SONERA MOBIILIASIOINTIVARMENNE

VARMENNUSKÄYTÄNTÖ

Versio 2.1

Voimassa 1.12.2016 lähtien

TeliaSonera Finland Oyj, kotipaikka: Helsinki, Teollisuuskatu 15, 00510 Helsinki,
puh. 020401, Y-tunnus 1475607-9, ALV rek

Yhteystiedot

Varmennuskäytäntöä hallinnoiva organisaatio

Tätä varmennuskäytäntöä hallinnoi TeliaSonera Finland Oyj:n (myöh. Soneran) varmennepolitiikkayksikkö,

Soneran yhteystiedot:

TELIASONERA FINLAND OYJ
00051 SONERA
Puhelin: +358 (0) 20401

Yhteyshenkilö varmennuskäytäntöön liittyvissä asioissa:

Sonera CA Tuotepäällikkö
Sähköposti: cainfo@sonera.com
Puhelin: +358 (0) 20401

Tämän varmennepolitiikan tekijänoikeudet kuuluvat Soneralle.

Asiakas- ja sulkupalvelu

Mobiilivarmenteen käytön voi estää Soneran sulkupalvelussa. Ilmoituksen voi tehdä:

Soittamalla operaattorin asiakaspalveluun: 020 017 000 (avoinna arkisin klo 8-20 ja la 9-16.30)
Soittamalla operaattorin tekniseen asiakaspalveluun: 020 690 101 (avoinna 24 tuntia vuorokaudessa 7 päivänä viikossa)
Operaattorin valtuutetuissa asiointipisteissä ja jälleenmyyjillä niiden aukioloaikoina

Varmennuskäytännön tunnisteet

Tämän varmennuskäytännön nimi on "**Sonera Mobiiliasiointivarmenne, Varmennuskäytäntö**" ja sen tunnus on ”TeliaSonera Finland Mobile ID CPS”.

Tämä varmennuskäytäntö kuvaa kuinka Sonera toteuttaa mobiilivarmennuspalvelun luottamusverkoston yhteisen varmennepolitiikan "MOBIILIASIOINTIVARMENNE - VARMENNEPOLITIIKKA - Operaattoreiden mobiiliasiointivarmenteita varten". Tämän varmennuskäytännön tunnisteet (Object Identifier) ovat:
1.2.246.277.1.11.4.1.2.1 (myönnetty 2010-2011)
1.2.246.277.1.11.4.1.2.2 (myönnetty 2011-02/2016)
1.2.246.277.1.11.4.2.2.3 (myönnetty 02/2016-)

Versionhallinta

Versio	Päiväys	Kuvaus
1.0	30.11.2010	Ensimmäinen hyväksytty ja julkaistu versio
1.0.1	20.12.2010	Lisätty CA-sulkulistan osoite. Korjattu kirjoitusvirheitä
1.0.2	6.6.2011	Uusi Soneran liikemerkki
1.0.3	4.10.2011	Lisätty ensimmäisen avainparin luonti kortilla (6.1.1.2)
2.0.0	1.2.2016	Lisätty uusi salausalgoritmi
2.1	1.12.2016	Korjattu ja täsmennetty virheellisyyksiä, käännös englanniksi

Käsitteitä ja aihepiiriin liittyvää sanastoa

Tässä dokumentissa käytetty suomenkielinen termi	**Yleisesti käytössä oleva englanninkielinen termi**	**Selitys**
Aktivointitieto, Tunnusluku	Activation Data	Yksityisen avaimen käyttöä suojaava PIN-koodi tai salasana, joka syöttämällä aktivoidaan yksityinen avain. Mobiiliasiointivarmenteen yksityiset avaimet sijaitsevat puhelimen SIM-kortilla.
Alivarmentaja, operatiivinen varmentaja	Subordinate CA	Varmentaja, jonka varmenteen juurivarmentaja on allekirjoittanut ja joka myöntää varmenteita määrittelemilleen loppukäyttäjille
Allekirjoituksen luomistiedot	Signature Creation Data	Allekirjoittajan sähköisen allekirjoituksen luomisessa käyttämä ainutkertainen tietokokonaisuus, kuten koodit ja yksityiset avaimet
Asiointivarmenne		Asiointivarmenne on varmenne, josta on säädetty laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009). Asiointivarmenne ei välttämättä ole laissa mainittu laatuvarmenne.
Digitaalinen allekirjoitus	Digital Signature	Sähköinen allekirjoitus, joka on tehty asiakirjan tai viestin allekirjoittajan yksityisellä avaimella julkisen avaimen menetelmän mukaisesti. Yleensä allekirjoitus on salattu tiiviste viestistä.
ECC	Elliptic Curve Cryprography	Epäsymmetrinen salausalgoritmi, jota käytetään epäsymmetrisen avainparin luontiin.
Hakemistopalvelu	Directory Service	Julkisen avaimen järjestelmässä palvelu, joka sisältää käyttäjien varmenteita ja niihin mahdollisesti liittyvää muuta tietoa sekä sulkulistoja sisältäviä hakemistoja. Yleensä varmentajan itsensä ylläpitämä.
Julkinen avain	Public Key	Julkinen osa epäsymmetrisestä avainparista, jota käytetään julkisen avaimen salaustekniikoissa. Julkinen avain sisältyy varmenteeseen, jonka varmentaja julkaisee hakemistopalveluun.
Julkisen avaimen järjestelmä	Public Key Infrastructure (PKI)	Julkisen avaimen menetelmän käytön mahdollistava järjestelmä, jossa varmentaja varmentaa avainparin julkisen osan digitaalisella allekirjoituksellaan ja jakaa näitä varmenteita muille käyttäjille, ylläpitää

		julkisten avainten hakemistoa ja sulkulistaa sekä mahdollisesti antaa muita järjestelmän käyttöön liittyviä palveluja.
Julkisen avaimen menetelmä	Public key method	Epäsymmetrinen salausmenetelmä, jossa kullakin salakirjoituksen käyttäjällä on kaksi toisiinsa liittyvää avainta. Toinen avainparin avaimista on julkisessa hakemistossa julkaistu julkinen avain, toinen on vain avainparin käyttäjän hallussa oleva yksityinen avain. Yksityisellä avaimella salakirjoitettu tieto voidaan avata vain vastaavalla julkisella avaimella, ja päinvastoin.
Juurivarmentaja	Root CA	Julkisen avaimen järjestelmässä ylin luotettu taho, joka allekirjoittaa, jakelee ja tarvittaessa peruuttaa varmenteet alemman tason varmentajille.
Kiistämättömyys	nonRepudiation	Avaimen käyttötarkoitus, jolla annetaan mainittua avainta käyttäen tehdylle kehittyneelle sähköiselle allekirjoitukselle sopimuksellinen sitovuus lain edessä. Kiistämättömyysavaimella on mahdollista allekirjoittaa sopimuksia. Allekirjoitettaessa dokumentti kiistämättömyysavaimella saavutetaan mahdollisuus todeta dokumentin eheys ja aitous käyttäen kyseistä avainta vastaavaa varmennetta. Katso *Sähköinen allekirjoitus* alla.
Liittymäkortti	Subscriber Identity Module	Kortti, johon puhelinliittymä on sidottu. Puhekielessä yleensä SIM-kortti.
Loppukäyttäjä, Varmenteen omistaja	End Entity	Henkilö, jolle varmentaja on myöntänyt varmenteen. Loppukäyttäjä käyttää varmennetta ja hänellä on laillisesti hallussaan varmenteen sisältämää julkista avainta vastaava yksityinen avain ja sen käyttöön tarvittavat tunnusluvut.
Luottava osapuoli	Relying Party	Sähköisiä palveluja varmenteiden loppukäyttäjille tarjoava taho. Luottava osapuoli toimii luottaen varmenteeseen ja/tai todentaa digitaalisen allekirjoituksen varmenteen avulla.
Luotettu varmenne	Trust Anchor	Varmenne, jonka luottavat osapuolet määrittelevät varmennehierarkiansa huipuksi ja jonka alapuolella olevat varmenteet he joutuvat varmentamaan.
Mobiiliasiointivarmenne	Mobile certificate Mobile ID certificate	Mobiiliasiointivarmenne on mobiilipäätelaitteen liittymäkorteilla sijaitseviin yksityisiin avaimiin perustuva

	Mobile Transaction Certificate	asiointivarmenne. Tämän varmennepolitiikan mukaista mobiiliasiointivarmennetta voidaan käyttää henkilön sähköiseen tunnistamiseen, viestinnän salaamiseen ja sähköiseen allekirjoitukseen. Mobiiliasiointivarmennetta voidaan käyttää käyttötarkoituksensa mukaisesti sekä hallinnollisissa että yksityisten organisaatioiden tarjoamissa sovelluksissa ja palveluissa. Tässä varmennepolitiikassa luettavuuden helpottamiseksi käytetään termiä Mobiilivarmenne isolla kirjoitettuna, ellei asiayhteys anna aihetta muuhun.
Mobiilivarmenne	Mobile Certificate	Tässä dokumentissa käytetty termi Mobiiliasiointivarmenteelle
Rekisteröijä	Registration Authority (RA)	Varmenteen hakijan tunnistamisesta ja varmennehakemukseen rekisteröitävien tietojen tarkistamisesta vastaava osapuoli. Rekisteröijä toimii varmentajan valtuuttamana varmenneorganisaation osana.
RSA	RSA	Epäsymmetrinen salausalgoritmi, jota käytetään epäsymmetrisen avainparin luontiin. Lyhenne tulee keksijöidensä sukunimistä; Rivest, Shamir ja Adleman.
Sulkulista	Certificate Revocation List (CRL)	Julkisen avaimen järjestelmässä käytöstä poistettujen varmenteiden luettelo. Varmentaja julkaisee sulkulistan hakemistopalvelussa.
Suostumus	Consent	Tapahtuman tai toimenpiteen vahvistaminen käyttäen avainta, jonka käyttötarkoitus on *digitalSignature* mutta ei *nonRepudiation*.
Sähköinen allekirjoitus	Electronic signature	Tietokoneen luettavassa muodossa oleva henkilön nimikirjoitus tai sen vastine, esimerkiksi digitaalinen allekirjoitus, todisteena nimikirjoitukseen liittyvän asiakirjan tai viestin yhteydestä tiettyyn henkilöön. Puhekielessä sähköisellä allekirjoituksella tarkoitetaan yleensä digitaalista allekirjoitusta, jonka tekemiseen käytetyn avaimen käyttötarkoituksiin kuuluu *nonRepudiation*.
Todentaminen	Authentication; Verification	Järjestelmän käyttäjän (henkilön, organisaation tai laitteen) tai viestinnässä toisen osapuolen tunnistuksen varmistaminen.

Tunnistaminen	Identification	Asioinnissa toisen osapuolen identiteetin selvittäminen. Yksinkertaisimmillaan tapahtuma, jossa vastataan kysymykseen: "Kuka sinä olet?"
Tunnistusväline		Liittymäkortti yksityisine avaimineen ja niihin liittyvät tunnusluvut.
Vahvistaminen	Validation	Varmenteen, varmenteella tehdyn operaation tai sen lopputuotoksen oikeellisuuden toteaminen.
Varmenne	Certificate	Varmenne on henkilön julkisesta avaimesta, nimitiedoista, sekä muista varmenteeseen sisällytettävistä tiedoista muodostuva kokonaisuus, jonka varmentaja on allekirjoittanut omalla yksityisellä avaimellaan. Varmenteen aitous on todennettavissa tarkistamalla varmentajan digitaalinen allekirjoitus.
Varmennehakemus	Certificate Application	Varmennehakemus on varmenteen hakijan täyttämä varmenteen hakijan henkilö-, organisaatio- ja yhteystiedot sisältävä, hakemuksen hyväksyjän hyväksymä ja tarvittaessa luotetun henkilön allekirjoittama lomake.
Varmenneorganisaatio		Varmenneorganisaation osapuolia ovat varmentaja, rekisteröijä, kortinvalmistaja, hakemisto- ja sulkulistapalvelujen tuottajat sekä muut palvelun tuottajat, joiden palveluja varmentaja käyttää.
Varmennepalvelu		Varmennepalvelu on varmenteisiin perustuva tunnistus- ja allekirjoituspalvelu, jota varmenteisiin luottava osapuoli hyödyntää varmenteen omistajille tarjoamissaan palveluissa.
Varmennepolitiikka	Certificate Policy (CP)	Nimetty joukko sääntöjä, joiden perusteella on mahdollista arvioida varmenteen soveltuvuus tiettyyn käyttötarkoitukseen ja yleiset turvallisuus- ja muut vaatimukset. **Varmennepolitiikka** (engl. *Certificate Policy, CP*) on varmentajan laatima kuvaus menettelytavoista ja toimintaperiaatteista, joita varmenteita myönnettäessä noudatetaan. Varmennuskäytäntö on varmennepolitiikkaa yksityiskohtaisempi kuvaus varmentajan toiminnasta.
Varmennepolku	Certificate Path	Varmenteen alkuperän varmistamiseksi tarvittava varmenteiden [looginen] ketju, joka ulottuu loppukäyttäjän varmenteesta juurivarmentajan varmenteeseen.

Varmennepyyntö	Certificate Request	Varmennepyyntö on varmentajalle lähetettävä, rekisteröijän muodostama, varmennehakemuksen perusteella tehty digitaalinen varmenteen muodostamis- ja julkaisupyyntö.
Varmennuskäytäntö	Certification Practice Statement (CPS)	Yksityiskohtainen selostus menettelytavoista, joita varmenneorganisaatio käyttää myöntäessään ja hallinnoidessaan varmenteita. **Varmennuskäytäntö** kuvaa kuinka varmentaja toteuttaa varmennepolitiikkaansa ja kuvaa yksityiskohtaisesti varmentajan noudattamat käytännöt ja toimintatavat. Varmennepolitiikan ja varmennuskäytännön rakenne noudattaa pääosin IETF RFC 3647:n [RFC3647] mukaista jaottelua.
Varmentaja	Certification Authority (CA)	Varmenneorganisaation osapuoli, joka myöntää varmenteita allekirjoittamalla varmennetiedot omalla yksityisellä avaimellaan.
Yksityinen avain, henkilökohtainen avain	Private Key	Salainen osa epäsymmetrisestä avainparista, jota käytetään julkisen avaimen salaustekniikoissa. Yksityistä avainta käytetään tyypillisesti digitaaliseen allekirjoittamiseen tai julkisella avaimella salatun viestin avaamiseen. Puhekielessä käytetään usein myös käsitettä salainen avain. Varmenteen omistajan yksityiset avaimet on talletettu liittymäkortille niiden suojaamiseksi oikeudettomalta käytöltä.

Lyhenteet

Lyhenne	Selitys	Tässä dokumentissa käytetty merkitys
ARL	Authority Revocation List	Juurivarmentajan julkaisema sulkulista, joka sisältää tiedot käytöstä poistetuista varmentajien varmenteista
CA	Certification Authority	Varmentaja
CP	Certificate Policy	Varmennepolitiikka
CPS	Certification Practice Statement	Varmennuskäytäntö
CRL	Certification Revocation List	Sulkulista
ECC	Elliptic Curve Cryptography	Elliptisiin käyriin perustuva salausmenetelmä
HSM	Hardware Secure Module	Varmentajien avainten luontiin ja säilytykseen käytettävä turvamoduuli
ICCID	Integrated Circuit Card Identifier	Liittymäkortin yksilöllinen sarjanumero
IETF	Internet Engineering Task Force	Internetin teknistä kehitystä edistävä kansainvälinen yhteisö
MSISDN	Mobile Subscriber ISDN Number	Matkapuhelimen puhelinnumero
MSSP	Mobile Signature Service Provider	Matkapuhelimessa tehtävän allekirjoituksen ja tunnistamisen mahdollistava palvelualusta.
OCSP	Online Certificate Status Protocol	Reaaliaikainen varmenteiden sulkutietoprotokolla
OID	Object Identifier	Varmennepolitiikan tunnistetieto
PDS	PKI Disclosure Statement	Yksinkertaistettu kuvaus varmenteen käytön ehdoista ja rajoituksista.
PIN	Personal Identification Number	Tunnusluku, PIN-koodi
PKI	Public Key Infrastructure	Julkisen avaimen varmennejärjestelmä
PKIX	-	IETF:n PKI –työryhmä
PUK	Personal Unblocking Key	PUK-koodi
RA	Registration Authority	Rekisteröijä
RSA	Rivest, Shamir ja Adleman,	Salausalgoritmi
X.509	-	Varmenteen ja sulkulistan rakenteen määrittelevä standardi

Roolit

Liittymän tilaaja	Vastaa laskujen maksusta. Luonnollinen henkilö tai yritys, joka sallii liittymän palvelut. Voi olla sama kuin liittymän käyttäjä.
Liittymän käyttäjä	Liittymän ja palveluiden käyttäjä, luonnollinen henkilö, joka on merkitty liittymän haltijaksi. Käyttäjä voi olla sama kuin liittymän tilaaja.
Varmenteen hakija	Aina sama luonnollinen henkilö kuin liittymän käyttäjä. Liittymän haltijaksi on oltava merkittynä varmenteen hakija.
Varmenteen omistaja	Luonnollinen henkilö, jolle on myönnetty Mobiilivarmenne. Aina sama luonnollinen henkilö kuin varmenteen hakija eli liittymän käyttäjä.

1 Johdanto

1.1 Mobiilivarmennepalvelu

Suomalaiset teleoperaattorit ovat yhdessä toteuttaneet mobiilivarmennepalvelun, jota matkapuhelimia käyttävät kuluttajat voivat hyödyntää asioidessaan turvallisesti palveluntuottajien erilaisissa sähköisissä palveluissa. Sonera Mobiilivarmenne on varmennepalvelu Soneran matkapuhelinasiakkaille.

Sonera Mobiilivarmenne on palvelu, jossa asiakkaan matkapuhelimen liittymäkorttiin (SIM-kortti) liitetään henkilön vahva sähköinen tunniste eli varmenne. Varmenteella ja sitä tukevalla SIM-kortilla varustettua matkapuhelinta voi käyttää tunnistus- ja allekirjoitusvälineenä erilaisissa asiointi- ja viestintäpalveluissa.

Sonera Mobiilivarmenne tarjoaa käyttäjilleen helpon ja turvallisen tavan tunnistautua kaikkiin mobiilivarmenteita tukeviin palveluihin sekä varmistautua asioinnin yhteydessä tekemiensä sitoumusten sisällöstä ja kiistämättömyydestä. Sonera Mobiilivarmenteen käyttäjien yksilöivänä tietona käytetään varmenteissa olevaa sähköistä asiointitunnusta (SATU). Tämä koodi ja siihen liittyvät henkilönimet tarkistetaan aina väestörekisterikeskuksen tietokannasta

Sonera Mobiilivarmenne perustuu X.509-varmenteisiin ja julkisen avaimen menetelmään, jossa varmenteisiin liittyvät yksityiset avaimet ovat SIM-kortilla suojattuna Tunnusluvulla. Sonera ID -palvelun allekirjoitusvarmenteella käyttäjä voi tehdä kehittyneitä sähköisiä allekirjoituksia, jotka perustuvat julkisen avaimen menetelmään, RSA- tai ECC-algoritmiin ja vähintään 1024-bittisiin (RSA) tai 256-bttisiin (ECC) tietoturva-avaimiin. Kaikki uudet avaimet alkaen 02/2016 ovat ECC-avaimia.

Sonera Mobiilivarmenteen käyttöönotto saattaa vaatia SIM-kortin vaihdon. Käyttäjän on noudatettava erityistä huolellisuutta, jotta matkapuhelin ja Sonera Mobiilivarmenteen tunnusluku ei ole muiden kuin käyttäjän itsensä käytettävissä.

1.2 Varmennuskäytäntö

Varmennuskäytäntö (CPS, Certification Practice Statement) on varmentajan (CA, Certification Authority) kuvaus käytännöistä, joita se noudattaa varmenteita myöntäessään. Tämän varmennuskäytännön tarkoituksena on kuvata menettelyt, joita Sonera-varmentajat TeliaSonera Mobile ID CA v1 ja TeliaSonera Mobile ID CA v2 käyttävät myöntäessään mobiilivarmenteita Soneraan asiakassuhteessa oleville luonnollisille henkilöille. Soneran mobiilivarmenteiden myöntämisessä noudatetaan myös geneerisemmän varmennekäytännön”TeliaSonera Production CPS” dokumentoimia käytäntöjä. Se löytyy julkisesta linkistä https://repository.trust.teliasonera.com/CPS. Siinä kuvataan yleiset turvajärjestelyt ja käytännöt jotka koskevat kaikkia Soneran myöntämiä varmenteita. Sen ja tämän dokumentin välisessä ristiriitatilanteessa noudatetaan tämän dokumentin käytäntöjä.

Varmennepolitiikka, joka ohjaa varmentajan palveluiden toteuttamista ja ylläpitoa ja määrittelevät säännöt varmenteiden hakemiselle, myöntämiselle ja käytölle on kuvattu mobiilivarmennuspalvelun luottamusverkoston yhteisessä varmennepolitiikassa "MOBIILIASIOINTIVARMENNE - VARMENNEPOLITIIKKA - Operaattoreiden mobiiliasiointivarmenteita varten".

Varmennuskäytäntö noudattaa varmennepolitiikan rakennetta.

1.3 Mobiilivarmenne

Mobiilivarmenteita voidaan käyttää tunnistamiseen, salaamiseen sekä tiedon tai tapahtuman eheyden, luottamuksellisuuden ja kiistämättömyyden varmistamiseen. Mobiilivarmenteet ovat mobiilipäätelaitteen liittymäkorteilla sijaitseviin yksityisiin avaimiin perustuvia varmenteita, jotka on myöntänyt luottamusverkostoon kuuluva varmentaja. Kaikki luottamusverkostoon kuuluvat varmentajat ovat itsenäisiä ja kullakin varmentajalla on oma juurivarmenteensa, johon varmenteen käyttäjät luottavat. Varmenteiden myöntö vaatii aina sopimuksen varmentajan ja varmenteen hakijan välille.

1.4 Varmennusorganisaatio

1.4.1 Varmentaja

Tämän varmennuskäytännön mukaisesti toimiva varmentaja on TeliaSonera Finland Oyj. Varmentajan yksilöivät tiedot löytyvät jokaisen myönnetyn varmenteen myöntäjä (*Issuer*) -kentästä. Soneran mobiilivarmenteet myöntää varmentajat ”TeliaSonera Mobile ID CA v1” (RSA-varmenteet) ja ”TeliaSonera Mobile ID CA v2” (ECC-varmenteet).

Varmentajan varmenteet on myöntänyt ja allekirjoittanut yksityisellä avaimellaan Soneran juurivarmentaja ”TeliaSonera Root CA v1”.

Varmentaja tuottaa varmennepalvelun ja vastaa siitä kokonaisuutena. Varmentaja luo loppukäyttäjävarmenteet ja sulkulistat ja allekirjoittaa ne varmentajan yksityisellä avaimella.

1.4.2 Rekisteröijä

Rekisteröijällä tarkoitetaan tahoa, joka toimii varmentajan toimeksiannosta ja vastuulla ja hoitaa varmennehakemusten käsittelyyn liittyvää käytännön työtä noudattaen varmennepolitiikkaa ja varmennuskäytäntöä. Rekisteröijän tehtäviin kuulu tunnistaa varmenteen hakija ja hyväksyä hakemus.

Mobiilivarmenteen rekisteröijinä toimivat valtuutetut Soneran paikalliset asiointipisteet ja jälleenmyyjät. Varmenteen hakija voi hakea varmennetta myös Soneran itsepalveluportaalien kautta, jolloin varmentajan rekisteröintijärjestelmä toimii rekisteröijänä.

1.4.3 Liittymäkortin liikkeellelaskija

Liittymäkortin liikkeellelaskija toimii mobiilivarmenteeseen liittyvien avainparien ja aktivointitietojen osalta varmentajan toimeksiannosta ja vastuulla. Liittymäkortin liikkeellelaskija toimittaa mobiilivarmenteen rekisteröinnissä tarvittavat asiakkuus- ja korttitiedot liittymän käyttäjälle ja varmentajalle.

Liittymäkortin liikkeellelaskijoina toimivat TeliaSonera Finland Oyj:n matkaviestinoperaattorit Sonera ja Tele Finland.

1.4.4 Sulkupalvelu

Varmenteiden sulkupalvelu sulkee varmenteet, jotka varmenteen omistaja, varmentaja, rekisteröijä tai kortin liikkeellelaskija haluaa suljettavaksi ennen varmenteen voimassaoloajan päättymistä. Sulkupalveluna toimii TeliaSoneran asiakaspalvelu. Sulkupalvelun yhteystiedot on kerrottu tämän varmennuskäytännön alussa kappaleessa ”Yhteystiedot”

1.4.5 Hakemistopalvelu

Hakemistopalvelu on varmenteeseen luottaville tahoille tarkoitettu palvelu, josta ovat saatavilla varmentajan varmennepolitiikat ja –käytännöt, varmenteet, sulkulista (CRL) tai sulkutieto (OCSP) ja mobiilivarmenteet. Osa hakemistopalvelun tiedoista on julkisesti saatavilla ja osa on vain varmentajien ja Mobiilivarmenteeseen luottavien palveluntarjoajien saatavilla sen mukaisesti mitä kappaleessa 2.1 ”Tietojen julkaiseminen ja saatavuus” on kerrottu.

1.4.6 Varmenteen omistaja

Varmenteen omistaja on luonnollinen henkilö, jolle varmentaja on myöntänyt mobiilivarmenteen varmennuskäytäntönsä mukaisesti.

1.4.7 Varmenteeseen luottava osapuoli

Varmenteeseen luottava osapuoli on henkilö tai organisaatio, joka luottaa varmenteen tietoihin ja joka käyttää varmennetta varmenteen omistajan henkilöllisyyden todentamiseen tai varmenteen omistajan tekemän sähköisen allekirjoituksen todentamiseen.

1.5 Turvallisuusjärjestelyt

Turvallisuusjärjestelyt noudattavat määrityksiä dokumentissa TeliaSonera Production CPS, joka on saatavilla osoitteesta

http://repository.trust.teliasonera.com/

1.6 Varmenteen käyttäminen

Mobiilivarmennetta voidaan käyttää henkilön sähköiseen tunnistamiseen ja sähköiseen allekirjoitukseen. Mobiilivarmennetta voidaan käyttää erilaisissa sovelluksissa ja palveluissa, joiden palveluntarjoaja on tehnyt sopimuksen varmentajan kanssa.

1.7 Osapuolten vastuut ja velvollisuudet

Mobiilivarmennuspalvelun luottamusverkoston muodostavat varmennuspalvelun tuottamisesta keskinäisen sopimuksen tehneet varmentajat. Tekemänsä sopimuksen perusteella varmentaja on sitoutunut noudattamaan mobiilivarmennuspalvelun luottamusverkoston yhteistä varmennepolitiikkaa.

Varmentajalla on kokonaisvastuu varmennepalvelusta. Varmentaja vastaa, että varmennepolitiikan ja tämän varmennuskäytännön mukaisesti myönnettyihin varmenteisiin pätevät seuraavat ominaisuudet:

- Varmentaja on myöntänyt varmenteen ja hallinnoi niitä varmennepolitiikan ja tämän varmennuskäytännön mukaisesti
- Varmenteen omistajasta rekisteröidyt tiedot ovat oikein varmenteessa
- Varmentajan yksityiset avaimet on talletettu turvalliselle välineelle
- Varmentajan varmenne ja ajantasainen sulkuinformaatio on saatavissa hakemistopalvelusta vuoden jokaisena päivänä vuorokauden ympäri

Varmentajan kaikessa toiminnassa noudatetaan voimassa olevaa lainsäädäntöä, varmennepolitiikkaa ja varmennuskäytäntöä.

Varmentaja voi käyttää muita osapuolia varmennepalveluiden tuottamisessa. Varmentaja edellyttää muiden osapuolten kanssa tekemissään sopimuksissa näiltä varmennepolitiikassa ja varmennuskäytännössä asetettuja käytäntöjä, vastuita ja velvollisuuksia.

Varmennusorganisaation eri osapuoliin liittyvät vastuut ja velvollisuudet on kuvattu liitteessä 1 ”Varmennusorganisaation osapuolten vastuut ja velvollisuudet”.

Tarkemmin osapuolien vastuista ja velvollisuuksista sovitaan varmentajan ja palveluntarjoajien sekä varmentajan ja varmenteen hakijan välisissä sopimuksissa.

2 Yleiset ehdot

2.1 Tietojen julkaiseminen ja saatavuus

2.1.1 Varmentajan tietojen julkaiseminen

2.2 TeliaSonera Mobile ID CA v1

Sulkulistat ovat yleisesti saatavilla varmentajan LDAP-hakemistossa ja verkkosivuilla. Mobiilivarmennepalvelun sulkulista löytyy osoitteista

- **ldap://**crl-1.trust.teliasonera.com/cn=TeliaSonera%20Mobile%20ID%20CA%20v1, o=TeliaSonera,c=fi?certificaterevocationlist;binary
- **http://**crl-3.trust.teliasonera.com/teliasoneramobileidcav1.crl

Varmentajan varmenteen sulkulista löytyy osoitteista

- **ldap**://crl-1.trust.teliasonera.com/cn=TeliaSonera%20Root%20CA%20v1, o=TeliaSonera?certificaterevocationlist;binary
- **http**://crl-2.trust.teliasonera.com/teliasonerarootcav1.crl

Mobiilivarmenteet ovat varmentajan saatavilla varmentajan omissa tietokannoissa.

Seuraavat varmentajaa ja varmennepalvelua koskevat tiedot ovat julkisesti saatavilla Internetin kautta osoitteessa https://repository.trust.teliasonera.com

- voimassa oleva varmennepolitiikka (CP) ja sen edelliset julkaistut versiot
- voimassa oleva varmennuskäytäntö (CPS) ja sen edelliset julkaistut versiot
- henkilötietolain mukainen rekisteriseloste
- varmentajan varmenteet

2.3 TeliaSonera Mobile ID CA v2

Sulkulistat ovat yleisesti saatavilla varmentajan verkkosivuilla. Mobiilivarmennepalvelun sulkulista tai sulkutieto löytyy osoitteista

- http://crl-3.trust.teliasonera.com/teliasoneramobileidcav2.crl
- http://ocsp.trust.teliasonera.com

Varmentajan varmenteen sulkulista löytyy osoitteista

- http://crl-3.trust.teliasonera.com/teliasonerarootcav1.crl
- http://ocsp.trust.teliasonera.com

Mobiilivarmenteet ovat varmentajan saatavilla varmentajan omissa tietokannoissa.

Seuraavat varmentajaa ja varmennepalvelua koskevat tiedot ovat julkisesti saatavilla Internetin kautta osoitteessa https://repository.trust.teliasonera.com/

- voimassa oleva varmennepolitiikka (CP) ja sen edelliset julkaistut versiot
- voimassa oleva varmennuskäytäntö (CPS) ja sen edelliset julkaistut versiot
- henkilötietolain mukainen rekisteriseloste
- varmentajan varmenteet

2.4

2.4.1 Sulkulistojen julkaisutiheys

Sulkulista julkaistaan vähintään tunnin välein ja se on voimassa 24 tuntia julkaisuhetkestä eteenpäin. Sulkulista päivitetään aina viipymättä muutoksen jälkeen. Varmentajan OCSP-palvelusta on saatavilla ajantasainen sulkutieto.

2.4.2 Tietojen saatavuus

Sulkulista ja OCSP-sulkutieto ovat kaikkien niitä tarvitsevien saatavilla varmentajan hakemistossa. Ne ovat saatavilla 24 tuntia päivässä, 7 päivää viikossa, lukuun ottamatta tarpeellisia huoltokatkoksia. Varmentaja ei vastaa käyttäjän kokemasta palvelun saatavuudesta, mikäli vika tai katkos ilmenee varmentajasta riippumattomissa järjestelmissä tai palveluissa.

Varmenteet julkaistaan hakemistossa, jonne vain varmentajan järjestelmillä on pääsy.

Varmennepolitiikka ja varmennuskäytäntö ovat julkisesti saatavilla olevia dokumentteja, jotka ovat jaossa varmentajan verkkosivulla.

2.4.3 Tietovarastot

Varmentajan julkaisemat tiedot ovat saatavilla varmentajan verkkosivulla. Varmenteet ovat talletettuina varmentajien luottamuksellisiin tietovarastoihin. Varmentajan tiedot arkistoidaan varmennepolitiikan vaatimusten ja tämän varmennuskäytännön mukaisesti.

2.5 Auditointi

2.5.1 Varmentajan itse suorittamat tarkastukset

Varmentaja valvoo varmennusjärjestelmän lokitietoja seuraamalla sekä satunnaisin tarkastuksin oman sekä toimittajiensa ja rekisteröijiensä toimitilojen, järjestelmien ja toiminnan vaatimustenmukaisuutta ja tietoturvallisuutta. Sisäisessä auditoinnissa voidaan käyttää hyväksi myös Soneran yritysturvallisuusyksikön resursseja. Mikäli varmentajan suorittamissa tarkastuksissa ilmenee puutteita, varmentaja ryhtyy tai edellyttää toimittajiensa ja rekisteröijien ryhtyvän tarvittaviin toimenpiteisiin niiden korjaamiseksi.

2.5.2 Ulkopuolisen auditoijan suorittama auditointi

Varmentajan toiminta auditoidaan vähintään vuosittain ulkopuolisen auditoijan toimesta.

2.5.2.1 Auditoija ja vaadittu pätevyys

Varmentajan hyväksymän auditoijan tulee olla varmentajasta riippumaton, tunnettu ja hyvämaineinen alan yritys. Auditoijalta edellytetään riittävää asiantuntemusta ja perehtyneisyyttä PKI-teknologioiden hyödyntämiseen ja varmennustoiminnan auditointiin.

2.5.2.2 Auditoinnin sisältö

Auditoinnissa selvitetään, toimiiko varmentaja varmennepolitiikan ja varmennuskäytännön mukaisesti ja noudattaako se määrittelemäänsä tietoturvapolitiikkaa. Auditoinnissa käydään

läpi kaikki varmennustoiminnan prosessit, varmentajan käyttämät järjestelmät sekä organisaatio. Auditointi kattaa myös varmentajan alihankkijoiden ja rekisteröijien toiminnan. Ulkopuolinen auditointi teetetään säännöllisesti sekä aina kun prosesseihin tai järjestelmiin tehdään merkittäviä muutoksia.

2.5.2.3 Toimenpiteet puutteen havaitsemisen jälkeen

Auditoija toimittaa raportin auditoinnin tuloksista varmentajalle. Mikäli toiminnassa on havaittu puutteita, varmentaja ryhtyy toimenpiteisiin niiden korjaamiseksi.

Varmentajan omassa toiminnassa havaittujen puutteiden korjaamiseksi laaditaan suunnitelma, johon sisältyvät korjausaikataulut määräytyvät puutteen vakavuuden ja korjaustoimenpiteen vaatiman ajan perusteella.

Mikäli puutteita on havaittu varmentajan alihankkijoiden toiminnassa, näistä tiedotetaan asianomaisille ja alihankkijaa edellytetään korjaamaan puutteet kohtuullisen ajan kuluessa.

Mikäli auditoinnista seuraa muutostarpeita varmennuskäytäntöön, näistä tiedotetaan kyseisen dokumentin kappaleessa 8 ”Varmennuskäytännön hallinnointi”. kuvattujen menettelyjen mukaisesti.

2.5.2.4 Tuloksista tiedottaminen

Auditoijan antama raportti on tarkoitettu varmentajan sisäiseen käyttöön. Varmentaja voi tiedottaa alihankkijalle tämän oman toiminnan auditoinnin tuloksista. Raportista voidaan tiedottaa kolmansille osapuolille tai se voidaan julkaista osittain tai kokonaan varmentajan organisaation johdon päätöksellä.

2.6 Tietojen luottamuksellisuus ja julkisuus

Varmennejärjestelmän tiedot ovat luottamuksellisia, elleivät ne perustu henkilötietolain, tai sähköisistä allekirjoituksista annetun lain säännöksiin tietojen luovuttamisesta tai varmennepolitiikassa määriteltyihin lain sallimiin tarkoituksiin.

Viranomaisille luovutettavat tiedot määritellään voimassaolevan lainsäädännön mukaisesti. Varmennejärjestelmän tietoja ei luovuteta muihin tarkoituksiin.

3 Varmentajan ja varmenteen hakijan yksilöinti

3.1 Varmentajan nimeämiskäytäntö TeliaSonera Mobile ID CA v1

Varmentajalla on yksikäsitteinen X.501:n mukainen Distinguished Name (DN) - nimi, joka löytyy varmentajan varmenteesta Subject-kentästä, sekä kaikkien Varmentajan myöntämien varmenteiden Issuer - kentästä. Varmentajan nimi koostuu seuraavista attribuuteista:

Attribuutti	**Sisältö**
commonName (CN)	TeliaSonera Mobile ID CA v1
Organization (O)	TeliaSonera Finland Oyj
Country (C)	FI

3.2 Varmentajan nimeämiskäytäntö TeliaSonera Mobile ID CA v2

Varmentajalla on yksikäsitteinen X.501:n mukainen Distinguished Name (DN) - nimi, joka löytyy varmentajan varmenteesta Subject-kentästä, sekä kaikkien Varmentajan myöntämien varmenteiden Issuer - kentästä. Varmentajan nimi koostuu seuraavista attribuuteista:

Attribuutti	**Sisältö**
commonName (CN)	TeliaSonera Mobile ID CA v2
Organization (O)	TeliaSonera Finland Oyj
Country (C)	FI

3.3 Varmenteen hakijan nimeäminen

Varmenteen hakijan yksikäsitteisenä nimenä käytetään varmenteen Subject-kentässä X.501:n mukaista Distinguished Name (DN) –nimeä, ja sisältää aina seuraavat attribuutit:

Attribuutti	**Sisältö**
commonName (CN)	Varmenteen hakijan nimi seuraavassa muodossa: Sukunimi Etunimet SaTu tai Etunimet Sukunimi Satu
givenName (GN)	Varmenteen hakijan etunimet
surName (SN)	Varmenteen hakijan sukunimi
serialNumber (SN)	Sähköinen asiointitunnus (SaTu)

Varmentajan teknisillä palveluilla (OCSP, Time-Stamping) voi olla käytössään tästä poikkeava DN-arvo jossa on vain CN-arvo.

3.3.1 Nimien merkitykset ja tulkinta

commonName-attribuutti sisältää varmenteen hakijan etunimet ja sukunimen. Attribuutissa määritellään varmenteen hakijan rekisteröity nimi, joka on tallennettu Väestörekisterikeskuksen väestötietojärjestelmään. Lempinimiä tai pseudonyymejä ei käytetä. Lisäksi attribuutti sisältää varmenteen hakijan sähköisen asiointitunnuksen (SaTu), joka on Väestörekisterikeskuksen luoma numeroista ja tarkistusmerkistä muodostettu tietojoukko, jonka avulla yksilöidään Suomen kansalaiset ja kotikuntalain mukaisesti Suomessa vakinaisesti asuvat ulkomaalaiset, jotka on merkitty väestötietojärjestelmään.

3.3.2 Nimien yksikäsitteisyys

Varmenteessa olevan Subject-kentän tulee olla yksikäsitteinen kaikille varmentajan luomille käyttäjäidentiteeteille ja noudattaa yksikäsitteisyyden suhteen X.500-standardia. Yksikäsitteisyys tarkoittaa, että varmentaja ei myönnä eri henkilöille varmenteita, joissa olisi identtiset kenttien arvot. Varmentaja voi kuitenkin myöntää samalle henkilölle useita varmenteita, joissa Subject-kentän arvot ovat samat.

3.4 Avainparin uusiminen varmenteen sulkemisen jälkeen

Avainparin uusiminen johtaa aina uuteen varmenteeseen uusilla avaimilla. Vanha varmenne ja avainpari pysyvät suljettuina ja uusi varmenne haetaan kuten varmennetta ensikertaa haettaessa.

4 Toiminnalliset vaatimukset

4.1 Varmenteen hakeminen

Mobiilivarmenne voidaan myöntää Suomen kansalaiselle tai kotikuntalain (201/1994) mukaisesti Suomessa vakinaisesti asuvalle ulkomaalaiselle, jonka henkilötiedot on talletettu Väestörekisterikeskuksen Väestötietojärjestelmään.

Varmenteen hakija voi hakea mobiilivarmennetta liittymäkortin liikkeellelaskijan paikallisissa asiointipisteissä tai itsepalveluportaalissa.

Varmenteen hakeminen paikallisessa asiointipisteessä	Mobiilivarmenteen käyttöön tarvitaan sitä tukeva liittymäkortti. Jos varmenteen hakijalla ei tällaista ennestään ole, toimitetaan uusi liittymäkortti mobiilivarmennepalvelun tilauksen yhteydessä. Mobiilivarmennepalvelu voidaan tilata ja liittymäkortti vaihtaa etukäteen tai samalla kertaa varmennetta haettaessa kappaleen 4.2.1 ”Tunnistusvälineen toimittaminen” mukaisesti. Liittymän käyttäjän tulee henkilökohtaisesti hakea mobiilivarmennepalvelua ja siihen liittyvää mobiilivarmennetta liittymäkortin liikkeellelaskijan paikallisessa asiointipisteessä. Jos liittymän käyttäjä on eri kuin liittymän tilaaja eikä liittymän tilaaja ole aikaisemmin tilannut mobiilivarmennepalvelua liittymään, niin myös liittymän tilaajan tulee olla henkilökohtaisesti läsnä varmennetta haettaessa. Paikallisen asiointipisteen rekisteröintivastaava hakee liittymän tiedot liittymäkortin liikkeellelaskijan järjestelmästä ja tunnistaa liittymän tilaajan henkilöllisyyden kappaleen 4.2 ”Varmenteen hakijan tunnistaminen” mukaisesti. Ennen varmenteen myöntämistä rekisteröintivastaava antaa varmenteen hakijalle mobiilivarmennepalvelun ehdot, joissa on kuvattu kummankin osapuolen oikeudet ja velvollisuudet. Varmenteen hakijan tulee hyväksyä varmenteen käyttöön liittyvät ehdot, vahvistaa henkilötietojen oikeellisuus
Varmenteen hakeminen itsepalveluportaalissa	Mobiilivarmenteen käyttöön tarvitaan sitä tukeva liittymäkortti. Jos varmenteen hakijalla ei tällaista ennestään ole, tulee mobiilivarmennepalvelu ja sen mukana liittymäkortti tilata ennen varmenteen hakemista kappaleen 4.2.1 ”Tunnistusvälineen toimittaminen” mukaisesti. Varmenteen hakija kirjautuu itsepalveluportaaliin ja aloittaa varmenteen rekisteröinnin. Varmentajan rekisteröintijärjestelmä tunnistaa varmenteen hakijan vahvalla sähköisellä tunnistamisella kappaleen 4.2 ”Varmenteen hakijan tunnistaminen” mukaisesti. Ennen varmenteen myöntämistä varmenteen hakijan tulee hyväksyä järjestelmässä varmenteen käyttöön liittyvät ehdot, vahvistaa henkilötietojen oikeellisuus

4.2 Varmenteen hakijan tunnistaminen

Mobiilivarmenteen hankkimisen edellytyksenä on se, että asiakkaalla on suomalainen henkilötunnus. Asiakkaan henkilöllisyys tulee voida tunnistaa luotettavasti ja henkilötunnus tulee voida liittää siihen luotettavasti. Mobiilivarmenteen hakija tunnistetaan joko henkilökohtaisesti rekisteröijän asiointipisteessä tai käyttäen vahvaa sähköistä tunnistamista.

Varmenteen hakeminen paikallisessa asiointipisteessä	Rekisteröintivastaava todentaa henkilökohtaisesti varmenteen hakijan henkilöllisyyden rekisteröitymisen yhteydessä suomalaisen viranomaisen myöntämästä ja voimassaolevasta henkilöllisyyden luotettavasti osoittavasta asiakirjasta. Näitä ovat: - Voimassa oleva Suomen passi tai Suomen poliisin myöntämä henkilökortti - Suomen poliisin 1 päivän lokakuuta 1990 jälkeen myöntämä voimassa oleva ajokortti, jollei se ole saatu vaihtamalla ulkomaalainen ajokortti suomalaiseen Jos varmenteen hakijan henkilöllisyyttä ei voida luotettavasti todentaa, hakijan henkilöllisyyden todentamisen tekee poliisi. Poliisin tekemästä tunnistamisesta aiheutuu varmenteen hakijalle poliisin hinnaston mukainen maksu.
Varmenteen hakeminen itsepalveluportaalissa	Varmenteen hakijan henkilöllisyys tarkistetaan rekisteröinnin yhteydessä liittymäkortin liikkeellelaskijan itsepalveluportaalissa käyttäen vahvaa sähköistä tunnistamista, jonka tarjoaja on tehnyt lain vaatiman ilmoituksen Viestintävirastolle ja jonka kanssa varmentaja on tehnyt sopimuksen tunnistuspalvelun tarjoajan tekemään ensitunnistamiseen luottamisesta. Tuetut vahvat sähköiset tunnistuspalvelut löytyvät osoitteesta: www.sonera.fi/soneraid/tunnistusmemetelmatverkkopalvelussa

4.2.1 Tunnistusvälineen toimittaminen

Tunnistusväline muodostuu liittymäkortista yksityisine avaimineen ja niihin liittyvistä tunnusluvuista. Mobiilivarmenteen käyttöön tarvitaan sitä tukeva liittymäkortti eikä varmennetta voi hakea ennen kuin hakijalla on sellainen. Vain liittymän tilaaja voi tilata omistamiinsa liittymiin mobiilivarmennepalvelun ja tarvittavan liittymäkortin, joka toimitetaan liittymän tilaajalle henkilökohtaisesti asiointipisteessä tai postitse.

Liittymäkortti toimitetaan asiakkaalle ilman rekisteröityjä varmenteita.

Mobiilivarmennepalvelun tilaaminen paikallisissa asiointipisteessä	Liittymäkortti annetaan mobiilivarmennepalvelun tilaamisen yhteydessä liittymän tilaajalle henkilökohtaisesti liittymäkortin liikkeellelaskijan paikallisessa asiointipisteessä. Tämä voi tapahtua joko samalla käynnillä varmenteen rekisteröinnin yhteydessä tai ennen sitä. Yksityisten avainten tunnusluku luodaan rekisteröinnin yhteydessä tijaajan asettamaksi arvoksi.

Mobiilivarmennepalvelun tilaaminen itsepalveluportaalissa	Liittymän tilaaja voi tilata mobiilivarmennepalvelun omalle tai muille omistamilleen liittymille itsepalveluportaalissa. Liittymän tilaaja määrittelee liittymät ja niiden käyttäjät, joille mobiilivarmennepalvelu tilataan. Liittymäkortti toimitetaan postitse liittymän tilaajan määrittelemään osoitteeseen.

4.3 Varmenteen myöntäminen

Varmentaja myöntää mobiilivarmenteen hyväksyessään varmennehakemuksen. Varmennehakemus voidaan hyväksyä, jos varmenteen hakijalla on mobiilivarmennetta tukeva liittymäkortti, varmenteen hakija tunnistetaan onnistuneesti, hän on hyväksynyt varmenteen käyttöön liittyvät ehdot ja hänet on rekisteröity Väestörekisterikeskuksen väestötietojärjestelmään.

Haettaessa varmennetta paikallisessa asiointipisteessä varmennehakemuksen hyväksyy ja sähköisesti allekirjoittaa paikallinen rekisteröintivastaava. Itsepalveluportaalissa hyväksynnän tekee varmentajan rekisteröintijärjestelmä hakijan puolesta sen jälkeen kun hakija on onnistuneesti tunnistettu..

Varmentaja vastaa myöntäessään mobiilivarmenteen, että sen tietosisältö on hakemuksen mukainen sen luovuttamishetkellä.

4.4 Varmenteen luominen

Varmentajan varmennusjärjestelmä hyväksyy vain rekisteröintijärjestelmästä tulevat varmennepyynnöt, joiden alkuperä tunnistetaan rekisteröintijärjestelmän varmenteen perusteella. Varmennusjärjestelmä luo mobiilivarmenteen ja allekirjoittaa sen varmentajan yksityisellä avaimella.

Varmenteen hakijan tiedot varmenteelle haetaan hakijan henkilötunnuksen perusteella Väestörekisterikeskuksen väestötietojärjestelmästä. Jos hakijalla ei ole entuudestaan ollut aktiivista sähköistä asiointitunnusta (SaTu), aktivoi Väestörekisterikeskus sen rekisteröinnin yhteydessä ja julkaisee sen omassa hakemistossaan.

Myöntämisprosessin yhteydessä varmenteen hakija käynnistää SIM-kortilla avaingeneroinnin, asettaa avaimia suojaavan PIN-koodin ja todistaa pitävänsä hallussa puhelinta jossa avainpari on allekirjoittamalla yksityisellä avaimella satunnaisen vasteen (Proof-Of-Possession). Hän saa tiedon myönnetystä varmenteesta matkapuhelimeensa ja varmenne julkaistaan varmentajan yksityiseen varmennehakemistoon.

4.5 Varmenteen voimassaolon päättyminen ja sulkeminen

4.5.1 Varmenteen sulkemisen edellytykset

Mobiilivarmenne tulee sulkea seuraavissa olosuhteissa:

- Varmenteen omistaja pyytää varmenteen peruuttamista (mistä tahansa syystä)
- Varmenteen omistajan yksityinen avain on tai sen epäillään olevan kadonnut, anastettu tai paljastunut
- Mobiilivarmennetta vastaava liittymä suljetaan

- Varmenteen omistaja käyttää yksityistä avaintaan vastoin sen käyttötarkoitusta
- Varmennetta ei ole myönnetty asianomaisen varmennepolitiikan tai tämän varmennuskäytännön mukaisesti
- Varmenteen tiedoissa on virhe
- Varmenteen omistaja tai liittymän tilaaja rikkoo oleellisesti varmentajan kanssa tehtyä sopimusta
- Varmenteen omistaja kuolee

Varmenne voidaan sulkea myös seuraavissa olosuhteissa

- Varmenteen omistaja tai liittymän tilaaja rikkoo varmentajan kanssa tehtyä sopimusta
- Varmenteen peruuttamiseen on joku muu erityinen syy, esimerkiksi kryptografisten hyökkäysmenetelmien kehitys.

Mobiilivarmenteen pysyvän sulkemisen sijasta matkapuhelinliittymä voidaan pyynnöstä sulkea toistaiseksi, jos varmenteen omistaja on menettänyt liittymäkortin hallinnan, mutta yksityisen avaimen tai aktivointitiedon paljastumista ei ole syytä epäillä (esim. matkapuhelin on kadonnut ja sen löytymistä pidetään todennäköisenä). Matkapuhelinliittymän ollessa tilapäisesti suljettu liittymäkortille tallennettujen yksityisten avainten käyttö estyy.

Sulkupyyntö on tehtävä välittömästi sen jälkeen, kun epäilys väärinkäytön mahdollisuudesta on syntynyt.

4.5.2 Sulkupyynnön tekijä

Mobiilivarmenteen sulkupyynnön tekee ensisijaisesti varmenteen omistaja. Mikäli pyytäjä on eri henkilö kuin suljettavan varmenteen omistaja, tunnistetaan omistajan lisäksi myös pyytäjä. Sulkupyynnön voi tehdä myös varmentaja, kortin liikkeellelaskija tai viranomainen.

Liittymän omistaja voi pyytää omistamansa liittymän sulkemista. Kun liittymä suljetaan, suljetaan automaattisesti siihen liittyvät varmenteet,

4.5.3 Sulkutapahtuma

Mobiilivarmenne voidaan sulkea soittamalla sulkupalvelunumeroon. Sulkupalvelun yhteystiedot on kerrottu tämän varmennuskäytännön alussa kappaleessa ”Yhteystiedot” Sulkupalvelunumero ottaa sulkupyyntöjä vastaan 24 tuntia vuorokaudessa 7 päivänä viikossa.

Sulkupalvelu tunnistaa sulkupyynnön tekijän kysymällä tältä määrättyjä tietoja ja vertaamalla näitä tietoja varmenteen omistajasta rekisteröinnin tai muissa yhteyksissä tallennettuihin tietoihin.

Sulkupalveluvastaava sulkee varmenteen viipymättä, kun pyyntö on vastaanotettu, pyytäjä tunnistettu ja pyyntö todettu luvalliseksi.

Liittymän omistaja voi irtisanoa liittymän tai mobiilivarmennepalvelun ottamalla yhteyttä asiakaspalveluun tai käymällä paikallisessa asiointipisteessä. Liittymän voi lisäksi irtisanoa itsepalveluportaalissa. Liittymän omistaja tunnistetaan asiakaspalvelussa kuten varmennetta suljettaessa. Itsepalveluportaalissa liittymän omistaja tunnistetaan salasanalla ja paikallisessa asiointipisteessä henkilöllisyystodistuksesta, Liittymäkortin liikkeellelaskijan järjestelmä lähettää automaattisen varmenteen sulkupyynnön varmentajan järjestelmään kun liittymä on suljettu.

Joissain tilanteissa, joissa yksityiseen avaimeen kohdistuu tunnistettu väärinkäytön riski tai on ilmeistä, että avainta ei voida oikeutetusti käyttää, voi olla tarpeen peruuttaa varmenne tai tilapäisesti sulkea liittymä jonkun muun kuin edellä mainittujen pyynnöstä. Tällöin peruuttamispyynnön oikeellisuuden selvittäminen voi vaatia muita tunnistamistapoja. Tapauksissa, joissa luotettavaa tunnistusta ei voida tehdä välittömästi, Varmentaja saattaa kuitenkin asettaa etusijalle varmenteen peruuttamisen riskien vähentämiseksi.

Peruuttamisen voi panna alulle myös varmentaja perustuen minkä tahansa osapuolen esille tuomaan luotettavaan ja pätevään tietoon, joka viittaa kappaleen 4.5.1 Varmenteen sulkemisen edellytykset mukaisiin peruuttamisolosuhteisiin.Varmentaja esimerkiksi sulkee varmenteet aina silloin, kun se on saanut tiedon varmenteen omistajan kuolemasta, jolloin varmentaja myös tekee sulkemista koskevan ilmoituksen kuolleen varmenteen omistajan oikeudenomistajille.

4.5.4 Sulkutapahtuman ajoitus

Mobiilivarmenteen sulkeminen toteutetaan viipymättä sulkupyynnön yhteydessä.

4.5.5 Varmenteen sulkeminen tilapäisesti

Mobiilivarmenne suljetaan aina pysyvästi, mutta matkapuhelinliittymä voidaan pyynnöstä sulkea toistaiseksi, jolloin liittymäkortille tallennettujen yksityisten avainten käyttö estyy.

4.5.6 Tilapäisen sulkupyynnön tekijä

Matkapuhelinliittymän tilapäistä sulkemista voivat pyytää liittymän tilaaja tai käyttäjä.

4.5.7 Tilapäisen sulkupyynnön tekemistapa

Pyynnöt koskien matkapuhelinliittymien sulkemista toistaiseksi vastaanotetaan liittymäkortin liikkeellelaskijan asiakaspalvelussa. Matkapuhelin suljetaan tilapäisesti viipymättä, kun pyyntö on vastaanotettu, pyytäjä tunnistettu ja pyyntö todettu luvalliseksi. Matkapuhelinliittymän tilapäisen sulkupyynnön tekijä tunnistetaan samalla tapaa kuin varmennetta suljettaessa.

Varmentaja voi lisäksi sulkea varmenteen, mikäli katsoo olosuhteiden tätä vaativan.

4.5.8 Tilapäisen sulun aikarajoitukset

Matkapuhelinliittymän tilapäinen sulku on voimassa kunnes se peruutetaan.

4.5.9 Tilapäisen sulun purkaminen

Pyyntö tilapäisesti suljetun matkapuhelinliittymän käyttöön palauttamisesta vastaanotetaan puhelimitse liittymäkortin liikkeellelaskijan asiakaspalvelussa. Pyyntö voidaan hyväksyä vain siltä henkilöltä, jolta otettiin vastaan liittymää koskeva tilapäinen sulkupyyntö. Pyynnön hyväksynnän perusteena käytetään salasanaa, joka on sovittu asiakkaan kanssa ja tallennettu liittymää suljettaessa.

Matkapuhelinliittymän käyttöön palauttamista pyytäneen henkilön nimi, käytetty salasana sekä matkapuhelinliittymä palauttamisaika tallennetaan.

4.5.10 Sulkulistan julkaisutiheys

Sulkulistapalvelu toteutetaan julkaisemalla Varmentajan sähköisesti allekirjoittamat sulkulistat julkisessa hakemistossa. Seuraavia sääntöjä noudatetaan:

- Uusi sulkulista julkaistaan hakemistossa aina viipymättä sulkupyynnön hyväksynnän jälkeen tai vähintään yhden (1) tunnin välein.
- Jokainen sulkulista on voimassa kaksikymmentäneljä (24) tuntia.

Yhdellä ajan hetkellä voi olla yhtä aikaa olemassauseita voimassa olevia sulkulistoja. Näistä viimeisimmäksi julkaistu sisältää ajantasaisimmat tiedot.

Järjestelmäpäivityksissä ja muissa poikkeavissa tilanteissa varmentaja voi julkaista sulkulistoja eri julkaisutiheyksillä ja pidennetyillä voimassaoloajoilla.

4.5.11 Sulkulistan jakelupisteet

Sulkulista julkaistaan pisteissä, joihin on viittaukset varmenteen ”CRL distribution points” -kentässä. Sulkulistojen osoitteet on kerrottu tämän varmennuskäytännön kappaleessa 2.1.1

Sulkulista on saatavilla hakemistosta 24 tuntia päivässä, 7 päivää viikossa. Varmentaja ei vastaa käyttäjän kokemasta palvelun saatavuudesta, mikäli vika tai katkos ilmenee varmentajasta riippumattomissa järjestelmissä tai palveluissa.

4.5.12 Suorakäyttöinen varmenteen tilan tarkistaminen

Varmentajalla on käytössä OCSP-palvelu. Palvelu on käytössä 24 tuntia päivässä, 7 päivää viikossa. Varmentaja ei vastaa käyttäjän kokemasta palvelun saatavuudesta, mikäli vika tai katkos ilmenee varmentajasta riippumattomissa järjestelmissä tai palveluissa.

4.6 Varmenteen uusiminen

Jos varmenne ei ole vanhentunut eikä se ole sulkulistalla, voi varmenteen omistaja uusia varmenteen itsepalveluportaalissa tunnistautumalla olemassa olevalla mobiilivarmenteella. Varmenteen uusimisen yhteydessä luodaan liittymäkortilla uudet avainparit.

Jos varmenne on mennyt vanhaksi, varmenne on suljettu, varmenteen omistaja on hukannut yksityisen avaimen tunnusluvun tai jos ensitunnistaminen halutaan uusia, tapahtuu varmenteen uusiminen pääosin samalla tavalla kuin varmennetta ensimmäistä kertaa haettaessa. Erona on, että liittymäkorttia ei tarvitse vaihtaa.

Vanha voimassa oleva varmenne suljetaan automaattisesti varmenteen uusimisen yhteydessä.

4.7 Järjestelmän valvonta

4.7.1 Tallennettavat tiedot

Varmentaja tallentaa automaattisesti tai manuaalisesti seuraavat oleelliset varmennustoimintaan liittyvät tiedot:

Varmentajan avaimen elinkaareen liittyvät tiedot

- avaimen luonti, varmuuskopiointi, palautus ja tuhoaminen
- salausteknisen laitteen elinkaareen liittyvät ylläpitotapahtumat

Varmentajan ja varmenteen omistajien varmenteiden elinkaareen liittyvät ylläpitotapahtumat

- varmennehakemukset ja -pyynnöt, varmenteiden uusimispyynnöt jo käytössä olleille tai uusille avaimille
- varmenteiden peruuttamiset
- varmenteiden luomiset
- sulkulistojen luomiset

Tietoturvallisuuden ylläpitoon liittyvät tapahtumat

- Varmentajan henkilöstön suorittamat varmennusjärjestelmään tai turvajärjestelmiin kohdistuvat toimenpiteet, mm. ohjelmistojen, laitteiden ja päivitysten asennukset, palautukset, järjestelmien alasajot ja uudelleenkäynnistykset sekä järjestelmän asetusten muutokset
- järjestelmien kaatumiset, laitteistoviat ja muut poikkeamat järjestelmissä
- reitittimien ja palomuurien ja hyökkäyksenhavaitsemisjärjestelmien tapahtumat
- kulunvalvontatapahtumat varmennusjärjestelmän tiloihin.

Tallennettaviin tietoihin sisältyy tietojen tyyppi, päivämäärä ja kellonaika sekä automaattisesti tallentuviin lokeihin juokseva numero ja lokia tuottavan järjestelmän tunniste.

Rekisteröintipisteessä tallennetaan:

- Tiedot hakijan ensitunnistamisesta sekä siinä käytetystä tunnistamisasiakirjasta
- Varmenteen hakijan kanssa tehty mobiilivarmennepalvelusopimus

Sulkupalvelussa tallennetaan peruuttamispyyntöihin liittyen:

- peruuttamista pyytävän henkilön tiedot
- pyynnön vastaanottoaika
- tiedot varmenteesta, joka halutaan peruuttaa.

Mobiilivarmenteen käyttöön liittyen tallennetaan:
- tiedot tunnistusvälineen käyttöön mahdollisesti liittyvistä estoista ja käyttörajoituksista
- yksittäisen tunnistustapahtuman ja sähköisen allekirjoittamisen tapahtuman todentamiseksi tarvittavat tiedot

4.7.2 Lokitietojen seuranta

Merkittäviä turvallisuuteen ja toimintaan liittyviä lokeja seurataan säännöllisesti varmentajan henkilöstön toimesta.

Järjestelmien tuottamien hälytysten perusteella suoritetaan lokien läpikäyntiä epäilyttävien tai poikkeavien tapahtumien selvittämiseksi.

4.7.3 Lokitietojen säilytysaika

Varmennusjärjestelmän lokitietoja säilytetään vähintään vuoden ajan niiden syntymisestä. Varmentajan muiden järjestelmien tuottamien lokitietojen säilytysaika vaihtelee riippuen järjestelmän ja lokin kriittisyydestä, lokitapahtumien määrästä sekä lain vaatimuksista.

Lokitietoja voidaan siirtää myös erilliselle lokipalvelimelle säilytettäväksi ja keskeiset tiedot arkistoidaan kappaleessa 4.8.2 ”Arkistojen säilytysaika” mainituksi ajaksi. Järjestelmästä riippuen lokitieto viedään sellaisenaan tai prosessoituna toiselle tallennusmedialle arkistointia varten.

4.7.4 Lokitietojen suojaus

Manuaalisesti tallennettavat lokit sekä varmentajan järjestelmien automaattisesti tuottamat lokit on suojattu muuttamiselta, tuhoamiselta ja oikeudettomalta lukemiselta järjestelmien käyttövaltuushallinnalla ja kulunvalvonnalla.

Varmennusjärjestelmän lokitiedot on suojattu digitaalisella allekirjoituksella.

4.7.5 Lokitietojen varmistus

Varmennusjärjestelmän lokitiedoista otetaan säännöllisesti erikseen määriteltyjen aikataulujen mukaisesti varmuuskopiot.

Muiden varmentajan järjestelmien tuottamien lokitietojen varmistuskäytäntö riippuu järjestelmästä ja lokitietojen kriittisyydestä. Oleellisimmista lokitiedoista otetaan säännöllisesti varmuuskopiot.

4.7.6 Lokitietojen keruujärjestelmä

Varmentajan järjestelmät tukevat lokitietojen keräystä. Tietyt tuotantojärjestelmälle tehtävät hallintatapahtumat, esim. järjestelmän muutokset ja päivitykset sekä varmentajan avaimiin liittyvät hallintatapahtumat kirjataan käsin erilliseen lokiin.

Varmentajan järjestelmissä automaattisesti syntyvät lokitiedot tallennetaan sovellus-, verkkolaite- ja käyttöjärjestelmätasolla. Manuaaliset lokit tuotetaan pöytäkirjoina fyysisessä tai sähköisessä muodossa varmentajan henkilöstön toimesta.

4.7.7 Järjestelmien haavoittuvuustestaukset

Varmentaja testaa säännöllisesti kriittisten järjestelmiensä haavoittuvuutta ulkopuolisten suorittamien tunkeutumisyritysten varalta. Testaustulosten perusteella päivitetään tarvittaessa palomuurien ja muiden järjestelmien konfiguraatioita sekä toimintapolitiikkoja ja käytäntöjä.

4.8 Varmenteisiin liittyvien tietojen arkistointi

4.8.1 Tallennettava aineisto

Varmentaja arkistoi vähintään alla olevat tiedot:

1) yksittäisen tunnistustapahtuman ja sähköisen allekirjoittamisen tapahtuman todentamiseksi tarvittavat tiedot
2) tarvittavat tiedot hakijan ensitunnistamisesta sekä siinä käytetystä asiakirjasta
3) tiedot tunnistusvälineen käyttöön mahdollisesti liittyvistä estoista ja käyttörajoituksista
4) varmenteen tietosisältö
5) varmenteen hakijan kanssa tehty mobiilivarmennepalvelusopimus
6) varmennusjärjestelmän tuottamat lokit sekä manuaalisesti syntyvät varmennusjärjestelmään kohdistuvista toimenpiteistä tehdyt lokit
7) sulkupalvelun vastaanottamat varmenteiden peruuttamispyynnöt,
8) kaikki julkaistut varmennepolitiikkaversiot,
9) kaikki varmentajan julkaisemat varmennuskäytäntöversiot,
10) raportit ulkopuolisista auditoinneista.

Tietoja voidaan arkistoida sekä sähköisessä muodossa että fyysisinä dokumentteina.

4.8.2 Arkistojen säilytysaika

Yksittäisen tunnistustapahtuman ja sähköisen allekirjoittamisen tapahtuman todentamiseksi tarvittavat tiedot (kappaleen 4.8.1 kohta 1) säilytetään viisi vuotta tunnistustapahtumasta ja kohtien 2 – 4 tiedot viisi vuotta varmentajan ja varmenteen omistajan välisen asiakassuhteen päättymisestä. Muut yllämainitut arkistoitavat tiedot säilytetään vähintään 5 vuotta.

4.8.3 Arkistojen suojaus

Arkistot, jotka sisältävät varmennusjärjestelmän tuottamat varmenteiden luomiseen ja peruuttamiseen liittyvät tiedot sekä itse varmenteet, sijaitsevat kulunvalvonnalla suojatuissa paloturvallisissa tiloissa ja ne on suojattu sähköisellä allekirjoituksella. Samoissa tiloissa arkistoidaan myös järjestelmän muutostiedot ja palvelutapahtumat sisältävät arkistot.

Muiden varmentajan järjestelmien tuottamat arkistoitavat tiedot arkistoidaan kulunvalvonnalla suojatuissa tiloissa joko lukollisessa kaapissa tai kassakaapissa riippuen tiedon kriittisyydestä.

4.8.4 Arkistojen varmistusmenettelyt

Varmennusjärjestelmän tuottamista sähköisistä arkistotiedoista otetaan varmuuskopiot tiedon häviämisen tai tuhoutumisen varalta, jotta varsinaisen arkiston tuhoutuessa tiedot voidaan palauttaa varmuuskopioista. Varmuuskopiot varastoidaan fyysisesti erilliseen tilaan alkuperäisistä tiedoista.

4.8.5 Arkistotietojen hankinta- ja varmistusmenetelmät

Arkistotietoja säilytetään siten, että vain valtuutetut Varmentajan henkilöt voivat päästä niihin käsiksi. Arkistotietojen katseluun oikeutettuja ovat ne henkilöt, jotka suorittavat kappaleen 2.2 ”Auditointi” mukaista auditointia. Muutoin tietoja toimitetaan ainoastaan kirjalliseen pyyntöön perustuen Suomen lain sallimissa ja velvoittamissa rajoissa ja Soneran yritysturvallisuusyksikön valvonnassa.

Varmenteen haltijalle luovutetaan häntä itseään koskevia arkistotietoja. Tiedot luovutetaan henkilötietolaissa määritellyn tarkastusoikeuden rajoissa veloituksetta. Muutoin tiedon hakemisesta ja toimittamisesta veloitetaan kohtuulliset työmäärään perustuvat maksut.

Varmentaja huolehtii siitä, että sen arkistoista kulloinkin tarvittavat tiedot ovat haettavissa ja luettavissa koko arkiston säilytyksen ajan. Kappaleen 4.8.1 kohtien 1 – 4 tiedot siinäkin tapauksessa, että varmentajan toiminta keskeytyy tai päättyy.

4.9 Varmentajan avainten uusiminen

Varmentajalle luodaan uusi allekirjoitusavain ennen kuin käytössä olevan (vanhan) allekirjoitusavaimen käyttöaika varmenteiden allekirjoittamiseen päättyy. Uutta allekirjoitusavainta varten Varmentajalle luodaan myös uusi nimi, joka näkyy Varmentajan myöntämien varmenteiden ”Issuer”-kentässä.

Avainta käytetään varmenteiden allekirjoittamiseen korkeintaan niin kauan, että sillä myönnetyn viimeisenkin varmenteen voimassaoloaika on päättynyt, ennen kuin avaimen käyttöaika päättyy. Näin varmistetaan, että sulkulista voidaan aina allekirjoittaa samalla avaimella, jolla sille mahdollisesti päätyvät varmenteet on allekirjoitettu.

Mobiilivarmentajan avainten vaihtamisen yhteydessä tehdään seuraavat toimenpiteet:

a. varmentajalle luodaan uusi avainpari
b. juurivarmentaja luo varmentajan uudelle julkiselle avaimelle uuden varmenteen ja allekirjoittaa sen yksityisellä avaimellaan
c. kohdassa b) luotu uusi varmenne julkaistaan varmentajan hakemistoihin
d. uudet mobiilivarmenteet allekirjoitetaan uuden varmentajan uudella yksityisellä avaimella

e. vanhan varmentajan yksityistä avainta käytetään sulkulistojen julkaisuun kunnes sillä myönnetyn viimeisenkin varmenteen voimassaoloaika on päättynyt

Juurivarmentajan avainten vaihtamisen yhteydessä tehtävät toimenpiteet on kuvattu juurivarmentajan omassa varmennuskäytännössä.

4.10 Toiminnan jatkumisenhallinta ja poikkeustapausten käsittely

Toiminnan jatkuvuus on pyritty varmistamaan kahdentamalla tuotantojärjestelmä, jolloin laitevian tapauksessa tuotanto siirtyy varalaitteelle. Ohjelmistovian tapauksessa suoritetaan ohjelmiston uudelleenasennus. Tiedon korruptoituessa tiedot palautetaan varmuuskopiolta. Kriittisimmistä tiedoista otetaan varmuuskopio vähintään 4 kertaa viikossa.
Poikkeus- ja vaaratilanteissa varmentaja noudattaa jatkuvuussuunnitelmassa määriteltyä prosessia ja kyseisen tilanteen varalta mahdollisesti laadittua muuta ohjeistusta, joilla pyritään minimoimaan poikkeus- ja vaaratilanteesta aiheutuvat vahingot sekä varmistumaan mahdollisimman nopea toipuminen.

4.10.1 Varmentajan yksityinen avain on paljastunut tai varmentajan varmenne on suljettu

Mikäli varmentajan yksityinen avain paljastuu, noudatetaan varmentajan määrittelemää proseduuria. Kaikki paljastuneella avaimella myönnetyt ja voimassa olevat varmenteet suljetaan yhdellä tai useammalla sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeisen suljetun varmenteen voimassaoloaika on päättynyt. Tämän jälkeen avaimen käyttö lopetetaan välittömästi. Tarvittaessa voidaan ensi tilassa avaimella allekirjoitetut sulkulistat poistaa sulkulistapalvelusta välittömästi, jolloin kyseisellä avaimella allekirjoitettuihin varmenteisiin ei voi riittävin perustein luottaa.

Mikäli varmentajan varmenteiden luonnissa käyttämä yksityinen avain tai muu tekninen menetelmä on paljastunut tai tullut muutoin käyttökelvottomaksi, varmentaja ilmoittaa avaimen paljastumisesta sekä sen edellyttämistä toimenpiteistä sähköpostilla tai kirjeitse varmenteen omistajille, palveluntarjoajille, Viestintävirastolle sekä muille mobiilivarmentajille. Toiminnan jatkaminen kyseisen varmenneluokan osalta vaatii uusien varmentajan allekirjoitusavainten luonnin sekä uusien varmenteiden luonnin varmenteen haltijoille.

4.10.2 Turvallisuuden vaarantuminen luonnonmullistuksen tai muun katastrofin seurauksena

Varmentajan tuotantotilat on rakennettu turvallisiksi ottaen huomioon tilojen maantieteellisen sijainnin mukaiset todennäköiset riskit. Varmentajan keskeisimmät järjestelmät mukaan luettuna hakemistopalvelut ja sulkulistajakelu on hajautettu maantieteellisesti useampaan eri paikkaan, jotta järjestelmän haavoittuvuus yhden pisteen vikaantumiselle olisi minimoitu.

4.11 Varmentajan toiminnan lakkauttaminen

Varmentajan toiminnan lopettaminen on tilanne, jossa varmenteiden myöntämiseen liittyvät palvelut lakkautetaan pysyvästi. Varmentajan allekirjoitusavainten vaihtamista tai varmennustoiminnan siirtämistä vastuineen toiselle organisaatiolle ei katsota Varmentajan toiminnan lopettamiseksi.

Varmentaja huolehtii, että varmenteen omistajille ja luottaville osapuolille koituu mahdollisimman vähän häiriöitä Varmentajan toiminnan lopettamisesta.

Varmentaja tiedottaa toimintansa lopettamisesta muille luottamusverkoston varmentajille ja asiakkailleen mahdollisimman pian, kuitenkin vähintään kuutta kuukautta ennen lakkauttamisen ajankohtaa.

Ennen kuin Varmentaja lopettaa toimintansa, vähintään seuraavat toimenpiteet on suoritettava:

- Kaikki myönnetyt ja voimassa olevat varmenteet suljetaan yhdellä tai useammalla sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeisten suljetun varmenteen voimassaoloaika on päättynyt.
- Varmentaja lakkauttaa kaikki sopimuskumppaniensa valtuudet suorittaa varmenteiden myöntämisprosessiin liittyviä tehtäviä varmentajan puolesta.
- Varmentaja tuhoaa tai poistaa käytöstä yksityiset allekirjoitusavaimensa siten, että niitä ei voida enää ottaa käyttöön.
- Varmentaja varmistaa, että kohdassa 4.8 mainittu saatavuus varmentajan arkistoihin säilyy varmentajan lakkauttamisen jälkeenkin.
- Varmentaja huolehtii sähköisen allekirjoituslain mukaisten tietojen arkistoinnista sekä noudattaa muutoinkin arkistolain säännöksiä tietojen arkistoinnin osalta.
- Varmentaja informoi kaikkia Tilaajia ja muita varmentajia, joiden kanssa Varmentajalla on sopimus,
- Varmentaja lopettaa kaikki valtuutukset, jotka koskevat Varmentajan ulkoistamia toimintoja varmenteen myöntämisprosessiin liittyen,
- Varmentaja huolehtii siitä, että sen myöntämiä varmenteita ei enää voi käyttää tai niihin ei voi enää riittävin perustein luottaa.

5 Fyysiset, toiminnalliset ja henkilöstöturvallisuuteen liittyvät vaatimukset

5.1 Fyysinen turvallisuus

Fyysisen turvallisuusvalvonnan avulla kontrolloidaan pääsyä varmentajan ohjelmistoihin ja laitteistoihin. Näihin sisältyvät varmennusjärjestelmän palvelimet ja työasemat sekä erilliset salaustekniset laitteet ja salaustekniset välineet. Kulunvalvontajärjestelmä kirjaa varmentajan tiloihin saapumiset ja niistä lähtemiset.

Varmentaja yksityiset avaimet, joilla allekirjoitetaan varmenteita ja sulkulistoja suojataan fyysisesti siten, että ne eivät voi paljastua fyysisen hyökkäyksen tuloksena.

Varmentajan tiloihin on varastoitu varmuuskopiot ja tietovälineet siten, että tallennetun tiedon häviäminen, peukalointi tai luvaton käyttö on riittävällä varmuudella estetty. Varmuuskopioita säilytetään sekä tiedon palautuksia varten että tärkeän tiedon arkistoimiseksi.

Tietoturvapolitiikassa kuvattujen fyysisen turvallisuuden periaatteiden toteuttamiseksi varmentaja ylläpitää kuvauksia tuotantojärjestelmän fyysisen turvallisuuden hallinnasta. Keskeisimpien tietoturvakäytäntöjen periaatteet on dokumentoitu erillisessä dokumentissa nimeltään ”TeliaSonera Production CPS” joka on löydettävissä varmentajan julkisesta sivustosta http://repository.trust.teliasonera.com/CPS

5.1.1 Sijainti ja rakennusten ominaisuudet

Varmentajan turvallinen laitteisto sijaitsee Suomessa sellaisissa tiloissa, joiden fyysinen suojaus vastaa vähintään Viestintäviraston määräyksen viestintäverkon fyysisestä suojaamisesta (Viestintävirasto 54/2008 M) vaatimuksia korkeimman tärkeysluokan laitetiloille (tärkeysluokka 1).

5.1.2 Fyysinen pääsy toimitilaan

Varmenteiden tuotantotilat ovat ympärivuorokautisen vartioinnin ja valvonnan piirissä. Pääsy tilaan, jossa varmennusjärjestelmä sijaitsee, on rajattu tietyille varmentajan luotetuissa rooleissa toimiville henkilöille. Pääsy laitteistoon, jossa varmentajan allekirjoitusavaimet sijaitsevat ja jossa niiden käyttö on mahdollista, vaatii kahden sellaisen henkilön läsnäoloa, joille on erikseen annettu oikeus saapua alueelle.

Pääsy muihin tiloihin, joissa sijaitsee muita varmentajanjärjestelmiä kuten rekisteröintijärjestelmä, on rajoitettu vain valtuutetuille laitteistojen ja tilojen ylläpidosta vastaaville henkilöille.

Pääsyä tiloihin valvotaan kulunvalvontajärjestelmällä. Mikäli henkilölle ei ole myönnetty pysyvää henkilökohtaista kulkuoikeutta, hän voi liikkua tiloissa ainoastaan jonkun kulkuun oikeutetun henkilön seurassa.

5.1.3 Varajärjestelyt

Varmentajan keskeiset järjestelmät ovat kahdennettu kahteen erilliseen turvalliseen laitetilaan siten, että laitevian sattuessa voidaan siirtyä käyttämään varajärjestelmää vaarantamatta järjestelmään sisältyvien tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä.

Varmennusjärjestelmän tiedoista otetaan säännöllisesti varmuuskopiot, jotka säilytetään varmentajan tuotantotiloista erillään sijaitsevissa tiloissa. Pääsy näihin tiloihin on rajoitettu erikseen valtuutetuille henkilöille. Tärkeiden laitteiden osalta varmentajalla on huoltosopimukset, joilla varmistetaan varaosien saanti ja huolto.

Laitetilat kuuluvat automaattisen palohälytysjärjestelmän piiriin. Tilat on varustettu savunilmaisimilla ja käsisammuttimilla. Inergen-kaasusammutus on käytössä osassa laitetiloja.

Varmennusjärjestelmän keskeytymätöntä toimintaa varmistetaan myös katkeamattoman virransyöttöjärjestelmän ja varavoimalaitteiden avulla. Laitetiloissa on ilmastointijärjestelmä, jonka tuottaman ilman lämpötilaa ja kosteutta monitoroidaan jatkuvasti. Rakenteellisilla ratkaisuilla estetään vesivahingoille altistuminen ja laitetiloja valvotaan kosteusilmaisimilla.

5.2 Toiminnalliset vaatimukset

5.2.1 Vastuunjako

Varmennustoimintaan osallistuva henkilöstö on jaoteltu luotettuihin rooleihin, jotka sisältävät seuraavanlaisia vastuita:

- **Tietoturvallisuusvastaava** (Security Manager): kokonaisvastuu turvakäytäntöjen toteutuksen hallinnasta ja järjestelmien tuottamien lokien tarkistaminen.
- **Järjestelmän pääkäyttäjä** (Certification Authority Administrator): rekisteröintiin, varmenteiden luontiin, allekirjoituksen luomisvälineen valmistamiseen ja toimittamiseen sekä varmenteiden peruuttamiseen liittyvien Varmentajan luotettavien järjestelmien konfigurointi, ylläpito ja asennustilaukset sekä PKI-vianselvitykset ja varmentajan yksityisten avainten hallintatoimenpiteet.
- **Järjestelmän ylläpitäjä** (System Administrator): Varmentajan luotettavan järjestelmän päivittäinen käytönvalvonta, varmuuskopioiden ottaminen, varajärjestelmän käyttöönotto ja toipumisen hallinta sekä tilausten mukaiset asennukset ja järjestelmätason vianselvitykset.
- **Rekisteröintivastaava** (Registration Officer): varmenteiden luontiin ja jakeluun liittyvien toimenpiteiden hyväksyntä.
- **Sulkupalveluvastaava** (Revocation Officer): varmenteiden peruuttamiseen ja sulkulistaan liittyvien toimenpiteiden hyväksyntä.

Varmentaja huolehtii siitä että jokaista tehtävää kohden on palkattu riittävästi henkilöstöä ja että yksittäiset henkilöt eivät voi toimia kaikissa rooleissa samanaikaisesti.

5.2.2 Tehtäviin vaadittavien henkilöiden lukumäärä

Tiettyihin toimenpiteisiin vaaditaan usean henkilön yhtäaikainen osallistuminen. Varmenteiden tuotantoon kohdistuvien kriittisten toimenpiteiden toteuttaminen tuotantotiloissa vaatii vähintään kahden henkilön osallistumisen. Varmentajan määrittelemien proseduurien mukaisesti tehtävä varmentajan yksityisen avaimen luonti, varmuuskopiointi, palauttaminen ja peruuttaminen sekä varmentajan yksityisen avaimen turvamoduulin alustus edellyttävät vähintään kahden henkilön paikallaoloa.

Muuhun järjestelmän käyttämiseen vaaditaan yhden tehtävään oikeutetun henkilön läsnäolo.

5.2.3 Tehtäväkohtainen tunnistaminen

Seuraavissa rooleissa toimivien tunnistamiseen vaaditaan varmenne:

Järjestelmän pääkäyttäjä (varmennusjärjestelmä)
Rekisteröintivastaava

Alla luetelluissa rooleissa tunnistamisessa käytetään pääsääntöisesti käyttäjätunnusta ja salasanaa. Silloin kun rooliin kuuluvien velvollisuuksien hoitaminen edellyttää Varmentajan kriittisimpien järjestelmien käyttöä, kirjautuminen näihin edellyttää myös alla luetelluissa rooleissa toimivilta varmenteeseen tai kertakäyttösalasanaan pohjautuvaa tunnistamista.

Järjestelmän pääkäyttäjä (rekisteröintijärjestelmä)
Tietoturvallisuusvastaava
Järjestelmän ylläpitäjä
Sulkupalveluvastaava

5.3 Henkilöturvallisuus

Varmentajan työntekijöiden palkkaamisessa noudatetaan Soneran normaaleja työhönottomenettelyjä työhönottotarkastuksineen. Varmentaja huolehtii siitä, että jokaisella sen varmennustoimintaan liittyviin tehtäviin palkkaamalla henkilöllä on tarvittava pätevyys ja kokemus tehtäviensä suorittamiseen. Alihankkijat, joiden työntekijöitä toimii Varmentajan tärkeissä rooleissa, velvoitetaan sopimuksella huolehtimaan tästä omien työntekijöidensä osalta.

Sonera on määritellyt ja ylläpitää kattavia yritysturvallisuuteen liittyviä ohjeistoja (politiikat, standardit, toimintaohjeet, määräykset ja säädökset), jotka jokaisen työntekijän on tiedettävä ja tunnettava.

Jokainen Varmentajan omaan organisaatioon kuuluva työntekijä, jonka työtehtäviin kuuluu varmennustoimintaan liittyviä tehtäviä, allekirjoittaa henkilökohtaisen salassapitosopimuksen. Myös jokainen varmenteen valmistaja tai muu varmentajan alihankkija, jonka työntekijöitä toimii Varmentajan luotetuissa rooleissa, allekirjoittaa salassapitosopimuksen, joka velvoittaa sen työntekijöitä.

5.3.1 Henkilökuntaa koskevan taustaselvityksen tekeminen

Seuraavissa rooleissa toimiville henkilöille suoritetaan kolmannen osapuolen toimesta taustatietojen tarkistaminen:

Tietoturvallisuusvastaava
Järjestelmän pääkäyttäjä
Järjestelmän ylläpitäjä

Muutoin varmentaja tarkistuttaa työntekijöidensä taustatiedot harkintansa mukaan riippuen työntekijän roolista varmentajan organisaatiossa. Varmentaja velvoittaa sopimuksin alihankkijansa huolehtimaan tärkeissä rooleissa toimivien työntekijöidensä taustatietojen tarkistuttamisesta.

5.3.2 Taustaselvityksen tekemisessä noudatettava menettely

Kaikkien varmentajan työtehtäviin palkattavien henkilöiden taustatietojen tarkistuksessa noudatetaan Soneran märittelemiä työhönottomenettelyjä työhönottotarkastuksineen.

Taustojen tarkistus tehdään poliisin tekemän perusmuotoisen turvallisuusselvityksen avulla kappaleessa 5.3.1 mainituissa rooleissa toimiville henkilöille.

Tarkistuttaminen uusitaan tarvittaessa varmentajan harkinnan mukaan lain sallimissa rajoissa.

5.3.3 Koulutukseen liittyvät vaatimukset

Varmentajan uudet työntekijät perehdytetään varmennustoimintaan yleisesti, siihen liittyviin turvallisuusvaatimuksiin sekä erityisesti omiin työtehtäviinsä. Käsiteltävään aineistoon kuuluu mm. tietoturvapolitiikka, varmennepolitiikka ja varmennuskäytäntö. Tarvittaessa järjestetään henkilön työtehtäviin ja rooliin sovitettu yksilöllinen perehdyttäminen ja koulutus.

Varmentaja perehdyttää alihankkijoiden työntekijät varmennustoiminnan turvallisuusvaatimuksiin. Muilta osin vastuu alihankkijoiden työntekijöiden koulutuksesta on alihankkijoilla itsellään sopimuksiin perustuen.

5.3.4 Asiantuntemuksen ja osaamisen ylläpito

Varmentajan työntekijöille järjestetään tarvittaessa täydennyskoulutusta, jotta tehtävän hoitamiseen liittyvä asiantuntemus on aina tehtävän edellyttämällä tasolla..

5.3.5 Poikkeamista johtuvat toimenpiteet

Poikkeustilanteissa voidaan varmentajan tehtäviin ottaa väliaikaisesti henkilöstöä, jonka koulutus ei ole täydellistä, mutta heidän työtänsä ohjataan ja valvotaan vakituisen henkilöstön toimesta erityisen huolellisesti.

Jos varmentaja havaitsee väärinkäytöksen, siihen syyllistynyt varmentajan työntekijä siirretään välittömästi toisiin tehtäviin ja kaikki hänen pääsyoikeutensa varmennustoimintaan liittyviin järjestelmiin peruutetaan. Jatkotoimenpiteiden suhteen noudatetaan Soneran voimassa olevia käytäntöjä.

Väärinkäytöstilanteissa alihankkijoiden tapauksessa noudatetaan sopimuksissa määriteltyjä menettelyjä.

5.3.6 Henkilökunnan käyttöön annettavat asiakirjat

Jokaiselle varmennustoimintaan liittyvään tehtävään palkattavalle varmentajan työntekijälle annetaan pääsy varmennustoimintaan ja varmentajan toimintaan liittyvään dokumentaatioon. Lisäksi työntekijöille annetaan erityisesti heidän omien työtehtäviensä suorittamiseen tarvittavat ohjeet ja muu materiaali. Ohjeistusta on saatavilla myös suoraan sähköisessä muodossa työntekijöiden käytössä olevien järjestelmien ja sovellusten käytön yhteydessä.

Varmentaja toimittaa alihankkijoille näiden tarvitseman perusdokumentaation, jonka toimittamisesta työntekijöilleen alihankkija vastaa. Tiettyjen alihankkijoiden työntekijöillä on heidän käyttämiensä sovellusten kautta pääsy varmentajan ylläpitämiin ohjeisiin. Varmentaja toimittaa dokumentaatiota myös henkilökohtaisesti tietyissä rooleissa toimiville alihankkijoiden työntekijöille. Lisäksi alihankkijat velvoitetaan toimittamaan muu tarvittava dokumentaatio työntekijöilleen.

6 Tekniset turvatoimet

Telia Company CA:n yleiset tietoturvakäytäntöjen periaatteet on dokumentoitu erillisessä dokumentissa nimeltään ”TeliaSonera Production CPS” joka on löydettävissä varmentajan julkisesta sivustosta http://repository.trust.teliasonera.com/CPS

6.1 Avainparin luominen, tallettaminen ja käyttöönotto

6.1.1 Avainparin luominen

6.1.1.1 Varmentaja

Varmentajan avainparin luonti tapahtuu varmentajan määrittelemän avaintenluontiproseduurin mukaisesti. Avainpari luodaan varmentajan fyysisesti suojatuissa tiloissa varmennusjärjestelmää hyväksi käyttäen turvamoduulissa (ks. kappale 6.2 ”Varmentajan yksityisten avainten suojaaminen”). Avaintenluontiin osallistuvat henkilöt ovat luotetuissa rooleissa toimivia varmentajan tähän tehtävään valtuuttamia henkilöitä, joista vähintään kahden on oltava paikalla. Avaintenluontiproseduurin toimenpiteet kirjataan pöytäkirjaan, ja jokainen proseduuriin osallistuva henkilö vahvistaa pöytäkirjan allekirjoituksellaan. Pöytäkirja säilytetään kappaleen 4.8 ”Varmenteisiin liittyvien tietojen arkistointi” mukaisesti.

6.1.1.2 Varmenteen omistaja

Varmenteen luomisen tai uusimisen yhteydessä avainparit luodaan SIM-kortin turvamoduulissa. Yksityisistä avaimista ei synny kopiota eivätkä ne ole siirrettävissä tai kopioitavissa liittymäkortilta.

Varmentajalla, kortin liikkeellelaskijalla ja kortinvalmistajalla ei ole pääsyä varmenteen omistajien yksityisiin avaimiin.

6.1.2 Liittymäkortin luovuttaminen hakijalle

Liittymäkortin luovutusprosessi on kuvattu kappaleessa 4.2.1. ”Tunnistusvälineen toimittaminen”

6.1.3 Varmenteen hakijan julkisen avaimen toimittaminen varmentajalle

Mobiilivarmenteen rekisteröinnin yhteydessä luodaan uudet avaimet liittymäkortin sisällä ja varmenteen hakijan henkilöllisyys liitetään ICCID-tunnisteeseen ja rekisteröintijärjestelmä tekee varmennepyynnön varmennusjärjestelmään. Varmennepyyntö sisältää julkisen avaimen ja muut mobiilivarmenteen tiedot.

6.1.4 Varmentajan julkisen avaimen jakelu

Varmentajan varmenne sisältää varmentajan julkisen avaimen. Varmentajan varmenne on saatavilla varmentajan hakemistossa kappaleen 2.1.1 ”Varmentajan tietojen julkaiseminen” mukaisesti.

6.1.5 Avainten pituudet

Mobiilivarmenteen ja sulkulistan allekirjoittamiseen käytetty varmentajan yksityinen avain sekä sitä vastaava julkinen avain ovat vähintään 4096-bittisiä RSA-avaimia. OCSP-sanomien ja aikaleimojen allekirjoittamisessa käytetty avain on vähintään 2048-bittinen RSA-avain tai 256-bittinen ECC-avain.

Varmenteen omistajan avain varmentajan TeliaSonera Mobile ID CA v1 tapauksessa on vähintään 1024-bittinen RSA-avain. TeliaSonera Mobile ID CA v2 tapauksessa avain on vähintään 256-bittinen ECC-avain.

6.1.6 Avainten käyttötarkoitukset

Varmenteen tietosisällössä käyttötarkoituksen määräävä kenttä ”Key usage” määrittelee varmenteisiin liittyvien avainten käyttötarkoituksen (esimerkiksi todentaminen ja kiistämättömyys). Avainten käyttö rajataan vain käyttötarkoituksiinsa. Kiistämättömyystarkoitukseen tarkoitettua avainta tulee siis käyttää vain tähän tarkoitukseen eikä esimerkiksi todentamiseen.

Varmenteen hakijan kortille luodaan avaimet erikseen sähköistä allekirjoitusta eli kiistämättömyyttä varten ja tunnistamista varten. Asiointivarmenteeseen liittyy kaksi avainparia ja vastaavasti kaksi varmennetta. Tunnistamiskäyttöön tarkoitettua avainta voidaan käyttää myös suostumustarkoitukseen. Lisäksi tunnistusavaimen käyttötarkoituksiin voidaan sisällyttää salaus. Varmenteen tietosisältö on kuvattu tarkemmin kappaleessa 7.1 ”Varmenteiden tekniset tiedot”.

Varmenteiden laajennuksessa Extended Key Usage voidaan tallentaa mobiilivarmenteen käyttötarkoitukseksi ”Käyttäjävarmenne” ja ”sähköpostivarmenne” (Client authentication ja Secure Email) ja näin tehdään aina kun allekirjoittajana on TeliaSonera Mobile ID CA v2 tai uudempi. Systeemivarmenteissa OCSP-sanomien tai aikaleimojen tekemisen yhteydessä käyttötarkoitus on näihin toimintoihin soveltuva erityinen käyttötarkoitus.

6.2 Varmentajan yksityisten avainten suojaaminen

Varmentaja on toteuttanut yksityisen allekirjoitusavaimensa suojaamisen fyysisten suojausten, määriteltyjen proseduurien, pääsynvalvonnan ja käyttöoikeuksien yhdistelmällä.

6.2.1 Turvamoduulia koskevat standardit

Varmentajan turvallisissa fyysisesti suojatuissa tiloissa sijaitsevaan varmennusjärjestelmään kuuluu turvamoduuli, jolla varmentajan allekirjoitusavain on suojattu. Turvamoduuli noudattaa vähintään FIPS 140-2 level 3 -standardia.

6.2.2 Varmentajan yksityisen avaimen käsittelyyn osallistuva henkilökunta

Varmentaja huolehtii teknisen valvonnan ja määriteltyjen proseduurien avulla, että kukaan ei yksinään saa haltuunsa keinoja siihen ympäristöön pääsemiseksi, jossa yksityinen avain on tallennettuna, tai pysty käyttämään avainta millään tavalla. Kriittisiä allekirjoitusavaimeen liittyviä toimenpiteitä, kuten avaimen luominen, varmistus ja palautus, on suorittamassa aina useampi kuin yksi henkilö.

6.2.3 Yksityisen avaimen varmuuskopio

Varmentajan yksityisen allekirjoitusavaimen tuhoutumisen varalta on olemassa järjestely sen palauttamiseksi. Varmentajan yksityisen avaimen varmuuskopiointi on hoidettu tavalla, joka takaa kaikissa tilanteissa vähintään saman turvatason, mitä vaaditaan varmennusjärjestelmässä käytössä olevien yksityisten avainten ylläpidolta.

Varmentajan yksityiset avaimet ja niiden varmuuskopiot säilytetään vahvasti salattuina. Avaimen palautus edellyttää sellaisen aktivointitiedon käyttöä, joka on tallennettu osiin jaettuna erillisiin turvallisiin tiloihin ja jonka haltuun saanti on hajautettu Varmentajan määrittelemälle määrälle luotetuissa rooleissa toimivia henkilöitä. Avaimen palauttaminen edellyttää, että tietty määrä näistä henkilöistä osallistuu palautusproseduuriin.

6.2.4 Yksityisen avaimen arkistointi

Varmentajan tai käyttäjän yksityisiä avaimia ei arkistoida.

6.2.5 Yksityisen avaimen hallinnointi turvamoduulissa

Varmentajan yksityisiä avaimia käytetään vain varmentajan turvalliseen ympäristöön sijoitetussa varmennusjärjestelmässä. Varmentajan yksityisen avaimen aktivointiin vaaditaan vähintään yksi varmentajan luotetussa roolissa toimiva henkilö, jonka varmennusjärjestelmä tunnistaa vahvalla tunnistamismekanismilla. Avain säilyy varmennusjärjestelmässä aktiivisena, kunnes sen käyttö keskeytetään esim. huoltotoimenpiteiden takia.

Varmentaja on laatinut ohjeen turvamoduulin elinkaaren hallintamenettelystä varmennepolitiikassa ja varmennuskäytännössä määriteltyjen vaatimusten toteuttamiseksi.

6.3 Varmenteen omistajan avainten suojaaminen

6.3.1 Liittymäkorttia koskevat standardit

Liittymäkortit valmistetaan GSMA-SAS -sertifioidussa tehtaassa ja ne ovat ISO 7816 -standardin sekä 3GPP:n standardien TS 31.102 ja TS 31.111 sekä TS 23.048 mukaisia.

6.3.2 Yksityisen avaimen luovutus luotetun osapuolen huostaan

Varmenteen omistajan yksityistä avainta ei luovuteta kenellekään muulle kuin sen hakijalle. Yksityinen avain luodaan vasta kun kortti on toimitettu liittymän omistajalle ja omistaja aktivoi avaingeneroinnin.

6.3.3 Yksityisen avaimen varmuuskopio

Mobiilivarmenteeseen liittyvistä varmenteen omistajan yksityisistä avaimista ei ole kopioita.

6.3.4 Yksityisen avaimen arkistointi

Mobiilivarmenteeseen liittyvää varmenteen omistajan yksityistä avainta ei arkistoida.

6.3.5 Yksityisen avaimen hallinnointi liittymäkortilla

Yksityistä avainta ei hallinnoida erityisesti. Yksityinen avain on vain ja ainoastaan liittymäkortilla.

6.4 Muut avainparin hallintaan liittyvät seikat

6.4.1 Julkisen avaimen arkistointi

Varmentaja arkistoi kaikki myöntämänsä varmenteet, jonka mukana julkinen avain tulee arkistoiduksi.

6.4.2 Julkisten ja yksityisten avainten voimassaoloaika

Mobiilivarmenteen voimassaoloaika on enintään viisi vuotta. Varmenteen voimassaoloaika voi olla lyhempi, mikäli käytettävissä olevan avainpituuden ei katsota pysyvän turvallisena täyttä viiden vuoden jaksoa.

Varmenne voidaan sulkea sen voimassaoloaikana. Varmenteen sulkutapahtumaa on käsitelty enemmän kohdassa 4.5 ”Varmenteen voimassaolon päättyminen ja sulkeminen”.

6.5 Liittymäkortilla olevien yksityisten avainten tunnusluvut

6.5.1 Tunnusluvun luominen ja käyttöönotto

Liittymäkortin yksityisten avainten käyttö on suojattu tunnusluvuilla, joita käytetään yksityisten avaimen aktivointitietona. Tunnusluvun pituus on 4-8 numeroa. Korttiohjelmisto luo tunnusluvun samalla kun avainpari luodaan liittymäkortille. Varmenteen omistaja voi asettaa tunnusluvun haluamakseen.

6.5.2 Tunnusluvun suojaus

Tunnusluvut on suojattu niin, ettei niitä voi lukea tai kopioida kortilta.

Yksityinen avain lukkiutuu, jos siihen liittyvä tunnusluku syötetään väärin viisi (5) kertaa peräkkäin. Lukkiutunutta avainta ei voi palauttaa käyttöön vaan jos avain lukkiutuu tai varmenteen omistaja unohtaa tunnusluvun tulee varmenteen omistajan luoda uudet avaimet ja rekisteröidä uusi varmenne kappaleen 4.6 ”Varmenteen uusiminen” mukaisesti.

6.6 Varmennejärjestelmän laitteiden käyttöön ja pääsyyn liittyvät turvallisuusvaatimukset

6.6.1 Laitteistoturvallisuus

Varmennejärjestelmän laitteistoina käytetään vain käyttötarkoitukseensa sopivia laitteistoja. Pääsy varmentajan laitteistoalustoille ja järjestelmiin on rajattu vain kappaleessa 5.2.1 ”Vastuunjako” kuvatuissa luotetuissa rooleissa toimiville henkilöille. Käyttäjät tunnistetaan käyttäen vahvaa käyttäjäntunnistusta. Laitteistoalustojen turva-asetukset on kovennettu Soneran ja varmentajan vaatimusten mukaisesti.

6.7 Varmennejärjestelmän elinkaaren hallinta

6.7.1 Varmennejärjestelmän kehittämiseen liittyvä valvonta

Varmentajan tuotantojärjestelmän kehityksessä käytetään kaksivaiheista testausta. Kehitystyön tuloksena syntyneet muutokset testataan ensin erillisessä kehitysjärjestelmässä. Onnistuneen testauksen jälkeen muutokset viedään tuotantojärjestelmän kanssa mahdollisimman identtiseen testijärjestelmään, jossa suoritetaan lopullinen hyväksyntätesti ennen muutosten vientiä tuotantoon.

Kaikki tuotantoon vietävät järjestelmän muutokset dokumentoidaan huolellisesti.

6.7.2 Turvallisuuden hallinta

Varmentaja noudattaa tietoturvallisuuden hallinnassa Soneran yritysturvallisuusyksikön määrittelemää politiikkaa. Lisäksi Varmentaja noudattaa kaikessa toiminnassaan määrittelemiänsä tietoturvapolitiikkaa ja varmennuskäytäntöä. Toiminnan auditointi on kuvattu kappaleessa 2.5 ”Auditointi”.

Varmentajan laatiman liiketoiminnan jatkuvuussuunnitelman ylläpitoon sisältyy liiketoiminnan riskien arviointi sekä toimintamallien luonti mahdollisten riskien varalta. Raportointi poikkeamista ja havaituista tai epäillyistä suojauksen heikkouksista hoidetaan varmentajan määrittelemien menettelytapojen mukaan.

Varmentaja huolehtii sopimuksin tietoturvan säilymisestä ulkoistettujen toimintojen osalta sekä määriteltyjen politiikkojen ja käytäntöjen noudattamisesta alihankkijoita käytettäessä.

6.8 Tietoverkon turvallisuus

Varmentajan järjestelmä on erotettu julkisesta verkosta palomuurein. Varmentajan verkko on jaettu eri turvavyöhykkeisiin ja liikenne vyöhykkeiden välillä on rajattu pääsylistoin, joilla sallitaan vain järjestelmien toiminnan ja ylläpidon kannalta välttämättömät tietoliikenneyhteydet. Kaikki muu liikenne on estetty. Kriittisimpiin järjestelmien osiin ei ole suoria yhteyksiä julkisista verkoista. Käytössä on myös hyökkäyksentunnistusjärjestelmä.

Keskeiset verkkokomponentit on kahdennettu niiden käytettävyyden turvaamiseksi.

Varmentajan järjestelmän osien välisessä liikenteessä käytetään vahvaa tunnistusta sekä salausta.

Varmentajan juurivarmenne ei ole verkossa lainkaan vaan sitä säilytetään verkosta kokonaan irrotetussa systeemissä.

6.9 Turvamoduulin käytön valvonta

Varmentajan yksityiset avaimet on suojattu turvamoduulilla. Pääsy turvamoduuliin on suojattu tiukalla fyysisellä ja loogisella pääsynhallinnalla. Turvamoduulin suojaukseen liittyvät turvamekanismit on tarkemmin kuvattu kappaleessa 6.2 ”Varmentajan yksityisten avainten suojaaminen”.

Varmentaja kirjaa lokille turvamoduulin hallinnointiin ja käyttöön liittyvät tapahtumat ja seuraa lokeja kappaleen 4.7 ”Järjestelmän valvonta” mukaisesti.

7 Varmenne- ja sulkulistaprofiilit

7.1 Varmenteiden tekniset tiedot

Varmenteen sisältömäärittely eli varmenneprofiili määrittelee varmenteessa käytettävät kentät. Mobiilivarmenteiden varmenneprofiili noudattaa ITU X.509 –standardissa määriteltyä versio 3:n mukaista profiilia. Varmenteiden profiili noudattaa myös dokumenttia RFC 5280 ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

7.1.1 Varmenteen kentät ja niiden sisällöt

7.1.1.1 Varmenteen peruskentät

Varmenteissa käytetään X.509-standardissa määritellyistä varmenteen peruskentistä ainoastaan kaikkia pakollisia kenttiä. Alla on lueteltu varmenteissa käytetyt peruskentät:

Kentän nimi	Kentän kuvaus ja sisältö
Version	Tässä kentässä ilmoitetaan minkä X.509-standardissa määritellyn version mukainen varmenne on. Mobiilivarmenteet ovat version 3 mukaisia.
Serial number	Varmentaja luo jokaiselle varmenteelle oman sarjanumeron. Tässä kentässä ilmoitettu numero on yksikäsitteinen jokaiselle varmenteelle, joka luodaan Varmentajan järjestelmässä. Ohjelmisto huolehtii automaattisesti sarjanumeron yksikäsitteisyydestä.
Signature algorithm	Allekirjoitusalgoritmi on se matemaattinen säännöstö, jonka mukaisesti Varmentajan ohjelmisto suorittaa varmenteen allekirjoituksen. Yleisesti käytetyille algoritmeille on määritelty tunnisteet. Tässä kentässä ilmoitetaan varmenteen allekirjoituksessa käytetyn algoritmin tunniste. Allekirjoitusta ei voi todentaa, jos käytetty algoritmi ei ole tiedossa. Mobiilivarmenteiden allekirjoituksessa käytetty algoritmi on sha256RSA.
Issuer	Tässä kentässä ilmoitetaan varmenteen myöntäjän nimi. Soneran mobiilivarmenteet myöntävän varmentaja Issuer-nimi on kuvattu kappaleessa 3.1”Varmentajan nimeämiskäytäntö”.
Valid from	Varmenteen voimassaoloaika on se aikaväli, jolloin Varmentaja takaa ylläpitävänsä tietoa varmenteen tilasta eli siitä, onko varmenne mahdollisesti peruutettu. Valid from -kentässä ilmoitetaan päivämäärä ja kellonaika, jolloin varmenne astuu voimaan,
Valid to	Valid to -kentässä ilmoitetaan päivämäärä ja kellonaika, jonka jälkeen varmenne ei ole enää voimassa. Varmenteeseen voi luottaa sen voimassaoloaikana, jollei varmennetta ole julkaistu sulkulistalla.
Subject	Tässä kentässä yksilöidään kenen henkilön hallussa on se yksityinen avain, jota vastaava julkinen avain varmenteessa on. Kenttä sisältää Varmenteen omistajan yksikäsitteisen nimen. Kentän sisältö on kuvattu kappaleessa 3.3 ”Varmenteen hakijan nimeäminen”

Public key	Tässä kentässä ilmoitetaan se algoritmi, jonka kanssa varmenteen omistajan julkista avainta käytetään. Mobiilivarmenteissa kyseinen algoritmi on varmentajan TeliaSonera Mobile ID CA v1 tapauksessa RSA ja TeliaSonera Mobile ID CA v2 tapauksessa ECC Tässä kentässä annetaan myös itse varmenteen omistajan julkinen avain.

7.1.1.2 Varmenteen lisäkentät

Varmenteissa käytetään seuraavia X.509–standardissa määriteltyjä lisäkenttiä. Lisäkenttä määritellään kriittiseksi, kun varmennetta hyödyntävän järjestelmän halutaan hylkäävän varmenteen, mikäli se ei tunnista kriittiseksi määriteltyä lisäkenttää.

Kentän nimi	**Kriittisyys**	**Kentän kuvaus ja sisältö**
Key usage	Kriittinen	Varmenteen sisältämän julkisen avaimen käyttötarkoitukset ilmoitetaan tässä kentässä. Varmentaja ei vastaa käyttötarkoitusten vastaisesta käytöstä. Alla on listattu varmenteiden julkisten avainten käyttötarkoitukset. Tunnistusvarmenne: digitalSignature, keyEncipherment, Allekirjoitusvarmenne: nonRepudiation
Extended key usage	Ei-kriittinen	Tässä kentässä ilmoitetaan julkisen avaimen muut kuin kentässä ”Key Usage” ilmoitetut sallitut käyttötarkoitukset. Tässä kentässä ilmoitettu käyttötarkoitus saattaa olla yleisesti tunnettu tai tiettyä sovellusta varten itse määritelty. Tässä kentässä voidaan käyttää arvoja ”Client authentication” ja ”Secure email”
Authority key identifier	Ei-kriittinen	Tässä kentässä annetaan varmentajan julkisen avaimen tunniste. Tunnisteen avulla voidaan yksilöidä julkinen avain, joka vastaa varmenteen allekirjoittamiseen käytettyä yksityistä avainta. Tunnisteen muodostamiseen käytetään tiivistealgoritmia RFC5280 mukaisesti.
Subject key Identifier	Ei-kriittinen	Tässä kentässä annetaan varmenteessa olevan varmenteen omistajan julkisen avaimen tunniste. Tunnistetta voidaan käyttää löytämään varmenteet, jotka sisältävät tietyn julkisen avaimen. Mobiilivarmenteissa tunnisteen muodostamiseen käytetään -tiivistealgoritmia RFC5280 mukaisesti.
CRL distribution points	Ei-kriittinen	Tässä kentässä ilmoitetaan mistä sulkulista on noudettavissa. Soneran mobiilivarmenteissa tässä kentässä on URI-tyyppinen sulkulistan osoite. Sulkulistojen tarkat osoitteet on ilmoitettu

		kappaleessa 2.1.1 ”Varmentajan tietojen julkaiseminen”.
Authority Information Access	Ei-kriittinen	Tässä kentässä ilmoitetaan mistä varmentajan varmenne on haettavissa. Kentässä on URI-tyyppinen varmentajan varmenteen osoite. Tässä kentässä ilmoitetaan myös URI josta voi tehdä mobiilivarmenteisiin liittyvä OCSP-tarkistukset.
Basic constraints	Kriittinen	Tässä kentässä ilmoitetaan, onko kyseessä varmentajan varmenne vai ei. Jos tämä kenttä on käytössä niin loppukäyttäjän mobiilivarmenteissa kentän arvona on ”false” eli kyseessä ei ole varmentajan varmenne.
Certificate policies	Kriittinen	Tätä kenttää käytetään ilmoittamaan varmennepolitiikka ja varmennuskäytännöt, joiden mukaisesti varmenne on myönnetty. Varmennepolitiikka tunnistetaan sille annetun yksilöllisen tunnisteen (Object identifier, OID) avulla. Kenttä sisältää seuraavat tiedot: Policy Identifier = varmennepolitiikan OID Policy Qualifier Info Policy Qualifier Id=CPS, Qualifier = Varmennuskäytännön URI Policy Qualifier Info Policy Qualifier Id=User Notice, Notice Text = Varmentajan info
Subject Alternative Name	Ei-kriittinen	Tässä kentässä on seuraavan tyyppinen URI-osoite: http://soneraid.sonera.fi/eid/<Subject SerialNumber> Missä <Subject SerialNumber>=varmenteen omistajan SaTu

X.509-standardi sallii myös itse määritellyt lisäkentät. Mobiilivarmenteissa käytetään seuraavia yksityisiä lisäkenttiä:

Kentän nimi	**Kriittisyys**	**Kentän kuvaus ja sisältö**
eidSmartCard SerialNumber	Ei-kriittinen	Varmenteen omistajan liittymäkortin sarjanumero ilmoitetaan tässä kentässä. Sarjanumeroa käytetään liittämään varmenteen omistaja tämän käytössä olevaan tunnistusvälineeseen. Sarjanumerona käytetään liittymäkortin ICCID-numeroa. eidSmartCardSerialNumber-attribuutin yksilöivä OID-tunniste on 1.2.752.34.2.1
Identification PathLength	Ei-kriittinen	Varmenteen myönnön yhteydessä tehdyn ensitunnistuksen mahdollisen ketjutuspolun pituus on talletettu tähän attribuuttiin, jonka arvo on nolla, jos

		henkilöllisyys on todettu henkilökohtaisesti kirjallisista asiakirjoista. Muussa tapauksessa sen arvo kertoo ensitunnistuksen tunnistusketjun pituuden. IdentificationPathLength -attribuutin yksilöivä OID-tunniste on 1.2.246.277.1.5.4.106

7.2 Sulkulistaprofiili

Alla on kuvattu sulkulistan sisältämät tiedot. Sulkulistalla ilmoitetaan mitkä niistä varmenteista, joiden voimassaoloaika ei ole vielä päättynyt, on peruutettu.

Sulkulistat ovat ITU X.509–standardissa määritellyn versio 2:n mukaisia. Ne noudattavat myös dokumenttia RFC 5280.

7.2.1 Sulkulistan peruskentät

Sulkulistoissa käytetään kaikkia X.509-standardissa määriteltyjä sulkulistan peruskenttiä, sekä pakollisia että valinnaisia.

Alla on lueteltu sulkulistoissa käytetyt peruskentät:

Kentän nimi	**Kentän kuvaus ja sisältö**
Version	Tässä kentässä ilmoitetaan minkä X.509-standardissa määritellyn version mukainen sulkulista on. Mobiilivarmennepalvelun sulkulistat ovat version 2 mukaisia.
Signature algorithm	Sulkulistojen allekirjoitukseen käytetään samaa algoritmia kuin varmenteiden allekirjoitukseen. Algoritmi on sha256RSA.
Issuer	Tässä kentässä ilmoitetaan Sulkulistan julkaisijan nimi. Mobiilivarmennepalvelussa nimi on aina sama kuin listalla olevien varmenteiden myöntäjän (Varmentajan) nimi.
This update	Päivämäärä ja kellonaika, jolloin sulkulista on julkaistu.
Next update	Päivämäärä ja kellonaika, johon mennessä seuraava sulkulista julkaistaan. Seuraava sulkulista voidaan julkaista milloin tahansa edellisen sulkulistan julkaisun jälkeen, kuitenkin ennen siinä ilmoitettua seuraavan sulkulistan julkaisuaikaa. Sulkulistan julkaisuväli on kuvattu kappaleessa 4.5.10 ”Sulkulistan julkaisutiheys”.
Revoked certificates	Tässä kentässä ilmoitetaan peruutettujen varmenteiden sarjanumerot sekä jokaisen peruutetun varmenteen osalta erikseen aika jolloin varmenne peruutettiin sekä peruuttamisen syy.

7.2.2 Sulkulistan lisäkentät

Sulkulistoissa käytetään seuraavia X.509–standardissa määriteltyjä lisäkenttiä:

Kentän nimi	Kentän kuvaus ja sisältö
Authority key identifier	Tässä kentässä annetaan sulkulistan julkaisijan julkisen avaimen tunniste. Tunnisteen avulla voidaan yksilöidä julkinen avain, joka vastaa sulkulistan allekirjoittamiseen käytettyä yksityistä avainta. Tunnisteen muodostamiseen käytetään tiivistealgoritmia RFC5280 mukaisesti.
CRL number	Järjestysnumero ilmaisee kuinka mones varmentajan julkaisema sulkulista on kyseessä. Numerointi alkaa 1:stä ja se kasvaa aina yhdellä seuraavaan sulkulistaan. Käyttäjä pystyy numeron perusteella päättelemään korvaako jokin tietty sulkulista jonkin toisen sulkulistan.

Yksityisiä itse määriteltäviä lisäkenttiä ei käytetä.

7.2.3 Sulkulistarivien sisällöt

Sulkulistalla ilmoitetaan kunkin suljetun varmenteen osalta varmenteen sarjanumero sekä aika jolloin varmenne peruutettiin. Lisäksi kunkin suljetun varmenteen osalta sulkulistalla voidaan julkaista seuraavat X.509–standardin mukaiset lisäkentät:

Kentän nimi	Kentän kuvaus ja sisältö
Reason Code	Tässä kentässä ilmoitetaan kunkin suljetun varmenteen sulkemisen syy. Sulkemisen syy voi olla jokin seuraavista: KeyCompromise, CACompromise, AffiliationChanged, Superseded, CessationOfOperation.
Invalidity Date	Invalidity date–kenttä kertoo päivän, jolloin tiedettiin tai epäiltiin, että yksityinen avain on paljastunut tai varmenne on muuten tullut käyttökelvottomaksi. Päivä voi olla aiemmin kuin sulkulistalla oleva varmenteen sulkupäivä, joka kertoo päivän jolloin varmentaja sulki varmenteen.

8 Varmennuskäytännön hallinnointi

8.1 Varmennuskäytännön muutosmenettely

Aina kun jotain kohtaa varmennepolitiikassa muutetaan, muutoksen vaikutukset varmennuskäytäntöön arvioidaan. Varmentajan Varmennepolitiikkayksikkö vastaa arvioinnin käynnistämisestä. Dokumentin muuttamiseen voi olla myös muita varmennepolitiikan muutoksista riippumattomia syitä.

8.1.1 Kohdat, joita voi muuttaa ilman tiedonantoa käyttäjille ja palveluntarjoajille

Tähän dokumenttiin voidaan tehdä oikeinkirjoitukseen ja ulkoasuun liittyviä korjauksia sekä muutoksia yhteystietoihin ilman ilmoitusta käyttäjille tai palveluntarjoajille. Lisäksi varmennuskäytännön kohtia, jotka varmentajan mielestä eivät merkittävästi vaikuta varmenteiden omistajiin ja luottaviin osapuoliin, voidaan muuttaa ilman erillistä ilmoitusta.

Dokumentista voidaan julkaista käännöksiä eri kielillä ilman erillistä ilmoitusta. Käännöksen ja suomenkielisen tekstin ollessa ristiriidassa keskenään suomenkielinen teksti on voimassa.

8.1.2 Kohdat, joiden muutos vaatii tiedonannon käyttäjille ja palveluntarjoajille

Kaikkia varmennuskäytännön kohtia voidaan muuttaa ilmoittamalla tulevista pääasiallisista muutoksista käyttäjille ja palveluntarjoajille vähintään 15 päivää ennen muutosten voimaan astumista.

8.2 Julkaiseminen ja tiedottaminen

Tämä varmennuskäytäntö on saatavilla varmentajan verkkosivuilla kappaleessa 2.1.1 ”Varmentajan tietojen julkaiseminen” kerrotussa osoitteessa.

Kaikki ilmoitusta vaativat ehdotetut muutokset julkaistaan varmentajan verkkosivuilla kappaleen Kohdat, joiden muutos vaatii tiedonannon käyttäjille ja palveluntarjoajille 8.1.2 mukaisesti. Sopimusehtoihin vaikuttavista muutoksista ilmoitetaan kirjallisesti palveluntarjoajille sopimuksen allekirjoittajan yhteystiedoissa mainittuun osoitteeseen.

8.3 Varmennuskäytännön muutos- ja hyväksymismenettely

8.3.1 Varmennuskäytännön hallitsija

Tätä varmennuskäytäntöä hallinnoi Soneran varmennepolitiikkayksikkö, jonka yhteystiedot on kerrottu varmennuskäytännön alussa.

8.3.2 Muutosmenettely

Varmentajan varmennepolitiikkayksikkö käy läpi ja hyväksyy kaikki varmennuskäytäntöön tehtävät muutokset ennen niiden julkaisua.

8.4 Versionhallinta

Varmentaja arkistoi kaikki hyväksymänsä varmennuskäytäntöversiot ja ne ovat pyydettäessä saatavilla.

Liite 1: Varmennusorganisaation osapuolten vastuut ja velvollisuudet

Osapuolet ja velvoitteet	Selitykset ja tarkennukset
Varmentaja	
Kokonaisvastuu varmennepalvelun tuottamisesta.	Varmentajalla on asianmukaiset sopimukset ja sopimussuhteet niiden palveluiden tuottamisesta, joihin liittyy ulkoistusta, alihankintaa tai muuta kolmansien osapuolten käyttöä. Varmentaja vastaa tämän politiikan vaatimusten täyttymisestä myös silloin, kun osa varmentajan toiminnoista on ulkoistettu alihankkijoille.
Varmennepalvelun tuottamisessa siihen liittyvän lainsäädännön sekä varmentajien yhteisten että varmentajan omien käytäntöjen noudattaminen.	Varmentajan toimintaa säätelee • Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) • Varmennepolitiikka • Varmentajan omat varmennuskäytäntö-dokumentit (CPS)
Varmennepalvelun tuottaminen varmennuskäytäntö-dokumentin (CPS) mukaisesti.	Varmentaja vastaa siitä, että Mobiilivarmenne on käytettävissä luovutushetkestä alkaen koko Mobiilivarmenteen voimassaoloajan, ellei varmennetta ole asetettu sulkulistalle. Kortin liikkeellelaskija voi irtisanoa liittymäsopimuksen esimerkiksi maksamattomien laskujen vuoksi, jolloin myös Mobiilivarmenne suljetaan. Varmentaja vastaa oman varmennejärjestelmänsä turvallisuudesta.
Varmennepolitiikan kehittäminen ja ylläpito	Varmentajat yhdessä huolehtivat varmennepolitiikan kehittämisestä ja ylläpidosta.
Varmenteen hakijan tunnistaminen luotettavasti ja sopimuksen tekeminen.	Varmenteen hakijan tunnistamisessa noudatetaan mitä laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) on määrätty. Hakijan kanssa tehtävä sopimus täyttää lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) vaatimukset. Varmentaja ilmoittaa hakijalle tai rekisteröijälle varmenteen myönnöstä tai peruuttamisesta. Varmentaja vastaa myös siitä, että Mobiilivarmenne on luovutettu henkilölle, joka on tunnistettu Mobiilivarmenteelta edellytettävällä tavalla.

	Mikäli hakijan tunnistamisen tekee asiamies (Rekisteröijä), on varmentajan tämän kanssa tekemässään sopimuksessa velvoitettava lain mukainen toimintatapa.
Huolehtii varmenteiden tietosisällön virheettömyydestä.	Tarkistaa varmenteen hakijan henkilötiedot Väestörekisterikeskuksen Väestötietojärjestelmästä. Allekirjoittaessaan Mobiilivarmenteen yksityisellä avaimellaan varmentaja vakuuttaa tarkistaneensa Mobiilivarmenteessa olevat henkilötiedot varmennepolitiikassa ja varmennuskäytännössä esitettyjen menettelyjen mukaisesti Väestötietojärjestelmästä. Varmentaja vastaa ainoastaan niistä tiedoista, jotka se on tallettanut Mobiilivarmenteeseen.
Huolehtii varmenteiden sulkemisesta ja varmenteiden sulkulistojen julkaisemisesta.	Kukin varmentaja on velvollinen julkaisemaan varmenteet ja sulkulistat siten, että ne ovat kaikkien niitä tarvitsevien tahojen saatavilla. Varmentaja vastaa siitä, että sulkulistalle viedään oikea Mobiilivarmenne ja että ne ilmestyvät tässä varmennepolitiikassa mainitussa ajassa sulkulistalle.
Noudattaa varmenteen omistajien henkilötietojen käsittelyssä voimassa olevaa lainsäädäntöä, Viestintäviraston ohjeistusta, hyvää tietosuojan tasoa sekä hyvää tietojenkäsittelytapaa.	Suojaa henkilötiedot riittävillä teknisillä ja organisatorisilla toimenpiteillä laittomalta tai luvattomalta käytöltä. Suojaa kaikki varmennuspalveluun liittyvät tärkeät tiedot ja tiedostot häviämiseltä, tuhoamiselta ja väärentämiseltä. Varmentajalla on tietoturvallisuuden hallintajärjestelmä, joka on riittävä sen tarjoamille varmennepalveluille. Varmenteen hakijan varmentajalle luovuttamaa henkilötietoa ei luovuteta muille ilman hakijan suostumusta, tuomioistuinpäätöstä tai muuta lakiin perustuvaa vaatimusta muutoin kuin varmenteen tietosisällön osana. Joitain tietoja saatetaan myöhemmin joutua palauttamaan oikeudellisista syistä.
Varmentaja on juridinen henkilö voimassa olevan lainsäädännön mukaisesti.	Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009
Varmentaja on huolehtinut riittävistä järjestelyistä, joiden avulla se pystyy hoitamaan toiminnastaan koituvat vastuut.	Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009

Varmentaja on taloudellisesti vakavarainen ja sillä on riittävät taloudelliset voimavarat toimia tämän politiikan mukaisesti.	Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)
Varmentajalla on varmennepalveluiden tarjoamiseen riittävä määrä työntekijöitä, joilla on tarvittava koulutus, tekninen osaaminen ja kokemus, ottaen huomioon varmennepalveluiden luonne, kattavuus ja volyymi.	Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)
Varmenteen luomiseen ja peruuttamiseen liittyviä tehtäviä hoitavien varmentajan organisaation osien rakenteen tulee olla dokumentoitu.	Laki vahvasta sähköisestä tunnistamisesta sähköisistä luottamuspalveluista 617/2009.
Rekisteröijä	
Hoitaa varmentajan puolesta varmenteen hakijan tunnistamisen varmennuskäytännön mukaisesti. Rekisteröijä toimii varmentajan lukuun ja vastuulla siten kuin varmentajan ja rekisteröijän välisessä sopimuksessa on sovittu.	Asianmukaisen ja täydellisen varmennepyynnön toimittaminen varmentajalle ensimmäistä varmennetta haettaessa, varmennetta uusittaessa ja avainpareja uusittaessa. Hakijan tunnistaminen tämän varmennuskäytännön mukaisesti. Varmistaa, että varmenteen hakijalle on toimitettu ennen sopimuksen solmimista Mobiilivarmenteen käyttöön liittyvät käyttöohjeet. Liittymän tilaajan lupa maksullisen lisäpalvelun käyttöönottamiseen sikäli, kun tämä on tarpeen. Edellä mainittu pätee myös siinä tapauksessa, että varmentaja toimii rekisteröijänä.
Liittymäkortin liikkeellelaskija	
Turvaa allekirjoituksen luomistietojen luottamuksellisuuden eikä tallenna tai jäljennä varmenteen omistajalle luovutettuja allekirjoituksen luomistietoja.	Kortilla luotavien avainten tapauksessa kortin liikkeellelaskija vastaa kortilla olevan alustan turvallisuudesta avaintenluontiohjelman ajamista varten, avaintenluontisovelluksesta, kortin turvamoduulin luotettavuudesta ja yksityisen avaimen luottamuksellisuudesta.
Varmenteen omistaja	

Antaa tarkat ja täydelliset henkilötiedot varmentajalle tai tämän edustajalle tämän politiikan mukaisesti rekisteröinnin yhteydessä.	Rekisteröijä varmistaa omalta osaltaan, että varmenteen hakijan antamat tiedot ovat täydelliset ja virheettömät. Varmenteen hakija hyväksyy hakemuksen henkilötiedot allekirjoituksella tai vastaavalla.
Ilmoitettava varmentajalle nimen vaihdoksesta enintään kolmen kuukauden kuluessa muutoksesta.	Käyttäjä velvoitettava tähän Varmentajan ja Varmenteen omistajan välisessä sopimuksessa.
Säilyttää tunnistusvälinettä ja siihen liittyviä tunnuslukuja huolellisesti estääkseen mobiilivarmenteen luvattoman käytön.	Määritetty varmenteen haltijan velvollisuudeksi laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009). Varmentajan on Varmenteen omistajan kanssa tekemässään sopimuksessa otettava tämä huomioon. Varmenteen omistajan on käytettävä avaimiensa suojaamiseen tunnuslukuja ja säilytettävä nämä luvut huolellisesti. Mobiilivarmenne on omistajansa sähköinen henkilöllisyys, eikä sitä tämän vuoksi saa luovuttaa toisen henkilön käytettäväksi. Mobiilivarmenteen omistaja on vastuussa varmenteen käytöstä, sillä tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista.
Varmenteen omistajan tulee viipymättä tehdä varmentajan Sulkupalveluun ilmoitus	Määritetty varmenteen haltijan velvollisuudeksi laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009). Varmentajan on Varmenteen omistajan kanssa tekemässään sopimuksessa otettava tämä huomioon. Ilmoitus on tehtävä välittömästi kun: • Varmenteen omistajalla on syytä epäillä että hänen liittymäkorttinsa on kadonnut, varastettu tai otettu luvattomasti käyttöön, • Varmenteen omistaja on menettänyt yksityisen avaimensa hallinnan, koska sen aktivointitieto (ts. tunnusluku) on kadonnut tai joutunut vääriin käsiin, tai jostain muusta syystä, • Varmenteen omistajalle on käynyt ilmi, että varmenteen tiedot eivät enää päde tai että niissä on epätarkkuuksia. Mobiilivarmenteen omistajan vastuu varmenteen käyttämisestä päättyy, kun hän on ilmoittanut sulkupalveluun tarvittavat tiedot sen sulkemiseksi. Tällöin vastuu siirtyy varmentajalle. Sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on

	havaittu. Varmenteen omistajan tulee säilyttää yksityisiä avaimiaan huolellisesti estääkseen yksityisten avaintensa eli käytännössä niihin liittyvien tunnuslukujen luvattoman käytön.
Varmenteeseen luottava osapuoli	
Tarkistaa ja varmistaa varmenteen voimassaolo varmenteen käytön yhteydessä	Varmenteeseen luottavan osapuolen tulee tarkistaa varmenteen voimassaolo seuraavasti: • Varmistettava varmenteen aitous ja eheys tarkistamalla sen myöntäjän sähköinen allekirjoitus käyttäen varmenteen myöntäjän julkista avainta. • Noudettava varmennetta koskevat sulkutiedot vähintään yhdestä varmenteeseen tallennetusta osoitteesta. • Varmistettava sulkutiedon aitous ja eheys tarkistamalla sen myöntäjän sähköinen allekirjoitus ja tähän käytetyn varmenteen voimassaolo. • Tarkistettava sulkutiedon voimassaoloajan kattavuus. Varmennetta ei pidä hyväksyä, mikäli ajantasaista ja voimassa olevaa sulkutietoa ei ole saatavilla. Kaikki varmenteen hyväksymiset ajantasaisen tiedon puuttuessa tapahtuvat varmenteeseen luottavan osapuolen omalla riskillä. • Varmistettava, että käytettävä varmenne ei ole sulkutietojensa perusteella suljettu. • Tarkistettava, että myönnetty varmenne vastaa käyttötarkoitustaan siinä oikeustoimessa, jossa sitä on käytetty.
Varmenteen käyttöön liittyvien tietojen tallentaminen.	Luottavan osapuolen vastuulla on säilyttää ne tiedot, jotka hän tarvitsee mobiilivarmenteella tehtyjen toimenpiteiden varmentamiseksi myöhempänä ajankohtana. Tällaisia tietoja ovat käytetyt varmenteet ja sulkulistat sekä allekirjoituksen luontiajankohta, joka on myös syytä pitää mukana allekirjoitetussa tietosisällössä.