirms likvidēšanas tiek padarīti nelasāmi.

5.1.9.3. 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. Pakalpojuma sniedzējs veic kritisku sistēmas datu, audita žurnāla datu un citas sensitīvas informācijas regulāru rezerves kopiju izveidi. Ārpus objekta vietas izvietotie datu nesēji tiek glabāti fiziski drošā veidā.

5.2. **Procesuālas kontroles**

5.2.1. **Uzticamības lomas**

5.2.1.1. Pakalpojuma sniedzēja darbību nodrošina Pakalpojuma sniedzēja darbinieki un ārējie sadarbības partneri, kuriem ir piešķirtas atbilstošas lomas Pakalpojuma sniedzēja struktūrā.

5.2.1.2. Pakalpojuma sniedzēja darbiniekiem, kuru lomas paredz Pakalpojuma sniedzēja darbībai kritisko darbību veikšanu tiek

piešķirtas uzticamības lomas. Pakalpojuma sniedzējs izšķir šādas uzticamības lomas:

5.2.1.2.1. Drošības pārvaldnieks – atbild par vispārējo drošības ieviešanu, uzturēšanu un uzraudzību procesos, procedūrās un dokumentos;

5.2.1.2.2. Sistēmas administrators – atbild par Pakalpojuma sniedzēja uzticamības sistēmas ieviešanu, konfigurēšanu un uzturēšanu;

5.2.1.2.3. Sistēmas operators – atbild par Pakalpojuma sniedzēja uzticamības sistēmu ikdienas darbību. Autorizēts veikt sistēmas dublēšanu;

5.2.1.2.4. Sistēmas auditors – autorizēts skatīt arhīvus, audita ierakstus un veikt Pakalpojuma sniedzēja sistēmu auditus;

5.2.1.3. Pakalpojuma sniedzējs uzskata šajā nodaļā identificētās personāla kategorijas kā uzticamās personas, kam ir uzticamības lomas.

5.2.1.4. Piekļuvi Pakalpojuma sniedzēja uzticamām sistēmām un drošības zonām uzticamām personām piešķir tikai pēc minētā personāla pārbaudes un uzticamības lomas piešķiršanas.

5.2.1.5. Uzticamības lomas un atbildības ietver prasību:

5.2.1.5.1. Ieviest un darboties saskaņā ar Pakalpojuma sniedzēja informācijas drošības politiku;

5.2.1.5.2. Aizsargāt resursus no nesankcionētas piekļuves, izpaušanas, modificēšanas, iznīcināšanas, nozaudēšanas vai uzlaušanas;

5.2.1.5.3. Izpildīt īpašus drošības procesus un aktivitātes;

5.2.1.5.4. Nodrošināt, ka personai par veiktajām nesankcionētām darbībām tiek noteikta atbildība;

5.2.1.5.5. Ziņot par esošiem vai iespējamiem drošības pārkāpumiem vai citiem drošības draudiem organizācijai.

5.2.2. **Uzdevumam nepieciešamo darbinieku skaits**

5.2.2.1. Pakalpojuma sniedzējs ir ieviesis, uztur un nodrošina stingras kontroles procedūras, lai nodrošinātu atbildības pienākumu atdalīšanu un to, ka kritisku 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 iekārtām;

5.2.2.2.2. Fiziska piekļuve datu arhīvam;

5.2.2.2.3. Loģiska piekļuve Pakalpojuma sniedzēja CA centrālajām, sensitīvajām vai kritiskajām sistēmām un to dublējošajām sistēmām;

5.2.2.2.4. CA un saistīto servisu atslēgu pārvaldībai.

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 tiek nozīmētas par uzticamības personām, identitātes pārbaude notiek šī personāla personīgā (fiziskā) klātbūtnē pret personu apliecinošu dokumentu. Turpmāka identitātes apstiprināšana notiek, veicot

personas datu pārbaudes procedūras. Pakalpojuma sniedzējs nodrošina, ka personāls ir sasniedzis uzticamu statusu, 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 Pakalpojuma sniedzēja CA specifiskos pienākumus.

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

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

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

5.3.3. **Personāla datu pārbaudes procedūras**

5.3.3.1. Pakalpojuma sniedzējs veiks atbilstošu visa personāla, kas darbojas uzticības lomās, izvērtēšanu (pirms lomas piešķiršanas un pēc tam periodiski pēc vajadzības), lai apliecinātu viņu uzticamību un kompetenci saskaņā ar šī CPS prasībām un Pakalpojuma sniedzēja personāla vadības procedūrām vai līdzīgiem noteikumiem. Viss personāls, kurš neiztur sākotnējo vai periodisko pārbaudi, nedarbosies vai neturpinās darboties uzticības lomā.

5.3.3.2. Visiem Pakalpojuma sniedzēja darbībā iesaistāmajiem darbiniekiem tiek izvirzītas šādas prasības:

5.3.3.2.1. Ir Pakalpojumu sniegšanai nepieciešamās speciālās zināšanas;

5.3.3.2.2. Pakalpojuma sniedzēja darbinieki, kam tiks piešķirtas uzticamības lomas, ir jāveic papildus uzticamības pārbaudes;

5.3.3.2.3. Pakalpojuma sniedzēja darbinieki, kuru lomas paredz darbu ar Pakalpojuma sniedzēja informācijas sistēmu, ir iepazīstināti ar nepieciešamo dokumentāciju;

5.3.3.2.4. Pakalpojuma sniedzēja darbiniekiem, kuru lomas paredz Pakalpojuma sniedzēja darbībai kritisko darbību veikšanu – t.s. uzticības lomas tiek veiktas arī atsevišķas – papildus pārbaudes.

5.3.4. **Apmācības prasības**

5.3.4.1. Pakalpojuma sniedzējs nodrošina, ka viss personāls, kas pilda vadības pienākumus attiecībā uz Pakalpojuma sniedzēja darbību, saņem visaptverošu apmācību šādās jomās:

5.3.4.1.1. Pakalpojuma sniedzēja drošības principi un mehānismi;

5.3.4.1.2. Drošības jautājumu izpratne;

5.3.4.1.3. Pakalpojuma sniedzēja lietotās 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. Šī dokumenta 5.3.4. nodaļā minēto apmācību prasības un saturs ir regulāri jāatjauno, un tajās ir jāiestrādā Pakalpojuma sniedzēja vai normatīvajos aktos notikušās izmaiņas. Pēc vajadzības jāveic

kvalifikācijas celšanas apmācības, un Pakalpojuma sniedzējam vismaz reizi gadā jāpārskata šīs prasības.

5.3.5.2. Pakalpojuma sniedzējs veic Pakalpojuma sniedzēja iesaistīto darbinieku un partneru apmācību vismaz vienu reizi gadā.

5.3.6. **Darbu rotācijas biežums un secība**

5.3.6.1. Šis dokuments neparedz ierobežojumus darbu rotācijas biežumam un secībai. Individuālas politikas, kuras uzliek šāda veida prasības, nodrošinās Pakalpojuma sniedzēja Pakalpojumu pastāvību un integritāti.

5.3.7. **Sankcijas par nesankcionētu darbību veikšanu**

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

5.3.8. **Prasības līgumdarbiniekiem**

5.3.8.1. Pakalpojuma sniedzējs ļauj neatkarīgiem līgumdarbiniekiem vai konsultantiem kļūt par uzticamām personām tikai tādā apjomā, kādā tas ir nepieciešams, lai izpildītu līgumā skaidri definētos pienākumus;

5.3.8.2. Pakalpojuma sniedzējs no pamatpakalpojumiem ārējām juridiskām personām var deleģēt reģistrācijas institūcijas pienākumus;

5.3.8.3. Uz neatkarīgiem līgumdarbiniekiem vai konsultantiem, kuriem Pakalpojuma sniedzējs piešķir uzticības lomu un deleģē veikt ar to saistītās darbības, attiecas visas tās pašas prasības un nosacījumi kā Pakalpojuma sniedzēja personālam, kam piešķir uzticamības lomas;

5.3.8.4. Neatkarīgi līgumdarbinieki un konsultanti, kuriem nav piešķirtas uzticamības lomas, var piekļūt Pakalpojuma sniedzēja objektiem tikai uzticamu personu pavadībā un tiešā uzraudzībā.

5.3.9. **Personālam izsniedzamā dokumentācija**

5.3.9.1. Pakalpojuma sniedzējs sniedz savam personālam (tostarp personālam, kas pilda uzticamības lomas) nepieciešamo apmācību un dokumentāciju, kas nepieciešama, lai savus darba pienākumus tas veiktu kompetenti.

5.4. **Audita reģistrācijas procedūras**

5.4.1. **Reģistrējamo notikumu tipi**

5.4.1.1. Pakalpojuma sniedzējs žurnalēs vismaz šādus notikumus:

5.4.1.1.1. Visa reģistrācijas pieteikuma informāciju ko sniegs Partneris;

5.4.1.1.2. Noraidītie pieteikumi sertifikātu izsniegšanai;

5.4.1.1.3. Kontu piekļuves pārkāpumi;

5.4.1.1.4. Galalietotāju un visu Pakalpojuma sniedzēja pārvaldīto CA un Laika zīmogošanas institūcijas sertifikātu;

5.4.1.1.5. Sertifikātu statusa maiņas gadījumi;

5.4.1.1.6. Pieslēgšanās sistēmai;

5.4.1.1.7. CRL izsniegšana;

5.4.1.1.8. CA programmatūras modifikācija;

5.4.1.1.9. Reģistrācijas institūcijas programmatūras modifikācija;

5.4.1.1.10. Sertifikātu termiņu beigas;

5.4.1.1.11. Uzticamo sistēmu startēšanas un apturēšanas gadījumi;
5.4.1.1.12. Sistēmas un iekārtu atteikumi;
5.4.1.1.13. Kvalificētu elektroniskā paraksta radīšanas ierīču personalizācijas procesi;
5.4.1.1.14. Visi notikumi kas saistīti ar uzticama laika avotu sinhronizāciju.

5.4.2. **Reģistrācijas žurnāla apstrādes biežums**

5.4.2.1. Pakalpojuma sniedzējs 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 Pakalpojuma sniedzēja manuālie un elektroniskie reģistri jāsalīdzina, ja kāda darbība tiek uzskatīta par aizdomīgu. Jādokumentē darbības, kas tiek veiktas pēc šiem pārskatiem.

5.4.3. **Audita žurnāla uzglabāšanas ilgums**

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

5.4.4. **Audita žurnāla aizsardzība**

5.4.4.1. 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.

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

5.4.5.1. Pakalpojuma sniedzējs veic regulāras rezerves kopiju izveides. Audita pierakstu rezerves kopēšana ir daļa no kopējās rezerves kopēšanas procedūras. Pakalpojuma sniedzējs ir izveidojis iekšējos normatīvos aktus kas nosaka rezerves kopēšanas pārvaldību.

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

5.4.6.1. Automatizēti audita dati tiek ģenerēti un ierakstīti lietojumprogrammu un operētājsistēmas līmenī. Neelektroniski ģenerētus audita datus pieraksta Pakalpojuma sniedzēja personāls, kam piešķirtas uzticamības lomas.

5.4.7. **Notikumu paziņošana**

5.4.7.1. Pierādījumi no audita sistēmas par sistēmas darbību (notikums vai notikumu kopa) tiek izsniegti tikai tām personām, kuru tiesības piekļūt šādai informācijai ir noteiktas normatīvajos aktos.

5.4.8. **Ievainojamību novērtēšana**

5.4.8.1. Pakalpojuma sniedzēja sistēmas iekšējās un ārējās ievainojamības tiek caurskatītas atbilstoši iekšējai risku pārvaldības dokumentācijai. Pakalpojuma sniedzēja sistēmai tiek veikti ikgadējie ielaušanās testi;

5.4.8.2. Pakalpojuma sniedzēja sistēmas audita pieraksti tiek apstrādāti automatizētā audita pierakstu apstrādes sistēma, kas veic ievainojamību novērtēšanu ikdienas režīmā.

5.5. **Ierakstu arhīvs**

5.5.1. **Arhivējamo ierakstu tipi**

5.5.1.1. Pakalpojuma sniedzēja ieraksti, kas attiecas uz tās Pakalpojumu darbību, tiek arhivēti un uzglabāti vismaz tik ilgi, cik norādīts šī dokumenta 5.5.2. nodaļā. Visi fiziskie ieraksti un identifikācijas informācija jāarhivē sadarbības partnerim, kas pasūtītājam tieši sniedz Pakalpojumus (t.i., Pakalpojuma sniedzēja klientu apkalpošanas punktiem). Visos gadījumos šie ieraksti jāarhivē papīra vai elektroniskā formā;

5.5.1.2. Papīra formas dokumenti tiks arhivēti klientu apkalpošanas punktos vai Pakalpojuma sniedzēja 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 pēc sertifikāta, kurš saistīts ar konkrētajiem ierakstiem, derīguma termiņa beigām bez jebkāda datu vai to integritātes zuduma. Šo laiku var pagarināt konkrētiem ierakstiem un informācijai pēc speciālu arhivēšanas pakalpojumu pieprasījuma.

5.5.3. **Arhīva aizsardzība**

5.5.3.1. Arhīvs tiek aizsargāts 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 šī dokumenta 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. Datu bāžu ieraksti satur precīzu notikuma datumu un laiku. Šāda laika informācija nav bāzēta uz kriptogrāfiskiem risinājumiem.

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

5.5.6.1. Pakalpojuma sniedzējs arhīva veidošanai izmanto iekšējo arhīva veidošanas (vākšanas) sistēmu;

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

5.5.7.1. Tikai pilnvarotas uzticības personas var iegūt piekļuves tiesības arhīvam;

5.5.7.2. Pierādījumu izsniegšana notiek atbilstoši šī dokumenta 5.4.7.punktā noteiktajam;

5.5.7.3. Informācijas integritāte tiek pārbaudīta, to atjaunojot.

5.6. **Atslēgu aizvietošana**

5.6.1. Detalizēti nosacījumi un prasības ir definētas atbilstošā Pakalpojumu politikā.

5.7. **Kompromitējums un pēcavārijas atjaunošana**

5.7.1. **Incidentu un kompromitējumu apstrādes procedūras**

5.7.1.1. Lai nodrošinātu Pakalpojuma sniedzēja sniegto Pakalpojumu nepārtrauktību, Pakalpojuma sniedzējs ir ieviesis virkni iekšējo plānu un procesu, kas sevī iekļauj darbības nepārtrauktības un avārijas seku novēršanas plānus, kā arī dažāda līmeņa incidentu pārvaldības un risku novērtēšanas procesus;

5.7.1.2. Darbības nepārtrauktības plāns satur visas identificētās ārkārtas situācijas, nepieciešamās darbības, resursus un personālu, kas iesaistīts lai atrisinātu konkrēto ārkārtas situāciju;
5.7.1.3. Avārijas seku novēršanas plāns satur visas nepieciešamās darbības, resursus un personālu, kas nepieciešams, lai pilnībā atjaunotu Pakalpojuma sniedzēja sistēmu no pilnīgas tās nepieejamības;
5.7.1.4. Risku novērtēšana notiek vismaz reizi gadā, kā arī mainoties normatīvajiem aktiem vai Pakalpojuma sniedzēja iekšējiem normatīvajiem aktiem, gadījumos, ja ir mainījušies vai identificēti jauni apdraudējumi un gadījumos, ja būtiski pieaug incidentu skaits vai noticis nozīmīgs drošības incidents;
5.7.1.5. Darbības nepārtrauktības plāns tiek pārbaudīts vismaz vienreiz gadā.
5.7.1.6. Ārkārtas situācijas iestāšanās gadījumā Pakalpojuma sniedzējs nekavējoties (bet ne vēlāk kā četras stundas pēc lēmuma pieņemšanas par ārkārtas situācijas iestāšanos) informēs Partneri, kas tālāk informēs gala lietotājus un iesaistītās puses, izmantojot sev pieejamos saziņas kanālus, papildus norādot potenciālos risinājumus (jā tādi pieejami), kā arī provizorisko ārkārtas situācijas novēršanas laiku;
5.7.1.7. Par ārkārtas situācijām, kuras var būtiski ietekmēt Pakalpojuma sniedzēja Pakalpojumus un to statusus, kā arī apstrādāto fizisko personu datus, Pakalpojuma sniedzējs bez liekas kavēšanās, bet jebkurā gadījumā 24 stundās pēc attiecīgās informācijas saņemšanas, informēs atbilstošās uzraudzības iestādes.

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

5.7.2.1. Pēc šķietamas vai patiesas resursu, programmatūras vai datu kompromitēšanas tiks piemērots avārijas seku novēršanas plāns un ar to saistītās procedūras (saskaņā ar šī dokumenta 5.7.4. nodaļu).

5.7.3. **Vienības privātās atslēgas kompromitējuma procedūras**

5.7.3.1. Ja ir kompromitēta Pakalpojuma sniedzēja CA vai laika zīmogošanas institūcijas privātā atslēga vai ir aizdomas par šādu kompromitējumu, Pakalpojuma sniedzējs veiks vismaz šādas darbības:
5.7.3.1.1. Informēs Partneri un citas iesaistītās puses;
5.7.3.1.2. Izbeigs sertifikātu un CRL, kas ir izsniegti ar kompromitēto privāto atslēgu, izplatīšanas pakalpojumus;
5.7.3.1.3. Veiks CA vai laika zīmogošanas institūcijas sertifikāta anulēšanu.

5.7.4. **Darbības nepārtrauktības iespējas pēc avārijas**

5.7.4.1. Pakalpojuma sniedzēja sniegto Pakalpojumu sniegšana tiks apturēta līdz pilnībā tiks novērstas avārijas sekas, kā arī atjaunotas visas nepieciešamās drošības prasības un darbības primārajā vai sekundārajā datu centrā;
5.7.4.2. Darbības atjaunošanai izmantoti iekšējie, ar darbības nepārtrauktības novēršanu saistītie plāni, kā arī, ar minētajiem plāniem saistītās procedūras.

5.8. **CA darbības izbeigšana**

5.8.1. **Pakalpojumu darbības izbeigšana**

5.8.1.1. Atbildīgs par Pakalpojuma sniedzēja darbības izbeigšanu ir Pakalpojuma sniedzēja vadītājs;

5.8.1.2. Galvenās Pakalpojumu izbeigšanas procedūras:

5.8.1.2.1. Pakalpojuma sniedzējs vismaz mēnesi pirms Pakalpojuma darbības izbeigšanas rakstveidā informē Partneri un nodrošina Pakalpojuma sniedzēja mājaslapā publiski pieejamu informāciju gala lietotājiem un atkarīgajām pusēm par to, ka Pakalpojumu sniegšana ir izbeigta.

5.8.1.2.2. Pakalpojuma sniedzējs anulē pilnvaras apakšuzņēmējiem Pakalpojuma sniedzēja vārdā veikt jebkādas darbības saistībā ar sertifikātu izsniegšanu;

5.8.2. **Partnera darbības izbeigšana**

5.8.2.1. Gadījumā, ja kāds no Partneriem pārtrauc savu darbību, tas vismaz mēnesi pirms Pakalpojuma darbības izbeigšanas rakstveidā informē Pakalpojumu sniedzēju.

5.8.2.2. Pakalpojumu sniedzējs Partnera darbības izbeigšanas gadījumā, pēc pakalpojumu izbeigšanas anulē visus konkrētajam Partnerim izsniegtos sertifikātus (ieskaitot gala lietotāju sertifikātus), ja savstarpēji noslēgtajā līgumā nav noteikts savādāk.

6. Tehniskās drošības kontroles

6.1. Atslēgu pāra ģenerēšana

6.1.1. Atslēgu pāra ģenerēšana

6.1.1.1. Pakalpojuma sniedzēja CA institūcijas 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 dokumentētiem CA atslēgu ģenerēšanas ceremonijas noteikumiem.

6.1.1.2. Pakalpojuma sniedzēja CA institūcijas atslēgas tiek ģenerētas un glabātas aparatūras drošības modulī (HSM iekārta), kas ir sertificēts FIPS 140-2 3.līmenī atslēgu ģenerēšanai un glabāšanai, kas aizsargā atslēgu no ārējas kompromitēšanas;

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

6.1.1.4. Pakalpojuma sniedzējs ir izstrādājis un uztur atslēgu ceremonijas norises protokolus, kuros ir minēti visu CA atslēgu ģenerēšanas ceremonijai nepieciešamie soļi;

6.1.1.5. Detalizēti gala lietotāju privāto atslēgu ģenerēšanas nosacījumi un prasības ir definētas atbilstošos Partnera sniegtā pakalpojuma noteikumos.

6.1.2. Privātās atslēgas piegāde gala lietotājiem

6.1.2.1. Privātās atslēgas piegāde gala lietotājam ir definēta atbilstošos Partnera sniegtā pakalpojuma noteikumos.

6.1.3. Sertifikācijas institūciju publiskās atslēgas piegāde

6.1.3.1. Pakalpojuma sniedzējs šī CPS 5.5.2. punktā norādīto termiņu glabā visus CA izsniegtos sertifikātus un ar tiem saistītās privātās atslēgas;

6.1.3.2. CA publiskās atslēgas piegāde atkarīgajām pusēm;
6.1.3.3. Visas Pakalpojuma sniedzēja Pakalpojumu sniegšanā iesaistītās publiskās atslēgas tiek publicētas Pakalpojuma sniedzēja mājaslapā www.eparaksts.lv/repository. Publiskās atslēgas tiek publicētas X.509 sertifikātu formātā;

6.1.4. **Atslēgu izmēri**

6.1.4.1. Pakalpojuma sniedzēja Pakalpojumu sniegšanā iesaistīto atslēgu algoritmiem un atslēgu garumiem jāatbilst [ETSI TS 119 312] minētajam.
6.1.4.2. Detalizēti Gala lietotāju atslēgu algoritmi un garumi ir definēti atbilstošos Partnera sniegtā pakalpojuma noteikumos.

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

6.1.5.1. Nav piemērojams.

6.1.6. **Atslēgu lietošanas mērķi**

6.1.6.1. Visi sertifikāti satur "Atslēgas lietojuma" (Key usage – angļu val.) un "Paplašinātā atslēgas lietojuma" (Extended key usage – angļu val.) paplašinājumus, kuros ir minēti atslēgas lietošanas mērķi;
6.1.6.2. Atļautie Gala lietotāju atslēgu lietošanas mērķi ir definēti atbilstošos Partnera sniegtā pakalpojuma noteikumos;
6.1.6.3. Saknes CA atslēgas tiek izmantotas, lai parakstītu izsniegšanas CA, laika zīmogošanas institūcijas sertifikātus un saknes CRL;
6.1.6.4. Izsniegšanas CA atslēgas tiek izmantotas, lai parakstītu OCSP un gala lietotāju sertifikātus, kā arī CRL.

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

6.2.1. **Kriptogrāfiskā moduļa standarti un kontroles**

6.2.1.1. Pakalpojuma sniedzējs izmanto HSM iekārtas, kas atbilst FIPS 140-2, 3. līmeņa noteiktajām prasībām. Visam HSM iekārām ir aktivizēts FIPS režīms;
6.2.1.2. Pakalpojuma sniedzējs veic nepieciešamās pārbaudes, lai pārliecinātos, ka ar HSM iekārtām nav notikušas manipulācijas to transportēšanas un uzglabāšanas laikā;
6.2.1.3. Detalizētas prasības un nosacījumi Gala lietotāju kriptogrāfiskajām iekārtām ir definēti atbilstošos Partnera sniegtā pakalpojuma noteikumos.

6.2.2. **Privātās atslēgas (N no M) vairāku personu kontrole**

6.2.2.1. Pakalpojuma sniedzējs ir ieviesis tehniskus un procesuālus mehānismus, kas prasa vairāku uzticamu personu klātbūtni, lai veiktu CA institūcijas kriptogrāfiskas darbības. Lai iegūtu piekļuvi privātajām atslēgām, ir nepieciešamas vismaz divas personas ar uzticības lomām. Nevienai atsevišķai personai nav visu aktivēšanas datu, kas nepieciešami piekļuvei jebkurai no CA institūcijas privātajām atslēgām.

6.2.3. **Privātās atslēgas aizbildniecība**

6.2.3.1. Pakalpojuma sniedzēja CA institūcijas privātās atslēgas tiek glabātas HSM iekārtās, kas atbilst FIPS 140-2, 3. līmeņa noteiktajām prasībām. CA institūcijas privāto atslēgu aktivēšana un lietošana ir

iespējama tikai vairāku personu kontrolē, kā tas aprakstīts šī dokumenta 6.2.2. punktā;

6.2.3.2. Gala lietotāju privāto atslēgu aizbildniecība ir aprakstīta atbilstošos Partnera sniegtā pakalpojuma noteikumos.

6.2.4. **Privātās atslēgas rezerves kopijas izveide**

6.2.4.1. Tiek nodrošināta Pakalpojuma sniedzēja CA institūcijas privātās atslēgas rezerves kopija, un tā tiek droši uzglabāta mazticamam atslēgas zaudējuma gadījumam negaidīta barošanas pārtraukuma vai aparatūras bojājuma dēļ. Rezerves CA institūcijas privātajā atslēgai tiek saglabāta slepenība, tās integritāte un autentiskums, un tā tiek glabāta fiziski drošā objektā;

6.2.4.2. Gala lietotāju privāto atslēgu rezerves kopēšana netiek pieļauta;

6.2.4.3. Pakalpojuma sniedzēja CA institūcijas privāto atslēgu atjaunošana var notikt tikai ar šī dokumenta 6.2.2. punktā minētajām kontrolēm.

6.2.5. **Privātās atslēgas arhivēšana**

6.2.5.1. Pakalpojuma sniedzējs neveikts CA institūcijas atslēgu arhivēšanu pēc to derīguma termiņa beigām. Pakalpojuma sniedzēja CA institūcijas atslēgu pāri, beidzoties to derīguma termiņam, tiks droši iznīcināti un to atjaunošana vairs nebūs iespējama.

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

6.2.6.1. Pakalpojuma sniedzējs ģenerē CA institūcijas atslēgu pārus HSM iekārtās, kurās šīs atslēgas tiks izmantotas.

6.2.7. **Privātās atslēgas glabāšana kriptogrāfiskajā modulī**

6.2.7.1. Pakalpojuma sniedzēja CA institūcijas privātā atslēga tiek glabāta HSM iekārtās šifrētā formā;

6.2.8. **Privātās atslēgas aktivēšanas metode**

6.2.8.1. Pakalpojuma sniedzēja CA privātā atslēga tiek aktivēta atbilstoši HSM iekārtas ražotāja specifikācijai. CA institūcijas atslēgu aktivēšanu veic ievērojot šī dokumenta 6.2.2. punktā minētās kontroles;

6.2.8.2. Gala lietotāju privāto atslēgu aktivēšanas nosacījumi ir definēti atbilstošos Partnera sniegtā pakalpojuma noteikumos.

6.2.9. **Privātās atslēgas deaktivēšanas metode**

6.2.9.1. Pakalpojuma sniedzēja CA institūcijas privātās atslēgas tiek deaktivētas ar katru sesijas pārrāvumu. CA institūcijas sesiju var pārtraukt autorizēts personāls, vai arī tehniskas HSM iekārtas kļūmes dēļ, piemēram, elektrības pārrāvums;

6.2.9.2. Gala lietotāju privāto atslēgu deaktivēšanas metodes ir definētas atbilstošos Partnera sniegtā pakalpojuma noteikumos.

6.2.10. **Privātās atslēgas iznīcināšanas metode**

6.2.10.1. Privātās atslēgas iznīcina, ja tās vairs nav nepieciešamas vai tām atbilstošo sertifikātu derīguma termiņš ir beidzies, vai arī tās ir anulētas. Privātās atslēgas iznīcina tādā veidā, kas novērš to pazušanu, zādzību, modificēšanu, nesankcionētu izpaušanu vai nesankcionētu lietošanu;

6.2.10.2. CA institūciju privātās atslēgas iznīcināšanas metodes ir atkarīgas no HSM iekārtas specifikas;

6.2.10.3. CA institūcijas privātā atslēga tiek uzskatīta par iznīcinātu, ja, atbilstoši HSM iekārtas ražotāja specifikācijai minētā HSM glabātās atslēgas un visas šo atslēgu rezerves kopijas ir iznīcinātas;

6.2.10.4. HSM iekārtas tiek uzskatītas par norakstītām kad ar konkrētajā HSM iekārtā glabātie kriptogrāfiskie materiāli ir iznīcināti un HSM iekārtas atmiņa ir izdzēsta vai iznīcināta atbilstoši HSM iekārtas ražotāja specifikācijā noteiktajā kārtībā.

6.2.11. **Prasības kriptogrāfiskajiem moduļiem**

6.2.11.1. Skatīt šī dokumenta 6.2.1. punktu.

6.3. **Citi atslēgu pāra pārvaldības aspekti**

6.3.1. **Publiskās atslēgas arhivēšana**

6.3.1.1. Kā daļa no Pakalpojuma sniedzēja IS regulārajām rezerves kopiju izveides procedūrām tiek veikta visu Pakalpojuma sniedzēja CA izsniegto publisko atslēgu rezerves kopiju izveide un saglabāšana;

6.3.1.2. Pakalpojuma sniedzējs šī dokumenta 5.5.2. punktā norādīto termiņu glabā visus CA izsniegtos sertifikātus un ar tiem saistītās privātās atslēgas.

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;

6.3.2.2. Turklāt Pakalpojuma sniedzēja CA pārtrauc izsniegt jaunus sertifikātus noteiktā datumā pirms minētā CA sertifikāta derīguma termiņa beigām tādā veidā, lai neviena minētā CA izsniegta sertifikāta derīguma termiņš nebeigtos pēc konkrētā CA sertifikāta derīguma termiņa beigām;

6.3.2.3. Maksimālais sertifikātu darbības laiks, kas izsniegti šo noteikumu darbības laikā:

6.3.2.3.1. Saknes CA sertifikātam – astoņpadsmit gadi;

6.3.2.3.2. Izsniegšanas CA sertifikātam – deviņi gadi;

6.3.2.3.3. Gala lietotāju sertifikātu darbības nepārsniegs trīs gadus.

6.4. **Aktivēšanas dati**

6.4.1. **Aktivēšanas datu ģenerēšana un instalēšana**

6.4.1.1. Pakalpojuma sniedzēja CA institūcijas privāto atslēgu aktivēšanas datu ģenerēšana un uzstādīšana tiek veikta atbilstoši izmantoto HSM iekārtas ražotāja specifikācijai;

6.4.1.2. Gala lietotāju privāto atslēgu PIN ģenerēšana un uzstādīšana ir definēta atbilstošos Partnera sniegtā pakalpojuma noteikumos.

6.4.2. **Aktivēšanas datu aizsardzība**

6.4.2.1. Pakalpojuma sniedzēja CA institūcijas privāto atslēgu 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;

6.4.2.2. Gala lietotāju privāto atslēgu PIN aizsardzības prasības ir definētas atbilstošos Partnera sniegtā pakalpojuma noteikumos.

6.4.3. **Citi aktivēšanas datu aspekti**

6.4.3.1. Citi aktivēšanas datu aspekti un nosacījumi ir definēti atbilstošos Partnera sniegtā pakalpojuma noteikumos.

6.5. **Datoru drošības kontroles**

6.5.1. **Pakalpojuma sniedzēja specifiskās datoru drošības tehniskās prasības**

6.5.1.1. Pakalpojuma sniedzējs ir ieviesis kontroļu kopu Pakalpojuma sniedzēja informācijas sistēmu aizsardzībai:

6.5.1.1.1. Operacionālās kontroles:

6.5.1.1.1.1. Visas darbības ar sistēmu ir dokumentētas atbilstošās rokas grāmatās un procesu aprakstos;

6.5.1.1.1.2. Ir izstrādāts darbības nepārtrauktības plāns;

6.5.1.1.1.3. Izstrādāta nepieciešamā dokumentācija un ieviesti atbilstoši risinājumi, lai nodrošinātu pret datorvīrusu un citu ļaunprātīgu kodu aizsardzību;

6.5.1.1.1.4. Lai nodrošinātu nepārtrauktu pieejamību un integritātes nodrošināšanu, visas iekārtas un sistēmas tiek patstāvīgi uzturētas;

6.5.1.1.1.5. Ir izstrādāta atbilstoša iekšējā dokumentācija un procesi vecu iekārtu, datu nesēju un noņemamo datu nesēju saglabāšanai un drošai iznīcināšanai;

6.5.1.1.1.6. Visas izmaiņas tiek testētas atbilstošā vidē un apstiprinātas pirms likšanas produkcijas vidē;

6.5.1.1.1.7. Visas kritiskās Pakalpojuma sniedzēja komponentes tiek uzstādītas un atjaunotas tikai no uzticamiem avotiem.

6.5.1.1.2. Datu apmaiņas kontroles:

6.5.1.1.2.1. Ir ieviesti risinājumi savienojumu šifrēšanai pirms reģistrācijas un reģistrācijas datu apmaiņai starp reģistrācijas institūciju un reģistrācijas datubāzi, kā arī datu apmaiņas savienojumiem starp RA un CA.

6.5.1.1.3. Tiek nodrošināta sertifikātu statusa pārbaudes servisa funkcionalitāte 2.1. punktā noteiktajā pieejamības režīmā.

6.5.1.1.4. Piekļuves kontroles:

6.5.1.1.4.1. Ir izstrādāta nepieciešamā iekšējā dokumentācija, kas detalizēti regulē piekļuves kontroles;

6.5.1.1.4.2. Tiek izmantoti unikāli lietotāju identifikatori, kas tiek piešķirti konkrētiem lietotājiem un tie ir atbildīgi var savām darbībām;

6.5.1.1.4.3. Lietotāju tiesības tiek piešķirtas izmantojot minimālo privilēģiju principu, nodrošinot piekļuves tikai tām darbībām, kas nepieciešamas savu pienākumu pildīšanai;

6.5.1.1.4.4. Gadījumos, ja lietotājs maina savu amatu vai pārtrauc darba tiesiskās attiecības ar Pakalpojuma sniedzēju, viņam piešķirtās piekļuves tiesības tiek anulētas nekavējoties;

6.5.1.1.4.5. Lietotājiem piešķirtās piekļuves tiesības un to nepieciešamība tiek regulāri pārskatīta;

6.5.1.1.4.6. Sistēmas privilēģijas tiek piešķirtas, izvērtējot katru gadījumu atsevišķi. Tās tiek nekavējoties noņemtas gadījumos, kad tās vairāk nav nepieciešamas;

6.5.1.1.4.7. Ir izstrādātas un noteiktas paroļu pārvaldības prasības.

6.5.1.1.5. Pakalpojuma sniedzējs ir izstrādājis un ieviesis informācijas drošības politiku un citus ar drošību un drošu pārvaldību saistītus dokumentus, lai nodrošinātu vairāku līmeņu aizsardzību.

6.5.2. **Partnera specifiskās datoru drošības tehniskās prasības**

6.5.2.1. Partneris ir definējis un ieviesis savas specifiskās datoru drošības tehniskās prasības un procedūras, kā arī noteicis to konfidencialitātes līmeni.

6.5.3. **Pakalpojumu sniedzēja sistēmu drošības reitings**

6.5.3.1. Visas Pakalpojuma sniedzēja uzticamas elektronisko parakstu sertifikātu un laika zīmogošanas pārvaldības sistēmas ir sertificētas atbilstoši [ISO/IEC 15408]

6.6. **Dzīves cikla tehniskās kontroles**

6.6.1. **Partnera dzīves cikla tehniskās kontroles**

6.6.1.1. Partneris ir definējis un ieviesis savu gala lietotāju dzīves cikla tehniskās kontroles, kā arī noteicis to konfidencialitātes līmeni.

6.6.2. **Pakalpojumu sniedzēja sistēmas izstrādes kontroles**

6.6.2.1. Visas programmatūras implementēšana produkcijas vidē tiek kontrolēta;

6.6.2.2. Lai izvairītos no potenciālā problēmām produkcijas vidē, tiek izmantotas sekojošas kontroles:

6.6.2.2.1. Tiek veikta pilnvērtīga analīze programmatūras prasību specifikācijas fāzē;

6.6.2.2.2. Jebkuras izmaiņas tiek akceptētas atbilstošā uzraudzības komisijā;

6.6.2.2.3. Visas piegādes tiek elektroniski parakstītas ar izstrādātāju elektronisko parakstu;

6.6.2.2.4. Visas izmaiņas tiek testētas vismaz vienā testa vidē;

6.6.2.2.5. Visas programmatūras implementēšana produkcijas vidē notiek tikai pēc noteiktām instrukcijām un ar visām atbildīgajām personām saskaņotu plānoto darbu laikā.

6.6.3. **Pakalpojumu sniedzēja drošības pārvaldības kontroles**

6.6.3.1. Pakalpojuma sniedzējs veic patstāvīgu sistēmu un komunikāciju uzraudzību, lai pārliecinātos, ka visas sistēmas un komunikācijas darbojās atbilstoši noteiktajām prasībām;

6.6.3.2. Visi procesi tiek žurnalēti un auditēti atbilstoši spēkā esošajiem normatīvajiem aktiem un iekšējiem noteikumiem.

6.6.4. **Dzīves cikla drošības kontroles**

6.6.4.1. Pakalpojuma sniedzējs regulāri pārskata visus, ar informācijas drošību saistītos dokumentus un aktīvus.

6.7. **Tīkla drošības kontroles**

6.7.1. **Partnera tīkla drošības kontroles**

6.7.1.1. Partneris ir definējis un ieviesis savas tīkla drošības kontroles, kā arī noteicis to konfidencialitātes līmeni.

6.7.2. **Pakalpojumu sniedzēja tīkla drošības kontroles**

6.7.3. Datortīklam uzstādīti ugunsmūri, kas atdala dažādus tīkla segmentus. Pakalpojuma sniedzējs uztur vismaz divus (ugunsmūrus, kur viens atdala ārējo tīklu no Pakalpojuma sniedzēja iekšējā tīkla un otrs atdala serveru tīklu no Pakalpojuma sniedzēja administratoru un lietotāju tīkla segmentiem.

Ugunsmūri ir konfigurēti, lai nodrošinātu vienīgi autorizētas datu pārraides izmantošanu;

6.7.4. Pakalpojuma sniedzējs nodrošina maršrutētāju un komutatoru atbilstošu konfigurēšanu, kas nodrošina vienīgi autorizētas datu pārraides izmantošanu, pēc nepieciešamības drošu datu pārraides protokolu izmantošanu, piekļuves kontroles sarakstus, drošu autentifikāciju, kā arī aizsardzību pret tipveida uzbrukumu scenārijiem datortīklā;

6.7.5. Pakalpojuma sniedzēja iekšējais datortīkls ir loģiski sadalīts tīkla segmentos, pēc principa, ka katra komponente pēc tās funkcijas atrodas savā nodalītā tīkla segmentā (vai vairākos);

6.7.6. Komunikācija iekšējā Pakalpojuma sniedzēja tīklā pēc nepieciešamības tiek šifrēta, izmantojot drošus šifrēšanas algoritmus, lai mazinātu noklausīšanās riskus;

6.7.7. Pakalpojuma sniedzējs izmanto pretielaušanās (IDS/IPS) sistēmu, lai stiprinātu aizsardzības kontroles pret ielaušanos Pakalpojuma sniedzēja datortīklā;

6.7.8. Pakalpojuma sniedzējs veic datortīkla datu plūsmas periodisku uzraudzību (sniffing – *angļu val.*), lai pārliecinātos par tīklā pārraidītās datu plūsmas atbilstību Pakalpojuma sniedzēja darbībai un identificētu iespējamos pārkāpumus;

6.7.9. Pakalpojuma sniedzēja atbildīgās personas veic iekšējā tīkla uzraudzības iekārtu un rīku (ugunsmūri, IDS/IPS iekārtas un sistēmas utt.) auditācijas pierakstu periodisku (vismaz reizi mēnesī) analīzi un sniedz ziņojumus drošības pārvaldniekam un Pakalpojuma sniedzēja vadītājam par atklātajiem drošības trūkumiem;

6.7.10. Pakalpojuma sniedzējs izmanto monitoringa sistēmu (SIEM), kas reālā laikā ziņo par aizdomīgiem notikumiem vai atklātajām trauksmēm. Monitoringa sistēmas tiek regulāri pilnveidotas, pamatojoties uz veikto analīzi par datortīkla notikumiem un piemītošajiem riskiem;

6.7.11. Pakalpojuma sniedzējs nodrošina darbinieku kiberdrošības apzināšanās apmācības, kā arī uztur un attīsta IT darbinieku zināšanu līmeni par kiberdrošības jautājumiem;

6.7.12. Pakalpojuma sniedzējam ir izstrādāts Rīcības plāns lielu (major – *angļu val.*) incidentu gadījumos, kurā aprakstītas plānošanas, sagatavošanās, incidenta apjoma apzināšanas, incidenta ierobežošanas, reaģēšanas un atjaunošanas prasības, kā arī noteikta darbinieku komanda, kas būs atbildīga par šāda plāna izpildi;

6.7.13. Pakalpojuma sniedzējs nodrošina tīkla iekārtu aizsardzību pret ļaunatūrām, nodrošinot tīkla iekārtas, serverus un lietotāju darbstacijas ar atbilstošiem risinājumiem, kā arī veic šo risinājumu efektivitātes ikdienas uzraudzību;

6.7.14. Pakalpojuma sniedzējs nodrošina e-pastu sistēmas aizsardzību pret e-pastiem, kas var saturēt ļaunprātīgu kodu, nepiemērotu vai neidentificējamu saturu;

6.7.15. Aizsargājamas informācijas apritei Pakalpojuma sniedzējs izmanto e-pastu vai datu (informācijas) šifrēšanas mehānismus, lai nodrošinātu drošu informācijas apmaiņu ar ārējiem sadarbības partneriem;

6.7.16. Attālināta piekļuve Pakalpojuma sniedzēja datortīklam ir pieļauta tikai no noteiktām gala iekārtām (tīkliem) un tikai izmantojot speciālas attālinātās piekļuves uzraudzības un nodrošināšanas iekārtas;
6.7.17. Pakalpojuma sniedzējs veic regulāru datortīkla ielaušanās testēšanu, kā arī datortīkla drošības pārvaldības kontroļu efektivitātes novērtēšanu un auditus;
6.7.18. Pakalpojuma sniedzējs uztur aktuālas datortīkla loģiskās un fiziskās shēmas;
6.7.19. HSM iekārtas atrodas atsevišķā drošības zonā, kurai nav tiešas piekļuves no publiskā tīkla;
6.7.20. Saknes CA atrodas augstas drošības zonā un nav pieslēgts nevienam tīklam;
6.7.21. Piekļuve drošības un augstas drošības zonām ir tikai personālam ar uzticības lomām;
6.7.22. Pakalpojuma sniedzēja sistēma ir dublēta vismaz divos datu centros. Komunikācija starp datu centriem tiek pilnībā kontrolēta ar Pakalpojuma sniedzēja resursiem.

6.8. **Laika zīmogošana**

6.8.1. Pakalpojuma sniedzējs kā uzticamības laika zīmogošanas pakalpojumu sniedzējs piedāvā kvalificētu elektronisko laika zīmogošanas servisu atbilstoši Pakalpojuma sniedzēja laika zīmogošanas politikai;
6.8.2. Pakalpojuma sniedzēja IS darbības nodrošināšanai neizmanto laika zīmogus. Pakalpojuma sniedzēja IS darbības nodrošināšanai tiek izmantots precīzs laiks, kas tiek saņemts no uzticama avota. Šāda laika informācija nav bāzēta uz kriptogrāfiskiem risinājumiem;
6.8.3. Pakalpojuma sniedzējs izmanto precīzu laiku, ko iegūst no vismaz 3 sertificētām NTP laboratorijām;
6.8.4. Visu Pakalpojuma sniedzēja IS saistīto komponenšu maksimālā laika nobīde nepārsniegs vienu sekundi.

7. Sertifikātu, CRL un OCSP profili

7.1. **Sertifikātu profils**

7.1.1. CA sertifikātu profilu nosacījumi un prasības ir definētas [Sertifikātu profili].
7.1.2. Gala lietotāju sertifikātu profili ir definēti atbilstošos Partnera sniegtā pakalpojuma noteikumos.

7.2. **CRL profili**

7.2.1. Detalizēti nosacījumi un prasības ir definētas [Sertifikātu profili].

7.3. **OCSP Profili**

7.3.1. Detalizēti nosacījumi un prasības definētas [Sertifikātu profili].

8. Citi biznesa un juridiskie jautājumi

8.1. **Maksājumi**

8.1.1. Partnera maksājumus nosaka savstarpēji noslēgtais līgums un cenrādis.

8.2. **Biznesa informācijas konfidencialitāte**

8.2.1. **Konfidenciāli glabājamas informācijas sfēra**

8.2.1.1. Visa informācija, kuru Pakalpojuma sniedzējs saņem, sniedzot Pakalpojumus un kura nav paredzēta publicēšanai, ir konfidenciāla

(neizpaužama) un paredzēta tikai Pakalpojuma sniedzēja iekšējai lietošanai atbilstoši normatīvajiem aktiem.

8.2.2. **Par konfidenciālu neuzskatāmas informācijas tipi**

8.2.2.1. Šī dokumenta 2.2. punktā minētā informācija tiek uzskatīta par publisku;

8.2.2.2. Pakalpojuma sniedzēja rīcībā esošā nepersonalizētā statistikas informācija var tikt uzskatīta par publisku un nepieciešamības gadījumā Pakalpojuma sniedzējam ir tiesības to publicēt.

8.2.3. **Pienākums aizsargāt konfidenciālu informāciju**

8.2.3.1. Pakalpojuma sniedzējs un Partneris veic nepieciešamās darbības, lai nodrošinātu konfidenciālas informāciju pret kompromitēšanu un nodrošinātu tās neizpaušanu trešajām pusēm, ieviešot dažādas drošības politikas.

8.2.3.2. Pakalpojuma sniedzējam ir tiesības izpaust konfidenciālu informāciju tikai saskaņā ar normatīvajiem aktiem.

8.3. **Fizisko personu datu informācijas privātums**

8.3.1.1. Pakalpojuma sniedzējs nodrošina fizisko personu datu privātumu atbilstoši Privātuma politikā noteiktajam, kas ir publicēta Pakalpojuma sniedzēja mājaslapā www.eparaksts.lv.

8.3.2. **Par konfidenciālu neuzskatāma informācija**

8.3.2.1. Sertifikātu un sertifikātu statusa informācija tiek atklāta visiem nolūkiem, kas var būt nozīmīgi šādas informācijas un sertifikātu statusa izmantošanai saskaņā ar personas sniegto piekrišanu Pakalpojuma sniedzējam, izņemot gadījumos, kas noteikti normatīvajos aktos. Pēc sertifikātu apstiprināšanas pakārtotās CA pilnvaro Pakalpojuma sniedzēju publicēt informāciju, kas norādīta izsniegtajā sertifikātā, un citu informāciju, kas nepieciešama Pakalpojumu nodrošināšanai.

8.3.3. **Pienākums aizsargāt personu datus**

8.3.3.1. Pakalpojuma un Partnera vienības apstrādā fizisko personu datus atbilstoši Pakalpojumu sniedzēja Privātuma politikai.

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

8.3.4.1. Pakalpojuma sniedzējs ir tiesīgs atklāt personas datus saskaņā ar Privātuma politikā noteikto.

8.3.5. **Citi informācijas atklāšanas apstākļi**

8.3.5.1. Nav nosacījumu

8.4. **Intelektuālā īpašuma tiesības**

8.4.1. Visas ar intelektuālo īpašumu saistītās tiesības, tostarp visu sertifikātu, atsaukto un apturēto sertifikātu sarakstu, OCSP sertifikāta statusa ziņojumu, sertifikātu direktoriju, visu procedūru, politiku, Pakalpojuma sniedzēja PKI ekspluatācijas un drošības dokumentu (elektronisku un citādu), kā arī līgumu autortiesības un/vai mantiskās tiesības pieder Pakalpojuma sniedzējam un turpinās būt tā īpašums, ja vien nav noteikts citādi.

8.5. **Pārstāvības un garantijas**

8.5.1. **Pakalpojuma sniedzēja pārstāvība un garantijas.**

8.5.1.1. Pakalpojuma sniedzējs izpilda savu daļu no tiesībām un pienākumiem, kas definēti šajā dokumentā, Privātuma politikā un savstarpēji noslēgtajos Līgumos.

8.5.1.2. Pakalpojuma sniedzējs:

8.5.1.2.1. Sniegs savus pakalpojumus saskaņā ar prasībām un procedūrām, kas noteiktas šajā dokumentā, Privātuma politikā un savstarpēji noslēgtajos līgumos;

8.5.1.2.2. Nodrošinās atbilstību Latvijas Republikā spēkā esošajiem normatīvajiem aktiem;

8.5.1.2.3. Publicēs šo dokumentu Pakalpojuma sniedzēja mājaslapā www.eparaksts.lv;

8.5.1.2.4. Publicēs Privātuma politiku Pakalpojuma sniedzēja mājaslapā www.eparaksts.lv;

8.5.1.2.5. Nodrošinās konfidenciālas informācijas konfidencialitāti;

8.5.1.2.6. Uzskaitīs visus izsniegtos produktus un to derīguma terminus;

8.5.1.2.7. Bez liekas kavēšanās informēs Partneri, ja drošības vai integritātes pārkāpums negatīvi ietekmē to;

8.5.1.2.8. Sniegs Pakalpojuma sniedzēja Pakalpojumus bez jebkādas tiešas vai netiešas diskriminācijas — neatkarīgi no personas rases, ādas krāsas, dzimuma, vecuma, invaliditātes, reliģiskās, politiskās vai citas pārliecības, nacionālās vai sociālās izcelsmes, mantiskā vai ģimenes stāvokļa, seksuālās orientācijas vai citiem apstākļiem;

8.5.2. **Partnera pārstāvība un garantijas**

8.5.2.1. Pakalpojuma sniedzēja reģistrācijas institūcijas:

8.5.2.1.1. Sniegs pakalpojumus atbilstoši prasībām un procedūrām, kas definēti līgumā starp Pakalpojuma sniedzēju un Partneri un šajā dokumentā;

8.5.2.1.2. Nodrošinās saviem darbiniekiem nepieciešamo apmācību;

8.5.2.1.3. Bez liekas kavēšanās informēs Pakalpojuma sniedzēju par ārkārtas situācijām, kuras var būtiski ietekmēt sniegtos Pakalpojumus un to statusu, kā arī apstrādāto personu datus;

8.5.2.1.4. Izmantos uzticamu personālu savu pakalpojumu sniegšanai, kas ir saņēmis nepieciešamo apmācību.

8.5.3. **Gala lietotāja pārstāvība un garantijas**

8.5.3.1. Gala lietotājs:

8.5.3.1.1. Iepazīsies ar šo dokumentu un Partnera sniegtā pakalpojuma noteikumiem;

8.5.3.1.2. Citas gala lietotāja pārstāvības un garantijas prasības nosaka atbilstošos Partnera sniegtā pakalpojuma noteikumos.

8.5.4. **Atkarīgo pušu pārstāvība un garantijas**

8.5.4.1. Atkarīgo pušu pārstāvība un garantijas prasības nosaka atbilstošos Partnera sniegtā pakalpojuma noteikumos.

8.5.4.2. Atkarīgajām pusēm jāpārbauda iesaistīto sertifikātu derīgums, izmantojot Pakalpojuma sniedzēja sniegtos sertifikātu pārbaudes pakalpojumus.

8.5.5. **Citu iesaistīto pušu pārstāvība un garantijas**

8.5.5.1. Atbilstošos Partnera sniegtā pakalpojuma noteikumos.

8.6. **Termiņi un darbības izbeigšana**

8.6.1. Termiņi ir definēti šī dokumenta 2.3. punktā;

8.6.2. Darbības izbeigšana:

8.6.2.1. Šīs dokuments ir spēkā līdz brīdim, kad šīs dokuments tiek aizvietots ar jaunu versiju, vai arī, līdz brīdim, kad Pakalpojuma sniedzējs pārtrauc savu darbību;

8.6.2.2. Līdz Pakalpojuma sniedzēja darbības pārtraukšanai, Pakalpojuma sniedzējam ir pienākums nodrošināt visas fizisko personu datu un konfidenciālās informācijas aizsardzību.

8.6.3. Šī dokumenta darbības izbeigšanas radītās sekas:

8.6.3.1. Visiem gala lietotājiem, kas izmanto sertifikātus, kas izsniegti šī dokumenta iepriekšējās versijas darbības laikā, ir jāievēro sertifikāta izmantošanas laikā spēkā esošā dokumentā noteiktās prasības tik tālu, ciktāl tas nav pretrunā ar šā dokumenta sertifikāta izsniegšanas brīdī spēkā esošo noteikumu versiju.

8.7. **Grozījumi**

8.7.1. Pakalpojuma sniedzējs var vienpusēji izdarīt grozījumus visās politikās un noteikumos, tajā skaitā šī dokumenta 2.2.2.punktā minētajos dokumentos. Šādi grozījumi stājas spēkā ar Pakalpojumu sniedzēja valdes noteikto datumu, bet ne ātrāk kā 30 (trīsdesmit) dienas no attiecīgā paziņojuma izvietošanas Pakalpojuma sniedzēja mājas lapā. Pakalpojumu sniedzējs pirms grozījumu spēkā stāšanās informēs par to Partnerus.

8.7.2. Grozījumu apstiprināšana notiek atbilstoši šī dokumenta 1.5.3. punktā definētajam;

8.7.3. Grozījumu publicēšana notiek atbilstoši šī dokumenta 2.3. punktā definētajam.

8.8. **Strīdu risināšanas kārtība ar Partneri.**

8.8.1. 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;

8.8.2. Ja puses nespēj atrisināt strīdu pārrunu ceļā viena mēneša laikā kopš strīda rašanās, tad puses piekrīt vērsties Latvijas Republikas vispārējās jurisdikcijas tiesā saskaņā ar noslēgto līgumu vai normatīvajiem aktiem. Strīdi netiek izskatīti šķīrējtiesā;

8.8.3. Ja vien puses, noslēgtais līgums vai normatīvie akti nenosaka citādi, visi strīdi starp pusēm tiek risināti Rīgas pilsētas Vidzemes priekšpilsētas tiesā (pirmā instance).

8.8.4. Visus strīdus ar gala lietotājiem risina Partneris, pēc savas noteiktās kārtības.

8.9. **Piemērojamie normatīvie akti**

8.9.1. Šis dokuments tiek pārvaldīts atbilstoši Latvijas Republikā spēkā esošajiem normatīvajiem aktiem.

8.10. **Atbilstība piemērojamiem normatīvajiem aktiem**

8.10.1. Pakalpojuma sniedzējs darbojas atbilstoši un nodrošina atbilstību šādiem normatīvajiem aktiem:

8.10.1.1. Eiropas Parlamenta un Padomes 2014. gada 23. jūlija regulai (ES) nr.910/2014 “Par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK”;

8.10.1.2. Fizisko personu datu aizsardzības likumam;

8.10.1.3. Fizisko personu elektroniskās identifikācijas likumam un saistītajiem Ministru kabineta noteikumiem.
8.10.1.4. Citiem uz Pakalpojumu sniedzēju darbību attiecināmajiem normatīvajiem aktiem.

8.11. **Dažādas prasības**

8.11.1. Katra šī dokumenta atruna ir spēkā pati par sevi (pēc būtības) un neietekmē pārējās atrunas.

8.11.2. Nevienu no šī dokumenta prasībām vai noteikumiem nevar grozīt, atteikties, papildināt vai likvidēt bez apstiprinātas rakstiskas Pakalpojuma sniedzēja piekrišanas.

8.11.3. Noteikumi ir sagatavoti latviešu valodā. Dokuments var tikt tulkots un var būt pieejams arī citās valodās. Dokumenta tulkojumu nesakritību gadījumā dokumenta versija latviešu valodā vienmēr ir vadoša.

8.12. **Citas prasības**

8.12.1. Nav nosacījumu.

9. Noslēguma noteikumi

9.1. Par Noteikumu pārvaldību ir atbildīga EPD.

9.2. Noteikumos tiek veikti grozījumi, mainoties Latvijas Republikas normatīvajiem aktiem vai saistošajos normatīvajos aktos.

9.3. Noteikumos neatrunātie darba kārtības jautājumi tiek risināti saskaņā ar Latvijas Republikas normatīvajiem aktiem.

9.4. Noteikumi stājas spēkā pēc to apstiprināšanas LVRTC valdes sēdē valdes lēmumā noteiktajā kārtībā.

9.5. Noteikumu spēkā esošā versija tiek uzturēta eParaksts portāla (www.eparaksts.lv) repozitorijā.