Uzticamības pakalpojumu sniegšanas
NOTEIKUMI

Publisks

SAISTĪTIE DOKUMENTI:

1. Uzticamības pakalpojumu vispārējie noteikumi
2. Uzticamības pakalpojuma “eID karte” sniegšanas politika
3. Uzticamības pakalpojuma “eParaksts” sniegšanas politika
4. Uzticamības pakalpojuma “eParaksts karte” sniegšanas politika
5. Uzticamības pakalpojuma “eParaksts karte+” sniegšanas politika
6. Uzticamības pakalpojumu “eZīmogs” un “eZīmogs+” sniegšanas politika
7. Uzticamības pakalpojumu sniedzēja laika zīmogošanas politika
8. [FPDAL] Fizisko personu datu aizsardzības likums
9. [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”
10. [ISO/IEC 15408] “Informācijas tehnoloģija. Drošības paņēmieni. IT drošības izvērtēšanas kritēriji”
11. [ETSI EN 319 403] Uzticamības pakalpojumu sniedzēju atbilstības revīzija – prasības atbilstības novērtēšanas struktūrām kuras veic uzticamu pakalpojumu sniedzēju uzraudzību
12. [ETSI EN 319 401] Vispārējās politikas prasības Uzticamības pakalpojumu sniedzējiem
13. [ETSI EN 319 411-1] Politikas un drošības prasības Uzticamības pakalpojumu sniedzējiem, kas izdod sertifikātus; 1.daļa – Vispārīgās prasības
14. [ETSI EN 319 411-2] Politikas un drošības prasības Uzticamības pakalpojumu sniedzējiem, kas izdod sertifikātus; 2.daļa – Politikas prasības sertifikācijas centriem, kas izdod kvalificētus sertifikātus

15. [ETSI TS 119 312] Šifrēšanas komplekti
16. [Sertifikātu profili] UPS izsniegto sertifikātu profilu apraksts
17. Ministru kabineta 2012.gada 21. februāra noteikumi Nr.134 "Personu apliecinošu dokumentu noteikumi"
18. Elektronisko dokumentu likums

IZMAIŅU VĒSTURE:

Pārskatītā varianta nr.	**Spēkā stāšanās datums**	**Izmaiņu kopsavilkums**
01.0	01.07.2017.	Sākotnējā versija
01.1.	01.07.2017	Pievienoti 1.5.4., 1.5.5., 6.2.10.4., 9.16.3. punkti 5.7.1.7. punkts papildināts ar laiku, kurā UPS ir jāinformē uzraudzības iestāde. 5.8.1.2.1. punkts papildināts ar laiku, kurā UPS informē uzraudzības iestādi un klientus.
02.0	01.08.2017	Papildināts ar uzticamības pakalpojumu “eParaksts”, un tā prasībām (1.1.3.1., 4.6.4, 4.7.3., 4.12.1.); Detalizēti 1.3.2.4.1. un 1.3.2.4.2. punkti; Precizēti sertifikātu apturēšanas gadījumi (4.9.6.) atbilstoši elektronisko dokumentu likumam.

SATURS

1. Ievads

Valsts akciju sabiedrība “Latvijas Valsts Radio un Televīzijas centrs” 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 uzticamu sertifikācijas pakalpojumu sniegšanu.

1.1. Dokumenta nolūks

1.1.1. Šis dokuments apraksta uzticamības pakalpojuma sniedzēja nodrošināto uzticamības pakalpojumu sniegšanas procedūras.

1.1.2. Šis dokuments attiecās tikai uz elektroniskajiem sertifikātiem, ko izsniedz “eParaksts Root CA” saknes sertifikācijas institūcija un zemākā līmeņa pakārtotās izsniegšanas institūcijas.

1.1.3. Atbilstošie uzticamības pakalpojumi un to politikas

1.1.3.1. Šis dokuments ir saistīts ar sekojošiem pakalpojumiem un to politikām

Pakalpojuma nosaukums	Politika	QSCD	Politikas OID vērtība
eID karte	Uzticamības pakalpojuma “eID karte” sniegšanas politika	Jā	1.3.6.1.4.1.32061.2.1.2.1
eParaksts	Uzticamības pakalpojuma “eParaksts” sniegšanas politika	Nē	1.3.6.1.4.1.32061.2.1.3.1
eParaksts karte	Uzticamības pakalpojuma “eParaksts karte” sniegšanas politika	Jā	1.3.6.1.4.1.32061.2.1.4.1
eParaksts karte+	Uzticamības pakalpojuma “eParaksts karte+” sniegšanas politika	Jā	1.3.6.1.4.1.32061.2.1.5.1
eZīmogs	Uzticamības pakalpojumu “eZīmogs” un “eZīmogs+” sniegšanas politika	Nē	1.3.6.1.4.1.32061.2.2.1.1
eZīmogs+	Uzticamības pakalpojumu “eZīmogs” un “eZīmogs+” sniegšanas politika	Jā	1.3.6.1.4.1.32061.2.2.1.1
Kvalificēti laika	Uzticamības pakalpojumu sniedzēja	Nē	ETSI OID =

Pakalpojuma nosaukums	Politika	QSCD	Politikas OID vērtība
zīmogi	laika zīmogošanas politika		0.4.0.2023.1.1

1.1.3.2. Politikas OID vērtības ir aprakstītas atbilstošās politikās kas minētas 1.1.3.1. punktā.

1.2. Dokumenta nosaukums un identifikācija

1.2.1. Šī dokumenta nosaukums ir “Uzticamības pakalpojumu sniegšanas noteikumi”

1.3. Publiskās atslēgas infrastruktūras dalībnieki

1.3.1. Uzticamības 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. Uzticamības pakalpojumu abonenti;

1.3.1.4. Atkarīgās puses.

1.3.2. Sertifikācijas institūcijas

1.3.2.1. Uzticamības pakalpojuma sniedzējs 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;

1.3.2.2.2. Laika zīmogošanas 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	SHA384RSA

X.509 V1	Content
Algorithm	
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 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

X.509 V1	Content
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. Uzticamības pakalpojuma sniedzējs pārvalda šādas izsniegšanas sertifikācijas institūcijas (CA):

1.3.2.4.1. “LV eID ICA 2017” sertifikātu izsniegšanas sertifikācijas institūciju (CA);

1.3.2.4.1.1. “LV eID ICA 2017” sertifikātu izsniegšanas sertifikācijas institūcija izsniedz:

1.3.2.4.1.1.1. Sertifikātus “eID karte” pakalpojumam;

1.3.2.4.1.1.2. Sertifikātus “eParaksts” pakalpojumam;

1.3.2.4.1.1.3. Sertifikātus tiešsaistes sertifikātu pārbaudes (OCSP) servisam;

1.3.2.4.1.1.4. Atsaukto sertifikātu sarakstus (CRL).

1.3.2.4.1.2. “LV eID ICA 2017” sertifikāta izvilkums:

X.509 V1	Content
Version	*V3*
Serial number	6d dd 89 45 49 f5 20 e3 58 a4 3a 89 6b 67 54 08
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	trešdiena, 2017. gada 15. februārī 13:24:57
Valid To	svētdiena, 2026. gada 15. februārī 13:24:57

Subject	CN = LV eID ICA 2017 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 d9 1d 26 0b 26 31 76 a9 eb 1d 45 05 3b 20 55 f2 ad a1 d8 9b 82 ac ac 0c f9 01 66 ce 0b e8 90 52 8a 99 63 56 46 d4 ab 31 f4 c9 9c e1 72 9f 51 ca ff 1c 92 11 16 4e 3d ca 97 42 07 c3 b3 b8 34 31 7a ad d7 3a 17 50 db 14 39 d4 a0 ba c6 ed 53 c4 fd ea 10 1a 92 11 7a 45 fb a2 68 b5 db 3a 11 01 f8 4e 5a b1 e5 05 5f 7b 59 a2 a8 34 66 83 79 67 86 d7 8a e6 04 da a0 3c 44 8b 1c 53 81 2f 4b fd c6 a9 b6 94 5a 55 08 0b aa ef b0 01 04 bc 12 5b 45 96 5c 79 c3 65 75 37 00 d2 bd 85 19 8f 53 4b 4a f8 81 d0 e2 9c 9e 07 11 1d 5f ea a4 7e 6a 0b b9 6a d2 ea e0 2c 5f 07 e2 6c 77 ef 77 4a da 00 b4 36 a6 28 ab 6e 91 61 14 fc be 9f d3 e3 5a 9c 3a bd ea ea a9 fe 3d e3 25 f1 68 df 2e 6f 1a 69 bf a0 fa 08 45 57 6a a1 1f d4 28 52 54 4b 05 1e 1e eb 2a e0 73 77 e7 08 ec c0 fc f0 fc ba 10 39 b5 05 85 ec 86 4c 62 39 41 c2 da f1 d6 b2 77 f0 03 bb 09 c5 14 1c 74 33 be 71 b0 59 9e a8 04 6c b9 b7 33 12 8c d0 78 fd b1 aa 94 41 b2 de a1 59 a1 05 37 ab 20 c8 13 21 2b 7a 5f 5f 5b 34 9f 90 98 bc fd 70 cb 4c de 3e d7 8c 25 8e 03 16 1e cd ef 6c 62 a1 ec 6b 3e 3f bf 84 75 b3 81 ea 29 c5 63 9b 5c 41 56 21 50 6c 8f 2f 4d 82 5c 5b a3 cf 42 11 fd 62 77 08 74 a7 43 01 1d f3 cd bd 1a 1b c8 80 68 06 be 97 e8 0b 48 1b 6d e2 20 1c 79 d0 9d a6 2d e9 8a 6c 29 fd 43 97 ef 01 73 dd ad c0 4d da b5 13 76 aa 88 a6 71 fa 67 ed 26 d7 33 b4 e2 4c 07 87 3c 46 5e 4f ba c1 dd 91 cf 2e cb 19 b1 b2 fa dd 27 ef 3a f4 45 41 91 84 f9 93 2f 71 fa 0a 2c 9d 53 58 82 77 e8 90 cc 27 f4 ee 66 49 71 8a 48 32 ec 7c 28 93 4f 2d 5e 48 de a3 bc c8 9f 8e 5e 4e 04 bf 7f 5b 10 1e ea c1 99 4c 11 81 02 03 01 00 01	
X.509 V3 Extensions	**Critical?**	**Content**
Subject Key Identifier	No	dd 91 3b 81 ef 5f d5 11 fc b5 81 6c 9e cb 89 31 9f 61 9c 94
Authority Key Identifier	No	KeyID=0e ff 89 3e 7f 5e 6d eb b5 67 a2 0a e7 b3 78 5c fb 93 bc e9

Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.0 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [3]Certificate Policy: Policy Identifier=0.4.0.2042.1.1 [3,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [4]Certificate Policy: Policy Identifier=0.4.0.2042.1.2 [4,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	No	[1]Authority Info 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
CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_Root_CA.crl
Basic Constraints	Yes	Subject Type=CA Path Length Constraint=None
Key Usage	Yes	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Properties		
Thumbprint Algorithm	sha1	
Thumbprint	7c e6 e2 c6 bf 58 2b a8 d5 70 fd 4a fc 3d 96 39 d1 89 6b 86	

1.3.2.4.2. “eParaksts ICA 2017” sertifikātu izsniegšanas sertifikācijas institūciju (CA):

1.3.2.4.1. “eParaksts ICA 2017” izsniegšanas sertifikācijas institūcija izsniedz:

1.3.2.4.1.1. Sertifikātus “eParaksts karte” pakalpojumam;

1.3.2.4.1.2. Sertifikātus “eParaksts karte+” pakalpojumam;

1.3.2.4.1.3. Sertifikātus “eZīmogs” pakalpojumam;

1.3.2.4.1.4. Sertifikātus “eZīmogs+” pakalpojumam;

1.3.2.4.1.5. Sertifikātus tiešsaistes sertifikātu pārbaudes (OCSP) servisam;

1.3.2.4.1.6. Atsaukto sertifikātu sarakstus (CRL).

1.3.2.4.2. “eParaksts ICA 2017” sertifikāta izvilkums

X.509 V1	**Content**
Version	*V3*
Serial number	3d c7 d6 32 b0 2e c4 b3 59 03 25 31 03 1b 35 16
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 28. aprīlī 14:19:13
Valid To	otrdiena, 2026. gada 28. aprīlī 14:19:13
Subject	CN = eParaksts ICA 2017 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 b1 a9 56 40 4a 80 e6 02 0a 86 cc eb 76 14 e1 9f dc d3 fa f2 02 42 be dc 96 84 d9 ba 7c 9c b4 ed 9b ea f0 ff b6 1d 81 7d 24 10 67 79 06 5c bc f7 29 48 02 90 24 96 e9 48 f7 19 cb d4 31 2b ca 8e dd 19 cf ea 45 5a a2 7e d9 6f e1 70 99 82 7d 51 a4 22 7b 64 45 05 9b 58 c5 98 05 5e 0d 3e f0 46 eb e5 d0 e2 4f ca a4 b3 20 22 7e 30 17 50 c3 52 cf 64 cc 33 ef 41 61 d1 4a 6a c3 e5 a0 78 63 cb 8b ba 8d 28 79 90 d5 cd a3 c3 8b 2d 18 31 0a ff 40 48 2e 55 7f 58 35 c8 97 9b e9 f5 43 94 95 79 0d 49 af 6e 8f 04 fc 00 5f 0a 02 04 8a 86 49 36 22 30 39 f0 73 a5 b3 0a 9c da 07 b9 2c 94 5a 29 fe 96 c8 40 b3 7d fb 20 b5 50 4b 09 b9 cd 30 52 ff 74 20 69 d9 2e 21 74 4a c9 6c 58 48 28 5d 57 4b 02 97 0b 57 24 99 5f 39 59 02 a0 9a 59 8e 23 e7 20 09 29 78 21 88 76 07 b6 3a 04 e5 66 74 85 b5 1c 4e a1 06 a5 25 1e 10 b4 b0 3c c5 7c 62 09 84 62 2e 66 7c 0b af d8 e4 f0 a5 bd 91 97 a7 c1 30 f9 6e 09 74 9c 23 31 aa 4b e8 d0 e8 a7 90 d0 e7 b8 09 ba 9f 1d bd 4a 91 b1 87 5d ad b0 1f f2 0c c6 34 44 76 a0 c5 55 f3 59 1b 7a f3 0d dd 3d 34 ce bf 32 9d 23 58 fc 4d 42 7f b3 0d 0e 81 be bc a1 71 43 67 ae 5f c1 a2 0f 54 16 9f 60 18 59 0b 12 f7 9f cb c0 c9 e1 94 6a 65 77 13 97 b8 61 9e 63 73 12 4d b3 65 f4 e1 89 ae e3 c0 27 0c d3 5d 1d c7 fd 83 16 b1 df dd 1d 51 d8 e4 96 85 a8 64 d6 ed 0d a3 2f 87 ec fe 33 c1 ed 0d a0 e6 2b c8 6f fa 2b 7c e6 77 5c 29 23 d3 93 c8 29 ed 29 49 a8 84 79 ed be 10 f9 6f 75 dc 90 80 48 d0 f3 ca 2d 8c bf b8 dd 12 e4 d0 86 67 aa 9e 8a c8 88 20 49 39 29 d3 69 57 82 39 32 71 8d 5c b0 3b 3b a9 7a 7a 1e b4 fa ed 10 f0 9b 45 1f 8b b9 ec d7 02 03 01 00 01	
X.509 V3 Extensions	**Critical?**	**Content**
Subject Key Identifier	No	6f 5b c3 24 7a ba a3 3c ea 0b f9 41 d8 a5 dd 84 48 ca e0 14
Authority Key Identifier	No	KeyID=0e ff 89 3e 7f 5e 6d eb b5 67 a2 0a e7 b3 78 5c fb 93 bc e9

Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.0 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [3]Certificate Policy: Policy Identifier=0.4.0.194112.1.1 [3,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [4]Certificate Policy: Policy Identifier=0.4.0.194112.1.3 [4,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [5]Certificate Policy: Policy Identifier=0.4.0.2042.1.1 [5,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [6]Certificate Policy: Policy Identifier=0.4.0.2042.1.2 [6,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	No	[1]Authority Info 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
CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_Root_CA.crl
Basic Constraints	Yes	Subject Type=CA Path Length Constraint=None
Key Usage	Yes	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Properties		

Thumbprint Algorithm	sha1
Thumbprint	23 f2 4e 3f 8b bf 5f 1c 3e d4 b8 7a e2 cc 53 cc ef 6b 2e a7

1.3.3. **Reģistrācijas institūcijas**

1.3.3.1. Šis dokuments attiecās uz visām reģistrācijas institūcijām, kurām Uzticamības pakalpojuma sniedzējs ir deleģējis veikt noteiktas vai visas reģistrācijas institūcijas funkcijas, kas saistītas ar Uzticamības pakalpojuma sniedzēja sniegtajiem uzticamības pakalpojumiem.

1.3.3.2. Reģistrācijas institūcija identificē pieteicējus un abonentus, pārbauda iesniegtos dokumentus un identitāti apliecinošos dokumentus (klātienes pārbaudē), pārstāvību apliecinošos dokumentus (ja attiecināms), pārbauda un apstiprina sertifikātu izsniegšanas, apturēšanas/anulēšanas un atjaunošanas pieprasījumus.

1.3.3.3. Reģistrācijas institūcijas funkcijas izpilda Uzticamības pakalpojuma sniedzējs vai juridiskās personas, ar kurām ir noslēgts līgums par noteiktu vai visu reģistrācijas funkciju deleģēšanu.

1.3.3.4. Papildu reģistrācijas institūcijas pienākumi un lomas ir detalizētas konkrētā uzticamības pakalpojumu politikā.

1.3.3.5. Reģistrācijas institūciju pienākumi un atbildības ir definētas šī dokumenta 9.6.2. punktā.

1.3.4. **Abonenti**

1.3.4.1. Abonenti ir definēti katrā konkrētā uzticamības pakalpojumu politikā.

1.3.4.2. Abonentu pienākumi un atbildība ir definētas šī dokumenta 9.6.3. punktā.

1.3.5. **Atkarīgās puses**

1.3.5.1. Atkarīgās puses ir definētas šī dokumenta 1.6. punktā.

1.3.5.2. Atkarīgo pušu pienākumi un atbildība ir definētas šī dokumenta 9.6.4. punktā.

1.4. Sertifikātu pielietojums

1.4.1. Uzticamības pakalpojuma sniedzējs izsniedz kvalificētus un nekvalificētus sertifikātus. Izsniegto sertifikātu veidi un pielietojums ir definēts atbilstošā uzticamības pakalpojumu politikā.

1.5. Noteikumu pārvaldība

1.5.1. Atbildīgais par šo "Uzticamības pakalpojuma sniegšanas noteikumu" pārvaldību ir valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs" (Reģ. Nr. 40003011203), kas darbojās kā uzticamības pakalpojumu sniedzējs atbilstoši šiem noteikumiem.

1.5.2. **Kontaktinformācija**

Valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs"	
Adrese	Ērgļu iela 7, Rīga, LV-1012, Latvija
Uzticamības pakalpojumu palīdzības dienests	
Tālrunis	+371 67108787
e-pasts	eparaksts@eparaksts.lv
Birojs	
Tālrunis	+371 67198704
e-pasts	lvrtc@lvrtc.lv

1.5.3. Uzticamības pakalpojumu sniedzēja noteikumu apstiprināšanas procesi

1.5.3.1. "Uzticamības pakalpojumu sniegšanas noteikumus" apstiprina Valsts akciju sabiedrības "Latvijas Valsts radio un televīzijas centrs" Valde.

1.5.4. Noteikumos veic grozījumus, mainoties Latvijas Republikā spēkā esošie normatīvie akti, kā arī pilnveidojot UPS sistēmu darbību vai biznesa procesus.

1.5.5. Noteikumi tiek caurskatīti vismaz vienu reizi gadā.

1.6. Termini un saīsinājumi

Termins, saīsinājums	Skaidrojums
Abonents	Fiziska vai juridiska persona, kas ir noslēgusi līgumu ar UPS vai kurai tiek sniegti UPS pakalpojumi, pamatojoties uz normatīvo aktu, nenoslēdzot līgumu par vienu vai vairākiem uzticamības vai citu UPS sniegto pakalpojumu saņemšanu. Iekļauj sevī Parakstītājus, Zīmoga radītājus, Laika zīmogu pieprasītājus un Autentifikācijas sertifikātu lietotājus.
Atkarīgā puse	Fiziska vai juridiska persona, kas paļaujas uz elektronisku identifikāciju vai uzticamības pakalpojumu
Autoritatīvs avots	Jebkura veida avots, uz kuru var paļauties, ka tas sniedz precīzus datus, informāciju un/vai pierādījumu, ko var izmantot identitātes pierādīšanai
CA	Sertifikātu izsniegšanas institūcija
CP	Uzticamības pakalpojumu politika
CPS	Uzticamības pakalpojumu sniedzēja noteikumi
CRL	Atsaukto sertifikātu saraksts
“eParaksts”	UPS sniegts uzticamības pakalpojums kas satur autentifikācijas sertifikātu “eParaksts mobile” mobilās ierīces atslēgu pārvaldības aplikācijā un kvalificētu elektroniskā paraksta sertifikātu “eParakstsTX” risinājumā.
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”
IS	Lietojums (informācijas sistēma)
Kvalificēts sertifikāts	Elektroniskā zīmoga vai elektroniskā paraksta sertifikāts, ko izsniedz kvalificēts uzticamības pakalpojumu sniedzējs un kas atbilst [eIDAS regulas] noteiktajām prasībām attiecībā uz kvalificētu sertifikātu;
eID	eID karte jeb personas apliecība – Latvijas Republikas personu

	apliecinošs dokuments, ko izsniedz PMLP un ar kuru fiziskā persona apliecināt savu identitāti un tiesisko statusu gan klātienē, gan attālināti – interneta vidē, kā arī veikt dokumentu parakstīšanu ar kvalificētu elektronisko parakstu
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	Valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs"
NTP	Tīkla laika protokols
LDAP	Direktoriju vieglpiekļuves protokols
Objekts	Fiziska vide, kurā atrodas ar Uzticamības pakalpojumu sniegšanu saistīti UPS resursi
PIN	PIN-kods. Personas identifikācijas numurs vai kods
PKI	Publisko atslēgu infrastruktūra
PMLP	Latvijas Republikas Iekšlietu ministrijas Pilsonības un migrācijas lietu pārvalde
RA	Sertifikātu reģistrēšanas institūcija
QSCD	Kvalificēta elektroniskā paraksta/zīmoga radīšanas ierīce
SLA	Sadarbības pakalpojuma līmeņa vienošanās
UPS	Uzticamības pakalpojuma sniedzējs
UPS mājaslapa	www.eparaksts.lv
Uzticamības pakalpojumi	a) Elektronisko parakstu, elektronisko zīmogu vai elektronisko laika zīmogu, elektroniski reģistrētu piegādes pakalpojumu un ar minētajiem pakalpojumiem saistītu sertifikāciju radīšana, verifikācija un validācija; b) Tīmekļa vietņu autentifikācijas sertifikātu radīšana, verifikācija

	un validācija; c) Ar minētajiem pakalpojumiem saistītu elektronisko parakstu, zīmogu vai sertifikātu glabāšana.
Uzticamības saraksts	Eiropas savienības dalībvalsts uzturēts pārraudzīto Uzticamības pakalpojumu saraksts
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.
X.509	Publiskās atslēgas infrastruktūras sertifikātu formāts

2. Publicēšanas un repozitorija pienākumi

2.1. Repozitoriji

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

2.2. Sertifikācijas informācijas publicēšana

2.2.1. UPS publicē šādu informāciju:

2.2.1.1. Izsniegto Saknes un izsniegšanas CA sertifikātus;

2.2.1.2. Ar uzticamības pakalpojumu sniegšanu saistītos sertifikātus;

2.2.1.3. Visus atsaukto sertifikātu sarakstus (CRL);

2.2.1.4. Uzticamības pakalpojuma sniegšanas noteikumus;

2.2.1.5. Uzticamības pakalpojumu politikas un ar tām saistīto informāciju;

2.2.1.6. Uzticamības pakalpojumam “eID karte” izsniegtos sertifikātus LDAP direktorijā (par kuriem to turētāji ir devuši atļauju, vai to publicēšanu nosaka normatīvie akti).

2.3. Publicēšanas laiks vai biežums

2.3.1. Izsniegtie sertifikāti tiek publicēti tiklīdz tie tiek uzģenerēti;

2.3.2. UPS 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. UPS, izmantojot UPS mājaslapu https://www.eparaksts.lv , apziņos visas iesaistītās puses par:

2.4.1.1. Izmaiņām, kas veiktas saistītajā UPS publicējamajā dokumentācijā;

2.4.1.2. Izmaiņām, kas veiktas Uzticamības pakalpojumu vispārējos noteikumos;

2.4.1.3. Izmaiņām, kas saistītas ar pakalpojumu cenrādi.

2.4.2. UPS apziņo par konkrētiem grozījumiem vismaz 30 kalendārās dienas pirms grozījumu, UPS publicējamā dokumentācijā, stāšanās spēkā.

2.5. Piekļuves kontrole repozitorijiem

2.5.1. UPS 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 autorizētiem UPS darbiniekiem.

3. Identifikācija un autentifikācija

3.1. Vārda piešķiršana

3.1.1. Visi UPS izsniegtie abonenta sertifikāti sertifikāta turētāja laukā (Subject - *angļu val.*) satur identificētus sertifikāta turētāja datus.

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

3.1.3. Detalizēti nosacījumi un prasības ir definētas atbilstošā uzticamības pakalpojumu politikā.

3.2. Sākotnējās identitātes validācija

3.2.1. Metode privātās atslēgas valdījuma pierādīšanai

3.2.1.1. Saknes CA, Izsniegšanas CA un Laika zīmogošanas institūciju privātās atslēgas valdījumu pierāda ar uzticamu atslēgu ģenerēšanas procedūru.

3.2.1.2. Metode abonentu privātās atslēgas valdījuma pierādīšanai ir definēta atbilstošā uzticamības pakalpojumu politikā.

3.2.2. Organizācijas identitātes identifikācija un validācija

3.2.2.1. UPS 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 UPS 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. UPS pēc saviem ieskatiem, nepaskaidrojot iemeslus, drīkst atteikties izsniegt sertifikātu.

3.2.3. Individuālās identitātes identifikācija un validācija

3.2.3.1. Saknes CA, Izsniegšanas CA un Laika zīmogošanas institūcijas atslēgu izsniegšanas gadījumā:

3.2.3.1.1. Atbilstoši iekšējai procedūrai, LVRTC Valdes priekšsēdētājs norīko personālu Saknes CA, Izsniegšanas CA un Laika zīmogošanas institūcijas atslēgu ģenerēšanas ceremonijas izpildei, kā arī izsniedzamo sertifikātu saturu.

3.2.3.1.2. Vismaz Saknes CA atslēgu ģenerēšanas ceremoniju novēro neatkarīgs auditors.

3.2.3.2. Personas apliecības izsniegšanas gadījumā:

3.2.3.2.1. Personas apliecības izsniegšanu un ar tām saistītu sertifikātu administrēšanu veic PMLP saskaņā ar Latvijas Republikas Ministru kabineta 2012. gada 21. februāra noteikumiem Nr. 134 “Personu apliecinošu dokumentu noteikumi”.

3.2.3.3. Individuālās identitātes validācija citos gadījumos notiek:

3.2.3.3.1. Fiziskā klātbūtnē kādā no RA. Fiziska persona tiek identificēta pret autoritatīvu avotu (piemēram, pase).

3.2.3.3.2. Izmantojot elektroniskos saziņas līdzekļus – identitāte tiek apliecināta ar datiem kvalificētā elektroniskajā parakstā, kas satur laika zīmogu.

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

3.2.3.5. Fizisku personu identifikāciju veic RA un tās personāls, kam piešķirtas uzticamības lomas.

3.2.3.6. Identitātes pārbaudes laikā personas dati tiek ievākti tikai tādā apjomā, kādā tas ir nepieciešams pakalpojuma pilnvērtīgai nodrošināšanai. Iesniegtie dati tiek apstrādāti un aizsargāti atbilstoši Latvijas Republikas Fizisko personu datu aizsardzības likumam un citiem normatīvajiem aktiem fizisko personu datu aizsardzības jomā.

3.2.3.7. Gadījumos, kad fiziska persona, pārstāvot organizāciju, piesakās vai saņem elektroniskā zīmoga sertifikātu:

3.2.3.7.1. UPS identificē pieteicēja tiesības pieteikties un saņemt elektroniskā zīmoga sertifikātu (pilnvarojumu un tā apjomu);

3.2.3.7.2. Pieteicējam jābūt tiesīgam darboties organizācijas vārdā.

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. Abonenta sertifikāta atsaukšanu var pieprasīt šādas personas:

3.4.1.1. Abonents jeb fiziska persona;

3.4.1.2. Sertifikāta pieteikumā norādītais abonenta autorizētais pārstāvis vai pilnvarotā persona;

3.4.1.3. UPS;

3.4.1.4. Citas personas, saskaņā ar Latvijas Republikā spēkā esošajiem normatīvajiem aktiem.

3.4.2. Atsaukšanas pieprasījuma pieteikumu iespējams iesniegt elektroniski (piemēram, nosūtot ar e-pasta starpniecību) parakstītu ar kvalificētu elektronisko parakstu vai apmeklējot RA.

3.4.3. RA identificēs pieteicēju un pārbaudīs viņa tiesības iesniegt pieteikumu. Pēc sekmīgas identifikācijas un pārstāvības tiesību pārbaudes RA reģistrēs pieteikumu.

3.4.4. UPS atsauks sertifikātu pēc RA veiktas atsaukšanas pieteikuma reģistrācijas.

3.4.5. 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. Abonenti aizpilda pieteikuma formu UPS mājaslapā, izveido pieteikumu un izvēlas iesniegšanas metodi - izmantojot elektroniskos saziņas līdzekļus vai fiziskā klātbūtnē:

4.1.1.1. Izmantojot elektroniskos saziņas līdzekļus – abonents paraksta pieteikumu ar kvalificētu elektronisko parakstu un iesniedz to.

4.1.1.2. Fiziskā klātbūtnē – abonents izvēlas, parakstīt pieteikumu ierodoties RA vai izmantot kurjeru, kas atved pieteikuma formu parakstīšanai un pēc tā parakstīšanas nogādā parakstīto formu RA. Abonenta identitātes pārbaude tiek veikta pirms pieteikuma parakstīšanas. Gadījumā, ja Abonents nav aizpildījis pieteikuma anketu pirms ierašanās RA, abonents pieteikuma anketu aizpilda RA klātienē.

4.1.2. Jebkurā scenārijā, abonenta identitātes pārbaude notiek atbilstoši šī dokumenta 3.2. punkta prasībām.

4.1.3. Parakstot pieteikumu abonents apstiprina uzticamam pakalpojumu sniedzējam iesniegtās informācijas patiesumu.

4.1.4. Parakstot pieteikumu abonents apstiprina uzticamības pakalpojumu vispārīgos noteikumus un to ievērošanu

4.1.5. Tikai parakstīti pieteikumi tiek pieņemti.

4.1.6. Citi nosacījumi ir definēti atbilstošā uzticamības pakalpojumu politikā.

4.2. Sertifikātu pieteikuma apstrāde

4.2.1. RA pārbauda visus pieteikumus un pieteicējus.

4.2.2. Visus pieteikumus apstrādā reģistrācijas operators un apstiprina reģistrācijas amatpersona.

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

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

4.2.5. Visus pieteikumus UPS apstrādās saskaņā ar piemērojamiem tiesību aktiem un nolīgumiem.

4.2.6. Visus pieteikumus UPS apstrādā 10 darba diena laikā.

4.3. Sertifikātu izsniegšana

4.3.1. UPS veic pasākumus pret sertifikātu viltošanu un gadījumos, kad UPS 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 tiek izsniegti saskaņā ar [Sertifikātu profili].

4.3.4. Gadījumā, ja UPS ģenerē abonenta atslēgas QSCD, abonenta privāto atslēgu saturošs QSCD tiek droši piegādāts reģistrētajam abonentam:

4.3.4.1. UPS uzreiz pēc sertifikātu izsniegšanas automātiski aptur abonentam izsniegtos sertifikātus;

4.3.4.2. UPS atjauno sertifikātus tikai pēc tam, kad abonents ir saņēmis QSCD, kas satur minētos sertifikātus un privāto atslēgu aktivēšanas datus.

4.4. Sertifikātu akceptēšana

4.4.1. Pirms līgumattiecību noslēgšanas ar abonentu vai, ja sertifikāti tiek izsniegti, nenoslēdzot līgumu, bet pamatojoties uz normatīvo aktu, UPS informē abonentu par uzticamības pakalpojumu vispārējajiem noteikumiem.

4.4.2. UPS publicē uzticamības pakalpojumu vispārējos noteikumus UPS mājaslapā www.eparaksts.lv. Pirms saistību uzņemšanās ar UPS par kādu no uzticamības pakalpojumu, abonentam ir pienākums iepazīties ar uzticamības pakalpojumu vispārējajiem noteikumiem.

4.4.3. UPS reģistrē parakstītu līgumu ar abonentu (ja sertifikāti tiek izsniegti, pamatojoties uz noslēgtu līgumu ar abonentu).

4.4.4. Piekrītot uzticamības pakalpojumu vispārējo noteikumu prasībām un parakstot līgumu, abonents akceptē sertifikātu.

4.5. Atslēgu pāra un sertifikātu lietošana

4.5.1. Abonentam un atkarīgajām pusēm privātās atslēgas un sertifikāti ir jālieto atbilstoši uzticamības pakalpojumu vispārējiem noteikumiem, šī dokumenta un atbilstošā uzticamības politikā noteiktajām prasībām.

4.5.2. Visas abonenta atslēgas tiek ģenerētas, izmantojot [ETSI TS 119 312] standartā noteikto atslēgu garumu un algoritmu.

4.6. Sertifikātu atjaunošana

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

4.6.2. Ja mainījušies kādi no UPS noteikumiem un nosacījumiem, par to tiek paziņots abonentam un tiek parakstīts jauns līgums. Ja sertifikāti ir izsniegti, nenoslēdzot līgumu ar abonentu, bet pamatojoties uz normatīvo aktu, abonents pastāvīgi un patstāvīgi seko līdzi UPS noteikumiem un nosacījumiem.

4.6.3. UPS izsniedz jaunu sertifikātu, izmantojot abonenta iepriekš sertificēto publisko atslēgu tikai tādā gadījumā, ja tās kriptogrāfiskā drošība joprojām ir pietiekama jaunā sertifikāta derīguma periodam un nav pamatotu iemeslu uzskatīt, ka abonenta privātās atslēgas drošums ticis apdraudēts, kā arī sertifikāts nav ticis atsaukts kāda drošības pārkāpuma dēļ.

4.6.4. Pakalpojuma “eParaksts” sertifikātu atjaunošana nav atļauta.

4.7. Sertifikātu jaunizdošana

4.7.1. Sertifikātu jaunizdošanas process ir identisks kā sākotnējās pieteikšanās procesam.

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

4.7.3. Pakalpojuma “eParaksts” sertifikātu jaunizdošana ir aprakstīta Uzticamības pakalpojuma “eParaksts” sniegšanas politikā.

4.8. Sertifikātu modificēšana

4.8.1. 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 šajā dokumentā noteiktajā kārtībā.

4.9. Sertifikātu atsaukšana un apturēšana

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

4.9.2. Sertifikātu atsaukšanas iemesli ir definēti atbilstošā uzticamības pakalpojumu politikas 4.9. punktā.

4.9.3. Informāciju par atsaukšanas pieprasītājiem un pieejamajiem atsaukšanas pieteikumu apstrādes kanāliem skatīt šī dokumenta 3.4. punktā.

4.9.4. Paziņojumi par sertifikāta atsaukšanu nosūtīti abonentam, tiklīdz UPS atsauc sertifikātu.

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

4.9.6. UPS veic sertifikātu apturēšanu šādos gadījumos:

4.9.6.1. izpildot tiesas nolēmumu;

4.9.6.2. pamatojoties uz parakstītāja rakstveida pieprasījumu;

4.9.6.3. noslēgtajā līgumā noteiktajos gadījumos.

4.10. Sertifikātu statusa pakalpojumi

4.10.1. UPS nodrošina atsaukšanas statusa informāciju ar publicēto CRL vai OCSP pakalpojuma starpniecību atbilstoši šī dokumenta 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. Abonents, ģenerējot atslēgas kvalificētam elektroniskā paraksta sertifikātam eParakstsTX risinājumā, tās ģenerē UPS nodrošinātā un pārvaldītā vidē un abonents ir vienīgais, kurš pilnībā kontrolē sava elektroniskā paraksta izveides un privātās atslēgas aktivēšanas datu pārvaldības vidi.

4.12.2. Citu produktu atslēgu nodošana glabāšanā trešajai pusei nav atļauta.

5. Operacionālās, fiziskās un pārvaldības kontroles

5.1. Fiziskās drošības kontroles

5.1.1. UPS 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. UPS 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 UPS. Prasību pārskats ir aprakstīts zemāk.

5.1.3. **Objekta novietojuma apsvērumi un izbūve**

5.1.3.1. UPS 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. UPS savām UPS CA darbībām uztur pēcavārijas atjaunošanas telpas un iekārtas. UPS pēcavārijas atjaunošanas telpas un iekārtas ir aizsargātas ar vairākiem fiziskās drošības līmeņiem, kas ir salīdzināmi ar UPS primārajām telpām un iekārtām.

5.1.4. **Fiziskā piekļuve**

5.1.4.1. UPS 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. UPS nodrošina, ka fiziska piekļuve drošības zonām, kurās atrodas ar uzticamības pakalpojumu sniegšanu saistītie resursi, tiek kontrolēta un potenciālie riski tās resursiem ir minimizēti.

5.1.4.3. Ir pieejams skaidrs UPS 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 UPS 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 UPS drošības pārvaldniekam. UPS vadības uzdevums ir periodiski pārskatīt iepriekšminēto aprakstu.

5.1.5. **Energoapgāde un gaisa kondicionēšana**

5.1.5.1. UPS objekti, kuros atrodas ar uzticamības 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. UPS ir veicis saprātīgus drošības pasākumus, lai samazinātu ūdens iedarbību uz informācijas sistēmām.

5.1.7. **Ugunsgrēka riska novēršana un ugunsdrošība**

5.1.7.1. UPS ir veicis saprātīgus drošības pasākumus, lai atklātu, aizkavētu un nodzēstu ugunsgrēkus vai novērstu citu kaitējošu liesmu vai dūmu iedarbību. UPS 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 UPS 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. UPS 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. UPS 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, izmantojot saistītu trešās puses datu glabātavu vai UPS pēcavārijas atjaunošanas līdzekļus.

5.2. Procesuālas kontroles

5.2.1. **Uzticamības lomas**

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

5.2.1.2. UPS darbiniekiem, kuru lomas paredz UPS darbībai kritisko darbību veikšanu tiek piešķirtas uzticamības lomas. UPS 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 UPS uzticamības sistēmas ieviešanu, konfigurēšanu un uzturēšanu;

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

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

5.2.1.2.5. Reģistrācijas amatpersona – atbild par sertifikātu reģistrācijas un izdošanas pieteikumu pārbaudi un pareizību, apstiprina vai noraida tos;

5.2.1.2.6. Anulēšanas amatpersona – atbild par sertifikātu statusa izmaiņu veikšanu.

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

5.2.1.4. Piekļuvi UPS 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 UPS informācijas drošības politikām;

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. UPS ir ieviesusi, 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 UPS 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. Kā aprakstīts šajā dokumentā, turpmāka identitātes apstiprināšana notiek, veicot personas datu pārbaudes procedūras. UPS nodrošina, ka personāls ir sasniedzis uzticamu statusu, un tiek sniegts struktūrvienības vadītāja apstiprinājums, pirms šim personālam tiek:

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

5.3.1.2. izsniegtas elektroniskās pilnvaras, lai piekļūtu un veiktu UPS 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 darba kandidātiem.

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

5.3.3. **Personāla datu pārbaudes procedūras**

5.3.3.1. UPS 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 UPS 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 UPS darbībā iesaistāmajiem darbiniekiem tiek izvirzītas šādas prasības:

5.3.3.2.1. Ir uzticamības pakalpojumu sniegšanai nepieciešamās speciālās zināšanas;

5.3.3.2.2. Nav sodīti par tīšu noziedzīgu nodarījumu izdarīšanu;

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

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

5.3.4. **Apmācības prasības**

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

5.3.4.1.1. UPS drošības principi un mehānismi;

5.3.4.1.2. Drošības jautājumu izpratne;

5.3.4.1.3. UPS lietotās UPS 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 dokumenta5.3.4. nodaļā minēto apmācību prasības un saturs ir regulāri jāatjauno, un tajās ir jāiestrādā UPS vai normatīvajos aktos

notikušās izmaiņas. Pēc vajadzības jāveic kvalifikācijas celšanas apmācības, un UPS vismaz reizi gadā jāpārskata šīs prasības.

5.3.5.2. UPS veic UPS 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 UPS pakalpojumu pastāvību un integritāti.

5.3.7. **Sankcijas par nesankcionētu darbību veikšanu**

5.3.7.1. UPS 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. UPS 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. UPS no pamatpakalpojumiem ārējām juridiskām personām var deleģēt reģistrācijas institūcijas pienākumus;

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

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

5.3.9. **Personālam izsniedzamā dokumentācija**

5.3.9.1. UPS 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. UPS žurnalēs vismaz šādus notikumus:

5.4.1.1.1. Visa reģistrācijas pieteikuma informācija, iekļaujot identitātes pierādījumus;

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 UPS 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. UPS 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 UPS 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. UPS veic regulāras rezerves kopiju izveides. Audita pierakstu rezerves kopēšana ir daļa no kopējās rezerves kopēšanas procedūras. UPS 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 UPS 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. UPS sistēmas iekšējās un ārējās ievainojamības tiek caurskatītas atbilstoši iekšējai risku pārvaldības dokumentācijai. UPS sistēmai tiek veikti ikgadējie ielaušanās testi;

5.4.8.2. UPS 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. UPS ieraksti, kas attiecas uz tās uzticamības 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 uzticamības pakalpojumus (t.i., UPS 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 UPS centralizētā arhīvā saskaņā ar Latvijas Valsts arhīva noteikumiem.

5.5.2. **Arhīva glabāšanas ilgums**

5.5.2.1. Arhīva ieraksti tiks uzglabāti vismaz desmit (10) gadus bez jebkāda datu 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. UPS arhīva veidošanai izmanto iekšējo arhīva veidošanas (vākšanas) sistēmu;

5.5.6.2. RA var izmantot ārējo arhīva veidošanas (vākšanas) sistēmu tikai fiziskiem arhīva ierakstiem.

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 Uzticamības pakalpojumu politikā.

5.7. Kompromitējums un pēcavārijas atjaunošana

5.7.1. **Incidentu un kompromitējumu apstrādes procedūras**

5.7.1.1. Lai nodrošinātu UPS sniegto pakalpojumu nepārtrauktību, UPS 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 UPS sistēmu no pilnīgas tās nepieejamības;

5.7.1.4. Risku novērtēšana notiek vismaz reizi gadā, kā arī mainoties normatīvajiem aktiem vai UPS 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 UPS nekavējoties (bet ne vēlāk kā četras stundas pēc lēmuma pieņemšanas par ārkārtas situācijas iestāšanos) informēs Abonentus un iesaistītās puses, izmantojot publiskus 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 UPS uzticamības pakalpojumus un to status, kā arī apstrādāto fizisko personu datus, UPS 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 UPS CA vai laika zīmogošanas institūcijas privātā atslēga vai ir aizdomas par šādu kompromitējumu, UPS veiks vismaz šādas darbības:

5.7.3.1.1. Informēs abonentus un 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. UPS sniegto uzticamības 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. **Uzticamības pakalpojumu darbības izbeigšana**

5.8.1.1. Atbildīgs par UPS darbības izbeigšanu ir UPS vadītājs;

5.8.1.2. Galvenās Uzticamības pakalpojumu izbeigšanas procedūras:

5.8.1.2.1. UPS vismaz mēnesi pirms darbības izbeigšanas rakstveidā informē uzraudzības iestādi un nodrošina UPS mājaslapā publiski pieejamu informāciju abonentiem un atkarīgajām pusēm par to, ka tā darbība ir izbeigta, tas ir pasludināts par maksātnespējīgu, uzticamības pakalpojumu sniegšana ir apturēta vai ir anulēta UPS akreditācija;

5.8.1.2.2. UPS anulē pilnvaras apakšuzņēmējiem UPS vārdā veikt jebkādas darbības saistībā ar sertifikātu izsniegšanu;

5.8.1.2.3. UPS nodod saistības uzturēt reģistrācijas informāciju un notikumu reģistrācijas arhīvu uzticamai trešajai pusei;

5.8.1.2.4. UPS anulē CA un/vai Laika zīmogošanas institūcijas sertifikātu;

5.8.1.2.5. UPS iznīcina CA un/vai Laika zīmogošanas institūcijas privātās atslēgas, ieskaitot visas minēto atslēgu kopijas;

5.8.1.2.6. UPS atkārtoti inicializē vai iznīcina visas ar minētajām atslēgām saistītās HSM iekārtas;

5.8.1.2.7. UPS uztur pieejamu laika zīmogošanas institūcijas un/vai CA publisko atslēgu vai sertifikātu. UPS var nodot uzticamai trešajai pusei šīs saistības, uzturēt pieejamu laika zīmogošanas institūcijas un/vai CA publisko atslēgu vai sertifikātu.

5.8.1.3. UPS ir izstrādājis UPS darbības izbeigšanas plānu, kas satur detalizētas procedūras plāna īstenošanai.

5.8.2. **Reģistrācijas institūcijas darbības izbeigšana**

5.8.2.1. Gadījumā, ja kāda no UPS deleģētajam RA pārtrauc savu darbību, tā:

5.8.2.1.1. Visu ar uzticamības pakalpojumu sniegšanu saistīto arhivējamo (saglabājamo) informāciju jānodod UPS (piemēram, audita pieraksti, arhīvs, visi fiziski iesniegtie pieteikumi);

5.8.2.1.2. Visu pārējo informāciju un dokumentus, kas ar šo CPS vai uzticamības pakalpojumu politikām nav noteikti kā arhivējami, jāiznīcina;

5.8.2.1.3. Visiem UPS deleģētās RA darbiniekiem jānoņem piešķirtās lomas un tiesības.

6. Tehniskās drošības kontroles

6.1. Atslēgu pāra ģenerēšana un instalēšana

6.1.1. **Atslēgu pāra ģenerēšana**

6.1.1.1. UPS CA un laika zīmogošanas 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 dokumentētu CA atslēgu ģenerēšanas ceremonijas noteikumiem. Vismaz Saknes CA atslēgu ģenerēšanas ceremoniju novēro neatkarīgs auditors;

6.1.1.2. UPS CA un laika zīmogošanas 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. UPS ir izstrādājis un uztur atslēgu ceremonijas norises protokolus, kuros ir minēti visu CA atslēgu ģenerēšanas ceremonijai nepieciešamie soļi;

6.1.1.5. Detalizēti abonentu privāto atslēgu ģenerēšanas nosacījumi un prasības ir definētas atbilstošā uzticamības pakalpojumu politikā.

6.1.2. **Privātās atslēgas piegāde Abonentiem**

6.1.2.1. Privātās atslēgas piegāde abonentam notiek atbilstoši šī dokumenta 4.3.4. punktā noteiktajam.

6.1.3. **Publiskās atslēgas piegāde sertifikātu izsniedzējam**

6.1.3.1. UPS šī CPS 5.5.2. punktā norādīto termiņu glabā visus CA izsniegto sertifikātus un ar tiem saistītās privātās;

6.1.3.2. Detalizēti nosacījumi un prasības ir definētas atbilstošā uzticamības pakalpojumu politikā;

6.1.3.3. CA publiskās atslēgas piegāde atkarīgajām pusēm;

6.1.3.4. Visas UPS uzticamības pakalpojumu sniegšanā iesaistītās publiskās atslēgas tiek publicētas UPS mājaslapā www.eparaksts.lv/repository. Publiskās atslēgas tiek publicētas X.509 sertifikātu formātā;

6.1.3.5. UPS pienākums ir nodrošināt visu atbilstošo UPS uzticamības pakalpojumu sniegšanā iesaistīto publisko atslēgu nodošanu Latvijas Republikas uzraudzības iestādei, to iekļaušanai Latvijas uzticamības sarakstā;

6.1.3.6. UPS darīs visu iespējamo, lai visas atbilstošās UPS uzticamības pakalpojumu sniegšanā iesaistītās atslēgas tiktu iekļautas citu produktu uzticamo sertifikātu sarakstos.

6.1.4. **Atslēgu izmēri**

6.1.4.1. UPS uzticamības pakalpojumu sniegšanā iesaistīto atslēgu algoritmiem un atslēgu garumiem jāatbilst [ETSI TS 119 312] minētajam.

6.1.4.2. Detalizēti abonentu atslēgu algoritmi un garumi ir definēti atbilstošā uzticamības pakalpojumu politikā.

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 abonentu atslēgu lietošanas mērķi ir definēti dokumentā [Sertifikātu profili], kā arī atbilstošā uzticamības pakalpojumu politikā;

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. UPS izmanto HSM iekārtas, kas atbilst FIPS 140-2, 3. līmeņa noteiktajām prasībām. Visam HSM iekārām ir aktivizēts FIPS režīms;

6.2.1.2. UPS 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 abonentu kriptogrāfiskajām iekārtām ir definēti atbilstošā uzticamības pakalpojumu politikā.

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

6.2.2.1. UPS ir ieviesis tehniskus un procesuālus mehānismus, kas prasa vairāku uzticamu personu klātbūtni, lai veiktu CA un laika zīmogošanas 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 un laika zīmogošanas institūcijas privātajām atslēgām.

6.2.3. **Privātās atslēgas aizbildniecība**

6.2.3.1. UPS CA un laika zīmogošanas institūcijas privātās atslēgas tiek glabātas HSM iekārtās, kas atbilst FIPS 140-2, 3. līmeņa noteiktajām prasībām. CA un laika zīmogošanas 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. Abonentu privāto atslēgu aizbildniecība ir aprakstīta atbilstošā uzticamības pakalpojumu politikā.

6.2.4. **Privātās atslēgas rezerves kopijas izveide**

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

6.2.4.2. Abonentu privāto atslēgu rezerves kopēšanas nosacījumi ir definēti atbilstošā uzticamības pakalpojumu politikā;

6.2.4.3. UPS CA un laika zīmogošanas 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. UPS neveikts UPS CA un laika zīmogošanas institūcijas atslēgu arhivēšanu pēc to derīguma termiņa beigām. UPS CA un laika zīmogošanas 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. UPS ģenerē CA un laika zīmogošanas institūcijas atslēgu pārus HSM iekārtās, kurās šīs atslēgas tiks izmantotas.

6.2.7. **Privātās atslēgas glabāšana kriptogrāfiskajā modulī**

6.2.7.1. UPS CA un laika zīmogošanas institūcijas privātā atslēga tiek glabāta HSM iekārtās šifrētā formā;

6.2.7.2. Abonentu privāto atslēgu glabāšanas nosacījumi kriptogrāfiskajā modulī ir definēti atbilstošā uzticamības pakalpojumu politikā.

6.2.8. **Privātās atslēgas aktivēšanas metode**

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

6.2.8.2. Abonentu privāto atslēgu aktivēšanas nosacījumi ir definēti atbilstošā uzticamības pakalpojumu politikā.

6.2.9. **Privātās atslēgas deaktivēšanas metode**

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

6.2.9.2. Abonentu privāto atslēgu deaktivēšanas metodes ir definētas atbilstošā uzticamības pakalpojumu politikā.

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 un Laika zīmogošanas institūciju privātās atslēgas iznīcināšanas metodes ir atkarīgas no HSM iekārtas specifikas;

6.2.10.3. CA un laika zīmogošanas 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 UPS IS regulārajām rezerves kopiju izveides procedūrām tiek veikta visu UPS CA izsniegto publisko atslēgu rezerves kopiju izveide un saglabāšana;

6.3.1.2. UPS šī dokumenta 5.5.2. punktā norādīto termiņu glabā visus CA izsniegto sertifikātus un ar tiem saistītās privātās.

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 UPS 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. Abonentu sertifikātu darbības nepārsniegs piecus gadus.

6.4. Aktivēšanas dati

6.4.1. Aktivēšanas datu ģenerēšana un instalēšana

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

6.4.1.2. Abonentu privāto atslēgu PIN ģenerēšana un uzstādīšana ir definēta atbilstošā uzticamības pakalpojumu politikā.

6.4.2. Aktivēšanas datu aizsardzība

6.4.2.1. UPS CA un laika zīmogošanas 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. Abonentu privāto atslēgu PIN aizsardzības prasības ir definētas atbilstošā uzticamības pakalpojumu politikā.

6.4.3. Citi aktivēšanas datu aspekti

6.4.3.1. Citi aktivēšanas datu aspekti un nosacījumi ir definēti atbilstošā uzticamības pakalpojumu politikā.

6.5. Datoru drošības kontroles

6.5.1. Specifiskās datoru drošības tehniskās prasības

6.5.1.1. UPS ir ieviesis kontroļu kopu UPS 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 UPS 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 ar noteikto SLA pieejamību.

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

6.5.2. **Sistēmu drošības reitings**

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

6.6. Dzīves cikla tehniskās kontroles

6.6.1. **Sistēmas izstrādes kontroles**

6.6.1.1. Visas programmatūras implementēšana produkcijas vidē tiek kontrolēta;

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

6.6.1.2.1. Tiek veikta pilnvērtīga analīze programmatūras prasību specifikācijas fāzē;

6.6.1.2.2. Jebkuras izmaiņas tiek akceptētas atbilstošā uzraudzības komisijā;

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

6.6.1.2.4. Visas izmaiņas tiek testētas vismaz vienā testa vidē;

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

6.6.2. **Drošības pārvaldības kontroles**

6.6.2.1. UPS veic patstāvīgu sistēmu un komunikāciju uzraudzību, lai pārliecinātos, ka visas sistēmas un komunikācijas darbojās atbilstoši noteiktajām prasībām;

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

6.6.3. **Dzīves cikla drošības kontroles**

6.6.3.1. UPS regulāri pārskata visus, ar informācijas drošību saistītos dokumentus un aktīvus.

6.7. Tīkla drošības kontroles

6.7.1. Datortīklam uzstādīti ugunsmūri, kas atdala dažādus tīkla segmentus. UPS uztur vismaz divus (ugunsmūrus, kur viens atdala ārējo tīklu no UPS iekšējā tīkla un otrs atdala serveru tīklu no UPS administratoru un lietotāju tīkla segmentiem. Ugunsmūri ir konfigurēti, lai nodrošinātu vienīgi autorizētas datu pārraides izmantošanu;

6.7.2. UPS 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;

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

6.7.4. Komunikācija iekšējā UPS tīklā pēc nepieciešamības tiek šifrēta izmantojot drošus šifrēšanas algoritmus, lai mazinātu noklausīšanās riskus;

6.7.5. UPS izmanto pretielaušanās (IDS/IPS) sistēmu, lai stiprinātu aizsardzības kontroles pret ielaušanos UPS datortīklā;

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

6.7.7. UPS 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 UPS vadītājam par atklātajiem drošības trūkumiem;

6.7.8. UPS 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;

6.7.9. UPS nodrošina darbinieku kiberdrošības apzināšanās apmācības, kā arī uztur un attīsta IT darbinieku zināšanu līmeni par kiberdrošības jautājumiem;

6.7.10. UPS 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;

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

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

6.7.13. UPS izmanto e-pastu šifrēšanas mehānismus, lai nodrošinātu drošu informācijas apmaiņu ar ārējiem sadarbības partneriem;

6.7.14. Attālināta piekļuve UPS datortīklam ir pieļauta tikai no noteiktām gala iekārtām (tīkliem) un tikai izmantojot speciālas attālinātās piekļuves uzraudzības un nodrošināšanas iekārtas;

6.7.15. UPS veic regulāru datortīkla ielaušanās testēšanu, kā arī datortīkla drošības pārvaldības kontroļu efektivitātes novērtēšanu un auditus;

6.7.16. UPS uztur aktuālas datortīkla loģiskās un fiziskās shēmas;

6.7.17. HSM iekārtas atrodas atsevišķā drošības zonā, kurai nav tiešas piekļuves no publiskā tīkla;

6.7.18. Saknes CA atrodas augstas drošības zonā un nav pieslēgts nevienam tīklam;

6.7.19. Piekļuve drošības un augstas drošības zonām ir tikai personālam ar uzticības lomām;

6.7.20. UPS sistēma ir dublēta vismaz divos datu centros. Komunikācija starp datu centriem tiek pilnībā kontrolēta ar UPS resursiem.

6.8. Laika zīmogošana

6.8.1. UPS kā uzticamības laika zīmogošanas pakalpojumu sniedzējs piedāvā kvalificētu elektronisko laika zīmogošanas servisu atbilstoši uzticamības pakalpojumu sniedzēja laika zīmogošanas politikai;

6.8.2. UPS IS darbības nodrošināšanai neizmanto laika zīmogus. UPS IS darbības nodrošināšanai tiek izmantots precīzs laiks, kas tiek saņemts no uzticama avota. Šāda laika informācija nav bāzēta uz kriptogrāfiskiem risinājumiem;

6.8.3. UPS izmanto precīzu laiku, ko iegūst no vismaz 3 sertificētām NTP laboratorijām;

6.8.4. Visu UPS IS saistīto komponenšu maksimālā laika nobīde nepārsniegs vienu sekundi.

7. Sertifikātu, CRL un OCSP profili

7.1. Sertifikātu profils

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

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. Atbilstības audits un citi vērtējumi

8.1. Atbilstības audita biežums un apstākļi

8.1.1. Atbilstības novērtēšanas struktūra veic UPS un tās sniegto uzticamības pakalpojumu atbilstības auditus atbilstoši Latvijas Republikā spēkā esošajiem normatīvajiem aktiem un standartiem;

8.1.2. Ārpuskārtas atbilstības audits UPS tiek veikta gadījumos, ja UPS veic būtiskas izmaiņas UPS pārvaldībā vai informācijas sistēmās.

8.2. Prasības Atbilstības novērtēšanas struktūrai

8.2.1. Atbilstības novērtēšanas struktūrai ir jābūt akreditētai atbilstoši Latvijas Republikā spēkā esošajiem normatīvajiem aktiem un standartiem.

8.3. Auditoru attiecības ar UPS

8.3.1. Tikai šī dokumenta 8.2.1. punktā prasībām atbilstoši neatkarīgi auditori var veikt atbilstības auditu;

8.3.2. Iekšējais auditors nedrīkst auditēt savas atbildības sfēru.

8.4. Atbilstības novērtējuma temati

8.4.1. Atbilstības revīzijā ietver:

8.4.1.1. Fizisko drošību;

8.4.1.2. Tehnoloģiju novērtējumu;

8.4.1.3. CA un RA pakalpojumu pārvaldību (tostarp CA vides kontroles, atslēgu pārvaldības darbības un infrastruktūras/administratīvos CA uzraudzības pasākumus, sertifikātu dzīves cikla pārvaldību);

8.4.1.4. Personāla pārbaudes;

8.4.1.5. Attiecīgās Uzticamības pakalpojumu politikas un [CPS];

8.4.1.6. Līgumus;

8.4.1.7. Datu aizsardzības un privātuma apsvērumus;

8.4.1.8. Avārijas atjaunošanās plānošanas dokumentu.

8.5. Reakcija uz atbilstības auditā atklātajiem trūkumiem

8.5.1. Atbilstības audita laikā identificētajiem nozīmīgajiem iebildumiem vai trūkumiem tiks noteiktas nepieciešamās veicamās darbības. Lēmumu pieņems UPS vadība, ievērojot auditora un/vai uzraudzības iestādes pausto viedokli. UPS vadība ir atbildīga par koriģējoša darbības plāna izveidošanu un ieviešanu.

8.6. Rezultātu paziņošana

8.6.1. Visi atbilstības novērtēšanas audita ziņojumi tiks iesniegti uzraudzība iestādei tālāko lēmumu pieņemšanai.

9. Citi biznesa un juridiskie jautājumi

9.1. Maksājumi

9.1.1. Sertifikātu pārvaldības maksa

9.1.1.1. Sertifikātu pieteikšanas process un sertifikātu izsniegšana, anulēšana vai atjaunošana var būt maksas pakalpojums, kur maksa ir noteikta publiski pieejamā cenrādī vai noslēgtajā līgumā. UPS nodrošinās cenrāža spēkā esošo versiju publicēšanu UPS mājaslapā www.eparaksts.lv .

9.1.2. Sertifikātu pārbaudes maksa

9.1.2.1. UPS sertifikātu pārbaudes pakalpojumi, lai pārbaudītu UPS izsniegtos sertifikātus, ir bezmaksas. UPS var prasīt maksu par sertifikātu pārbaudes pakalpojumiem gadījumos, kurus to neaizliedz normatīvie akti.

9.1.3. Kompensācijas politika

9.1.3.1. UPS Saknes CA vai pakārtota sertificēšanas institūcija var ieviest kompensācijas politiku. Kad kompensācijas politika attiecas uz gala lietotājiem, tiem tiks nodrošināta tās jaunākā versija, kura tiks publicēta UPS mājaslapā www.eparaksts.lv .

9.2. Finansiālā atbildība

9.2.1. UPS atbildības ierobežojumi attiecībā uz pakārtotām izsniegšanas sertificēšanas institūcijām tiek noteikti savstarpējos UPS līgumos. Šie CPS ir iekļauti šādos līgumos kā to sastāvdaļa;

9.2.2. Ja nav tieši norunāts savādāk vai skaidri noteikts konkrētā uzticamības pakalpojumu politikā, UPS atbildība pret pakārtotām CA, abonentiem, atkarīgām pusēm un jebkurām citām vienībām, kas nav pakārtotās CA, ir ierobežota attiecībā uz visu veidu prasībām, kā līgumiskām, tā ārpus līgumiskām, pamatojoties uz katru sertifikātu atsevišķi, neatkarīgi no transakciju vai elektronisko parakstu skaita, kā arī no sertifikātiem vai jebkādu attiecībā uz šiem sertifikātiem nodrošinātu pakalpojumu izrietošiem darbību iemesliem, kā arī uz kumulatīva pamata;

9.2.3. Jebkādas un visas prasības, kas saistītas ar UPS pakalpojumiem attiecībā uz sertifikātu (neatkarīgi no zaudējumus radošās vienības vai sertifikātus izsniedzošās un uzticamības pakalpojumus nodrošinošās vienības), tiek pakļautas saskaņā ar šo CPS piemērojamiem atbildības ierobežojumiem;

9.2.4. Kvalificētam sertifikātam norādītais darījuma summas ierobežojums ir ar mērķi noteikt UPS atbildības ierobežojumu, kaitējuma rašanās gadījumā abonentam, ja par iemeslu zaudējumu rašanās ir UPS normatīvajos aktos noteikto prasību neievērošana vai pārkāpšana;

9.2.5. UPS noteiktais summas ierobežojums darījumiem, kuru veikšanai var izmantot UPS izsniegtu sertifikātu un/vai laika zīmogu, ir EUR 150 000,00

(viens simts piecdesmit tūkstoši *euro*) par katru darījumu (turpmāk - Summas ierobežojums);

9.2.6. Ja Abonents izmanto UPS izsniegtu sertifikātu darījumu veikšanai, kura summa pārsniedz šī CPS 9.2.5.punktā minēto Summas ierobežojumu, UPS atbild tikai par zaudējumiem, kas radušies no UPS neatbilstības normatīvajos aktos noteiktajām prasībām, ļauna nolūka vai rupjas neuzmanības dēļ un tikai tādā apmērā, kas nepārsniedz šī CPS 9.2.5.punktā minēto Summas ierobežojumu (EUR 150 000,00 (viens simts piecdesmit tūkstoši *euro*));

9.2.7. UPS neuzņemas atbildību par darījumu, kura veikšanai tiek izmantots UPS izsniegts sertifikāts, saturu, apjomu un izpildi. Abonents var ierobežot sertifikāta lietošanu, to apturot vai anulējot;

9.2.8. Nekādos apstākļos UPS atbildība nepārsniedz šī dokumenta 9.2.puntkā minētos ierobežojumus.

9.3. Biznesa informācijas konfidencialitāte

9.3.1. Konfidenciāli glabājamas informācijas sfēra

9.3.1.1. Visa informācija, kuru UPS saņem, sniedzot uzticamības pakalpojumus un kura nav paredzēta publicēšanai, ir konfidenciāla un paredzēta tikai UPS iekšējai lietošanai atbilstoši normatīvajiem aktiem. Abonentiem ir tiesības saņemt informāciju par sevi normatīvajos aktos noteiktajā apmērā un kārtībā.

9.3.2. Par konfidenciālu neuzskatāmas informācijas tipi

9.3.2.1. Visa informācija, kas nav noteikta kā konfidenciāla vai informācija iekšējai lietošanai, tiek uzskatīta par publisku informāciju;

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

9.3.2.3. UPS rīcībā esošā nepersonalizētā statistikas informācija var tikt uzskatīta par publisku un nepieciešamības gadījumā UPS ir tiesības to publicēt.

9.3.3. Pienākums aizsargāt konfidenciālu informāciju

9.3.3.1. UPS veic nepieciešamās darbības, lai nodrošinātu konfidenciālas un iekšējās lietošanas informāciju pret kompromitēšanu un nodrošinātu tās neizpaušanu trešajām pusēm, ieviešot dažādas drošības politikas.

9.3.3.2. UPS ir tiesības izpaust konfidenciālu informāciju tikai saskaņā ar normatīvajos aktos noteikto.

9.4. Fizisko personu datu informācijas privātums

9.4.1.1. Visi UPS apstrādātie fizisko personu dati tiek aizsargāti saskaņā ar Latvijas Republikā spēkā esošajiem normatīvajiem aktiem fizisko personu datu aizsardzības jomā. Fizisko personas dati tiek atklāti trešajām personām normatīvajos aktos noteiktajos gadījumos, kārtībā un termiņos;

9.4.1.2. UPS veic fizisko personu datu apstrādi, tajā skaitā uztur datu bāzes ar personas datiem. Personas dati ir jebkura informācija, kas attiecināma uz identificētu vai identificējamu personu. Personas datu apstrāde ietver to vākšanu, uzglabāšanu, ievadīšanu, nodošanu, pārraidīšanu un citus iespējamos datu apstrādes veidus. Piekrītot saņemt UPS sniegtu pakalpojumu, ir uzskatāms, ka persona ir devusi savu piekrišanu UPS apstrādāt savus personas datus saskaņā ar šo CPS;

9.4.1.3. Personas datu apstrāde notiek saskaņā ar normatīvajiem aktiem un tās mērķis ir:

9.4.1.3.1. UPS sniegto pakalpojumu nodrošināšana,

9.4.1.3.2. Normatīvajos aktos noteikto pienākumu izpilde,

9.4.1.3.3. Risku vadības nodrošināšana,

9.4.1.3.4. Mārketinga aktivitāšu nodrošināšana (tai skaitā, piedāvājumu nosūtīšana, reklamēšana, klientu aptauju un pētījumu veikšana);

9.4.1.3.5. UPS tiesību aizstāvēšanai.

9.4.1.4. Personas dati tiek saņemti no paša abonenta vai tā pārstāvja, kā arī no trešajām personām (piemēram, no LR Iekšlietu ministrijas Iedzīvotāju reģistra centrālās datu bāzes, u.c.), normatīvajos aktos noteiktajā kārtībā un apjomā;

9.4.1.5. UPS ir tiesīgs nodot ziņas par abonentu, tai skaitā abonenta personas datus un ziņas par abonenta veiktajiem darījumiem:

9.4.1.5.1. Trešajām personām, kas sniedz UPS pakalpojumus un ar kuriem UPS sadarbojas tās darbības nodrošināšanā un funkciju izpildē, lai nodrošinātu UPS likumisko pienākumu un līgumisko saistību izpildi;

9.4.1.5.2. Valsts un pašvaldību institūcijām normatīvajos aktos noteiktajā kārtība;

9.4.1.5.3. Citos gadījumos, ja saņemta abonenta piekrišana.

9.4.2. **Par konfidenciālu uzskatāma informācija**

9.4.2.1. Visi fizisko personu dati UPS tiek apstrādāti saskaņā ar Latvijas Republikā spēkā esošiem normatīvajiem aktiem;

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

9.4.2.3. Gadījumos, kad CA pārstāj sniegt uzticamības pakalpojumus, kā daļu no darbības izbeigšanas procedūras, šai CA ir jānodod uzticamības pakalpojumu nodrošināšanai nepieciešamie personas un citi dati citai CA vai uzraugošās iestādes nozīmētai vienībai.

9.4.3. **Par konfidenciālu neuzskatāma informācija**

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

9.4.4. **Pienākums aizsargāt privātu informāciju**

9.4.4.1. Visas UPS vienības, kas apstrādā fizisko personu datus, ievēro Latvijas Republikā spēkā esošos normatīvos aktus fizisko personu datu aizsardzības jomā prasības.

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

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

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

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

9.4.7. **Citi informācijas atklāšanas apstākļi**

9.4.7.1. Nav nosacījumu

9.5. Intelektuālā īpašuma tiesības

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

9.6. Pārstāvības un garantijas

9.6.1. **Uzticamības pakalpojuma sniedzēja pārstāvība un garantijas.**

9.6.1.1. UPS izpilda savu daļu no tiesībām un pienākumiem, kas definēti šajā dokumentā un konkrēto uzticamības pakalpojumu politikās vai noteikumos pret abonentiem un atkarīgajām pusēm.

9.6.1.2. UPS:

9.6.1.2.1. Sniegs savus pakalpojumus saskaņā ar prasībām un procedūrām, kas noteiktas šajā CPS un konkrēto uzticamības pakalpojumu politikās/noteikumos;

9.6.1.2.2. Nodrošinās atbilstību Latvijas Republikā spēkā esošajiem normatīvajiem aktiem;

9.6.1.2.3. Publicēs šo dokumentu un konkrēto uzticamības pakalpojumu politikas UPS mājaslapā www.eparaksts.lv, nodrošinot to pieejamību atbilstoši šī dokumenta 2.1. punktā definētajam līmenim;

9.6.1.2.4. Publicēs uzticamības pakalpojumu vispārējos noteikumos UPS mājaslapā www.eparaksts.lv, nodrošinot to pieejamību atbilstoši šī dokumenta 2.1.punktā definētajam līmenim;

9.6.1.2.5. Izpildīs uzticamības pakalpojumu vispārējos noteikumos minētās saistības;

9.6.1.2.6. Nodrošinās tādas UPS pakalpojumu sniegšanas laikā iegūtas informācijas konfidencialitāti, kura tiek uzskatīta par konfidenciālu un nav paredzēta publicēšanai;

9.6.1.2.7. Uzskaitīs visus izsniegtos produktus un to derīguma terminus;

9.6.1.2.8. Informēs uzraudzības iestādi par jebkādām uzticamības pakalpojumu sniegšanā iesaistīto publisko atslēgu izmaiņām;

9.6.1.2.9. Bez liekas kavēšanās informēs uzraudzības iestādi par ārkārtas situācijām, kuras var būtiski ietekmēt sniegtos uzticamības pakalpojumus un to statusu, kā arī apstrādāto fizisko personu datus;

9.6.1.2.10. Bez liekas kavēšanās informēs konkrētu personu, ja drošības vai integritātes pārkāpums negatīvi ietekmē to;

9.6.1.2.11. Saglabās visus dokumentus, pierakstus un žurnālus, kas saistīti ar Uzticamības pakalpojumiem atbilstoši šī dokumenta 5.4. un 5.5.punktā minētajam;

9.6.1.2.12. Nodrošinās atbilstības auditu atbilstoši prasībām un iesniegs atbilstības audita ziņojumu uzraudzības iestādei, lai nodrošinātu uzticamības pakalpojumu nepārtrauktu statusu Latvijas uzticamības sarakstā;

9.6.1.2.13. Ir pietiekoši finansiālie resursi un stabilitāte, kas nepieciešami, lai darbotos saskaņā ar šo dokumentu;

9.6.1.2.14. Izmantos uzticamu personālu, kam ir uzticamības pakalpojumu sniegšanai nepieciešamās speciālās zināšanas, pieredze, kvalifikācija, kas ir iepazīstināts ar attiecīgajiem uzticamības pakalpojumu sniegšanas drošības noteikumiem un kas nav sodīts par tīšu noziedzīgu nodarījumu izdarīšanu;

9.6.1.2.15. sniedz UPS 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;

9.6.1.2.16. Gadījumos, kad persona ar invaliditāti vēlās saņemt UPS pakalpojumu, tā var sazināties ar UPS, izmantojot jebkuru šī CPS

1.5.2.punktā minēto saziņas kanālu un iegūt informāciju kā visērtāk saņemt UPS pakalpojumu;

9.6.1.2.17. Ja tas ir praktiski iespējams, UPS atbalstīs pieejamību UPS piedāvātajiem uzticamības pakalpojumiem personām ar invaliditāti un minēto pakalpojumu sniegšanā izmantotajiem tiešā lietotāja produktiem personām ar invaliditāti.

9.6.2. **Reģistrācijas institūcijas pārstāvība un garantijas**

9.6.2.1. UPS reģistrācijas institūcijas:

9.6.2.1.1. Sniedz pakalpojumus atbilstoši prasībām un procedūrām, kas definēti līgumā starp UPS un deleģēto RA, šajā dokumentā un konkrēto uzticamības pakalpojumu politikās un noteikumos;

9.6.2.1.2. Nodrošina saviem darbiniekiem nepieciešamo apmācību;

9.6.2.1.3. Bez liekas kavēšanās informē UPS par ārkārtas situācijām, kuras var būtiski ietekmēt sniegtos uzticamības pakalpojumus un to statusu, kā arī apstrādāto fizisko personu datus;

9.6.2.1.4. Izmanto uzticamu personālu, kas ir saņēmis nepieciešamo apmācību un kas nav sodīts par tīšu noziedzīgu nodarījumu izdarīšanu.

9.6.3. **Abonenta pārstāvība un garantijas**

9.6.3.1. Abonents:

9.6.3.1.1. Iepazīstas ar šo dokumentu un saņemtā uzticamības pakalpojuma politiku un noteikumiem;

9.6.3.1.2. Iesniedzot pieteikumu uzticamības pakalpojuma saņemšanai, sniedz pilnīgu, patiesu un precīzu informāciju. Ja pēc uzticamības pakalpojuma saņemšanas abonenta iesniegtie dati ir mainījušies, abonenta pienākums ir nekavējoties paziņot aktuālos datus atbilstoši saņemtā uzticamības pakalpojumu politikā vai noteikumos atrunātajai kārtībai;

9.6.3.1.3. Ņem vērā, ka UPS var atteikt uzticamības pakalpojumu sniegšanu, ja abonents iesniedzis viltotu, nekorektu vai nepilnīgu informāciju uzticamības pakalpojumu pieteikumā;

9.6.3.1.4. Ir pilnībā atbildīgs par savas privātās atslēgas un tās nesēja uzturēšanu atbilstoši šim dokumentam, saņemto uzticamības pakalpojumu politikas un noteikumu, kā arī uzticamības pakalpojumu vispārējo noteikumu prasībām.

9.6.4. **Atkarīgo pušu pārstāvība un garantijas**

9.6.4.1. Atkarīgām pusēm:

9.6.4.1.1. Jāizvērtē riskus un atbildības, kas saistīti ar paļaušanos uz UPS izsniegtajiem produktiem un sniegtajiem pakalpojumiem. Riski un atbildības ir uzskaitīti šajā dokumentā, konkrētu uzticamības pakalpojumu politikā un noteikumos, kā arī uzticamības pakalpojumu vispārējos noteikumos;

9.6.4.1.2. Jāpārbauda iesaistīto sertifikātu derīgums, izmantojot UPS sniegtos sertifikātu un elektroniski parakstīto dokumentu pārbaudes pakalpojumus.

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

9.6.5.1. Definēta atbilstošās uzticamības pakalpojumu politikās un noteikumos.

9.7. Garantijas atrunas

9.7.1. UPS ir atbildīgs:

9.7.1.1. Par visu šī dokumenta 9.6.1. punktā minēto prasību izpildi;

9.7.1.2. Par uz UPS darbību attiecināmo normatīvo aktu ievērošanu;

9.7.1.3. Atbilstošas apdrošināšanas polises uzturēšanu un tās prasību izpildi.

9.7.2. UPS nenes nekādu atbildību par kaitējumu un zaudējumiem, neatkarīgi no tā, vai par tiem (vai to iestāšanās iespēju) abonents ir informēts, tajā skaitā, bet ne tikai, tie ir bijuši saprātīgi paredzami un izriet no:

9.7.2.1. Veiktajām transakcijām starp abonentiem un atkarīgajām pusēm;

9.7.2.2. Sertifikātu, kriptogrāfisko atslēgu, elektronisko parakstu un uzticamības pakalpojumu tādu lietošanu vai paļaušanos uz tiem, kas nav atbilstoša šim dokumentam vai mērķiem, kas nav atļauti šajā dokumentā;

9.7.2.3. Trešo pušu produktiem vai sniegtajiem pakalpojumiem (ieskaitot aparatūru un programmatūru);

9.7.2.4. Sertifikāta neatjaunošanu dēļ neatbilstības šajā dokumentā norādītajām sertifikāta atjaunošanas prasībām;

9.7.2.5. Jebkura netieša vai izrietoša kaitējuma vai zaudējumiem, tai skaitā, bet ne tikai, iespējamās peļņas atrāvumu, paredzamo ietaupījumu zuduma, ieņēmumu zuduma, biznesa zaudējuma, biznesa pārtraukuma, kaitējumu reputācijai vai informācijas zuduma;

9.7.2.6. Pakalpojuma sniegšanā iesaistīto trešo pušu darbību vai bezdarbību, piemēram uzraudzības iestādi, uzticamo pakalpojumu sarakstu, vai citām uzticamības pakalpojumu sniegšanā iesaistītām publiskajām pusēm;

9.7.2.7. Nepārvaramas varas *(Force Majore)* ietekmē radītu kaitējumu vai zaudējumiem.

9.8. Atbildības ierobežojumi

9.8.1. UPS atbildība ir ierobežota un par katru pieteikto gadījumu nepārsniedz šī dokumenta 9.2.5. punktā noteikto summas ierobežojumu;

9.8.2. Lai nodrošinātos pret finansiālo atbildību, UPS ir iegādājies un pārvalda atbilstošu apdrošināšanas polisi.

9.9. Atlīdzība

9.9.1. Atlīdzība starp abonentu un UPS ir definēta uzticamības pakalpojumu vispārējos noteikumos.

9.10. Termiņi un darbības izbeigšana

9.10.1. Termiņi ir definēti šī dokumenta 2.3. punktā;

9.10.2. Darbības izbeigšana:

9.10.2.1. Šīs dokuments vai saistīto uzticamības pakalpojumu politikas ir spēkā līdz brīdim, kad šīs dokuments tiek aizvietota ar jaunu versiju, vai arī, līdz brīdim, kad UPS pārtrauc savu darbību;

9.10.2.2. Līdz UPS darbības pārtraukšanai, UPS ir pienākums nodrošināt visas fizisko personu datu un konfidenciālās informācijas aizsardzību.

9.10.3. Darbības izbeigšanas radītās sekas:

9.10.3.1. Visiem abonentiem, kas izmanto sertifikātus, kas izsniegti iepriekšējās versijas šī dokumenta darbības laikā, ir jāievēro spēkā esošās dokumenta versijas noteiktās prasības tik tālu, ciktāl tas nav pretrunā ar iepriekšējo versiju.

9.11. Individuāli paziņojumi un saziņa ar dalībniekiem

9.11.1. UPS mājaslapa www.eparaksts.lv primāri tiek izmantots individuāliem paziņojumiem un saziņai ar dalībniekiem;

9.11.2. Cita veida komunikācija ir detalizēta konkrēto uzticamības pakalpojumu politikā vai noteikumos.

9.12. Grozījumi

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

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

9.13. Domstarpību risināšanas kārtība

9.13.1. Ja izceļas strīds, kas izriet vai ir saistīts ar šīm procedūrām vai saistītajiem līgumiem, pirms sākt tiesvedību, strīdā iesaistītajām pusēm ir jāmēģina atrisināt strīdu vai uzskatu atšķirības labticīgi ar pārrunām starp pusēm;

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

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

9.14. Piemērojamie normatīvie akti

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

9.15. Atbilstība piemērojamiem normatīvajiem aktiem

9.15.1. UPS darbojās atbilstoši un nodrošina atbilstību šādiem normatīvajiem aktiem:

9.15.1.1. 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”;

9.15.1.2. Fizisko personu datu aizsardzības likums;

9.15.1.3. Saistītie Eiropas standarti;

9.15.1.3.1. ETSI EN 319 401 Vispārējās politikas prasības Uzticamības pakalpojumu sniedzējiem;

9.15.1.3.2. ETSI EN 319 411 – 1 Politikas un drošības prasības Uzticamības pakalpojumu sniedzējiem, kas izdod sertifikātus; 1.daļa – Vispārīgās prasības;

9.15.1.3.3. ETSI EN 319 411 – 2 Politikas un drošības prasības Uzticamības pakalpojumu sniedzējiem, kas izdod sertifikātus; 2.daļa – Politikas prasības sertifikācijas centriem, kas izdod kvalificētus sertifikātus;

9.15.1.3.4. Citiem uz UPS darbību attiecināmajiem normatīvajiem aktiem.

9.16. Dažādas prasības

9.16.1. Katra šī dokumenta atruna ir spēkā pēc pati par sevi (pēc būtības) un neietekmē pārējās atrunas. Nederīga vai nepilnīga atruna var tikt aizstāta ar citu līdzvērtīgu atrunu.

9.16.2. Nevienu no šī dokumenta prasībām vai noteikumiem, kas tieši ietekmē UPS tiesības un pienākumus un neietekmē pārējās puses, nevar grozīt, atteikties, papildināt, vai likvidēt bez apstiprinātas rakstiskas UPS piekrišanas.

9.16.3. Šis dokuments ir sagatavots latviešu valodā. Šis dokuments var tikt tulkots un var būt pieejams arī citās valodās. Dokumenta tulkojumu nesakritību gadījumā dokumenta versija latviešu valodā vienmēr ir vadoša.

9.17. Citas prasības

9.17.1. Nav nosacījumu.