AS Sertifitseerimiskeskus – ESTEID-SK sertifitseerimispõhimõtted

Tõlge AS Sertifitseerimiskeskuse originaaldokumendile "AS Sertifitseerimiskeskus – ESTEID-SK Certification Practice Statement"

Versioon 1.0

Kehtiv alates 01.11.2016

Versioonide ajalugu		
Kuupäev	**Versioon**	**Muudatused**
1.11.2016	1.0	Esmane versioon.

4. Sertifikaadi elutsükli tegevusnõuded

- 4.1. Sertifikaadi taotlemine
  - 4.1.1. Kes võib sertifikaaditaotluse esitada
    - 4.1.1.1. ID-kaart ja digi-ID
    - 4.1.1.2. Mobiil-ID
  - 4.1.2. Registreerimisprotsess ja vastutus
    - 4.1.2.1. ID-kaart
    - 4.1.2.2. Digi-ID
    - 4.1.2.3. Mobiil-ID
- 4.2. Sertifikaaditaotluse menetlemine
  - 4.2.1. Identifitseerimis- ja autentimisfunktsioonide sooritamine
    - 4.2.1.1. ID-kaart ja digi-ID
    - 4.2.1.2. Mobiil-ID
  - 4.2.2. Sertifikaaditaotluste heakskiitmine või tagasilükkamine
    - 4.2.2.1. ID-kaart
    - 4.2.2.2. Digi-ID
    - 4.2.2.3. Mobiil-ID
  - 4.2.3. Sertifikaaditaotluste menetlemise aeg
- 4.3. Sertifikaadi väljastamine
  - 4.3.1. CA tegevused sertifikaadi väljastamisel
    - 4.3.1.1. ID-kaart ja digi-ID
    - 4.3.1.2. Mobiil-ID
  - 4.3.2. Kliendi teavitamine sertifikaadi väljastamisest CA poolt
    - 4.3.2.1. ID-kaart ja digi-ID
    - 4.3.2.2. Mobiil-ID
- 4.4. Sertifikaadi vastuvõtmine
  - 4.4.1. Käitumine sertifikaadi vastuvõtmisel
    - 4.4.1.1. ID-kaart ja digi-ID
    - 4.4.1.2. Mobiil-ID
  - 4.4.2. Sertifikaadi avaldamine CA poolt
    - 4.4.2.1. ID-kaart ja digi-ID
    - 4.4.2.2. Mobiil-ID
  - 4.4.3. Sertifikaadi väljastamisest teatamine CA poolt teistele üksustele
- 4.5. Võtmepaar ja sertifikaadi kasutamine
  - 4.5.1. Kliendi isiklik võti ja sertifikaadi kasutamine
  - 4.5.2. Huvitatud isiku avalik võti ja sertifikaadi kasutamine
- 4.6. Sertifikaadi uuendamine
- 4.7. Sertifikaadi võtmevahetus
  - 4.7.1. Sertifikaadi võtmevahetuse asjaolud
    - 4.7.1.1. ID-kaart ja digi-ID
    - 4.7.1.2. Mobiil-ID
  - 4.7.2. Kes võib uue avaliku võtme sertifitseerimist taotleda
    - 4.7.2.1. ID-kaart ja digi-ID
    - 4.7.2.2. Mobiil-ID
  - 4.7.3. Sertifikaadi võtmevahetuse taotluste menetlemine
    - 4.7.3.1. ID-kaart ja digi-ID
    - 4.7.3.2. Mobiil-ID
  - 4.7.4. Kliendi teavitamine uue sertifikaadi väljastamisest
    - 4.7.4.1. ID-kaart ja digi-ID
    - 4.7.4.2. Mobiil-ID
  - 4.7.5. Käitumine uue võtmega sertifikaadi vastuvõtmisel
    - 4.7.5.1. ID-kaart ja digi-ID
    - 4.7.5.2. Mobiil-ID
  - 4.7.6. Uue võtmega sertifikaadi avaldamine CA poolt
  - 4.7.7. Sertifikaadi väljastamisest teatamine CA poolt teistele üksustele
- 4.8. Sertifikaadi muutmine
  - 4.8.1. Sertifikaadi muutmise asjaolud
    - 4.8.1.1. ID-kaart ja digi-ID
    - 4.8.1.2. Mobiil-ID
  - 4.8.2. Kes võib sertifikaadi muutmist taotleda
    - 4.8.2.1. ID-kaart ja digi-ID
    - 4.8.2.2. Mobiil-ID
  - 4.8.3. Sertifikaadi muutmise taotluste menetlemine
    - 4.8.3.1. ID-kaart ja digi-ID
    - 4.8.3.2. Mobiil-ID
  - 4.8.4. Kliendi teavitamine uue sertifikaadi väljastamisest
  - 4.8.5. Käitumine muudetud sertifikaadi vastuvõtmisel
  - 4.8.6. Muudetud sertifikaadi avaldamine CA poolt
  - 4.8.7. Sertifikaadi väljastamisest teatamine CA poolt teistele üksustele
- 4.9. Sertifikaadi kehtetuks tunnistamine ja kehtivuse peatamine
  - 4.9.1. Kehtetuks tunnistamise asjaolud
  - 4.9.2. Kes võib kehtetuks tunnistamist taotleda
    - 4.9.2.1. ID-kaart ja digi-ID
    - 4.9.2.2. Mobiil-ID
  - 4.9.3. Sertifikaadi kehtetuks tunnistamise taotlemise kord
    - 4.9.3.1. ID-kaart ja digi-ID
    - 4.9.3.2. Mobiil-ID
  - 4.9.4. Kehtetuks tunnistamise taotlemise ajapikendus

1. Sissejuhatus

AS Sertifitseerimiskeskus (edaspidi SK) asutati 26. märtsil 2001. Ettevõtte omanikud on AS Swedbank, AS SEB Pank ja Telia Eesti AS. SK peamisteks tegevusaladeks on usaldusteenuste ja nendega seotud tehniliste lahenduste osutamine Baltimaades. Need teenused tagavad nii riigiasutustes kui ka ettevõtetes igapäevase turvalise ja kontrollitud elektroonilise kommunikatsiooni.

Käesolevas CPS-is on täielikult ümber kujundatud eelmine „AS Sertifitseerimiskeskus – sertifitseerimispõhimõtted“ [1] , „ESTEID-kaardi sertifitseerimispoliitika“ [2] ja „Mobiil-ID kujul digitaalse isikutunnistuse sertifitseerimispoliitika“ [3]. Nimetatud dokumentide ümberkujundamine standardi IETF RFC 3647 [4] kohaselt ja käesoleva CPS-i jõustamine ei muuda oluliselt vastavate sertifitseerimisteenuste osutamist.

ETSI EN 319 400 seeria eeskujul on SK jaotanud dokumentatsiooni kolmeks osaks:

- „AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted“ [5] (edaspidi SK PS) kirjeldavad kõikidele usaldusteenustele kehtivaid üldisi praktikaid;
- sertifitseerimispõhimõtted ja ajatempli teenuse osutaja põhimõtted kirjeldavad neid osi, mis kehtivad konkreetsele alam-CA-le või ajatembeldusüksusele;
- tehnilised profiilid asuvad eraldi dokumentides.

IETF RFC 3647 [4] kohaselt jaguneb käesolev CPS üheksaks osaks. IETF RFC 3647 [4] ülesehituse säilitamiseks on nende lõikude pealkirjade juures, mis ei kehti, märge **„Ei kohaldata“.** Viited SK PS-ile [5] ning dokumentidele „Sertifikaadi, CRL-i ja OCSP profiilid Eesti Vabariigi isikut tõendavatel dokumentidel“ [6] (edaspidi sertifikaadi profiil) on lisatud vajaduse korral.

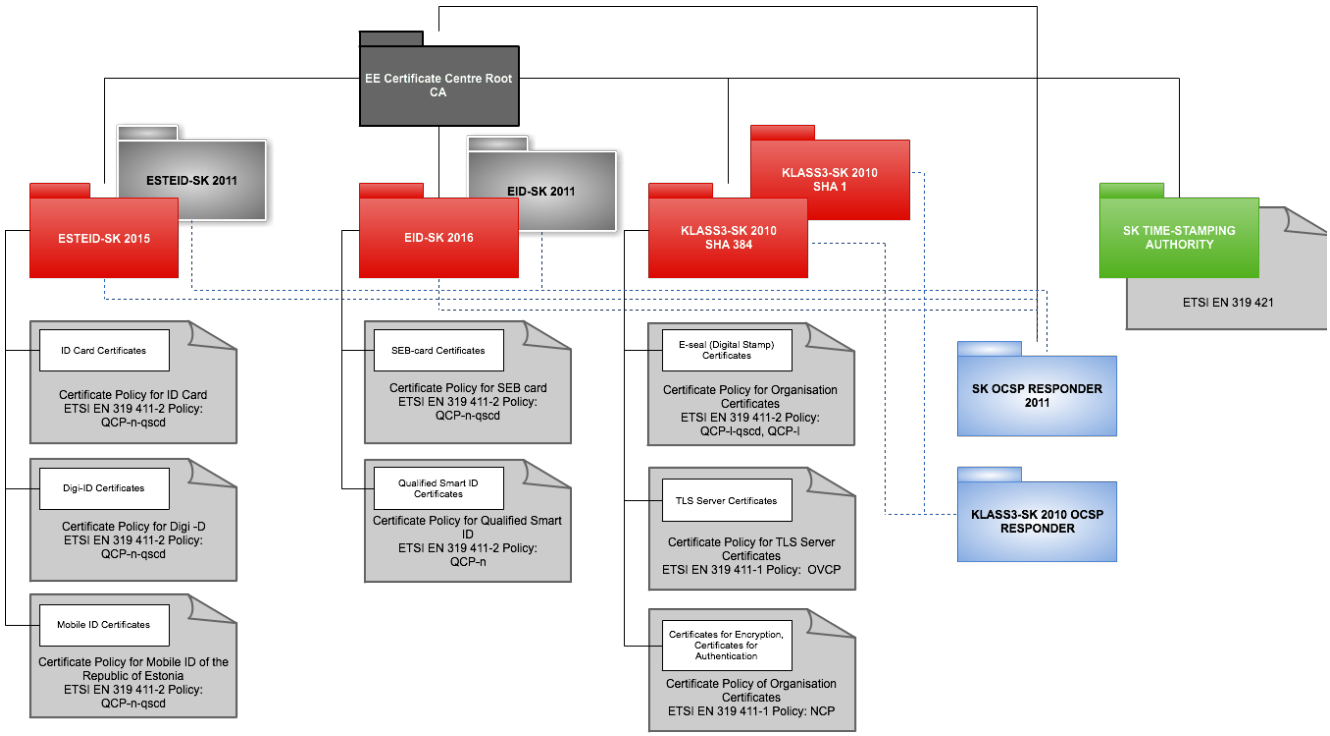
1.1. Ülevaade

Käesolevas CPS on kirjeldatud tavasid, mida kasutatakse vastavuse tagamiseks dokumentidega „AS Sertifitseerimiskeskus – ID-kaardi sertifitseerimispoliitika“ [7] (edaspidi
„CP“), „AS Sertifitseerimiskeskus – digi-ID sertifitseerimispoliitika“ [8] (edaspidi digi-ID CP) ja „AS Sertifitseerimiskeskus
- Eesti Vabariigi Mobiil-ID sertifitseerimispoliitika“ [9] (edaspidi Mobiil-ID CP).

Poliitikad vastavad standardile ETSI EN 319 411-2 Poliitika: QCP-n-qscd [10] ja ETSI EN 319 411-1 Poliitika: NCP+ [11].

SK kasutab hetkel järgmist sertifitseerimisahelat:

EE Certification Centre Root CA ahel, kehtiv 2010–2030



Käesolev CPS hõlmab ESTEID-SK 2011 ja ESTEID-SK 2015 tegevust. Viimane on praegune väljastav CA, samas kui vanem pakub lihtsalt olekuteavet enne 2016. aastat väljastatud sertifikaatide kohta.

Käesolevas CPS-s kirjeldatud isikut tõendava dokumendi ja elamisloakaardi (edaspidi ID-kaart), digitaalse isikutunnistuse ning e-elamisloakaardi (edaspidi koos digi-ID) ja Mobiil-ID vormis digitaalse isikutunnistuse (edaspidi Mobiil-ID) kvalifitseeritud elektroonilise allkirja sertifikaadi sertifitseerimisteenus on Eesti usaldusnimekirjas kvalifitseeritud olekuga.

Vastuolude korral arvestatakse dokumente järgmises järjekorras (ülimuslikud eespool):

- QCP-n-qscd;
- NCP+;
- CP [7] või digi-ID CP [8] või Mobiil-ID CP [9];
- käesolev CPS.

1.2. Dokumendi nimi ja identifitseerimine

Käesoleva dokumendi nimi on on „AS Sertifitseerimiskeskus – ESTEID-SK sertifitseerimispõhimõtted“. Käesolev on dokumendi esimene versioon.

1.3. Avalik infrastruktuur

1.3.1. Sertifitseerimisasutus

SK tegutseb sertifitseerimisasutusena, mis väljastab ID-kaardi, digi-ID ja Mobiil-ID sertifikaate.

ID-kaardi ja digi-ID puhul tegutseb SK Trüb Baltic AS-i alltöövõtjana. PPA-l on Trüb Baltic AS-i ning Politsei- ja Piirivalveametiga (edaspidi PPA) leping ID-kaardi, digi-ID tootmiseks, isikustamiseks ning sertifikaatide väljastamiseks ja teenindamiseks.

Mobiil-ID puhul osutab SK sertifitseerimisteenust PPA ja SK vahel allkirjastatud lepingu alusel.

SK sertifitseerimisteenus hõlmab vaikimisi kogu võtmepaaride ja sertifikaatide elutsükliga seotud protseduure, mida on kirjeldatud käesolevas CPS-is.

Sertifikaate väljastavad vahendajatest CA-d ESTEID-SK 2011 ja ESTEID-SK 2015, mida identifitseeritakse järgmiste sertifikaatidega:

1) ESTEID-SK 2011

```
Sertifikaat:
    Andmed:
        Versioon: 3
        (0x2)
        seerianumber:
            29:52:93:aa:fd:8c:c6:d4:4d:83:30:a3:c2:64:51:0d
        Signeerimisalgoritm: sha1WithRSAEncryption
        Väljastaja: C=EE, O=AS Sertifitseerimiskeskus, CN=EE Certification
Centre Root CA/emailAddress=pki@sk.ee
        Kehtivus
            Mitte enne: 18. märts 10:14:59 2011
            GMT Mitte pärast: 18. märts 10:14:59
            2024 GMT Mitte pärast:
        Subjekt: C=EE, O=AS Sertifitseerimiskeskus, CN=ESTEID-SK
2011/emailAddress=pki@sk.ee
        Subjekti avaliku võtme teave:
            Avaliku võtme algoritm: rsaEncryption
            RSA avalik võti: (2048
                bitti) Moodul (2048
                bitti):
                    00:b3:e9:7c:6c:66:1e:ab:fd:a5:dc:35:ed:e4:4a:
                    93:4c:3a:a9:90:a0:05:d4:a7:3c:dc:af:86:52:68:
                    66:61:ff:b2:47:22:2a:65:bc:d8:ba:b5:b5:bf:94:
                    ae:ec:02:24:6c:6f:ae:4a:cc:c5:91:38:46:ae:95:
                    de:ba:82:06:c3:3e:06:ba:91:4f:7b:0b:e0:17:1a:
                    ee:fe:0d:13:97:b2:d8:d4:3a:fe:95:96:b1:d9:54:
                    09:cb:98:83:a4:c9:ca:56:6b:18:cc:f8:47:d0:3d:
                    9b:83:c4:46:e4:c3:de:81:df:f7:c6:eb:d6:5b:a7:
                    7b:3d:cb:a5:84:87:05:39:63:d2:22:42:5f:18:4e:
```

```
                    41:a7:35:4c:62:75:06:ce:37:50:46:42:6f:87:54:
                    4b:20:4d:fd:b6:27:aa:fa:1b:71:6c:13:4e:eb:9c:
                    c3:6c:90:d0:b7:0e:3b:8b:48:25:0a:17:89:07:d2:
                    b5:46:54:af:41:76:20:9d:15:a6:63:1c:4c:a4:8f:
                    08:c8:1b:3a:a7:cb:1c:91:29:ee:18:6c:9e:81:f4:
                    00:66:f7:97:92:16:03:01:1e:d6:44:61:4f:aa:d1:
                    55:08:40:68:40:18:0b:ab:39:35:e3:5a:2d:53:b2:
                    c0:38:da:69:cb:19:06:44:23:91:97:31:7b:5a:6e:
                    9e:75
                Eksponent: 65537
        (0x10001) X509v3 laiendused:
            X509v3 Põhipiirangud: kriitiline
                CA:TRUE, pathlen:0
            X509v3 Põhiskasutusvaldkond: kriitiline
                Sertifikaadi märk, CRL-i märk
            X509v3 Sertifitseerimispoliitikad:
                Poliitika: 1.3.6.1.4.1.10015.100.1.1.1
                  Teatis
                    kasutajale:
                    Otsene tekst:
                  CPS: https://www.sk.ee/CPS
            X509v3 Subjekti võtme
            identifikaator:

7B:6A:F2:55:50:5C:B8:D9:7A:08:87:41:AE:FA:A2:2B:3D:5B:57:76
            X509v3 Asutuse võtme identifikaator:

keyid:12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99
            X509v3 Tühistusnimekirjade levituspunktid: URI:
                http://www.sk.ee/repository/crls/eeccrca.crl
    Signeerimisalgoritm: sha1WithRSAEncryption
        a0:b8:20:dd:c5:0b:68:15:0c:81:f4:e5:33:4c:80:5a:d0:38:
        21:92:9d:78:73:a0:97:25:44:ba:10:f3:50:42:39:74:d9:23:
        8a:a7:ec:de:f8:14:71:27:ac:0c:ba:b8:d1:bb:49:2e:6a:00:
        da:92:68:f2:0b:f1:da:7a:de:38:3f:2f:8a:a7:e2:25:9a:07:
        9a:b9:18:62:4e:57:4e:d2:9d:31:d2:ee:05:2b:a8:28:46:0a:
        59:d4:78:7c:62:65:b2:f5:dc:f9:0f:df:b2:e7:73:e4:ca:97:
        54:8a:7e:0b:67:e4:56:c7:e5:ca:ab:86:f6:c0:fd:51:77:63:
        39:62:9a:ef:8b:ec:45:68:85:6f:47:2b:16:7f:ff:3f:24:0e:
        7e:a2:7a:23:c5:7d:97:53:3a:8b:ff:d1:e5:d5:2e:5c:6a:92:
        5c:9b:52:e4:ba:2d:84:51:0e:2a:90:ba:98:01:29:00:53:c0:
        d6:c2:f3:1d:14:1d:7d:34:1e:89:16:f9:d0:95:71:0b:ec:51:
        bb:f8:c4:b8:51:ab:f3:2f:c9:3b:61:13:e4:5d:6e:4a:d5:d0:
```

```
            9b:b3:6d:f6:6f:00:37:e3:ef:99:c0:df:e6:40:cc:56:12:e5:
            9a:4c:3a:36:7d:a7:8a:d0:54:aa:73:41:39:25:ac:5d:26:ea:
            69:1d:70:4a
```

2) ESTEID-SK 2015

```
Sertifikaat:
    Andmed:
        Versioon: 3
        (0x2)
        seerianumber:
            45:48:09:0b:87:9c:ef:21:56:72:ac:d3:de:6c:1b:5b
        Signeerimisalgoritm: sha384WithRSAEncryption
        Väljastaja: C=EE, O=AS Sertifitseerimiskeskus, CN=EE
        Certification
Centre Root CA/emailAddress=pki@sk.ee
        Kehtivus
            Mitte enne: 17. dets 12:38:43 2015
            GMT Mitte pärast: 17. dets 23:59:59
            2030 GMT
        Subjekt: C=EE, O=AS
Sertifitseerimiskeskus/2.5.4.97=NTREE-10747013, CN=ESTEID-SK 2015
        Subjekti avaliku võtme teave:
            Avaliku võtme algoritm: rsaEncryption
            RSA avalik võti: (4096
                bitti) Moodul (4096
                bitti):
                    00:d2:81:fa:d4:d0:f1:6d:d5:bd:93:c9:cb:03:5a:
                    86:68:be:01:ee:fc:9d:a1:dd:84:c2:9f:d2:4c:16:
                    41:df:01:2d:20:90:8b:76:4a:44:b1:2f:29:5d:f1:
                    62:46:ac:03:56:c8:06:19:bb:be:43:df:6d:ae:56:
                    f9:2c:8e:f2:8b:ba:c8:91:1a:2f:e4:d7:ed:05:d4:
                    8d:3d:25:39:ac:08:58:3d:08:6f:65:94:20:3b:04:
                    5a:1d:ae:44:cb:e0:5a:2c:91:e6:2e:a6:10:4b:d8:
                    50:bd:0b:02:63:2c:2c:fb:15:6f:34:55:29:2b:4a:
                    46:0f:ae:22:c9:ca:9d:32:e0:65:fe:75:aa:dd:f2:
                    ee:66:9a:70:06:1d:15:16:5b:66:e2:78:6b:ff:54:
                    b4:47:d4:d1:26:9a:85:50:66:c6:af:83:8a:fc:3c:
                    1e:6d:0e:4f:8e:17:52:e3:48:02:50:dc:26:0b:b7:
                    cf:43:8b:c8:1f:ec:7e:4c:29:36:68:6f:ae:dc:ca:
                    00:cf:42:2b:a5:55:aa:8b:0c:c6:fe:fc:6b:7a:e3:
                    cf:02:48:17:78:50:9e:61:fe:9f:5c:bb:06:cf:85:
                    a2:be:c6:45:6e:98:76:a4:c8:c4:2e:ee:ac:96:d9:
                    41:5d:f0:06:dd:f1:af:e3:7b:7d:d5:55:e2:73:2c:
                    d1:fd:e4:f9:76:c0:7e:cc:5b:16:d6:c1:d5:fb:53:
                    8d:3e:bf:aa:ce:00:f1:08:7d:9c:9a:ea:a8:64:d7:
                    c8:22:af:9b:ba:86:f7:78:0f:1e:7b:e5:e9:24:a2:
                    50:af:ed:6a:1a:b9:a1:82:08:ef:02:17:3b:9b:a7:
                    14:e3:1f:d0:7f:1c:11:62:12:15:36:12:5f:fa:c2:
                    95:4e:19:10:85:b2:7d:5f:1b:8a:93:77:35:f3:0c:
                    a6:c0:bd:66:a4:30:f4:3c:81:89:aa:5b:2c:31:e8:
                    ae:27:82:33:6a:01:5b:80:44:86:34:35:1d:e2:27:
                    26:d2:14:13:f0:29:90:79:49:b5:19:b5:9e:05:8b:
                    1e:a8:f8:4c:41:7f:7b:40:50:4b:5c:92:d5:cb:64:
                    82:ca:80:33:ec:1a:b5:a8:0e:37:fb:e1:1c:89:b3:
                    7e:c8:17:35:9d:0b:36:66:8a:bc:72:4f:4c:2b:46:
                    c2:c4:33:1e:52:44:14:cf:a5:5e:40:6a:7a:f4:89:
                    8e:42:bb:30:e3:aa:93:cf:49:ad:75:0a:cc:49:b9:
```

e4:5c:2b:8b:6a:7e:5d:3e:6d:bc:e0:9f:47:99:aa:

```
                    a2:62:2e:a3:e8:a2:dc:67:63:64:52:70:d0:15:eb:
                    01:56:53:04:9b:e7:c7:6b:68:91:ea:59:c0:15:86:
                    74:e9:41
                Eksponent: 65537
        (0x10001) X509v3 laiendused:
            X509v3 Asutuse võtme identifikaator:

keyid:12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99
            X509v3 Subjekti võtme identifikaator:

B3:AB:88:BC:99:D5:62:A4:85:2A:08:CD:B4:1D:72:3B:83:72:47:51
            X509v3 Põhiskasutusvaldkond: kriitiline
                 Sertifikaadi märk, CRL-i
                           märk
            X509v3
                Poliiti 0.4.0.2042.1.2
                Poliiti 0.4.0.194112.1.2
                Poliiti 1.3.6.1.4.1.10015.1.1
                  CPS: https://www.sk.ee/CPS
                Poliiti 1.3.6.1.4.1.10015.1.2
                Poliiti 1.3.6.1.4.1.10015.1.3


            X509v3 Põhipiirangud: kriitiline
                CA:TRUE, pathlen:0
            X509v3 Nimepiirangud:
                Välistatud:
                  DNS:""
                  IP:0.0.0.0/0.0.0.0
                  IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0
            X509v3 Sertifikaadi lisakasutusvaldkond:
                OCSP signeerimine, TLS veebikliendid autentimine, e-post
Kaitse
            Asutuse teabe juurdepääs:
                OCSP - URI:
                http://ocsp.sk.ee/CA CA
                väljastajad -
URI: http://www.sk.ee/certs/EE_Certification_Centre_Root_CA.der.crt
            X509v3 Tühistusnimekirjade levituspunktid: URI:
                http://www.sk.ee/repository/crls/eeccrca.crl
    Signeerimisalgoritm: sha384WithRSAEncryption
        74:56:0c:62:37:3f:4d:2b:da:c3:a7:96:f2:c7:2a:4f:5e:13:
        b5:fd:dd:e4:fe:e1:ee:53:79:a4:2c:3a:91:39:cd:04:54:4e:
        db:21:c4:df:01:9f:1d:93:a1:0f:6b:82:2d:7c:ab:e3:30:5e:
        6d:9f:d2:6a:c6:6a:46:18:1b:46:e2:c7:b6:60:0d:0b:c2:30:
        3f:e4:b9:16:26:c0:b1:9d:7e:c4:d7:c2:1f:0a:b8:be:ae:48:
        71:7e:53:f6:53:b2:ce:aa:1b:b9:b1:08:71:bd:62:f7:9b:90:
        de:58:8f:fa:d8:46:f6:7d:fe:e2:7d:ae:27:81:cb:1c:38:c2:
        8e:db:d7:da:76:d8:f5:e4:02:45:cf:e7:2d:fe:a8:af:ce:7a:
        df:7c:96:ac:08:f7:b9:09:86:24:b6:cf:11:58:46:4f:9d:5d:
        b6:b3:9a:85:47:9e:8c:d8:2a:6b:19:69:25:2f:a1:83:4d:1f:
        5f:6d:a5:2e:c1:2d:db:20:8b:d2:a9:6e:f4:0b:6f:9c:b0:20:
        ca:bd:ba:dd:fe:6f:65:ef:ce:af:32:ce:61:cc:16:d2:c8:27:
```

```
a0:1f:bb:58:c9:a6:a0:fc:d8:15:00:15:cb:e2:e6:f8:67:3f:
c3:3b:6f:de:f8:47:5f:16:08:ea:60:35:0b:d7:0c:8f:b6:ff:
c6:48:35:e5
```

1.3.2. Registreerimisasutused

1.3.2.1. ID-kaart ja digi-ID

Registreerimisasutused on sätestatud isikut tõendavate dokumentide seaduse [12] (edaspidi ITDS) 3. peatükis.

PPA ja Välisministeerium võivad esineda protsessis läbivalt mitmes rollis. Käesolevas CPS-is eristatakse rolli alusel läbivalt järgmist:

- mõlemat asutust nimetatakse RA-ks, kui nad sooritavad tehnilisi toiminguid nagu silmast silma autentimine või ID-kaardi või digi-ID üleandmine;
- neid nimetatakse koos PPA-ks, kui nad esindavad ITDS-i [12] kohaselt Eesti Vabariiki dokumentide väljastaja rollis, nt isikute esialgse tuvastamise või otsuste tegemise ajal nende ID-kaardi või digi-ID taotlemise kõlblikkuse kohta.

PPA-ga võib võtta ühendust järgmiselt:

Pärnu mnt 139,

15060 Tallinn

Teave: +372 612 3000

Faks: +372 612 3009

E-post: info@politsei.ee

https://www.politsei.ee/

Välisministeeriumiga saab võtta ühendust saatkondade ja esinduste kaudu, mida saab kontrollida välisministeeriumi veebilehel http://www.vm.ee/en/embassies-and-representations.

1.3.2.1.1 PPA klienditeeninduspunkt

Taotlusi võetakse vastu ning ID-kaarte ja digi-ID-sid väljastatakse PPA büroodes ning Eesti Vabariigi saatkondades (edaspidi PPA klienditeeninduspunkt).

ID-kaardi ja digi-ID sertifikaatide teenindamine (kehtivuse peatamine, kehtivuse peatatuse lõpetamine, kehtetuks tunnistamine ja PIN-koodidega ümbrike kehtivuse peatamine ning asenduste määramine)
toimub PPA klienditeeninduspunktides ja/või SEB Panga ning Swedbanki teeninduspunktides.

ID-kaardi ja digi-ID sertifikaatide vahetamine toimub PPA klienditeeninduspunktides või avalikus andmesidevõrgus oleva rakenduse abil.

PPA klienditeeninduspunktide nimekirja ja lahtiolekuaegu saab kontrollida järgmistel veebilehtedel:

- https://www.politsei.ee/en/kontakt/kmb/;
- http://www.vm.ee/en/country-representations/estonian-representations;
- https://www.sk.ee/kontakt/klienditeeninduspunktid/ .

1.3.2.1.2 SK klienditeeninduspunkt

ID-kaardi ja digi-ID sertifikaatide teenindamine (kehtivuse peatamine, kehtivuse peatatuse lõpetamine, kehtetuks tunnistamine ja PIN-koodidega ümbrike kehtivuse peatamine ning asenduste määramine)
toimub SEB Panga ning Swedbanki teeninduspunktides (edaspidi SK klienditeeninduspunkt). SK klienditeeninduspunkt

tegutseb SK ja kliendi vahelistes suhetes SK esindajana.

SK klienditeeninduspunkti ja SK vaheline suhe on ära määratud kahepoolse(te) lepingu(te)ga.

Teave SK klienditeeninduspunktide kohta ja nende kontaktandmed on saadaval SK veebilehel https://www.sk.ee/kontakt/klienditeeninduspunktid/ /.

1.3.2.2. Mobiil-ID

PPA ja mobiilside operaator (edaspidi MO) võivad esineda protsessis läbivalt mitmes rollis. Käesolevas CPS-i ülejäänud osas eristatakse rolli alusel läbivalt järgmist:

- PPA-d ja MO-d nimetatakse RA-ks, kui nad sooritavad tehnilisi toiminguid, mis ei ole konkreetse organisatsiooni suhtes spetsiifilised, nt kliendi autentimine;
- PPA-le ja MO-le viidatakse sõnaselgelt nende vastavate nimedega, kui nad sooritavad konkreetse organisatsiooniliigi jaoks spetsiifilisi toiminguid (nt QSCD väljastamine kliendile või riigilõivu kogumine) või kui PPA esindab Eesti Vabariiki dokumentide väljastaja rollis vastavalt ITDS-ile [12] või isikute esialgse tuvastamise või otsuste tegemise ajal nende Mobiil-ID taotlemise kõlblikkuse kohta.

PPA-ga võib võtta ühendust järgmiselt:

Pärnu mnt 139,

15060 Tallinn

Teave: +372 612 3000

Faks: +372 612 3009

E-post: info@politsei.ee

https://www.politsei.ee/

MO kontaktandmeid saab kontrollida SK veebilehel http://www.sk.ee.

QSCD väljastamiseks on SK ja MO vahel allkirjastatud lepingud. SK on andnud punktis 1.3.2.2.1 kirjeldatud kohustused lepinguliselt üle MO-le.

1.3.2.2.1 MO klienditeeninduspunkt

QSCD-de väljastamine ja teenindamine, Mobiil-ID sertifikaatide asendamise taotluse edastamine QSCD asendamise korral (sertifikaadi võtmevahetus), Mobiil-ID sertifikaatide teenindamine ja mobiiltelefoninumbri vahetamine toimub MO volitatud klienditeeninduspunktides.

MO klienditeeninduspunkt võtab klientidelt vastu Mobiil-ID sertifikaatide kehtetuks tunnistamise taotlusi. Enne kehtetuks tunnistamise taotluse vastuvõttu kontrollib MO klienditeeninduspunkt kliendi identiteedi vastavalt oma sisemisele identifitseerimiskorrale.

MO klienditeeninduspunktide nimekirja ja lahtiolekuaegu saab kontrollida SK veebilehel https://www.sk.ee/kontakt/klienditeeninduspunktid/ ja MO juures.

1.3.2.2.2 SK klienditeeninduspunkt

SK tegutseb klienditeeninduspunktina.

SK klienditeeninduspunkt võtab vastu elektrooniliselt allkirjastatud Mobiil-ID sertifikaatide kehtivuse peatamise ja kehtivuse peatatuse

lõpetamise taotlusi. Kontaktteave on saadaval SK veebilehel https://sk.ee /kontakt/.

1.3.2.3. Abiliin

Abiliin tegeleb SK esindajana klientide telefoniteenindusega. Abiliin pakub vajadusel tuge ID-kaardi ja digi-ID-ga seotud probleemide lahendamisel.

Abiliin võtab vastu ID-kaardi ja digi-ID sertifikaatide kehtivuse peatamise taotlusi klientidelt ning teistelt isikutelt.

Abiliin pakub ka täiendavat teavet ja abistab vajaduse korral kliente Mobiil-ID osas. Abiliin ei võta vastu Mobiil-ID sertifikaatide kehtivuse peatamise taotlusi.

Abiliini puudutav teave ja kontaktandmed on saadaval SK veebilehel https://www.sk.ee/kontakt/id-abiliin-1777/ .

Abiliini saab võtta ühendust numbril 1777 või (+ 372) 677 3377.

1.3.3. Kliendid

Vaadake CP [7] punkti 1.3, digi-ID CP-d [8] ja Mobiil-ID CP-d [9].

1.3.4. Huvitatud isikud

Huvitatud isik on füüsiline või juriidiline isik, kes võtab vastu otsuse kasutades selleks ka SK poolt väljastatud sertifikaati.

1.3.5. Teised pooled

1.3.5.1. ID-kaart ja digi-ID

Trüb Baltic AS:

- võtab vastu ID-kaartide tellimusi;
- toodab ID-kaartide ja digi-ID toorikuid;
- isikustab ID-kaarte PPA-st saadetud tellimuste alusel;
- loob ID-kaardi jaoks kaardil olevad võtmed ja taotleb vastavad sertifikaadid;
- laadib sertifikaadid ID-kaardile;
- annab ID-kaardid üle PPA-le;
- annab digi-ID toorikud üle PPA-le;
- tagab RA büroos tehnilise keskkonna digi-ID isikustamiseks;
- toodab ID-kaardi ja digi-ID jaoks asendus-PIN-koodidega ümbrikud.

Trüb Baltic AS-iga võib võtta ühendust järgmiselt:

Laki 5,

10621 Tallinn

Teave: +372 658 11

E-post: info@trueb.ee

http://www.trueb.ee/trub-avaleht

1.3.5.2. Mobiil-ID

SIM-kaardi valmistaja (edaspidi SCM):

- toodab QSCD, loob võtmepaarid ja laadib need QSCD-le. MO:
- seob kliendi konkreetse QSCD-ga ja väljastab QSCD kliendile.

Telekommunikatsiooniteenuse osutaja:

- käitab tarkvara DigiDoc Service [18], mis võimaldab Mobiil-ID kasutamist.

1.4. Sertifikaadi kasutamine

1.4.1. Sertifikaadi sobivad kasutusviisid

Vaadake CP [7] punkti 1.4, digi-ID CP-d [8] ja Mobiil-ID CP-d [9].

1.5. Poliitika haldamine

1.5.1. Dokumenti haldav organisatsioon

CPS-i haldab SK. AS

Sertifitseerimiskeskus

Registrikood 10747013

Pärnu mnt 141, 11314 Tallinn

Tel +372 610 1880

Faks: +372 610 1881

E-post: info@sk.ee

http://www.sk.ee/en/

1.5.2. Kontaktisik

Ärijuht

E-post: info@sk.ee

1.5.3. CPS-i sobivust poliitikaga määrav isik

Ei kohaldata.

1.5.4. CPS-i heakskiitmise kord

Käesoleva CPS-i tähendust mittemuutvad muudatused, nagu õigekirjavigade parandamine, tõlkimine ja kontaktandmete ajakohastamine, dokumenteeritakse käesoleva dokumendi jaotises „Versioonid ja muudatused”. Sellise juhul suurendatakse dokumendi versiooninumbri murdarvulist osa.

Kui muudetakse CP-d [7] ja/võiDigi-ID CP-d [8] ja/või Mobiil-ID CP-d [9], vaadatakse muudatuste vajalikkuse ülekontrollimiseks läbi ka CPS.

Sisuliste muudatuste puhul on CPS-i uus versioon eelnevatest selgelt eristatav ja seerianumbrit suurendatakse ühe võrra. Muudetud CPS koos jõustumiskuupäevaga, mis ei või olla varasem kui 30 päeva avaldamisest, avaldadatakse elektrooniliselt SK kodulehel.

Kõik käesoleva CPS-i ID-kaardi ja/või digi-ID-ga seotud muudatused kooskõlastatakse PPA ning Trüb Baltic AS-iga.

Kõik käesoleva CPS-i Mobiil-ID-ga muudatused kooskõlastatakse PPA ning MO-ga.

Kõik muudatused kiidab heaks ärijuht ja muudetud CPS-i jõustab tegevjuht.

1.6. Määratlused ja lühendid

1.6.1. Kasutatud terminoloogia

Käesolevas CPS- is kasutatakse termineid järgnevas tähenduses.

Termin	Määratlus
AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted	Põhimõtted, mida SK rakendab usaldusteenuse osutamisel.
Autentimine	Isiku unikaalne tuvastamine tema väidetava identiteedi kontrollimise teel.
Sertifikaat	Kasutaja avalik võti koos muu teabega, mis on sätestatud sertifikaadi profiilis [6] ja mis on tänu selle väljastanud sertifitseerimisasutuse isikliku võtme abil šifreerimisele võltsimiskindel.
Sertifitseerimisasutus	SK struktuuri osa, mis vastutab elektrooniliste sertifikaatide ning sertifikaatide tühistusnimekirjade väljastamise ja kontrollimise eest oma elektroonilise allkirjaga.
Sertifikaadipaar	Sertifikaadipaar, mis sisaldab üht isikutuvastamist võimaldavat sertifikaati ja üht kvalifitseeritud elektroonilise allkirja sertifikaati.
Sertifitseerimispoliitika	Eeskirjad, mis näitavad konkreetse sertifikaadi rakendatavust mingis kindlas kogukonnas ja/või avalikus infrastruktuuris ühiste turvanõuetega.
Sertifitseerimis-põhimõtted	Üks mitmest dokumendist, mis kõik kokku moodustavad juhtimisraamistiku, mille alusel sertifikaate luuakse, väljastatakse, hallatakse ja kasutatakse.
Sertifikaadi profiil	Dokument, milles on määratud sertifikaadis sisalduv teave ja sertifikaadi miinimumnõuded.
Sertifikaat Tühistusnimekiri	Kehtetute (kehtetuks tunnistatud, kehtivus peatatud) sertifikaatide nimekiri.
Sertifitseerimisteenus	Sertifikaatide väljastamise, kehtivuse peatamise haldamise, kehtivuse peatatuse lõpetamise, kehtetuks tunnistamise, muutmise ja sertifikaatide võtmevahetusega seotud usaldusteenus.
Kvalifitseeritud sertifikaat	Elektrooniliste allkirjade sertifikaat, mille väljastab usaldusteenuse osutaja ja mis vastab määruse eIDAS [13] I lisas sätestatud nõuetele.
Kvalifitseeritud elektrooniline allkiri	Täiustatud elektrooniline allkiri, mis luuakse kvalifitseeritud elektroonilise allkirja andmise vahendiga ja mis põhineb elektrooniliste allkirjade kvalifitseeritud sertifikaadil.
Kataloogiteenus	Sertifikaatide kehtivuse teabe avaldamisega seotud usaldusteenus.
DigiDoc Service	SOAP-il põhinev veebiteenus, mille abil saab lisada hõlpsalt e-teenusele või rakendusele identifitseerimise, digitaalallkirja, allkirja identifitseerimise ja Mobiil-ID funktsionaalsuse.
Eraldusnimi	Subjekti unikaalne nimi sertifikaatide infrastruktuuris.
Digi-ID	Digitaalne isikut tõendav dokument.
Krüpteerimine	Teabe töötlemise meetod, mis muudab teabe loetamatuks neile, kellel ei ole vajalikke oskusi või õigusi.
E-resident	Välismaalane, kelle jaoks Eesti on loonud digitaalse identiteedi ja väljastanud digitaalse identifitseerimisdokumendi, e-residendi digi-ID, tema kodakondsusriigi identifitseerimistunnuste alusel.
Residendi digi-ID	Digitaalne identifitseerimisdokument, mis on väljastatud välismaalasele, kellel puudub õigus ja vajadus taotleda ID-kaart või EL-kaarti.
ID-kaart	Identifitseerimisdokument, mis on Eesti kodaniku ja Eestis püsivalt elava Euroopa Liidu kodaniku kohustuslik isikut tõendav dokument.
ID-1	Vorm, millega on määratletud isikutunnistuste füüsilised omadused vastavalt standardile ISO/IEC 7816 [14].

Terviklus	Massiivi omadus: teavet ei ole pärast massiivi loomist muudetud.
Mobiil-ID	Mobiil-ID vormis digitaalne isikutunnistus on elektrooniline isikutunnistus, mille elektroonilist identifitseerimist võimaldav sertifikaat ja elektroonilist allkirjastamist võimaldav sertifikaat on seotud mobiiltelefoni SIM-kaardiga.
Objekti identifikaator	Objekti unikaalseks nimetamiseks kasutatav identifikaator (OID).
Isikuandmete fail	ID-kaardi ja digi-ID fail, mis sisaldab kliendi isikuandmeid.
PIN-kood	Autentimissertifikaadi ja kvalifitseeritud elektroonilise allkirja sertifikaadi aktiveerimiskood.
Isiklik võti	Võtmepaari võti, mida võtmepaari omanik hoiab salajas ja mida kasutatakse elektrooniliste allkirjade andmiseks ja/või selliste elektrooniliste dokumentide või failide dekrüpteerimiseks, mida krüpteeriti vastava avaliku võtmega.
Avalik võti	Võtmepaar, mida vastava isikliku võtme omanik võib avalikustada ja mida huvitatud isikud kasutavad selleks, et kontrollida omaniku vastava isikliku võtmega antud elektroonilisi allkirju ja/või krüpteerida teateid selliselt, et neid saaks dekrüpteerida vaid omaniku vastava isikliku võtmega.
PUK-kood	PIN-koodide lahtiblokeerimise koodid, kui need on pärast järjestikuste valede sisestuste lubatud arvu blokeeritud.
Kvalifitseeritud sertifikaat	Elektrooniliste allkirjade sertifikaat, mille väljastab usaldusteenuse osutaja ja mis vastab määruse eIDAS [13] I lisas sätestatud nõuetele.
Kvalifitseeritud elektrooniline allkiri	Täiustatud elektrooniline allkiri, mis luuakse kvalifitseeritud elektroonilise allkirja andmise vahendiga ja mis põhineb elektrooniliste allkirjade kvalifitseeritud sertifikaadil.
Kvalifitseeritud elektroonilise allkirja andmise vahend	Turvalise allkirja andmise vahend, mis vastab määruses eIDAS [13] sätestatud nõuetele. Mobiil-ID puhul on QSCD nõuetele vastav SIM-kaart QSCD.
Huvitatud isik	Üksus, mis kasutab sertifikaadis sisalduvat teavet.
Registreerimisasutus	Üksus, mis vastutab sertifikaatide subjektide identifitseerimise ja autentimise eest. Lisaks võib registreerimisasutus võtta vastu sertifikaatide taotlusi, kontrollida ja/või edastada neid sertifitseerimisasutusele.
EL-kaart	Elamisloakaart on Eestis kehtiva elamisloa või elamisõiguse alusel püsivalt elava välismaalase kohustuslik isikut tõendav dokument, mida väljastatakse õigustatud isikutele ITDS-i [12] alusel 2011. aastast. Käesolevas CPS-is nimetatakse ID-kaardiks. Eesti elamisluba ei ole sama mis EL-i elamisluba.
Turvaline krüptograafiline seade	Seade, mis sisaldab kasutaja isiklikku võtit, kaitseb võtit ohtu sattumise eest ja sooritab kasutaja nimel allkirjastamis- või dekrüpteerimisfunktsioone.
Klient	Füüsiline isik, kellele väljastatakse ID-kaardi, digi-ID või Mobiil-ID sertifikaadid avaliku teenusena, kui tal on selleks seadusjärgne õigus. Käesolevas CPS-i hõlmab termin „klient“ ka füüsilise isiku esindajat. Füüsilise isiku esindaja volituste kehtivust kontrollitakse vastavalt käesoleva CPS-i punktile 3.2.5.
Subjekt	Käesolevas dokumendis on subjekt sama mis klient.
Tingimused	Dokument, milles on kirjeldatud kliendi kohustusi ja vastutust seoses sertifikaatide kasutamisega. Sertifikaatide vastuvõtmisel peab klient olema tingimustega tutvunud ja nõustunud.
Trüb Baltic AS	ID-kaartide valmistaja. Lisaks valmistab Trüb Baltic AS digi-ID toorikud tehases ette ja tagab RA büroos tehnilise keskkonna isikustamiseks.

1.6.2. Lühendid

Lühend	Määratlus
CA	Sertifitseerimisasutus
CP	Sertifitseerimispoliitika
CPS	Sertifitseerimispõhimõtted Käesolev dokument on CPS.
CRL	Sertifikaatide tühistusnimekiri
CSR	Sertifikaadi signeerimise taotlemine
eIDAS	Euroopa Parlamendi ja nõukogu 23. juuli 2014. amäärus (EL) nr 910/2014 [13] e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ

ITDS	Isikut tõendavate dokumentide seadus [12]
MO	Mobiilside operaator
OCSP	Sertifikaadi oleku võrguprotokoll
OID	Objekti identifikaator, objekti identifitseerimise unikaalne kood
PPA	Politsei- ja Piirivalveamet
PKI	Avaliku võtme infrastruktuur
QSCD	Kvalifitseeritud elektroonilise allkirja andmise vahend
RA	Registreerimisasutus
SCM	SIM-kaardi valmistaja
SK	AS Sertifitseerimiskeskus, sertifitseerimisteenuse osutaja
SK PS	AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted [5]

2. Avaldamine ja repositooriumi vastutus

2.1. Repositooriumid

Vaadake SK PS-i [5] punkti 2.1.

2.2. Sertifitseerimisteabe avaldamine

Vaadake SK PS-i [5] punkti 2.2.

2.2.1. Avaldamis- ja teavitamispoliitika

Käesolev CPS on avaldatud SK kodulehel: https://sk.ee/en/repository/CPS/.

Käesolev CPS ja viidatud dokumendid – CP [7], digi-ID CP [8] ja Mobiil-ID CP [9] ning sertifikaadi profiil [6] ja „Eesti Vabariigi isikut tõendavate dokumentide sertifikaatide kasutustingimused“ [15] (edaspidi „tingimused“) – koos jõustamise kuupäevadega on avaldatud SK kodulehel https://sk.ee/en/repository vähemalt 30 päeva enne jõustumist.

2.2.2. Sertifitseerimispõhimõtetes avaldamata jäänud kirjed

Vaadake CP [7] punkti 2.2.2, digi-ID CP-d [8] ja Mobiil-ID CP-d [9].

Vaadake SK PS-i [5] punkti 9.3.1.

2.3. Avaldamise aeg ja sagedus

Vaadake käesoleva CPS-i punkti 2.2.1.

2.3.1. Kataloogiteenus

Vaadake SK PS-i [5] punkti 2.3.3.

2.4. Repositooriumide juurdepääsu kontrollimine

Vaadake SK PS-i [5] punkti 2.4.

3. Identifitseerimine ja autentimine

3.1. Nimetamine

3.1.1. Nimede liigid

Kliendile määratavate nimede tüüpe on kirjeldatud sertifikaadi profiilis [6].

Organisatsiooni nime väärtus (O) näitab, kas sertifikaat on väljastatud ID-kaardi, digi-ID või Mobiil-ID jaoks: ID-kaart

ja EL-kaart O = ESTEID digi-ID:

Digi-ID: O = ESTEID (DIGI-ID)

Mobiil-ID: O = ESTEID (MOBIIL-ID)

Residendi digi-ID: O = ESTEID (DIGI-ID E-RESIDENT)

E-residendi Mobiil-ID: O = ESTEID (MOBIIL-ID E-RESIDENT)

3.1.2. Vajadus, et nimed oleksid tähendusega

Kõik sertifikaadi klienditeabejaotises sisalduvad väärtused on tähendusega.

Sertifikaatide erinevatel väljadel esinevate nimede tähendust on kirjeldatud sertifikaadi profiilis [6].

3.1.3. Klientide anonüümsus või pseudonüümsus

Ei ole lubatud.

3.1.4. Erinevate nimevormide tõlgendamise reeglid

ITDS-i [12] kohaselt kodeeritakse võõrtähed vajaduse korral vastavalt ICAO ümberkirjutusreeglitele. Erinevate

nimevormide tõlgendamise eeskirju on kirjeldatud sertifikaadi profiilis [6].

3.1.5. Nimede unikaalsus

Kliendi eraldusnimi koostatakse vastavalt sertifikaadi profiilis [6] kirjeldatud sertifikaadi profiilile. SK ei väljasta erinevatele klientidele identse üldnime (CN), seerianumbri (S) ega e-posti aadressidega subjekti lisanime (SAN) väljadel.

3.1.6. Kaubamärkide tunnustamine, autentimine ja roll

Kaubamärgid ei ole lubatud.

3.2. Identiteedi esialgne kinnitamine

3.2.1. Isikliku võtme omamise tõendamise meetod

3.2.1.1. ID-kaart ja digi-ID

Kliendi isiklik võti luuakse QSCD-I ID-kaardi kiibi või digi-ID isikustamise käigus vastavalt Trüb Baltic AS-is ja PPA-s.

Kaarte käideldakse enne kliendile üleandmist turvalisel ja jälgitaval viisil.

3.2.1.2. Mobiil-ID

MO sooritab kliendi autentimise ja väljastab kliendile isikustatud QSCD eelnevalt loodud võtmetega. Klient allkirjastab vastava avalduse ja kinnitab väljastatud QSCD omandiõigust.

3.2.2. Organisatsiooni identiteedi autentimine

Ei kohaldata.

3.2.3. Üksikisiku identiteedi autentimine

3.2.3.1. ID-kaart ja digi-ID

PPA kontrollib ID-kaardi või digi-ID väljastamisel kliendi identiteedi vastavalt ITDS-ile [12].

PPA esitab isiku tuvastamise andmed Trüb Baltic AS-ile. Trüb Baltic AS edastab sertifikaadi andmed SK-le.

Trüb Baltic AS ja SK kasutavad isiku tuvastamise andmeid, mille esitab PPA.

3.2.3.2. Mobiil-ID

Identiteedi esialgse kinnitamise QSCD väljastamise taotlemisel sooritab MO füüsilise kohaloleku kontrolli teel.

Kui klient on kaotanud Mobiil-ID hooletuse tõttu ja taotleb uut Mobiil-ID-d, autendib PPA kliendi elektrooniliste autentimisvahendite abil enne SK-lt Mobiil-ID sertifikaatide väljastamise taotlemist. PPA võib sooritada elektroonilise autentimise ainult juhul, kui kliendile on väljastatud kehtiv ID-kaart või digi-ID.

3.2.4. Kontrollimata kliendiandmed

Kontrollimata kliendiandmed ei ole sertifikaadil lubatud.

3.2.5. Volituste kinnitamine

Kliendi esindaja esindusõigust kontrollitakse vastavalt ITDS-ile [12].

Klient ei saa taotleda Mobiil-ID-d esindaja kaudu ja Mobiil-ID-d ei saa väljastada esindajale.

3.2.6. Koostoimivuse kriteeriumid

Ei kohaldata.

3.3. Identifitseerimine ja autentimine võtmevahetuseks

3.3.1. Identifitseerimine ja autentimine tavapäraseks võtmevahetuseks

3.3.1.1. ID-kaart ja digi-ID

Kui võtmevahetus sooritatakse selleks ettenähtud rakendusega kliendi arvutis, autenditakse klient kehtiva ID-kaardi või digi-ID autentimissertifikaadiga, mis vajab võtmevahetust.

Kui võtmevahetus on osa füüsilise kaardi asendamisest, on identifitseerimis- ja autentimiskord sarnane käesoleva CPS-i punktis 3.2.3.1 kirjeldatud esialgse väljastamisega.

3.3.1.2. Mobiil-ID

Kehtiva Mobiil-ID QSCD asendamise korral (sertifikaadi võtmevahetus) kontrollib MO kliendi identiteedi elektrooniliselt ja kinnitab kliendi elektroonilist allkirja. MO võib autentida kliendi ka füüsilise kohaloleku kaudu.

3.3.2. Identifitseerimine ja autentimine võtmevahetuseks pärast kehtetuks tunnistamist

3.3.2.1. ID-kaart ja digi-ID

Klient täidab ja allkirjastab ID-kaardi või digi-ID taotluse PPA klienditeeninduspunktis. PPA kontrollib

kliendi identiteedi vastavalt ITDS-ile [12].

3.3.2.2. Mobiil-ID

Sertifikaatide kehtetuks tunnistamise korral peab klient taotlema uut Mobiil-ID-d ja uusi sertifikaate.

Kliendi autentimine toimub vastavalt käesoleva CPS-i punktile 3.2.3.2.

3.4. Identifitseerimine ja autentimine kehtetuks tunnistamise taotlemiseks

Vaadake käesoleva CPS-i punkti 4.9.3.1 ja 4.9.3.2.

4. Sertifikaadi elutsükli tegevusnõuded

4.1. Sertifikaadi taotlemine

4.1.1. Kes võib sertifikaaditaotluse esitada

4.1.1.1. ID-kaart ja digi-ID

Klient esitab ID-kaardi või digi-ID taotluse PPA-le.

PPA kontrollib kliendi ID-kaardi või digi-ID taotlemise kõlblikkust vastavalt ITDS-ile [12].

PPA suhtleb SK-ga on ainult Trüb Baltic AS-i kaudu. SK võtab CSR-e vastu ainult Trüb Baltic AS-ilt.

4.1.1.2. Mobiil-ID

Sertifikaaditaotluse võib klient esitada RA kaudu. SK võtab sertifikaatide taotlusi vastu ainult RA-lt.

Mobiil-ID saab väljastada kliendile, kellel on kehtiv ID-kaart või digi-ID.

4.1.2. Registreerimisprotsess ja vastutus

4.1.2.1. ID-kaart

Klient täidab ja allkirjastab ID-kaardi taotluse PPA klienditeeninduspunktis ning kinnitab selles esitatud andmete õigsust. PPA kontrollib kliendi ID-kaardi taotlemise kõlblikkust vastavalt ITDS-ile [12].

Positiivse otsuse korral koostab PPA uue kaardi tellimuse ja edastab selle Trüb Baltic AS-ile. Pärast uue kaardi taotluse kättesaamist ja vastuvõtmist valmistab Trüb Baltic AS kaardi, jäädvustab sellele visuaalsed elemendid, täidab kaardil oleva isikuandmete faili, loob autentimise ning kvalifitseeritud elektroonilise allkirja võtmepaarid. Trüb Baltic AS esitab CSR-ide paari SK-le.

Trüb Baltic AS ja SK kasutavad isiku tuvastamise andmeid, mille esitab PPA.

Taotlusele vastavad sertifikaadid väljastab SK PPA-st edastatud taotlusandmete ehtsuse ja tervikluse automaatsel kontrollimisel.

SK vastutab õige e-posti aadressi määramise eest autentimissertifikaadile keskkonnas eesti.ee. Kui e-posti aadress on kliendile juba määratud, kasutab SK määratud aadressi uuesti. Kui klient on muutnud nime või kui kliendile ei ole eelnevalt aadressi määratud, loob SK uue aadressi vastavalt sertifikaadi profiili [6] punktile 6.1.

SK edastab sertifikaadid Trüb Baltic AS-ile. Trüb Baltic AS laadib sertifikaadid ID-kaardile ja annab PPA-le üle isikustatud, kuid aktiveerimata ja kasutamiskõlbmatu ID-kaardi.

4.1.2.2. Digi-ID

Klient täidab ja allkirjastab digi-ID taotluse PPA klienditeeninduspunktis ning kinnitab selles esitatud andmete õigsust. PPA kontrollib kliendi digi-ID taotlemise kõlblikkust vastavalt ITDS-ile [12]. PPA kontrollib, et digi-ID väljastatakse kliendile, kellele on väljastatud ID-kaart või kes taotleb ID-kaarti samal ajal digi-ID-ga.

Positiivse otsuse korral isikustab PPA uue digi-ID, täidab isikuandmete faili, loob autentimise ja kvalifitseeritud elektroonilise allkirja võtmepaarid ning esitab CSR-ide paari Trüb Baltic AS-ile. Trüb Baltic AS edastab sertifikaaditaotluse SK-le.

Trüb Baltic AS ja SK kasutavad isiku tuvastamise andmeid, mille esitab PPA.

Taotlusele vastavad sertifikaadid väljastab SK PPA-st edastatud taotlusandmete ehtsuse ja tervikluse automaatsel kontrollimisel.

SK vastutab õige e-posti aadressi määramise eest autentimissertifikaadile keskkonnas eesti.ee. Kui e-posti aadress on kliendile juba määratud, kasutab SK määratud aadressi uuesti. Kui klient on muutnud nime või kui kliendile ei ole eelnevalt aadressi määratud, loob SK uue aadressi vastavalt sertifikaadi profiili [6] punktile 6.1.

PPA laadib sertifikaadid digi-ID-e ja isikustab digi-ID. SK edastab aktiveerimata sertifikaadid Trüb Baltic AS-ile.

4.1.2.3. Mobiil-ID

MO sooritab autentimise vastavalt käesoleva CPS-i punktile 3.2.3.2. Õnnestunud autentimise korral allkirjastab klient MO-ga Mobiil-ID lepingu ja kinnitab teabe õigsust.

MO väljastab QSCD kliendile ning edastab teabe, mis seob kliendi isiklike võtmetega väljastatud QSCD-le, SK-le.

Klient esitab Mobiil-ID sertifikaatide taotluse PPA veebipõhises taotluste esitamise keskkonnas või MO kaudu. PPA sooritab kliendi autentimise vastavalt käesoleva CPS-i punktile 3.2.3.2 ja kontrollib kliendi Mobiil-ID taotlemise kõlblikkust vastavalt ITDS-ile [12]. Positiivse otsuse korral edastab PPA sertifikaatide taotluse SK-le.

Taotlusele vastavad sertifikaadid väljastab SK RA-st edastatud taotlusandmete ehtsuse ja tervikluse automaatsel kontrollimisel.

SK vastutab õige e-posti aadressi määramise eest autentimissertifikaadile keskkonnas eesti.ee. Kui e-posti aadress on kliendile juba määratud, kasutab SK määratud aadressi uuesti. Kui klient on muutnud nime või kui kliendile ei ole eelnevalt aadressi määratud, loob SK uue aadressi vastavalt sertifikaadi profiili [6] punktile 6.1.

SK kasutab isiku tuvastamise andmeid, mille esitab PPA.

Kui klient taotleb uut Mobiil-ID-d, lõpetab PPA kehtiva Mobiil-ID ja väljastab kliendile uue Mobiil-ID.

Klient võib taotleda uut Mobiil-ID-d, kui klient on Mobiil-ID hooletuse tõttu kaotanud. Uue Mobiil-ID taotlust menetletakse vastavalt käesoleva CPS-i punktile

3.2.3.2. Vana Mobiil-ID sertifikaadid tunnistatakse

kehtetuks.

4.2. Sertifikaaditaotluse menetlemine

4.2.1. Identifitseerimis- ja autentimisfunktsioonide sooritamine

4.2.1.1. ID-kaart ja digi-ID

PPA kinnitab kliendi identiteedi ITDS-i [12] 3. peatükis kirjeldatud viisil.

ID-kaardi puhul koostab PPA uue kaardi tellimuse ja edastab selle Trüb Baltic AS-ile.

Digi-ID puhul saadab PPA sertifikaaditaotlused SK-le Trüb Baltic AS-i kaudu.

Trüb Baltic AS edastab ID-kaardi ja digi-ID sertifikaatide taotlused SK-le turvalise sidekanali kaudu.

SK võtab CSR-e vastu ainult Trüb Baltic AS-ilt.

Trüb Baltic AS ja SK kasutavad isiku tuvastamise andmeid, mille esitab PPA.

4.2.1.2. Mobiil-ID

Klient võib taotleda sertifitseerimist järgmisel viisil:

- kui klient taotleb uut Mobiil-ID-d, taotleb klient sertifitseerimist PPA-lt PPA taotluste esitamise veebikeskkonnas või MO kaudu. PPA taotleb kliendi nimel sertifitseerimist SK-s X-tee andmevahetuskihi kaudu.

RA sooritab autentimise vastavalt käesoleva CPS-i punktile 3.2.3.2.

Õnnestunud autentimise korral võib klient taotleda sertifitseerimist, allkirjastades vastava taotluse RA-s.

SK võtab sertifitseerimistaotlusi vastu ainult RA-lt. Mobiil-ID sertifikaatide taotlused sisaldavad selgesõnalist teatist selle kohta, et QSCD kuulub kliendile. RA kinnitab QSCD omandiõigust ja tagab sertifitseerimiseks esitatud avalike võtmete kehtivuse. SK kasutab RA

esitatud identifitseerimisandmeid.

4.2.2. Sertifikaaditaotluste heakskiitmine või tagasilükkamine

4.2.2.1. ID-kaart

ID-kaardi taotluse vastuvõtmise või tagasilükkamise otsustab PPA.

SK keeldub sertifikaadi väljastamisest, kui sertifikaaditaotlus ei vasta kehtivate lepingutega kehtestatud tehnilistele nõuetele. Kui CSR-is sisalduvaid andmeid on vaja muuta, kooskõlastab SK muudatuse PPA-ga.

SK teavitab Trüb Baltic AS-i sertifikaadi väljastamisest keeldumisest.

4.2.2.2. Digi-ID

Digi-ID taotluse vastuvõtmise või tagasilükkamise otsustab PPA.

SK keeldub sertifikaadi väljastamisest, kui sertifikaaditaotlus ei vasta kehtivate lepingutega kehtestatud tehnilistele nõuetele. Kui CSR-is sisalduvaid andmeid on vaja muuta, kooskõlastab SK muudatuse PPA-ga.

SK teavitab Trüb Baltic AS-i sertifikaadi väljastamisest keeldumisest.

4.2.2.3. Mobiil-ID

Mitme sertifikaadi väljastamiseks ühele kliendile piisab ühest otsusest, kui mingil ajahetkel jääb kehtivaks maksimaalselt üks Mobiil-ID. Vaadake käesoleva CPS-i punkte 4.7 ja 4.8.

SK keeldub sertifikaadi väljastamisest, kui sertifikaaditaotlus ei vasta kehtivate lepingutega kehtestatud tehnilistele nõuetele. Kui sertifikaaditaotluses sisalduvaid andmeid on vaja muuta, kooskõlastab SK vastava muudatuse RA-ga.

SK teavitab sertifitseerimist taotlenud üksust sertifikaadi väljastamisest keeldumisest.

4.2.3. Sertifikaaditaotluste menetlemise aeg

Vaadake CP [7] punkti 4.2.3, digi-ID CP-d [8] ja Mobiil-ID CP-d [9].

4.3. Sertifikaadi väljastamine

4.3.1. CA tegevused sertifikaadi väljastamisel

4.3.1.1. ID-kaart ja digi-ID

SK väljastab pärast Trüb Baltic AS-i poolt edastatud sertifikaaditaotluse ehtsuse ja tervikluse kontrolli automaatselt vastavad sertifikaadid ja eraldab kliendile keskkonnas eesti.ee õige ning unikaalse e-posti aadressi ID-kaardile Trüb Baltic AS-is või digi-ID-le PPA-s.

Kõik sertifikaadid on aktiveerimata olekus, mis tähendab, et OCSP teenus ei kinnita nende kehtivust ja sertifikaadid ei ole kataloogiteenuse kaudu kättesaadavad. Aktiveerimata sertifikaate hoitakse SK eraandmebaasis. Sertifikaadid aktiveeritakse alles pärast seda, kui klient on need vastu võtnud.

4.3.1.2. Mobiil-ID

SK väljastab pärast RA poolt edastatud sertifikaaditaotluse ehtsuse ja tervikluse kontrolli automaatselt vastavad sertifikaadid ja määrab keskkonnas
eesti.ee õige ning unikaalse e-posti aadressi.

4.3.2. Kliendi teavitamine sertifikaadi väljastamisest CA poolt

4.3.2.1. ID-kaart ja digi-ID

PPA teavitab klienti ID-kaardi või digi-ID väljastamisest, millele on eelnevalt laaditud sertifikaadid. ID-kaart ja digi-ID väljastatakse kliendile PPA klienditeeninduspunktis ning ID-kaardi või digi-ID PIN-koode sisaldav turvaümbrik antakse üle kliendile.

4.3.2.2. Mobiil-ID

PPA teavitab klienti Mobiil-ID väljastamisest. SK teavitab RA-d uue sertifikaadi väljastamisest kliendile. RA teavitab klienti uue sertifikaadi väljastamisest.

4.4. Sertifikaadi vastuvõtmine

4.4.1. Käitumine sertifikaadi vastuvõtmisel

4.4.1.1. ID-kaart ja digi-ID

ID-kaardi või digi-ID väljastamise käigus allkirjastab klient ID-kaardi või digi-ID väljastamise faili. Vastav fail sisaldab teavet, et klient on tingimused [15] läbi lugenud ja nendega nõustunud .

Klient kinnitab samuti, et ID-kaart või digi-ID on talle üle antud. PPA klienditeeninduspunkti töötaja edastab sertifikaatide aktiveerimise taotluse SK-le. SK aktiveerib sertifikaadid ID-kaardil ja digi-ID-l kohe.

SK teavitab PPA klienditeeninduspunkti töötajat sertifikaatide aktiveerimisest.

Tingimustega [15] nõustumist ja nende allkirjastamist ning kinnitust, et ID-kaart või digi-ID on kliendile üle antud, loetakse sertifikaadi vastuvõtmiseks.

4.4.1.2. Mobiil-ID

Sertifikaadi vastuvõtmiseks loetakse piisavaks järgmisi tingimusi:

- klient on allkirjastanud PPA-s sertifitseerimistaotluse vastavalt käesoleva CPS-i punktile 4.2.1.2; SK
- on PPA-lt vastava sertifitseerimistaotluse kätte saanud.

4.4.2. Sertifikaadi avaldamine CA poolt

4.4.2.1. ID-kaart ja digi-ID

SK avaldab sertifikaadid kataloogiteenuses aadressil ldap://ldap.sk.ee/ kohe pärast seda, kui klient on need vastu võtnud.

Peatatud kehtivusega ja kehtetuks tunnistatud sertifikaadid kustutatakse kataloogiteenusest.

Sertifikaatide kehtivuse peatatuse lõpetamisel avaldatakse sertifikaadid kataloogiteenuses uuesti. Aegunud sertifikaadid kustutatakse kataloogiteenusest aegumisele järgneval päeval.

4.4.2.2. Mobiil-ID

Sertifikaadid tehakse kättesaadavaks kataloogiteenuses aadressil ldap://ldap.sk.ee/ ja tarkvara DigiDoc Service [18] kaudu pärast seda,

kui SK on sertifikaadid väljastanud. Peatatud kehtivusega ja kehtetuks tunnistatud sertifikaadid kustutatakse kataloogiteenusest.

Sertifikaatide kehtivuse peatatuse lõpetamisel avaldatakse sertifikaadid kataloogiteenuses uuesti. Aegunud sertifikaadid kustutatakse kataloogiteenusest aegumisele järgneval päeval.

4.4.3. Sertifikaadi väljastamisest teatamine CA poolt teistele üksustele

SK annab ID-kaardi ja digi-ID jaoks väljastatud sertifikaadid kohe üle Trüb Baltic AS-ile kaartidele

laadimiseks. SK teavitab telekommunikatsiooniteenuse osutajat väljastatud Mobiil-ID sertifikaatidest.

4.5. Võtmepaar ja sertifikaadi kasutamine

4.5.1. Kliendi isiklik võti ja sertifikaadi kasutamine

Klient on kohustatud kasutama isiklikku võtit ja sertifikaati seaduslikul viisil ning vastavalt järgmisele:

- CP [7], digi-ID CP [8] ja Mobiil-ID CP [9];
- käesolev CPS;
- tingimused [15].

4.5.2. Huvitatud isiku avalik võti ja sertifikaadi kasutamine

Huvitatud isik on kohustatud kasutama kliendi avalikku võtit ja sertifikaati seaduslikul viisil ning vastavalt järgmisele:

- CP [7], digi-ID CP [8] ja Mobiil-ID CP [9];
- käesolev CPS;
- tingimused [15].

4.6. Sertifikaadi uuendamine

ID-kaardi, digi-ID või Mobiil-ID asendust väljastamisel pärast selle aegumist loetakse võtmevahetuseks asjaolu tõttu, et vanu isiklikke võtmeid ei ole võimalik uuele QSCD-le kopeerida.

4.7. Sertifikaadi võtmevahetus

Kui klient taotleb korduvat ID-kaarti, digi-ID-d või Mobiil-ID-d, menetletakse taotlust uue ID-kaardi, digi-ID või Mobiil-ID taotlusena.

Mobiil-ID ja kiipkaartide puhul on võtmevahetuse kord ning tingimused tehnilistel põhjustel teistsugused.

Võtmevahetuse käigus tunnistatakse kõik vigased või kasutamiskõlbmatud sertifikaadid kohe kehtetuks.

4.7.1. Sertifikaadi võtmevahetuse asjaolud

4.7.1.1. ID-kaart ja digi-ID

Sertifikaadi võtmevahetus on lubatud järgmiseks:

- aegunud või rikkis ID-kaardi või digi-ID asendamine;
- tootmisvigade parandamine;
- sertifikaatide ASN.1 kodeerimisvigade parandamine;
- SHA-1 allkirjade asendamine tugevama krüptograafiaga.

Sertifikaadi võtmevahetus tootmisvigade parandamiseks toimub ID-kaardi või digi-ID esialgsel taotlemisel. Sellisel juhul kirjutatakse kaardi või digi-ID andmekandjale ainult viimased sertifikaadid, mis jäävad kehtivaks.

Sertifikaadi võtmevahetust sertifikaatide ASN.1 kodeerimisvigade parandamiseks või SHA-1 allkirjade asendamiseks tugevama krüptograafiaga võib taotleda järgmiselt:

- vastavas avaliku andmesidevõrgu rakenduses ainult juhul, kui ID-kaardi või digi-ID isikutuvastamist võimaldav sertifikaat on kehtiv ja aktiivses olekus, ning PPA klienditeeninduspunktis.

Sertifikaadi võtmevahetust sertifikaatide ASN.1 kodeerimisvigade parandamiseks või SHA-1 allkirjade asendamiseks tugevama krüptograafiaga võib taotleda PPA klienditeeninduspunktis juhul kui:

- sertifikaadi võtmevahetuse ebaõnnestumisega avaliku andmesidevõrgu rakenduses on kaasnenud sertifikaatide kehtetuks tunnistamine;
- sertifikaatide kehtivus on peatatud;
- Autentimissertifikaadi (PIN1) aktiveerimiskood on blokeeritud;
- sertifikaadid on aktiveerimata olekus.

Kui klient on taotlenud sertifikaatide kehtetuks tunnistamist, ei ole sertifikaadi võtmevahetus sertifikaatide ASN.1 kodeerimisvigade parandamiseks või SHA-1 allkirjade asendamiseks võimalik.

4.7.1.2. Mobiil-ID

Sertifikaadi võtmevahetus on lubatud ainult juhul, kui on vaja asendada QSCD.

4.7.2. Kes võib uue avaliku võtme sertifitseerimist taotleda

4.7.2.1. ID-kaart ja digi-ID

Sertifikaadi võtmevahetuse protsessi ID-kaardi tootmisvigade parandamiseks saab algatada ainult Trüb Baltic AS.

Sertifikaadi võtmevahetuse protsessi digi-ID tootmisvigade parandamiseks saab algatada ainult PPA.

Sertifikaadi võtmevahetuse protsessi sertifikaatide ASN.1 kodeerimisvigade parandamiseks või SHA-1 allkirjade asendamiseks tugevama krüptograafiaga saab algatada ainult klient.

Kõik sertifikaaditaotlused antakse SK-le üle Trüb Baltic AS-i kaudu.

4.7.2.2. Mobiil-ID

Sertifikaadi võtmevahetuse protsessi saab algatada ainult klient.

Kõik sertifikaaditaotlused antakse SK-le üle MO kaudu.

4.7.3. Sertifikaadi võtmevahetuse taotluste menetlemine

4.7.3.1. ID-kaart ja digi-ID

Pärast seda, kui Trüb Baltic AS on avastanud kvaliteedikontrolli käigus ID-kaardi tootmisvead, esitab Trüb Baltic AS SK-le uue CSR-i.

Pärast seda, kui PPA on avastanud kvaliteedikontrolli käigus digi-ID tootmisvead, esitab PPA SK-le Trüb Baltic AS-i kaudu uue CSR-i.

Kui kordustaotluses ei ole muudetud andmeid, edastatakse uuesti juba väljastatud sertifikaat. Ülejäänud protsess on sarnane esialgse ID-kaardi või digi-ID väljastamisega.

Sertifikaadi võtmevahetuse protsess avaliku andmesidevõrgu rakenduse abil on järgmine:

- klient tuvastatakse ID-kaardi kehtiva autentimissertifikaadi abil;
- klient kinnitab, et on tingimused [15] läbi lugenud ja nendega nõustunud ; sooritatakse
- sertifikaadi võtmevahetus;
- klienti teavitatakse uue sertifikaadi väljastamisest sama rakenduse kaudu. Sertifikaadi

võtmevahetuse protsess PPA klienditeeninduspunktis on järgmine:

- PPA klienditeeninduspunkti töötaja tuvastab kliendi;
- klient allkirjastab PIN- ja PUK-koodide asendamise taotluse ning kinnitab, et on tingimused [15]läbi lugenud ja nendega nõustunud
- [4; sooritatakse sertifikaadi võtmevahetus;
- klienti teavitab uue sertifikaadi väljastamisest PPA klienditeeninduspunkti töötaja.

Väljastatud sertifikaatide kehtivusaeg ei ületa alusdokumendi kehtivusaega. SK tunnistab asendatud

sertifikaadid kohe kehtetuks.

4.7.3.2. Mobiil-ID

Klient võib taotleda uut Mobiil-ID-d, kui klient on Mobiil-ID hooletuse tõttu kaotanud. Uue Mobiil-ID taotlust menetletakse vastavalt käesoleva CPS-i punktile 3.2.3.2.

MO sooritab autentimise vastavalt käesoleva CPS-i punktile 3.2.3.2. Õnnestunud autentimise korral allkirjastab klient MO-ga elektrooniliselt lepingu ja kinnitab teabe õigsust.

MO väljastab kliendile uue QSCD ning edastab SK-le teabe, mis seob kliendi isiklike võtmetega väljastatud QSCD-le ning vastavate avalike võtmetega.
SK kasutab vastavaid avalikke võtmeid sertifitseerimiseks.

MO edastab sertifikaatide taotluse, mille klient on elektrooniliselt allkirjastanud, turvalise sidekanali kaudu SK-le. SK kontrollib elektrooniliselt kliendi identiteedi ja kinnitab kliendi elektroonilise allkirja.

Positiivse otsuse korral allkirjastab SK registreeritud avalikud võtmed ja väljastab kehtiva Mobiil-ID jaoks uued sertifikaadid ning teavitab PPA-d uute sertifikaatide väljastamisest.

Väljastatud sertifikaatide kehtivusaeg ei ületa alusdokumendi kehtivusaega.

MO esitab SK-le sertifikaatide kehtetuks tunnistamise taotluse. SK tunnistab sertifikaadid kohe kehtetuks ja teavitab seejärel sertifikaatide kehtetuks tunnistamisest PPA-d.

4.7.4. Kliendi teavitamine uue sertifikaadi väljastamisest

4.7.4.1. ID-kaart ja digi-ID

Kui sertifikaadi võtmevahetus toimub tootmisvigade parandamiseks või aegunud või rikkis ID-kaardi või digi-ID asendamiseks, on kliendi teavitamine sarnane esialgse teavitamisega vastavalt käesoleva CPS-i punktile 4.3.2.1.

Kui sertifikaadi võtmevahetus sertifikaatide ASN.1 kodeerimisvigade parandamiseks või SHA-1 allkirjade asendamiseks toimub avaliku andmesidevõrgu rakenduses, teavitatakse klienti uue sertifikaadi väljastamisest rakenduse kaudu kohe pärast sertifikaadi väljastamist.

Kui sertifikaadi võtmevahetus sertifikaatide ASN.1 kodeerimisvigade parandamiseks või SHA-1 allkirjade asendamiseks toimub PPA klienditeeninduspunktis, teavitab klienti uue sertifikaadi väljastamisest PPA klienditeeninduspunkti töötaja.

4.7.4.2. Mobiil-ID

SK teavitab MO-d uue sertifikaadi väljastamisest kliendile. MO

teavitab klienti uue sertifikaadi väljastamisest.

4.7.5. Käitumine uue võtmega sertifikaadi vastuvõtmisel

4.7.5.1. ID-kaart ja digi-ID

Kui sertifikaadi võtmevahetus toimub tootmisvigade parandamiseks või aegunud või rikkis ID-kaardi või digi-ID asendamiseks, kinnitab klient, et ta on lugenud läbi ja nõustunud tingimustega [15], mis on esitatud käesoleva CPS-i punktis 4.4.1.1.

Kui sertifikaadi võtmevahetus toimub avaliku andmesidevõrgu rakenduses, teavitatakse klienti uue sertifikaadi väljastamisest rakenduse kaudu. Rakenduse kaudu teavitamist loetakse uue võtmega sertifikaadi vastuvõtuks.

Kui sertifikaadi võtmevahetus toimub PPA klienditeeninduspunktis, teavitab klienti uue sertifikaadi väljastamisest PPA klienditeeninduspunkti töötaja. Teavitamist PPA klienditeeninduspunkti töötaja poolt loetakse uue võtmega sertifikaadi vastuvõtmiseks.

4.7.5.2. Mobiil-ID

Kui klient taotleb QSCD asendamist (sertifikaadi võtmevahetust), loetakse sertifikaadi vastuvõtmiseks piisavaks järgmisi tingimusi:

- klient on allkirjastanud MO juures sertifitseerimistaotluse vastavalt käesoleva CPS-i punktile
- 4.2.1.2; SK on MO-lt vastava sertifitseerimistaotluse kätte saanud.

SK väljastab sertifikaadid ja teavitab RA-d uue sertifikaadi väljastamisest kliendile. RA teavitab klienti uue sertifikaadi väljastamisest ja vastavat teavitamist loetakse sertifikaadi vastuvõtmiseks.

4.7.6. Uue võtmega sertifikaadi avaldamine CA poolt

Vaadake käesoleva CPS-i punkti 4.4.2.

4.7.7. Sertifikaadi väljastamisest teatamine CA poolt teistele üksustele

Vaadake käesoleva CPS-i punkti 4.4.3.

4.8. Sertifikaadi muutmine

Kui muutmine nõuab alusdokumendi asendust (nt visuaalselt ID-kaardile jäädvustatud andmete muutmist), käsitatakse seda uue taotlusena.

Mobiil-ID ja kiipkaartide puhul on muutmise kord ning tingimused tehnilistel põhjustel teistsugused. Muutmise

käigus tunnistatakse kõik vigased või kasutamiskõlbmatud sertifikaadid kohe kehtetuks.

Viimati väljastatud sertifikaatide kehtivusaeg ei ületa alusdokumendi kehtivusaega.

4.8.1. Sertifikaadi muutmise asjaolud

4.8.1.1. ID-kaart ja digi-ID

Sertifikaadi muutmine on lubatud järgmiseks:

- visuaalselt ID-kaardile või digi-ID-le jäädvustatud ning isikuandmete faili salvestatud andmete
- muutmine, kvaliteedikontrolli käigus avastatud tootmisvigade parandamine;
- e-posti aadresside muutmine, mis on kirjutatud autentimissertifikaadi subjekti lisanime väljale;
- sertifikaatide ASN.1 kodeerimisvigade parandamine;
- SHA-1 allkirjade asendamine tugevama krüptograafiaga.

Sertifikaadi muutmine kvaliteedikontrolli käigus avastatud tootmisvigade parandamiseks toimub ID-kaardi või digi-ID esialgsel taotlemisel. Sellisel juhul kirjutatakse kaardile või digi-ID andmekandjale ainult viimased sertifikaadid, mis jäävad kehtivaks.

Sertifikaadi muutmist võib taotleda e-posti aadresside muutmiseks, mis on kirjutatud autentimissertifikaadi subjekti lisanime väljale, või sertifikaatide ASN.1 kodeerimisvigade parandamiseks või SHA-1 allkirjade asendamiseks tugevama krüptograafiaga:

- avalikus andmesidevõrgus, kui ID-kaardi või digi-ID isikutuvastamist võimaldav sertifikaat on kehtiv ja aktiivses
- olekus, või PPA klienditeeninduspunktis.

4.8.1.2. Mobiil-ID

Sertifikaadi muutmine on lubatud järgmistel asjaoludel:

- e-posti aadresside muutmine, mis on kirjutatud isikutuvastamist võimaldavate sertifikaatide subjekti lisanime väljale;
- sertifikaatide ASN.1 kodeerimisvigade parandamine;
- SHA-1 allkirjade asendamine tugevama krüptograafiaga.

4.8.2. Kes võib sertifikaadi muutmist taotleda

4.8.2.1. ID-kaart ja digi-ID

Sertifikaadi muutmise ID-kaardi tootmisvigade parandamiseks saab algatada ainult Trüb Baltic AS.

Sertifikaadi muutmise digi-ID tootmisvigade parandamiseks saab algatada ainult PPA.

Sertifikaadi muutmise e-posti aadresside muutmiseks, mis on kirjutatud isikutuvastamist võimaldavate sertifikaatide subjekti lisanime väljale, või sertifikaatide ASN.1 kodeerimisvigade parandamiseks või SHA-1 allkirjade asendamiseks tugevama krüptograafiaga võib algatada ainult klient.

Kõik sertifikaaditaotlused antakse SK-le üle Trüb Baltic AS-i kaudu.

4.8.2.2. Mobiil-ID

Sertifikaadi muutmise saab algatada ainult SK.

4.8.3. Sertifikaadi muutmise taotluste menetlemine

4.8.3.1. ID-kaart ja digi-ID

Vaadake käesoleva CPS-i punkti 4.7.3.1.

4.8.3.2. Mobiil-ID

SK menetleb sertifikaadi muutmise taotlusi ega ole kohustatud seda kliendiga kooskõlastama.

4.8.4. Kliendi teavitamine uue sertifikaadi väljastamisest

SK teavitab klienti uue sertifikaadi väljastamisest.

4.8.5. Käitumine muudetud sertifikaadi vastuvõtmisel

Vaadake käesoleva CPS-i punkti 4.7.5.

4.8.6. Muudetud sertifikaadi avaldamine CA poolt

Vaadake käesoleva CPS-i punkti 4.7.6.

4.8.7. Sertifikaadi väljastamisest teatamine CA poolt teistele üksustele

Vaadake käesoleva CPS-i punkti 4.7.7.

4.9. Sertifikaadi kehtetuks tunnistamine ja kehtivuse peatamine

4.9.1. Kehtetuks tunnistamise asjaolud

Vaadake CP [7] punkti 4.9.1, digi-ID CP-d [8] ja Mobiil-ID CP-d [9].

4.9.2. Kes võib kehtetuks tunnistamist taotleda

4.9.2.1. ID-kaart ja digi-ID

ID-kaardi või digi-ID sertifikaadi kehtetuks tunnistamise taotluse võib PPA esitada vastavalt ITDS-ile [12].

Sertifikaadi kehtetuks tunnistamise taotluse võib esitada klient või kolmas isik.

4.9.2.2. Mobiil-ID

Mobiil-ID sertifikaadi kehtetuks tunnistamise taotluse võib PPA esitada vastavalt ITDS-ile [12].

MO võib esitada sertifikaadi kehtetuks tunnistamise taotluse kliendi nimel.

Sertifikaadi kehtetuks tunnistamise taotluse võib esitada klient või kolmas isik.

4.9.3. Sertifikaadi kehtetuks tunnistamise taotlemise kord

4.9.3.1. ID-kaart ja digi-ID

Sertifikaatide kehtetuks tunnistamisel lähtutakse ITDS-iga [12] reguleeritud isikut tõendava dokumendi kehtetuks tunnistamise sätetest ja korrast.

Klient esitab allkirjastatud kehtetuks tunnistamise taotluse SK-le PPA või SK klienditeeninduspunkti kaudu. Kehtetuks tunnistamise taotluse registreerib PPA või SK klienditeeninduspunkti töötaja.

PPA või SK klienditeeninduspunkti töötaja kontrollib kehtetuks tunnistamise taotluse esitavat isikut vastavalt sisemisele identiteedi kontrolli korrale ja tuvastab kehtetuks tunnistamise taotluse õiguspärasuse.

PPA või SK klienditeeninduspunkti töötaja edastab kehtetuks tunnistamise taotluse SK-le turvalise sidekanali kaudu.

Pärast seda, kui SK on kehtetuks tunnistamise taotluse kätte saanud, on taotluse menetlemise kord järgmine:

- kehtetuks tunnistamise taotluse CP-le [7] või digi-ID CP-le [8] vastavuse kontrollimine;
- SK tunnistab sertifikaadi kehtetuks;
- sertifikaat eemaldatakse kohe kataloogiteenusest ja OCSP lakkab vastamast olekuga „HEA“;
- uus CRL avaldatakse vastavalt käesoleva CPS-i punktile 4.9.7;
- kehtetuks tunnistamise taotluse aluseks olnud dokumentatsioon arhiveeritakse;
- klienti teavitatakse sertifikaadi kehtetuks tunnistamisest.

Pärast seda, kui SK on kehtetuks tunnistamise taotluse kätte saanud, menetleb SK seda kohe.

Sertifikaadi kehtetuks tunnistamine dokumenteeritakse SK sertifikaatide andmebaasis. Kliendil on võimalus kontrollida sertifikaadi kehtetuks tunnistamist kataloogiteenuse, CRL-i või OCSP põhjal.

Kehtetuks tunnistatud sertifikaati ei ole võimalik ennistada.

4.9.3.2. Mobiil-ID

Sertifikaatide kehtetuks tunnistamisel lähtutakse ITDS-iga [12] reguleeritud isikut tõendava dokumendi kehtetuks tunnistamise sätetest ja korrast.

Kliendil on võimalik taotleda sertifikaatide kehtetuks tunnistamist, esitades elektrooniliselt allkirjastatud taotluse PPA taotluse esitamise veebikeskkonnas. Sertifikaatide kehtetuks tunnistamise allkirjastatud taotluse saab esitada ka MO klienditeeninduspunktis.

Kehtetuks tunnistamise taotluse edastab SK-le PPA X-tee andmevahetuskihi kaudu ja MO klienditeeninduspunkti töötaja turvalise sidekanali kaudu.

Kui klient taotleb sertifikaadi kehtetuks tunnistamist PPA veebikeskkonnas, kontrollib PPA kliendi identiteeti vastavalt ID-kaardi või digi-ID-ga seotud isikutuvastamist võimaldavale sertifikaadile.

Kui klient esitab kehtetuks tunnistamise taotluse MO klienditeeninduspunktis, registreerib kehtetuks tunnistamise taotluse MO klienditeeninduspunkti töötaja. MO klienditeeninduspunkti töötaja kontrollib kehtetuks tunnistamise taotluse esitavat isikut vastavalt sisemisele identiteedi kontrolli korrale ja tuvastab kehtetuks tunnistamise taotluse õiguspärasuse.

Pärast seda, kui SK saab kas PPA või MO klienditeeninduspunktilt kehtetuks tunnistamise taotluse, menetletakse taotlust järgmise automaatse korra alusel:

- kontrollitakse kehtetuks tunnistamise taotluse vastavust Mobiil-ID CP-le [9];
- SK tunnistab sertifikaadi kehtetuks;
- sertifikaat eemaldatakse kohe kataloogiteenusest ja OCSP lakkab vastamast olekuga „HEA“;
- uus CRL avaldatakse vastavalt käesoleva CPS-i punktile 4.9.7;
- kehtetuks tunnistamise taotluse aluseks olnud dokumentatsioon arhiveeritakse;
- klienti teavitatakse sertifikaadi kehtetuks tunnistamisest.

Pärast seda, kui SK on kehtetuks tunnistamise taotluse kätte saanud, menetleb SK seda kohe.

Kui kehtetuks tunnistamise taotluse esitab kolmas isik, algatab protseduuri SK käsitsi. SK arhiveerib dokumentatsiooni, mille alusel kolmas isik kehtetuks tunnistamise taotluse esitas, käsitsi.

Sertifikaadi kehtetuks tunnistamine dokumenteeritakse SK sertifikaatide andmebaasis. Kliendil on võimalus kontrollida sertifikaadi kehtetuks tunnistamist kataloogiteenuse, CRL-i või OCSP põhjal.

Sertifikaadi kehtetuks tunnistamist kohaldatakse ainult sertifikaadipaaridele.

Kui sertifikaadipaari üks sertifikaat tunnistatakse kehtetuks, tunnistatakse kehtetuks terve sertifikaadipaar. Muud sertifikaadipaarid

võivad jääda kehtivaks. Mobiil-ID kehtetuks tunnistamise korral tunnistatakse kehtetuks kõik seotud sertifikaadipaarid.

Kehtetuks tunnistatud sertifikaate ei ole võimalik ennistada.

4.9.4. Kehtetuks tunnistamise taotlemise ajapikendus

4.9.4.1. ID-kaart ja digi-ID

Klient on kohustatud taotlema kehtetuks tunnistamist kohe pärast ID-kaardi või digi-ID kaotamise või varguse tuvastamist või selle muul põhjusel kasutuskõlbmatuks muutumist.

4.9.4.2. Mobiil-ID

Klient on kohustatud taotlema kehtetuks tunnistamist kohe pärast seadme kaotamises või varguses veendumist.

4.9.5. Aeg, mille jooksul CA peab kehtetuks tunnistamise taotlemist menetlema

Pärast seda, kui PPA või MO on edastanud kehtetuks tunnistamise taotluse SK-le, menetleb SK kehtetuks tunnistamise taotlust kohe.

SK menetleb kolmanda isiku kehtetuks tunnistamise taotlust kohe pärast vastava taotluse õigsuse ja täielikkuse ning taotleja kehtetuks tunnistamise taotlemise volituste kontrollimist.

4.9.6. Kehtetuks tunnistamise kontrollimise nõuded huvitatud isikutele

Mehhanismid, mida huvitatud isikul on võimalik soovitud sertifikaatide oleku kontrollimiseks kasutada, on sätestatud tingimustes [15].

4.9.7. CRL-i väljastamise sagedus

CRL-i välja nextUpdate väärtuseks seatakse pärast CRL-i väljastamist 12 tundi.

4.9.8. CRL-ide maksimaalne latentsusaeg

SK jälgib SK veebilehel avaldatud CRL-i aegumise tähtaega. Kui uut CRL-i ei avaldata 120 minutit enne eelmise aegumist, edastatakse alarm.

4.9.9. Kehtetuks tunnistamise / oleku kontrollimise kättesaadavus veebis

OCSP teenus on tasuta ja avalikult kättesaadav.

OCSP teenus on sertifikaadi oleku peamine teabeallikas.

4.9.10. Kehtetuks tunnistamise veebis kontrollimise nõuded

Mehhanismid, mida huvitatud isikul on võimalik soovitud sertifikaadi oleku kontrollimiseks kasutada, on sätestatud tingimustes [15].

4.9.11. Kehtetuks tunnistamise teadete muud kättesaadavad vormid

SK pakub lepingu ja hinnakirja kohaselt OCSP teenust parema SLA-ga.

4.9.12. Võtme ohtu sattumisega seotud erinõuded

Ei kohaldata.

4.9.13. Kehtivuse peatamise asjaolud

Vaadake CP [7] punkti 4.9.13, digi-ID CP-d [8] ja Mobiil-ID CP-d [9].

4.9.14. Kes võib kehtivuse peatamist taotleda

Sertifikaadi kehtivuse peatamist võivad taotleda kõik.

4.9.15. Kehtivuse peatamise taotlemise kord

4.9.15.1. ID-kaart ja digi-ID

Kehtivuse peatamise taotluse registreerib abiliini operaator või kehtivuse peatamise registreerib PPA või SK klienditeeninduspunkti töötaja.

Abiliini kaudu esitatud kehtivuse peatamise taotlus dokumenteeritakse. Kehtivuse peatamist taotlevat isikut ja kehtivuse peatamise taotlust kontrollitakse abiliini operaatori professionaalsete oskuste abil.

Teise võimalusena esitab isik allkirjastatud kehtivuse peatamise taotluse PPA või SK klienditeeninduspunkti töötajale. PPA või SK klienditeeninduspunkti töötaja kontrollib kehtivuse peatamise taotluse esitavat isikut vastavalt sisemisele identiteedi kontrolli korrale ja tuvastab kehtivuse peatamise taotluse õiguspärasuse.

Abiliini, PPA või SK klienditeeninduspunkti töötaja edastab kehtivuse peatamise taotluse SK-le turvalise sidekanali kaudu.

Pärast seda, kui SK on ID-kaardi või digi-ID sertifikaadi kehtivuse peatamise taotluse kätte saanud, on taotluse menetlemise kord järgmine:

- sertifikaadi kehtivuse peatamise taotluse CP-le [7] või digi-ID CP-le [8] vastavuse kontrollimine;
- kehtivuse peatamise taotluse registreerimine SK infosüsteemis;
- SK peatab sertifikaadi kehtivuse;
- sertifikaatide andmebaasis tehakse sertifikaadile märge, et selle kehtivus on peatatud;
- sertifikaat eemaldatakse kohe kataloogiteenusest ja OCSP lakkab vastamast olekuga „HEA“;
- uus CRL avaldatakse vastavalt käesoleva CPS-i punktile 4.9.7;
- kehtivuse peatamise taotluse aluseks olnud dokumentatsioon arhiveeritakse.

Pärast seda, kui SK on kehtivuse peatamise taotluse kätte saanud, menetleb SK seda

kohe.

Abiliini kaudu esitatud sertifikaadi kehtivuse peatamise taotluse korral teavitatakse klienti sertifikaadi kehtivuse õnnestunud peatamisest kohe pärast kehtivuse peatamise lõpetamist. Kliendil on võimalus kontrollida sertifikaadi kehtivuse peatatust kataloogiteenuse, CRL-i või OCSP põhjal.

Klient saab taotleda sertifikaatide kehtivuse peatamist abiliini kaudu 7 päeva nädalas ööpäev läbi.

4.9.15.2. Mobiil-ID

Klient võib esitada elektrooniliselt allkirjastatud taotluse sertifikaatide kehtivuse peatamiseks SK klienditeeninduspunktile. Pärast seda, kui SK on sertifikaatide kehtivuse peatamise taotluse kätte saanud, on taotluse menetlemise kord järgmine:

- kehtivuse peatamise taotluse registreerib SK klienditeeninduspunkti töötaja;
- SK klienditeeninduspunkti töötaja kinnitab kehtivuse peatamise taotluse esitava isiku elektroonilise allkirja;
- SK klienditeeninduspunkti töötaja kontrollib kehtivuse peatamise taotluse õiguspärasust;
- kontrollitakse sertifikaadi kehtivuse peatamise taotluse vastavust Mobiil-ID CP-le [9];
- sertifikaatide andmebaasis tehakse sertifikaadile märge, et selle kehtivus on peatatud;
- sertifikaat eemaldatakse kohe kataloogiteenusest ja DigiDoc Service [18] lakkab vastamast olekuga „KEHTIV“ ja OCSP lakkab vastamast olekuga „HEA“;
- uus CRL avaldatakse vastavalt käesoleva CPS-i punktile 4.9.7;
- kehtivuse peatamise taotluse aluseks olnud dokumentatsioon arhiveeritakse;
- klienti teavitatakse sertifikaadi kehtivuse peatamisest.

Pärast seda, kui SK on kehtivuse peatamise taotluse kätte saanud, menetleb SK seda kohe.

Kliendil on võimalus kontrollida sertifikaadi kehtivuse peatatust kataloogiteenuse, DigiDoc Service [18], CRL-i või OCSP põhjal.

Sertifikaadi kehtivuse peatamist kohaldatakse ainult sertifikaadipaaridele.

Kui sertifikaadipaari ühe sertifikaadi kehtivus peatatakse, peatatakse terve sertifikaadipaari kehtivus. Muud sertifikaadipaarid võivad jääda

kehtivaks. Klient võib taotleda telekommunikatsiooniteenuse peatamist telekommunikatsiooniteenuse osutaja abiliini kaudu 7 päeva nädalas

ööpäev läbi.
Telekommunikatsiooniteenuse osutaja abiliini operaator kontrollib klienti, küsides kliendilt tema salasõna või esitades kontrollküsimusi kliendi isiklike üksikasjade kohta (nt nimi, isikukood, aadress).

Teise võimalusena võib klient taotleda telekommunikatsiooniteenuse peatamist, esitades taotluse telekommunikatsiooniteenuse osutajale. Telekommunikatsiooniteenuse osutaja töötaja kontrollib klienti vastavalt sisemisele isikusamasuse kontrolli korrale.

Telekommunikatsiooniteenuse peatamisega võib kaasneda järgmine:

- Mobiil-ID sertifikaatide kehtetuks
- tunnistamine või Mobiil-ID kasutamise võimatus.

Telekommunikatsiooniteenuse peatamisega ei kaasne automaatselt sertifikaatide kehtetuks tunnistamine, klient on kohustatud taotlema kehtetuks tunnistamist, kui ta on veendunud, et tema seade on kadunud või varastatud. Vastasel juhul jäävad sertifikaadid kehtivaks, kuid Mobiil-ID kasutamine blokeeritakse.

Kui klient taotleb Mobiil-ID sertifikaatide kehtetuks tunnistamist, menetletakse taotlust vastavalt käesoleva CPS-i punktile 4.9.3.2.

4.9.16. Kehtivuse peatamise aja piirid

Kehtivuse peatamise aeg ei ole piiratud.

4.9.17. Kehtivuse peatatuse lõpetamise asjaolud

Vaadake CP [7], punkti 4.9.17, digi-ID CP-d [8] ja Mobiil-ID CP-d [9].

4.9.18. Kes võib kehtivuse peatatuse lõpetamist taotleda

4.9.18.1. ID-kaart ja digi-ID

Vaadake CP [7] punkti 4.9.18.

4.9.18.2. Mobiil-ID

Vaadake Mobiil-ID CP [9] punkti 4.9.18.

4.9.19. Kehtivuse peatatuse lõpetamise kord

4.9.19.1. ID-kaart ja digi-ID

Isik esitab allkirjastatud kehtivuse peatatuse lõpetamise taotluse PPA või SK klienditeeninduspunkti töötajale. Kehtivuse peatatuse lõpetamise taotluse registreerib PPA või SK klienditeeninduspunkti töötaja.

PPA või SK klienditeeninduspunkti töötaja kontrollib kehtivuse peatatuse lõpetamise taotluse esitavat isikut vastavalt sisemisele identiteedi kontrolli korrale ja tuvastab kehtivuse peatatuse lõpetamise taotluse õiguspärasuse.

PPA või SK klienditeeninduspunkti töötaja edastab kehtivuse peatatuse lõpetamise taotluse turvalise sidekanali kaudu SK-le.

Pärast seda, kui SK on ID-kaardi või digi-ID sertifikaadi kehtivuse peatatuse lõpetamise taotluse kätte saanud, on taotluse menetlemise kord järgmine:

- sertifikaadi kehtivuse peatatuse lõpetamise taotluse CP-le [7] või digi-ID CP-le [8] vastavuse kontrollimine;
- kehtivuse peatatuse lõpetamise taotluse registreerimine SK infosüsteemis;
- SK lõpetab sertifikaadi kehtivuse peatatuse;
- pärast sertifikaadi kehtivuse peatatuse lõpetamist avaldatakse see kataloogiteenuses kohe uuesti ja OCSP hakkab vastama olekuga „HEA“;
- uus CRL avaldatakse vastavalt käesoleva CPS-i punktile 4.9.7;
- kehtivuse peatatuse lõpetamise taotluse aluseks olnud dokumentatsioon arhiveeritakse. Pärast

seda, kui SK on kehtivuse peatatuse lõpetamise taotluse kätte saanud, menetleb SK seda kohe.

Klienti teavitatakse sertifikaadi kehtivuse peatatuse lõpetamise õnnestunud läbiviimisest kohe. Kliendil on võimalus veenduda kataloogiteenuse, järgmise CRL-i või OCSP põhjal, et sertifikaadi kehtivuse peatatus on lõpetatud.

4.9.19.2. Mobiil-ID

Klient võib taotleda sertifikaatide kehtivuse peatatuse lõpetamist, esitades SK klienditeeninduspunktile elektrooniliselt allkirjastatud taotluse. Pärast seda, kui SK on kehtivuse peatatuse lõpetamise taotluse kätte saanud, on taotluse menetlemise kord järgmine:

- kehtivuse peatatuse lõpetamise taotluse registreerib SK klienditeeninduspunkti töötaja;
- SK klienditeeninduspunkti töötaja kinnitab kehtivuse peatatuse lõpetamise taotluse esitava isiku elektroonilise allkirja;

- SK klienditeeninduspunkti töötaja kontrollib kehtivuse peatatuse lõpetamise taotluse õiguspärasust;
- kontrollitakse sertifikaadi kehtivuse peatatuse lõpetamise taotluse vastavust Mobiil-ID CP-le [9];
- kehtivuse peatatuse lõpetamise taotluse registreerimine SK infosüsteemis;
- SK lõpetab sertifikaadi kehtivuse peatatuse;
- pärast sertifikaadi kehtivuse peatatuse lõpetamist avaldatakse see kataloogiteenuses kohe uuesti, DigiDoc Service [18] hakkab vastama olekuga „KEHTIV“ ja OCSP olekuga „HEA“;
- uus CRL avaldatakse vastavalt käesoleva CPS-i punktile 4.9.7;
- kehtivuse peatatuse lõpetamise taotluse aluseks olnud dokumentatsioon arhiveeritakse.

Pärast seda, kui SK on kehtivuse peatatuse lõpetamise taotluse kätte saanud, menetleb SK seda kohe.

Klient võib taotleda ka sertifikaatide kehtivuse peatatuse lõpetamist, esitades MO klienditeeninduspunktile elektrooniliselt allkirjastatud taotluse. Pärast seda, kui MO klienditeeninduspunkt on kehtivuse peatatuse lõpetamise taotluse kätte saanud, on taotluse menetlemise kord järgmine:

- taotluse registreerib MO klienditeeninduspunkti töötaja;
- MO klienditeeninduspunkti töötaja kinnitab kehtivuse peatatuse lõpetamise taotluse esitava isiku elektroonilise allkirja;

- MO klienditeeninduspunkti töötaja kontrollib kehtivuse peatatuse lõpetamise taotluse õiguspärasust;
- sertifikaadi kehtivuse peatatuse lõpetab MO infosüsteemis MO klienditeeninduspunkti töötaja; MO infosüsteem
- teavitab SK-d kohe kehtivuse peatatuse lõpetamisest;
- SK kinnitab kehtivuse peatatuse lõpetamist ja avaldab sertifikaadi kohe kataloogiteenuses uuesti, DigiDoc Service [18] hakkab vastama olekuga „KEHTIV“ ja OCSP olekuga „HEA“;
- uus CRL avaldatakse vastavalt käesoleva CPS-i punktile 4.9.7;

Sertifikaadi omanikku teavitatakse sertifikaadi kehtivuse peatatuse lõpetamise õnnestunud läbiviimisest kohe. Kliendil on võimalus veenduda kataloogiteenuse, tarkvara DigiDoc Service [18], järgmise CRL-i või OCSP põhjal, et sertifikaadi kehtivuse peatatus on lõpetatud.

Kehtivuse peatatuse lõpetamist kohaldatakse ainult sertifikaadipaaridele.

Kui sertifikaadipaari ühe sertifikaadi kehtivuse peatatus lõpetatakse, lõpetatakse terve sertifikaadipaari kehtivuse peatatus.

Kui klient on taotlenud telekommunikatsiooniteenuse peatamist käesoleva CPS-i punktis 4.9.15.2 kirjeldatud viisil, võib klient taotleda telekommunikatsiooniteenuse osutajalt telekommunikatsiooniteenuse taastamist. Telekommunikatsiooniteenuse taastamine võimaldab kasutada Mobiil-ID-d, välja arvatu juhul, kui klient on taotlenud sertifikaatide kehtetuks tunnistamist telekommunikatsiooniteenuse peatatuse ajal.

4.10. Sertifikaadi staatuse kontrollimise teenused

4.10.1. Kasutusomadused

SK pakub sertifikaadi oleku kontrollimiseks CRL-i ja OCSP teenuseid. Teenused on ligipääsetavad HTTP-protokolli kaudu.

CRL-i teenuse URL asub vastavalt sertifikaadi profiilile [6] tühistusnimekirjade levituspunktis (CDP) olevas sertifikaadis. OCSP teenuse URL asub alates 1. novembrist 2016 vastavalt sertifikaadi profiilile [6] asutuse teabe juurdepääsu väljal (AIA) olevas sertifikaadis.

4.10.2. Teenuse kättesaadavus

SK tagab oma sertifikaadi staatuse kontrollimise teenuste kättesaadavuse 7 päeva nädalas ööpäev läbi kokku minimaalselt 99,44% aastas, kusjuures kavandatud seisakuaeg ei ületa 0,28% aastas.

4.10.3. Kasutusfunktsioonid

Ei ole.

4.11. Tellimuse lõppemine

Klient võib lõpetada sertifikaadi tellimuse, tunnistades sertifikaadi kehtetuks seda asendamata.

4.12. Deponeerimine ja taastamine

4.12.1. Deponeerimise ja taaste poliitika ning tavad

SK ei osuta kliendile deponeerimis- ega taastamisteenust.

4.12.2. Seansivõtme kapselduse ja taaste poliitika ning tavad

Ei kohaldata.

5. Vahendid, haldamine ja tegevuskontroll

5.1. Füüsiline kontroll

Vaadake SK PS-i [5] punkti 5.1.

5.2. Menetluslikud kontrollimeetmed

Vaadake SK PS-i [5] punkti 5.2.

5.3. Personali juhtimine

Vaadake SK PS-i [5] punkti 5.3.

5.4. Kontrolljälgedega seotud protseduurid

Vaadake SK PS-i [5] punkti 5.4.

QSCD koostamisega seotud sündmuste kohta säilitatakse kontrolljäljed.

5.5. Andmete arhiveerimine

5.5.1. Arhiveeritud andmete liigid

Vaadake SK PS-i [5] punkti 5.5.1.

Kõiki füüsilisi dokumente asendus-PIN-koodidega ümbriku väljastamise, kehtivuse peatamise, kehtivuse peatatuse lõpetamise ja kehtetuks tunnistamise taotluste kohta säilitatakse RA-des ning need arhiveeritakse vastavalt asjassepuutuvatele eeskirjadele.

5.5.2. Arhiivis säilitamise aeg

Vaadake SK PS-i [5] punkti 5.5.2.

5.5.3. Arhiivi kaitse

Vaadake SK PS-i [5] punkti 5.5.3.

5.5.4. Arhiivi varundamine

Vaadake SK PS-i [5] punkti 5.5.4.

5.5.5. Dokumentide ajatembelduse nõuded

Vaadake SK PS-i [5] punkti 5.5.5.

5.5.6. Arhiivi kogumissüsteem (sisemine või väline)

Vaadake SK PS-i [5] punkti 5.5.6.

RA-d võivad kasutada arhiivi välist kogumissüsteemi füüsiliste arhiividokumentide jaoks.

5.5.7. Arhiiviandmete saamine ja kontrollimine

Vaadake SK PS-i [5] punkti 5.5.7.

5.6. Võtme üleminek

CA avalik võti ei muutu. OCSP-responderi avalik võti saadetakse OCSP vastuse sees, mille kaudu on võtme üleminek teada.

Vajaduse korral arvestatakse võtme ülemineku üksikasju iga kord. CA üldnimi sisaldab alati selle väljastamise aastaarvu (nt ESTEID-SK 2011).

5.7. Kompromiteerumise ja avarii järgne taaste

Vaadake SK PS-i [5] punkti 5.7.

5.8. CA või RA lõpetamine

Vaadake SK PS-i [5] punkti 5.8.

6. Tehniline turvakontroll

6.1. Võtmepaari loomine ja installeerimine

Vaadake SK PS-i [5] punkti 6.1.

6.1.1. Võtmepaari loomine

Vaadake SK PS-i [5] punkti 6.1.1.

6.1.1.1. ID-kaart

Kliendi isiklikud võtmed loob Trüb Baltic AS isikustamise käigus ID-kaardi kiibis. Loodud võtmeid ei ole võimalik kaardist eraldada ega taastada. Kliendi võtmed on kaitstud ainult kliendile üleantud ja teadaolevate aktiveerimise PIN-koodidega. Võtmevahetuse käigus loob klient kaardis uued võtmed.

6.1.1.2. Digi-ID

Kliendi isiklikud võtmed luuakse RA büroos isikustamise käigus. Loodud võtmeid ei ole võimalik kaardist eraldada ega taastada. Kliendi võtmed on kaitstud ainult kliendile üleantud ja teadaolevate aktiveerimise PIN-koodidega. Võtmevahetuse käigus loob klient kaardis uued võtmed.

6.1.1.3. Mobiil-ID

SCM loob isiklikud võtmed eelnevalt FIPS 140-2 (3. tasandi) sertifitseeritud krüptograafilisel seadmel. Võtmed laaditakse QSCD-le turvaliselt. Kliendi võtmed on kaitstud ainult kliendile üleantud ja teadaolevate aktiveerimise PIN-koodidega. SCM kustutab isiklikud võtmed infosüsteemist kohe pärast nende QSCD-le kandmist. Isiklikke võtmeid ei salvestata ülekande käigus väljaspoole QSCD-d.

6.1.2. Isikliku võtme üleandmine kliendile

Kliendi isiklikud võtmed antakse üle kaardi ja QSCD kiibis.

Loodud isiklike võtmete ja PIN-koodide konfidentsiaalsuse ning mittekasutamise kuni kaardi kliendile üleandmiseni garanteerivad kaartide käitlemisse kaasatud vastavad isikud.

Loodud isiklike võtmete ja aktiveerimiskoodide konfidentsiaalsuse ning mittekasutamise garanteerib ka ID-kaardi ja digi-ID sertifikaatide aktiveerimata olek ning asjaolu, et QSCD on enne kliendile üleandmist isikustamata.

6.1.3. Avaliku võtme üleandmine sertifikaadi väljastajale

6.1.3.1. ID-kaart

Trüb Baltic AS saadab sertifitseeritava avaliku võtme SK-le turvalise ja privaatse elektroonilise kanali kaudu sõnumiga, mille on allkirjastanud Trüb Baltic AS.

6.1.3.2. Digi-ID

RA kasutab kaardile võtme loomise korralduse andmiseks eritellimuslikku rakendust. Protsessi käigus antakse avalik võti Trüb Baltic AS-ile üle turvalise ja privaatse elektroonilise kanali kaudu, mis omakorda loob allkirjastatud sõnumi sertifikaatide taotlemiseks SK-le.

6.1.3.3. Mobiil-ID

Eelnevalt loodud avalikud võtmed antakse SCM-ilt MO-le üle partiidena. MO volitatud esindaja allkirjastab partii elektrooniliselt ja taotleb võtmete laadimist SK-s andmebaasi. Sertifikaadi väljastamisel leiab SK eelnevalt laaditud võtmete andmebaasist õige avaliku võtme QSCD seerianumbri alusel.

6.1.4. CA avaliku võtme üleandmine huvitatud isikutele

Vaadake SK PS-i [5] punkti 6.1.4.

6.1.5. Võtmete suurused

Kliendi võtmed on RSA algoritmi kasutamisel 2047- või 2048-bitised ja ECC algoritmi kasutamisel 256-bitised.

6.1.6. Avaliku võtme parameetrite genereerimine ja kvaliteedikontroll

Avalike võtmete kvaliteet garanteeritakse kiipkaarti või HSM-i sisseehitatud turvaliste juhuslike numbrite generaatoritega. Kasutaja loodud võtmed ei ole vastuvõetavad. Enne sertifikaadi väljastamist kontrollitakse võtit duplikaatide suhtes ja rakendatakse teatud analüütilist põhikontrolli (nt RSA puhul e > 1). Põhjalikum kontroll toimub regulaarselt väljastatud sertifikaatide andmebaasi kaudu.

6.1.7. Võtme kasutuseesmärgid (X.509 v3 võtme kasutusala kohta)

Vaadake SK PS-i [5] punkti 6.1.7.

Võtme kasutamise otstarbeid on kirjeldatud käesoleva CPS-i punktis 7.1.

6.2. Isikliku võtme kaitse ja krüptograafilise mooduli tehniline kontroll

6.2.1. Krüptograafilise mooduli standardid ja kontroll

6.2.1.1. ID-kaart ja digi-ID

Vaadake SK PS-i [5] punkti 6.2.1.

Kliendi isiklike võtmete salvestamiseks kasutatavad kiibid on vastavalt määrusele eIDAS [13] QSCD-l.

6.2.1.2. Mobiil-ID

Vaadake SK PS-i [5] punkti 6.2.1.

Kliendi isiklike võtmete salvestamiseks kasutatavad kiibid on vastavalt määrusele eIDAS [13]

QSCD-l. Võtmed luuakse FIPS 140-2 (3. tasandi) sertifitseeritud seadmel.

6.2.2. Isikliku võtme (n m-ist) kontrollimine mitme inimese poolt

Vaadake SK PS-i [5] punkti 6.2.2.

Mitme inimese poolt kontrollimist kliendi isiklikele võtmetele ei rakendata.

6.2.3. Isikliku võtme deponeerimine

Vaadake SK PS-i [5] punkti 6.2.3.

SK ei paku klientidele deponeerimisteenuseid.

6.2.4. Isikliku võtme varundamine

Vaadake SK PS-i [5] punkti 6.2.4.

Kliendi isiklikke võtmeid ei ole võimalik kiibist eraldada ega taastada ja neid ei varundata.

6.2.5. Isikliku võtme arhiveerimine

Vaadake SK PS-i [5] punkti 6.2.5.

Kliendi isiklikke võtmeid ei ole võimalik kiibist eraldada ega taastada ja neid ei arhiveerita.

6.2.6. Isikliku võtme edastamine krüptograafilisse moodulisse ja sealt välja

Vaadake SK PS-i [5] punkti 6.2.6.

Kliendi ID-kaardi ja digi-ID isiklikud võtmed luuakse kaardi sees.

Kliendi Mobiil-ID isiklikud võtmed kantakse HSM-ilt QSCD-le üle kaitstud keskkonnas turvalise elektroonilise kanali kaudu.

6.2.7. Isikliku võtme hoidmine krüptograafilises moodulis

Vaadake SK PS-i [5] punkti 6.2.7.

Kliendi isiklikud võtmed salvestatakse ID-kaardi, digi-ID või Mobiil-ID kiibile.

6.2.8. Isikliku võtme aktiveerimine

Vaadake SK PS-i [5] punkti 6.2.8.

Kliendi isiklikke võtmeid kaitstakse PIN-koodidega. Kohaldatakse järgmisi reegleid:

- Iga isikliku võtme või isiklike võtmete rühma jaoks, mis vastab unikaalse eraldusnimega sertifikaadile, on eraldi PIN (st autentimis- ja allkirjavõtme jaoks on eraldi PIN-id, kuid autentimise RSA-võtit ja ECC-võtit võib kaitsta sama PIN-iga);
- Klient peab sisestama autentimissertifikaadi aktiveerimiskoodi (PIN1) vähemalt üks kord pärast ID-kaardi või digi-ID kaardilugejasse sisestamist või mobiiltelefoni buutimist;
- Kliendil tuleb sisestada kvalifitseeritud elektroonilise allkirja sertifikaadi aktiveerimiskood (PIN2) enne iga toimingut, mis tehakse vastava isikliku võtmega;
- Kõikide ühe PIN-iga kaitstud isiklike võtmete kasutamine blokeeritakse pärast 3 järjestikust ebaõiget
- katset; PIN-i saab vabastada blokeeringust PUK-koodi abil;
- PUK-koodi kasutamine blokeeritakse pärast 3 järjestikust ebaõiget katset;
- kasutaja võib PIN- ja PUK-koodi muuta.

Aktiveerimiskoodide pikkuse piirang on järgmine:

- autentimisvõti (PIN1) 4–12 numbrit;
- allkirjavõti (PIN2) 5–12 numbrit;
- lukust vabastamise kood (PUK) 8–12 numbrit.

Kui ID-kaardi või digi-ID PUK-koodid lähevad kaduma või blokeeritakse, võib klient PPA või SK klienditeeninduspunktides asenduskoode taotleda.
Asendus-PIN-koodidega ümbrikke ei väljastata e-residendi digi-ID ega Mobiil-ID jaoks.

Mobiil-ID isiklike võtmete aktiveerimise PIN- ja PUK-koodid on SIM-kaardi PIN- ja PUK-koodidest erinevad.

6.2.9. Isikliku võtme deaktiveerimine

Vaadake SK PS-i [5] punkti 6.2.9.

Isiklik võti deaktiveeritakse, lahutades toite või lähtestades seadme kaardi.

Klient võib isikliku võtme deaktiveerida, tunnistades sertifikaadid kehtetuks või sisestades kõik PIN- ja PUK-koodid 3 korda järjest ebaõigesti.

6.2.10. Isikliku võtme hävitamine

Vaadake SK PS-i [5] punkti 6.2.9.

Kliendi isiklikud võtmed võib hävitada füüsiliselt kiibi hävitamise või kahjustamise teel.

6.2.11. Krüptograafilise mooduli hindamine

Vaadake käesoleva CPS-i punkti 6.2.1.

ID-kaardid, digi-ID kaardid ja Mobiil-ID SIM-kaardid on vastavalt määrusele eIDAS [12] QSCD-l.

6.3. Võtmepaari haldamise muud aspektid

6.3.1. Avaliku võtme arhiveerimine

Vaadake SK PS-i [5] punkti 6.3.1.

Kõiki kliendi avalikke võtmeid hoitakse SK andmebaasis ja neid on võimalik arhiveerida pärast sertifikaadid väljastanud CA tegevuse lõppemist.

6.3.2. Sertifikaadi ja võtmepaari kasutusaeg

Vaadake SK PS-i [5] punkti 6.3.2.

Kliendi sertifikaatide puhul on kehtivusaeg määratletud käesoleva CPS-i punktis 7.1.

6.4. Aktiveerimisandmed

6.4.1. Aktiveerimisandmete genereerimine ja installeerimine

Vaadake SK PS-i [5] punkti 6.4.1.

6.4.1.1. ID-kaart

Trüb Baltic AS trükib aktiveerimiskoodid ühes eksemplaris otse turvaümbrikusse, mis antakse kliendile üle avamata kujul. Trüb Baltic AS ei säilita aktiveerimiskoodide koopiaid.

Aktiveerimiskoode kaitstakse nii, et neid ei ole võimalik ilma turvaelementi rikkumata lugeda. Kliendil on kohustatud rikutud turvaelemendiga aktiveerimiskoodide vastuvõtmisest keelduma.

Asendus-PIN-koodidega ümbrikud on enne klienditeeninduspunktis väljastamist anonüümsed. Ümbrikud on nummerdatud ja ümbriku numbri ning selles olevate vastavate koodide vahel on krüptograafiliselt kaitstud seos. Väljastamisel sisestab klienditeeninduspunkti töötaja ümbriku numbri süsteemi ja kaart programmeeritakse vastavate koodidega neid klienditeeninduspunkti töötajale avaldamata. Kasutatavat algoritmi ja sideprotokolli üksikasju on kirjeldatud ID-kaardi dokumentatsioonis [19].

RA väljastab kliendile asendusaktiveerimiskoodid, kui neid on vaja asendada või uuendada. Ühe ID-

kaardi kõik aktiveerimiskoodid asendatakse korraga.

Enne asendusaktiveerimiskoodide väljastamist sooritab RA kliendi autentimise.

6.4.1.2. Digi-ID

Anonüümsed kaardid initsialiseeritakse fikseeritud PIN-koodiga. Isikustamise käigus väljastatakse asendusümbrik kohe vastavalt käesoleva CPS-i punktis 6.4.1.1 ja ID-kaardi dokumentatsioonis [19]kirjeldatud protokollile.

6.4.1.3. Mobiil-ID

SCM on loonud aktiveerimiskoodid eelnevalt QSCD ümbrise plastosale turvakihi alla. Aktiveerimiskoode kaitstakse nii, et neid ei ole võimalik ilma turvaelementi rikkumata lugeda. Kliendil on kohustatud rikutud turvaelemendiga aktiveerimiskoodide vastuvõtmisest keelduma.

6.4.2. Aktiveerimisandmete kaitse

Vaadake SK PS-i [5] punkti 6.4.2 ja käesoleva CPS-i punkti 6.4.1.

6.4.3. Aktiveerimisandmete muud aspektid

Ei kohaldata.

6.5. Arvuti turvakontroll

6.5.1. Arvuti tehnilised turvanõuded

Vaadake SK PS-i [5] punkti 6.5.1.

Klient vastutab oma seadme mõistliku kaitsmise eest.

6.5.2. Arvuti turvalisuse hindamine

Vaadake SK PS-i [5] punkti 6.5.2.

Klient vastutab oma seadme mõistliku kaitsmise eest.

6.6. Elutsükli tehniline kontroll

Vaadake SK PS-i [5] punkti 6.6.

Klient vastutab oma seadme mõistliku kaitsmise eest.

6.7. Võrgu turvalisuse kontroll

Vaadake SK PS-i [5] punkti 6.7.

Klient vastutab oma seadme mõistliku kaitsmise eest.

6.8. Ajatemplid

Vaadake SK PS-i [5] punkti 6.8.

Ei kohaldata klientidele.

7. Sertifikaadi, CRL-i ja OCSP profiilid

7.1. Sertifikaadi profiil

Sertifikaadi profiili on kirjeldatud sertifikaadi profiilis [6], mis on avaldatud SK avaliku teabe repositooriumis https://www.sk.ee/repositoorium/profiil/ .

7.2. CRL-i profiil

CRL-i profiili on kirjeldatud sertifikaadi profiilis [6], mis on avaldatud SK avaliku teabe repositooriumis https://www.sk.ee/repositoorium/profiil/ .

7.3. OCSP profiil

OCSP profiili on kirjeldatud sertifikaadi profiilis [6], mis on avaldatud SK avaliku teabe repositooriumis https://www.sk.ee/repositoorium/profiil/ .

8. Vastavusaudit ja muud hindamised

Vaadake SK PS-i [5] punkti 8.

9. Muud tegevus- ja õigusalased küsimused

9.1. Tasud

9.1.1. Sertifikaadi väljastamise ja uuendamise tasud

9.1.1.1. ID-kaart ja digi-ID

Klient maksab ID-kaardi ja digi-ID väljastamise eest taotluse läbivaatamise tasu vastavalt riigilõivuseaduses [16] sätestatud määrale. Vastav tasu sisaldab sertifikaadi väljastamise tasu.

Sertifikaadi väljastamise tasu loetakse SK ja Trüb Baltic AS-i vaheliseks ärisaladuseks.

Sertifikaati ei uuendata.

9.1.1.2. Mobiil-ID

Klient maksab Mobiil-ID eest igakuist tasu vastavalt MO hinnakirjas sätestatud määrale. MO-l on

õigus võtta tasu uue Mobiil-ID ja uue QSCD eest.

Klient allkirjastab MO-ga Mobiil-ID ja QSCD kohta erinevad lepingud.

MO allkirjastab lepingu Mobiil-ID kohta ainult kliendiga ja võib allkirjastada lepingu QSCD kohta ka muu isikuga (nt juriidilise isikuga) peale kliendi.

MO-l on õigus võtta tasu, kui Mobiil-ID on rohkem kui 365 päeva endiselt kehtivas olekus ja klient taotleb sertifikaate, mille kehtivuse lõppkuupäev on võrreldes kehtiva Mobiil-ID jaoks väljastatud sertifikaatide kehtivuse lõppkuupäevaga pikem.

Sertifikaadi väljastamise tasu loetakse SK ja MO vaheliseks ärisaladuseks. Sertifikaati

ei uuendata.

9.1.2. Sertifikaadi juurdepääsu tasud

Kehtivad ja aktiveeritud sertifikaadid on saadaval OCSP teenuse ja kataloogiteenuse

kaudu. Mobiil-ID sertifikaadid on samuti saadaval tarkvara DigiDoc Service [18] kaudu.

Kataloogiteenus on tasuta kättesaadav aadressil ldap://ldap.sk.ee.

9.1.3. Kehtetuks tunnistamise ja oleku kontrolli teabe juurdepääsu tasud

ID-kaardi, digi-ID ja Mobiil-ID sertifikaadi kehtetuks tunnistamine on tasuta.

Kehtiv CRL on tasuta ja kättesaadav SK veebilehel https://sk.ee/en/repository/CRL/.

OCSP veebipõhise kontrolli teenus on tasuta ja avalikult kättesaadav.

Tarkvara DigiDoc Service [18] tasu on määratud kliendi või huvitatud isiku lepingus.

Sertifikaadi oleku teiste avaldamisviiside puhul võib SK kehtestada hinnakirjaga määratava tasu ja/või nõuda vastava lepingu olemasolu.

9.1.4. Muude teenuste tasud

Muude teenuste tasud on määratud SK hinnakirjas või kliendi või huvitatud isiku lepingus. Asendus-PIN-

koodidega ümbrike väljastamise tasud on määratud SK klienditeeninduspunkti lepingus.

9.1.5. Tagastamispoliitika

Kliendil on õigus taotleda ID-kaardi ja digi-ID väljastamise taotluse läbivaatamise tasu hüvitamist vastavalt riigilõivuseadusele [16].

9.2. Rahaline vastutus

9.2.1. Kindlustuskate

Vaadake SK PS-i [5] punkti 9.2.1.

9.2.2. Muud varad

Ei kohaldata.

9.2.3. Kindlustus- ja garantiikaitse lõppüksustele

Vaadake SK PS-i [5] punkti 9.2.1.

9.3. Tegevusalase teabe konfidentsiaalsus

Vaadake SK PS-i [5] punkti 9.3.

9.4. Isikuandmete privaatsus

Vaadake SK PS-i [5] punkti 9.4.

9.5. Intellektuaalomandi õigused

SK omandab käesoleva CPS-i intellektuaalomandi õigused.

9.6. Kinnitused ja garantiid

9.6.1. CA kinnitused ja garantiid

9.6.1.1. ID-kaart ja digi-ID

Vaadake SK PS-i [5] punkti 9.6.1.

SK tagab, et:

- sertifitseerimisteenust osutatakse vastavalt asjakohastele õigusaktidele;
- sertifitseerimisteenust osutatakse vastavalt käesolevale CPS-ile, CP-le [7] ja digi-ID CP-le [8];
- peetakse arvestust väljastatavate sertifikaatide ja nende kehtivuse üle;
- sertifikaatide kehtivuse peatamise taotlusi võetakse vastu ööpäev läbi;
- sertifikaatide kehtivuse kontrollimise võimalust pakutakse ööpäev läbi;
- sertifitseerimisteenuse osutamisel kasutatavad kinnitusvõtmed on riistvaraliste turvamoodulite (st HSM) abil kaitstud ning on SK ainukontrolli all; sertifitseerimisteenuse osutamisel kasutatavate kinnitusvõtmete aktiveerimine toimub jagatud kontrolli alusel; turvalisus kindlustatakse sisemiste turvaprotseduuridega.

9.6.1.2. Mobiil-ID

Vaadake SK PS-i [5] punkti 9.6.1.

SK tagab, et:

- sertifitseerimisteenust osutatakse vastavalt asjakohastele õigusaktidele;
- sertifitseerimisteenust osutatakse vastavalt käesolevale CPS-ile ja Mobiil-ID CP-le [9];
- peetakse arvestust väljastatavate sertifikaatide ja nende kehtivuse üle;
- sertifikaatide kehtivuse peatamise taotlusi võetakse vastu ööpäev läbi;
- sertifikaatide kehtivuse kontrollimise võimalust pakutakse veebilehel ööpäev läbi;
- võetakse vastu ja registreeritakse QSCD-de ning MO esitatavate vastavate avalike võtmete väljastamist;
- võetakse vastu ja registreeritakse MO esitatavate sertifikaatide taotlusi (sertifikaadi võtmevahetuse puhul), otsustatakse sertifikaatide väljastamine ning PPA-le edastatakse teavet sertifikaatide väljastamise kohta;
- võetakse vastu ja registreeritakse PPA esitatavate sertifikaatide taotlusi ning väljastatakse vastavaid sertifikaate;
- võetakse vastu, registreeritakse ja menetletakse MO esitatavaid Mobiil-ID sertifikaatide kehtetuks tunnistamise taotlusi;
- võetakse vastu, registreeritakse ja menetletakse MO esitatavaid Mobiil-ID sertifikaatide kehtetuks tunnistamise taotlusi ning PPA-le edastatakse teavet sertifikaatide kehtetuks tunnistamise kohta;
- sertifitseerimisteenuse osutamisel kasutatavad kinnitusvõtmed on riistvaraliste turvamoodulite (st HSM) abil kaitstud ning on SK ainukontrolli all; sertifitseerimisteenuse osutamisel kasutatavate kinnitusvõtmete aktiveerimine toimub jagatud kontrolli alusel; turvalisus kindlustatakse sisemiste turvaprotseduuridega.

9.6.2. RA kinnitused ja garantiid

9.6.2.1. ID-kaart ja digi-ID

9.6.2.1.1 PPA klienditeeninduspunkt

Vaadake SK PS-i [5] punkti 9.6.2.

PPA klienditeeninduspunkt tagab, et:

- klientidele väljastatakse ID-kaart ja digi-ID, aktiveerides esmalt sellele laaditud sertifikaadid;
- võetakse vastu kliendi taotlusi ID-kaardi ja digi-ID sertifikaatide loomiseks, kehtivuse peatamiseks, kehtivuse peatatuse lõpetamiseks,
- kehtetuks tunnistamiseks; võetakse vastu kliendi põhjendatud taotlusi sertifikaatide ASN.1 kodeerimisvigade parandamiseks ja SHA-1 allkirjade asendamiseks tugevama krüptograafia ning asendus-PIN-koodide määramisega;
- kontrollitakse nimetatud taotluste õigsust ja täielikkust;
- nimetatud taotlusi esitav klient tuvastatakse ja teda kontrollitakse;
- tagab turvalisuse sisemiste turvaprotseduuridega. PPA

klienditeeninduspunkt edastab SK-le tõesed ja täielikud andmed.

PPA klienditeeninduspunkt teavitab teenuse osutamist takistava tehnilise rikke korral sellest kohe SK-d ja Trüb Baltic AS-i ning teeb kõik endast oleneva võimaliku rikke likvideerimiseks esimesel võimalusel.

9.6.2.1.2 SK klienditeeninduspunkt

Vaadake SK PS-i [5] punkti 9.6.2.

SK klienditeeninduspunkt tagab, et:

- võetakse vastu taotlusi ID-kaardi ja digi-ID sertifikaatide kehtivuse peatamiseks, kehtivuse peatatuse lõpetamiseks, kehtetuks tunnistamiseks ja asendus-PIN-koodide määramiseks;
- kontrollitakse nimetatud taotluste õigsust ja täielikkust;
- nimetatud taotlusi esitav klient tuvastatakse ja teda kontrollitakse;
- turvalisus kindlustatakse sisemiste turvaprotseduuridega.

SK klienditeeninduspunkt teavitab teenuse osutamist takistava tehnilise rikke korral sellest kohe SK-d ja teeb kõik endast oleneva võimaliku rikke likvideerimiseks esimesel võimalusel.

9.6.2.1.3 Abiliin

Vaadake SK PS-i [5] punkti 9.6.2.

Abiliin tagab, et:

- võetakse vastu taotlusi ID-kaardi ja digi-ID sertifikaatide kehtivuse peatamiseks;
- turvalisus kindlustatakse sisemiste turvaprotseduuridega.

Abiliin vastab klientide ja teiste isikute kõnedele 7 päeva nädalas ööpäev läbi.

Abiliin teavitab teenuse osutamist takistava tehnilise rikke korral sellest kohe SK-d ja tegema kõik endast oleneva võimaliku rikke likvideerimiseks esimesel võimalusel.

9.6.2.2. Mobiil-ID

9.6.2.2.1 RA

Vaadake SK PS-i [5] punkti 9.6.2.

RA tagab, et:

- klientidelt võetakse vastu sertifikaatide väljastamise taotlusi ja need edastatakse SK-le;
- kontrollitakse klientide esitatud taotluste õigsust ja täielikkust;
- sertifikaatide väljastamise taotlust esitav klient tuvastatakse ja teda kontrollitakse; kinnitatakse QSCD
- omandiõigus ja tagatakse sertifitseerimiseks esitatud avalike võtmete kehtivus; SK-lt võetakse vastu
- teateid SK väljastatavate sertifikaatide kohta;
- töötajaid, kes tegelevad sertifitseerimisteenust puudutava teabega, ei ole karistatud kuriteo tahtliku toimepanemise eest;
- tagab turvalisuse sisemiste turvaprotseduuridega. RA

edastab SK-le tõesed ja täielikud andmed.

RA teavitab teenuse osutamist takistava tehnilise rikke korral sellest kohe SK-d ja teeb kõik endast oleneva võimaliku rikke likvideerimiseks esimesel võimalusel.

9.6.2.2.2 PPA

PPA tagab, et:

- võetakse vastu sertifikaatide taotlusi, otsustatakse taotluste heakskiitmine ja heakskiidetud taotlused edastatakse SK-le; võetakse
- vastu sertifikaatide kehtetuks tunnistamise taotlusi, otsustatakse taotluste heakskiitmine ja heakskiidetud sertifikaatide kehtetuks tunnistamise taotlused edastatakse SK-le;
- nimetatud taotluste menetlemise ajal kontrollitakse taotluste õigsust ja terviklust;
- SK-lt võetakse vastu teateid SK väljastatavate sertifikaatide kohta;
- SK-lt võetakse vastu teateid SK poolt kehtetuks tunnistatud sertifikaatide kohta;
- kontrollitakse taotleja identiteeti ja tema volitusi sooritada toiming vastavalt kehtivatele õigusaktidele;
- sertifitseerimisteenusega seotud infosüsteemis (sh veebipõhises taotluste esitamise keskkonnas) täidetakse käesolevas CPS-is kirjeldatud nõudeid
  ;

- veebipõhises taotluste esitamise keskkonnas täidetakse kättesaadavuse ja turvalisuse nõudeid vähemalt käesolevas CPS-is kirjeldatud nõuete tasemeni;
- töötajaid, kes tegelevad sertifitseerimisteenust puudutava teabega, ei ole karistatud kuriteo tahtliku toimepanemise eest;
- turvalisus kindlustatakse sisemiste turvaprotseduuridega.

9.6.2.2.3 Mobiilside operaator

MO tagab, et:

- Mobiil-ID teenusega seotud infosüsteemis täidetakse kättesaadavuse ja turvalisuse nõudeid vähemalt käesolevas CPS-is kirjeldatud nõuete tasemeni;
- turvalisus kindlustatakse sisemiste turvaprotseduuridega;
- tagatakse, et töötajaid, kes võtavad vastu QSCD-ga seotud taotlusi ning sertifikaate ja/või tegelevad sertifitseerimisteenust puudutava teabega, ei ole karistatud kuriteo tahtliku toimepanemise eest.

9.6.2.2.4 MO klienditeeninduspunkt

Vaadake SK PS-i [5] punkti 9.6.2.

MO klienditeeninduspunkt tagab, et:

- võetakse vastu QSCD väljastamise ja kehtiva Mobiil-ID asendamise taotlusi (sertifikaadi võtmevahetus);
- võetakse vastu Mobiil-ID sertifikaatide kehtivuse peatatuse lõpetamise taotlusi;
- võetakse vastu telekommunikatsiooniteenuse peatamise ja sulgemise taotlusi;
- võetakse vastu sertifikaatide kehtetuks tunnistamise taotlusi ja need edastatakse SK-le;
- QSCD taotlused edastatakse SK-le ja QSCD antakse üle kliendile;
- kehtiva Mobiil-ID QSCD asendamise taotlused (sertifikaadi võtmevahetus) edastatakse SK-le;
- QSCD muutmise ja kehtiva Mobiil-ID QSCD asendamise allkirjastatud taotlused (sertifikaadi võtmevahetus) hoitakse alles;
- kontrollitakse nimetatud taotluste õigsust ja terviklust;
- kontrollitakse taotleja identiteeti ja tema volitusi sooritada toiming vastavalt kehtivatele õigusaktidele ning sisemistele turvaprotseduuridele;
- turvalisus kindlustatakse sisemiste turvaprotseduuridega.

9.6.2.2.5 SK klienditeeninduspunkt

Vaadake SK PS-i [5] punkti 9.6.2.

SK klienditeeninduspunkt tagab, et:

- võetakse vastu elektrooniliselt allkirjastatud Mobiil-ID sertifikaatide kehtivuse peatamise ja kehtivuse peatatuse lõpetamise taotlusi;
- turvalisus kindlustatakse sisemiste turvaprotseduuridega.

SK klienditeeninduspunkt teavitab teenuse osutamist takistava tehnilise rikke korral sellest kohe SK-d ja
teeb kõik endast oleneva võimaliku rikke likvideerimiseks esimesel võimalusel.

9.6.3. Kliendi kinnitused ja garantiid

9.6.3.1. ID-kaart ja digi-ID

Vaadake SK PS-i [5] punkti 9.6.3.

Klient tagab, et:

- ta järgib SK poolt käesolevas CPS-is kehtestatud nõudeid;
- ta esitab ID-kaardi ja digi-ID taotlemisel PPA-le tõest ning õiget teavet;
- ta teavitab isikuandmete muutumise korral PPA-d kohe õigetest andmetest vastavalt kehtestatud õigusaktidele;
- ta kasutab isiklikke võtmeid ja neile vastavaid sertifikaate SK poolt ettenähtud korras ja viisil;
- ta kasutab isiklikku võtit vastavalt käesolevale CPS-ile;
- ta teavitab isikliku võtme tema nõusolekuta kasutamise võimalusest kohe SK-d ning peatab oma sertifikaatide kehtivuse või tunnistab need kehtetuks;
- ta peatab kohe sertifikaatide kehtivuse või tunnistab need kehtetuks, kui isiklik võti ei ole tema valduses;
- ta on teadlik, et aegunud, kehtetuks tunnistatud või peatatud kehtivusega sertifikaatide alusel antud elektroonilised allkirjad kehtetud.

Klient ei vastuta sertifikaatide kehtivuse peatatuse ajal tehtud toimingute eest. Juhul kui klient sertifikaatide kehtivuse peatatuse lõpetab, vastutab klient ainuisikuliselt ning täies ulatuses sertifikaatidega tehtud autentimisest ja elektroonilisest allkirjast tulenevate tagajärgede eest ajal, mil sertifikaadid olid peatatud olekus.

Kui kliendil on kahtlus, et ID-kaart või digi-ID on sertifikaatide kehtivuse peatatuse ajal kliendi kontrolli alt väljunud, peab klient sertifikaadid kehtetuks tunnistama.

Klient vastutab ainuisikuliselt oma isikliku võtme hoidmise eest. Klient peab

olema tingimustega [15] nõustunud.

9.6.3.2. Mobiil-ID

Vaadake SK PS-i [5] punkti 9.6.3.

Klient tagab, et:

- ta järgib SK poolt käesolevas CPS-is kehtestatud nõudeid;
- ta esitab QSCD või QSCD muutmise taotluse esitamisel MO-le tõesed ja õiged isikuandmed;
- ta esitab Mobiil-ID sertifikaatide taotluse esitamisel PPA-le tõesed ja õiged isikuandmed;
- ta esitab kehtiva Mobiil-ID QSCD asendamise taotluse esitamisel MO-le tõesed ja õiged isikuandmed (sertifikaadi võtmevahetus);
- ta teavitab isikuandmete muutumise korral PPA-d vastavalt kehtivatele õigusaktidele;
- ta teavitab Mobiil-ID kasutuskõlbmatuks muutumise, kadumise või hävinemise korral MO-d vastavalt kehtivatele õigusaktidele;
- kasutab isiklikke võtmeid ja neile vastavaid sertifikaate SK poolt ettenähtud korras ja viisil; kasutab isiklikku võtit vastavalt
- käesolevale CPS-ile;
- ta taotleb sertifikaadile salvestatud isikuandmete muutumise korral Mobiil-ID teenuse kasutamise jätkamiseks uut QSCD-d ja Mobiil-ID sertifikaate;
- ta teavitab isikliku võtme tema nõusolekuta kasutamise võimalusest kohe SK-d ning peatab oma sertifikaatide kehtivuse või tunnistab need kehtetuks;
- ta peatab kohe sertifikaatide kehtivuse või tunnistab need kehtetuks, kui isiklik võti ei ole tema valduses või seade on varastatud;
- ta on teadlik, et aegunud, kehtetuks tunnistatud või peatatud kehtivusega sertifikaatide alusel antud elektroonilised allkirjad kehtetud.

Klient ei vastuta sertifikaatide kehtivuse peatatuse ajal tehtud toimingute eest. Juhul kui klient sertifikaatide kehtivuse peatatuse lõpetab, vastutab klient ainuisikuliselt ning täies ulatuses sertifikaatidega tehtud autentimisest ja elektroonilisest allkirjast tulenevate tagajärgede eest ajal, mil sertifikaadid olid peatatud olekus.

Kui kliendil on kahtlus, et Mobiil-ID on sertifikaatide ja/või telekommunikatsiooniteenuse peatatuse ajal väljunud tema kontrolli alt, on klient kohustatud sertifikaadid kehtetuks tunnistama.

Klient vastutab ainuisikuliselt oma isikliku võtme hoidmise eest. Klient peab

olema tingimustega [15] nõustunud.

9.6.4. Huvitatud isiku kinnitused ja garantiid

Vaadake SK PS-i [5] punkti 9.6.4.

Huvitatud isik tutvub sertifikaadi vastuvõtmisega seotud riskide ja kohustustega. Riskid ja kohustused on esitatud käesolevas CPS-is, CP-s [7], digi-ID CP-s [8] ja Mobiil-ID CP-s [9].

Kui sertifikaadiga või elektroonilise allkirjaga ei kaasne piisavalt tõendusmaterjali sertifikaadi kehtivuse kohta, kontrollib huvitatud isik sertifikaadi kehtivust sertifikaadi kasutamise või kvalifitseeritud elektroonilise allkirja andmise ajal SK kehtivuskinnitusteenuse abil.

Huvitatud isik järgib sertifikaadis esitatud piiranguid ja tagab, et vastuvõetav tehing vastab CP-le [7], digi-ID CP-le [8] ja Mobiil-ID CP-le [9].

Huvitatud isik kasutab CRL-i teenust omal vastutusel.

9.6.5. Teiste poolte kinnitused ja garantiid

9.6.5.1. ID-kaart ja digi-ID

9.6.5.1.1 Trüb Baltic AS

Trüb Baltic AS-i töötajat ei ole karistatud kuriteo tahtliku toimepanemise eest.

Trüb Baltic AS kindlustab turvalisuse sisemiste turvaprotseduuridega.

9.6.5.2. Mobiil-ID

9.6.5.2.1 SIM-kaardi valmistaja

SCM vastutab kõikide QSCD tootmisega seotud toimingute ja menetluste, sh võtme turvalise loomise ning laadimise ja avaliku võtme SK-le üleandmise eest.

9.7. Garantiidest lahtiütlemine

Vaadake SK PS-i [5] punkti 9.7.

9.8. Vastutuse piirangud

Vaadake SK PS-i [5] punkti 9.8.

9.9. Hüvitised

Kliendi ja SK vahelisi hüvitisi reguleeritakse tingimustes [15].

9.10. Tähtaeg ja lõpetamine

9.10.1. Tähtaeg

Vaadake käesoleva CPS-i punkti 2.2.1.

9.10.2. Lõpetamine

Vaadake SK PS-i [5] punkti 9.10.2.

9.10.3. Lõpetamise tagajärjed ja kehtima jäävad sätted

SK teavitab käesoleva CPS-i lõpetamise tingimustest ja tagajärgedest avaliku repositooriumi kaudu. Teavituses on täpsustatud, millised sätted jäävad pärast lõpetamist kehtima.

Pärast lõpetamist jäävad kehtima vähemalt kõik isikuandmete ja konfidentsiaalse teabe kaitsega seotud kohustused, samuti SK arhiivide haldamine kindlaksmääratud ajaks ja logid. Kõik kliendi kokkulepped jäävad jõusse seni, kuni sertifikaat tunnistatakse kehtetuks või kuni see aegub, isegi juhul, kui käesolev CPS lõpeb.

Käesolevat CPS-i ei saa lõpetada enne käesoleva CPS-i punktis 5.8 kirjeldatud lõpetamistegevusi.

9.11. Individuaalsed teated ja suhtlemine pooltega

Kliendile antakse õigus tingimustega [15] enne nendega nõustumist ja nende allkirjastamist tutvuda.

Kliendi individuaalsed teated edastatakse autentimissertifikaadil oleval kliendi e-posti aadressil.

9.12. Muudatused

9.12.1. Muudatuste tegemise kord

Vaadake käesoleva CPS-i punkti 1.5.4.

9.12.2. Teavitusmehhanism ja -aeg

Vaadake käesoleva CPS-i punkti 2.2.1.

9.12.3. Asjaolud, mis nõuavad OID-i muutmist

Ei kohaldata.

9.13. Vaidluste lahendamise sätted

Vaadake SK PS-i [5] punkti 9.13.

Klient või muu pool saab esitada oma nõude või kaebuse järgmisel e-posti aadressil info@sk.ee.

9.14. Kohaldatav õigus

Käesolevat CPS-i reguleerib Euroopa Liidu ja Eesti seadusandlus.

9.15. Vastavus kohaldatava õigusega

Vaadake SK PS-i [5] punkti 9.15.

Lisaks SK tagab järgmiste nõuete täitmise:

- ITDS [12];
- riigilõivuseadus [16];
- isikuandmete kaitse seadus [17].

9.16. Muud sätted

9.16.1. Kogu lepingu ulatus

SK kohustab lepinguliselt iga RA-d käesolevale CPS-ile ja valdkonna kohaldatavatele juhistele. SK nõuab ka igalt tema tooteid ja teenuseid kasutavalt poolelt lepingu sõlmimist, mis sätestab toote või teenusega seotud tingimused. Kui lepingus on sätteid, mis erinevad käesolevast CPS-ist, siis kohaldatakse konkreetse lepingu poolega sõlmitud kokkulepet. Kolmandad pooled ei või sellele lepingule tugineda ega kasutada meetmeid sellise lepingu jõustamiseks.

9.16.2. Loovutamine

Ükski käesoleva CPS-i alusel tegutsev üksus ei või loovutada oma õigusi või kohustusi ilma SK eelneva kirjaliku nõusolekuta. Kui poolega sõlmitud lepingus ei ole määratud teisiti, ei esita SK loovutamise kohta teavitust.

9.16.3. Sätete kehtivus

Kui pädev kohtuasutus on tunnistanud käesoleva CPS-i mistahes sätte kehtetuks või tühiseks, jääb ülejäänud CPS kehtivaks ja kuulub täitmisele. Iga käesoleva CPS-i säte, mis näeb ette vastutuse piirangud, garantiidest lahtiütlemise või kahjude välistamise, on kõikidest teistest sätetest lahutatav ja iseseisev.

9.16.4. Jõustamine (õigusabikulud ja õigustest loobumine)

SK võib nõuda poolelt tema käitumisega seotud kahjude, kaotuste ja kulude eest hüvitist ja õigusabikulusid. Kui SK-l ei õnnestu mõnda käesoleva CPS-i sätet jõustada, ei tähenda see seda, et SK loobub õigusest jõustada sama sätet hiljem või jõustada mingit muud käesoleva CPS-i sätet. Loobumiste kehtimiseks peavad need olema esitatud kirjalikult ja SK poolt allkirjastatuna.

9.16.5. Vääramatu jõud

Vaadake SK PS-i [5] punkti 9.16.5.

9.17. Muud sätted

Ei kohaldata.

10. Viidatud dokumendid

1. AS Sertifitseerimiskeskus – sertifitseerimispõhimõtted, avaldatud: https://sk.ee/en/repository/CPS/;
2. ESTEID-kaardi sertifitseerimispoliitika, avaldatud: https://sk.ee/en/repository/CP/;
3. AS Sertifitseerimiskeskus – Mobiil-ID kujul digitaalse isikutunnistuse sertifitseerimispoliitika, avaldatud: https://sk.ee/repositoorium/CP/ ;
4. RFC 3647 – Palve kommenteerimiseks 3647, internet X.509 avaliku võtme infrastruktuur, sertifitseerimispoliitika ja -tavade raamistik;
5. AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted, avaldatud: https://sk.ee/en/repository/sk-ps/;
6. Sertifikaadi, CRL-i ja OCSP profiilid Eesti Vabariigi isikut tõendavatel dokumentidel, avaldatud: https://www.sk.ee/repositoorium/profiil/;
7. AS Sertifitseerimiskeskus – ID-kaardi sertifitseerimispoliitika, avaldatud:
8. https://sk.ee/en/repository/CP/; AS Sertifitseerimiskeskus – Digi-ID sertifitseerimispoliitika,
9. avaldatud: https://sk.ee/en/repository/CP/;
10. AS Sertifitseerimiskeskus – Eesti Vabariigi Mobiil-ID sertifitseerimispoliitika, avaldatud: https://sk.ee/en/repository/CP/; ETSI EN 319 411-2 V2.1.1 (2016-02) Elektroonilised allkirjad ja infrastruktuurid (ESI); Poliitika- ja turvanõuded sertifikaate väljastavatele usaldusteenuse osutajatele; 2. osa: Poliitikanõuded kvalifitseeritud sertifikaate väljastavatele sertifitseerimisasutustele;

11. ETSI EN 319 411-1 V1.1.1 (2016-02) Elektroonilised allkirjad ja infrastruktuurid (ESI); Poliitika- ja turvanõuded sertifikaate väljastavatele usaldusteenuse osutajatele; 1. osa: Üldised nõuded;
12. Isikut tõendavate dokumentide seadus, RT I 1999, 25, 365, avaldatud:https://www.riigiteataja.ee/en/eli/ee/511042016001/consolide/current;
13. eIDAS – Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014 (23. juuli 2014) e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ;
14. ISO/IEC 7816, 1.–4. osa, avaldatud aadressil http://iso.org;
15. Eesti Vabariigi isikut tõendavate dokumentide sertifikaatide kasutustingimused, avaldatud: https://sk.ee/repositoorium/kasutustingimused// ;
16. Riigilõivuseadus, RT I, 30.12.2014, 1, avaldatud: https://www.riigiteataja.ee/en/eli/ee/511022015002/consolide/current;
17. Isikuandmete kaitse seadus, RT I 2007, 24, 127, avaldatud: https://www.riigiteataja.ee/en/eli/ee/507032016001/consolide/current; DigiDoc Service: https://sk.ee/en/services/validity-confirmation-services/digidoc-service/;
18. ID-kaardi dokumentatsiooni veebileht: http://www.id.ee/index.php?id=35772
19.