MOBIILIASIOINTIVARMENNE

VARMENNEPOLITIIKKA

Operaattoreiden mobiiliasiointivarmenteita varten

Versio 1.1

Voimassa 15.4.2011 lähtien

Yhteystiedot

Varmennepolitiikkaa hallinnoiva organisaatio

Tämän varmennepolitiikan ovat hyväksyneet kaikki luottamusverkostosopimuksen allekirjoittaneet varmentajat, jotka huolehtivat yhdessä tämän varmennepolitiikan hallinnoinnista ja päivityksistä.

Tämän varmennepolitiikan tekijänoikeudet kuuluvat mobiilivarmennuspalvelun luottamusverkoston jäsenille. Varmennepolitiikkaan liittyviin kysymyksiin vastaavat kaikki mobiilivarmennuspalvelun luottamusverkostoon kuuluvat varmentajat. Varmentajaan saa yhteyden sähköpostiosoitteella, joka löytyy osoitteesta www.mobiilivarmenne.fi.

Varmennepolitiikan tunnisteet

Tämän varmennepolitiikan nimi on "MOBIILIASIOINTIVARMENNE - VARMENNEPOLITIIKKA - Operaattoreiden mobiiliasiointivarmenteita varten".

Varmennepolitiikan tunniste (Object Identifier) on: 1.2.246.277.1.11.4.1.2.2

ISO(1).MemberBody(2).Suomi(246).HPY(277).Services(1).caService(11).MobileCertificates(4).CertificatePolicies(1).Elisa-ID CA(2).Serial no(2)

Varmennepolitiikan tunnistetieto on sijoitettu varmenteen X.509 v3 määrityksen [X.509] mukaiseen varmennepolitiikan tunnistetietokenttään (Policy OID). Tätä varmenteen kenttää tutkimalla varmenteeseen luottava osapuoli voi varmistua varmenteen varmennepolitiikasta ja sopivuudesta kyseessä olevaan käyttötarkoitukseen.

Yhteystiedot 2
Varmennepolitiikkaa hallinnoiva organisaatio 2
Varmennepolitiikan tunnisteet 2
Käsitteitä ja aihepiiriin liittyvää sanastoa 6
Lyhenteet 10
Roolit 11
1 Johdanto 12
1.1 Mobiilivarmennepalvelu 12
1.2 Varmennepolitiikka 12
1.3 Mobiilivarmenne 12
1.4 Varmennusorganisaatio 13
1.4.1 Varmentaja 13
1.4.2 Rekisteröijä 13
1.4.3 Liittymäkortin liikkeellelaskija 13
1.4.4 Sulkupalvelu 14
1.4.5 Hakemistopalvelu 14
1.4.6 Varmenteen omistaja 14
1.4.7 Varmenteeseen luottava osapuoli 14
1.5 Varmenteen käyttäminen 14
1.6 Osapuolten vastuut ja velvollisuudet 14
2 Yleiset ehdot 15
2.1 Tietojen julkaiseminen ja saatavuus 15
2.1.1 Varmentajan tietojen julkaiseminen 15
2.1.2 Sulkulistojen julkaisutiheys 15
2.1.3 Tietojen saatavuus 15
2.1.4 Tietovarastot 15
2.2 Auditointi 15
2.3 Tietojen luottamuksellisuus ja julkisuus 15
3 Varmentajien yksilöinti 16
3.1 Varmentajien nimeämiskäytäntö 16
4 Toiminnalliset vaatimukset 17
4.1 Varmenteen hakeminen 17
4.2 Varmenteen hakijan tunnistaminen 17
4.2.1 Tunnistusvälineen toimittaminen 17
4.3 Varmenteen myöntäminen 17
4.4 Varmenteen luominen 17
4.5 Varmenteen voimassaolon päättyminen ja sulkeminen 18
4.5.1 Varmenteen sulkemisen edellytykset 18
4.5.2 Sulkupyynnön tekijä 18
4.5.3 Sulkutapahtuma 18
4.5.4 Sulkutapahtuman ajoitus 18
4.5.5 Varmenteen sulkeminen tilapäisesti 19
4.5.6 Tilapäisen sulkupyynnön tekijä 19
4.5.7 Tilapäisen sulkupyynnön tekemistapa 19
4.5.8 Tilapäisen sulun aikarajoitukset 19
4.5.9 Varmenteen tilapäisen sulun purkaminen 19
4.5.10 Sulkulistan julkaisutiheys 19
4.5.11 Sulkulistan jakelupisteet 19
4.5.12 Suorakäyttöinen varmenteen tilan tarkistaminen 19
4.6 Varmenteen uusiminen 19
4.6.1 Varmenteen uusiminen varmenteen vanhenemisen vuoksi 20
4.6.2 Varmenteen uusiminen nimenmuutoksen vuoksi 20
4.6.3 Varmenteen uusiminen uuden ensitunnistamisen vuoksi 20
4.6.4 Avainparin uusiminen varmenteen sulkemisen jälkeen 20
4.7 Järjestelmän valvonta 20
4.8 Varmenteisiin liittyvien tietojen arkistointi 20
4.8.1 Tallennettava aineisto 20
4.8.2 Arkistojen suojaus 21
4.8.3 Arkistojen varmistusmenettelyt 21

4.8.4 Arkistotietojen hankinta- ja varmistusmenetelmät 21
4.9 Varmentajan avainten uusiminen 21
4.10 Toiminnan jatkumisenhallinta ja poikkeustapausten käsittely 21
4.10.1 Varmentajan yksityinen avain on paljastunut tai varmentajan varmenne on suljettu 21
4.10.2 Turvallisuuden vaarantuminen luonnonmullistuksen tai muun katastrofin seurauksena 21
4.11 Varmentajan toiminnan lakkauttaminen 21
5 Fyysiset, toiminnalliset ja henkilöstöturvallisuuteen liittyvät vaatimukset 22
5.1 Fyysinen turvallisuus 22
5.1.1 Sijainti ja rakennusten ominaisuudet 22
5.1.2 Fyysinen pääsy toimitilaan 22
5.1.3 Varajärjestelyt 22
5.2 Toiminnalliset vaatimukset 22
5.2.1 Vastuunjako 22
5.2.2 Tehtäviin vaadittavien henkilöiden lukumäärä 22
5.2.3 Tehtäväkohtainen tunnistaminen 22
5.3 Henkilöturvallisuus 23
5.3.1 Henkilökuntaa koskevan taustaselvityksen tekeminen 23
5.3.2 Taustaselvityksen tekemisessä noudatettava menettely 23
5.3.3 Koulutukseen liittyvät vaatimukset 23
5.3.4 Asiantuntemuksen ja osaamisen ylläpito 23
5.3.5 Poikkeamista johtuvat toimenpiteet 23
5.3.6 Henkilökunnan käyttöön annettavat asiakirjat 23
6 Tekniset turvatoimet 24
6.1 Avainparin luominen, tallettaminen ja käyttöönotto 24
6.1.1 Avainparin luominen 24
6.1.2 Liittymäkortin luovuttaminen hakijalle 24
6.1.3 Varmenteen hakijan julkisen avaimen toimittaminen varmentajalle 24
6.1.4 Varmentajan julkisen avaimen jakelu 24
6.1.5 Avainten pituudet 24
6.1.6 Avainten käyttötarkoitukset 25
6.2 Varmentajan yksityisten avainten suojaaminen 25
6.2.1 Turvamoduulia koskevat standardit 25
6.2.2 Varmentajan yksityisen avaimen käsittelyyn osallistuva henkilökunta 25
6.2.3 Yksityisen avaimen varmuuskopio 25
6.2.4 Yksityisen avaimen arkistointi 25
6.2.5 Yksityisen avaimen hallinnointi turvamoduulissa 25
6.3 Varmenteen omistajan avainten suojaaminen 25
6.3.1 Liittymäkorttia koskevat standardit 25
6.3.2 Yksityisen avaimen luovutus luotetun osapuolen huostaan 25
6.3.3 Yksityisen avaimen varmuuskopio 26
6.3.4 Yksityisen avaimen arkistointi 26
6.3.5 Yksityisen avaimen hallinnointi liittymäkortilla 26
6.4 Muut avainparin hallintaan liittyvät seikat 26
6.4.1 Julkisen avaimen arkistointi 26
6.4.2 Julkisten ja yksityisten avainten voimassaoloaika 26
6.5 Liittymäkortilla olevien yksityisten avainten tunnusluvut 26
6.5.1 Tunnusluvun luominen ja käyttöönotto 26
6.5.2 Tunnusluvun suojaus 26
6.6 Varmennejärjestelmän laitteiden käyttöön ja pääsyyn liittyvät turvallisuusvaatimukset 26
6.6.1 Laitteistoturvallisuus 26
6.7 Varmennejärjestelmän elinkaaren hallinta 26
6.7.1 Varmennejärjestelmän kehittämiseen liittyvä valvonta 26
6.7.2 Turvallisuuden hallinta 26
6.8 Tietoverkon turvallisuus 27
6.9 Turvamoduulin käytön valvonta 27
7 Varmenne- ja sulkulistaprofiilit 28
7.1 Varmenteiden tekniset tiedot 28

7.1.1 Yhteiset attribuutit 28
7.1.2 Varmentajakohtaiset attribuutit 28
7.2 Sulkulistaprofiili 28
8 Varmennepolitiikan hallinnointi 29
8.1 Varmennepolitiikan muutosmenettely 29
8.1.1 Kohdat, joita voi muuttaa ilman tiedonantoa käyttäjille ja palveluntarjoajille 29
8.1.2 Kohdat, joiden muutos vaatii tiedonannon käyttäjille ja palveluntarjoajille 29
8.1.3 Muutokset, joiden johdosta täytyy laatia uusi varmennepolitiikka 29
8.2 Julkaiseminen ja tiedottaminen 29
8.3 Varmennepolitiikan muutos- ja hyväksymismenettely 29
8.3.1 Varmennepolitiikan hallitsija 29
8.3.2 Muutosmenettely 29
8.4 Versionhallinta 30
Viiteluettelo 31
Liite 1: Varmenteen tietosisältö 32
Liite 2: Varmennusorganisaation osapuolten vastuut ja velvollisuudet 34
Liite 3: Testikäyttöön myönnettävän varmenteen näennäinen henkilöllisyys 40

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 allekirjoituksista (617/2009). Asiointivarmenne ei 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.
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		Mobiiliasiointivarmenne on mobiilipäätelaitteen liittymäkorteilla sijaitseviin yksityisiin avaimiin perustuva 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.
Sulkulista	Certificate Revocation List (CRL)	Julkisen avaimen järjestelmässä käytöstä poistettujen varmenteiden luettelo. Varmentaja julkaisee sulkulistan hakemistopalvelussa.
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
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,	Epäsymmetrinen salausalgoritmi, jota käytetään epäsymmetrisen avainparin luontiin. Lyhenne tulee keksijöidensä sukunimistä Rivest, Shamir ja Adleman.
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 luoneet Mobiilivarmennepalvelun, jota matkapuhelimia käyttävät kuluttajat voivat hyödyntää asioidessaan palveluntuottajien erilaisissa sähköisissä palveluissa. Palvelu tarjoaa kuluttajille helpon ja turvallisen tavan tunnistautua palveluihin sekä varmistua asioinnin yhteydessä tekemiensä sitoumusten sisällöstä ja kiistämättömyydestä. Palveluntarjoajille Mobiilivarmennepalvelu mahdollistaa käyttäjien henkilöllisyyden luotettavan tunnistamisen ja todentamisen sekä palveluun liittyvien, asiakkaan hyväksyntää vaativien, tapahtumien vahvistamisen asiakkaan sähköisellä allekirjoituksella. Mobiilivarmennepalvelu täyttää vahvan sähköisen tunnistamisen kriteerit, jotka on määritetty laissa vahvasta sähköisestä tunnistamisesta.

1.2 Varmennepolitiikka

Tämä varmennepolitiikka kuvaa operaattoreiden noudattamat periaatteet ja käytännöt niiden myöntäessä mobiilivarmenteita niihin asiakassuhteessa oleville luonnollisille henkilöille. Tähän on seuraavat poikkeukset: Varmentaja voi halutessaan myöntää varmenteita oman toimintansa vaatimille palveluille ja luottamusverkostoon kuuluvan varmentajan tekniselle henkilökunnalle käyttäen myöhemmin määriteltyä testihenkilön profiilia. Nämä varmenteet eivät ole mobiilivarmenteita, eivät noudata tätä varmennepolitiikkaa, eivätkä sisällä varmennepolitiikan tunnistetta, vaikka ne ovatkin mobiilivarmentajan myöntämiä. Varmennepolitiikan tunnisteen (*Policy Identifier*) puuttuminen varmenteen tietosisällöstä merkitsee, ettei varmenne ole luonnolliselle henkilölle myönnetty mobiilivarmenne eikä tällaiseen varmenteeseen pidä luottaa henkilön tunnistusvälineenä. Liitteessä 3 on määritelty testihenkilöllisyydet, joita käyttäen operaattorit voivat myöntää testivarmenteita.

Varmenteiden myöntö vaatii aina sopimuksen varmentajan ja varmenteen hakijan välille.

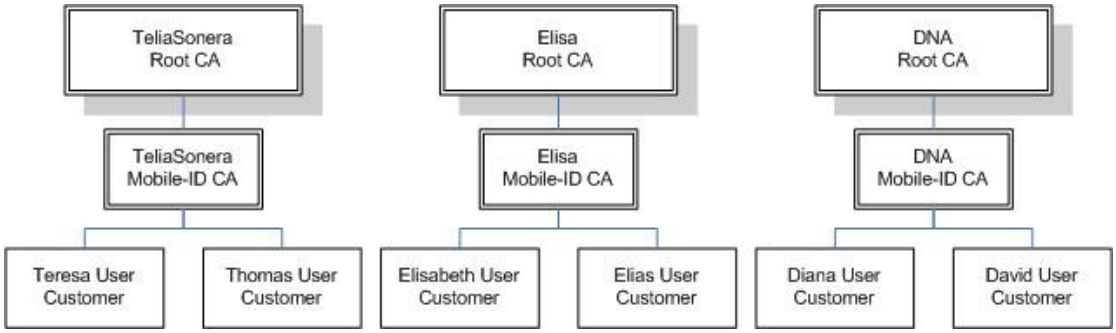
Varmennepolitiikka on laadittu IETF:n suosituksen RFC-3647 [RFC3647] mukaisesti ja sitä noudattaen myönnettävät varmenteet ovat RFC-5280 standardin [RFC5280] mukaisia X.509 varmenteita [X.509].

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.

Mobiilivarmenteet myöntää varmentaja, jonka yksilöivät tiedot löytyvät jokaisen myönnetyn varmenteen myöntäjä (*Issuer*) –kentästä. Varmentajan varmenteen on myöntänyt ja allekirjoittanut yksityisellä avaimellaan varmennepalvelun juurivarmentaja.

Mobiilivarmenteita käytetään kuvan 1 mukaisessa hierarkiassa. Kaikki varmentajat ovat itsenäisiä ja kullakin tätä politiikkaa käyttävällä varmentajalla on oma juurivarmenteensa, johon varmenteen käyttäjät luottavat.



Kuva 1: Mobiilivarmenteisiin liittyvä varmennehierarkia.

Varmentaja takaa, että tämän varmennepolitiikan mukaisiin varmenteisiin pätevät seuraavat ominaisuudet:

- Varmentaja on myöntänyt varmenteen ja hallinnoi niitä tämän varmennepolitiikan mukaisesti
- Loppukäyttäjän mobiilivarmenteen on myöntänyt luottamusverkostoon kuuluva varmentaja. Varmentajan varmenteen on myöntänyt varmentajan varmennepalvelun juurivarmentaja.
- Varmenteen omistajasta rekisteröidyt tiedot ovat oikein varmenteessa.
- Varmentajan yksityiset avaimet on talletettu turvalliselle välineelle, josta niitä ei saa kopioitua toiselle välineelle.
- Varmentajan varmenne ja ajantasainen sulkuinformaatio ovat saatavissa hakemistopalvelusta vuoden jokaisena päivänä vuorokauden ympäri.

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

1.4 Varmennusorganisaatio

1.4.1 Varmentaja

Varmentaja tuottaa varmennepalvelun. Kukin luottamusverkoston varmentaja laatii oman varmennuskäytäntönsä, joka perustuu tähän varmennepolitiikkaan ja on saatavilla varmentajan omilta verkkosivuilta.

1.4.2 Rekisteröijä

Rekisteröijällä tarkoitetaan tahoa, joka toimii varmentajan toimeksiannosta ja vastuulla ja hoitaa varmennehakemusten käsittelyyn liittyvää käytännön työtä noudattaen tätä varmennepolitiikkaa ja vastaavaa varmennuskäytäntöä. Mobiilivarmenteen rekisteröijinä toimivat varmentajan paikalliset asiointipisteet sekä muut varmentajan kanssa rekisteröintiä koskevan sopimuksen tehneet organisaatiot. Tarkempi menettelytapa kuvataan kyseessä olevaa teknistä alustaa kuvaavassa varmennuskäytännössä. Itsepalvelurekisteröitymisessä rekisteröijäksi katsotaan varmenteen myöntäjä.

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.

1.4.4 Sulkupalvelu

Varmenteiden sulkupalvelu sulkee varmenteet, jotka varmenteen omistaja, varmentaja, rekisteröijä tai kortin liikkeellelaskija haluaa suljettavaksi ennen varmenteen voimassaoloajan päättymistä.

1.4.5 Hakemistopalvelu

Hakemistopalvelu on *julkinen* Internet-palvelu, josta ovat saatavilla varmentajan varmenteet, sulkulista sekä ne mobiilivarmenteet, joiden julkaisemiseen on varmenteen omistajan suostumus.

1.4.6 Varmenteen omistaja

Varmentaja myöntää Mobiilivarmenteen varmenteen omistajalle 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. Tässä varmennepolitiikassa varmenteeseen luottavalla osapuolella tarkoitetaan luottamusverkostosopimuksen allekirjoittanutta varmentajaa, joka on sopimussuhteessa sähköisiä palveluja loppukäyttäjälle tuottavan tahon kanssa.

1.5 Varmenteen käyttäminen

Tämän varmennepolitiikan mukaista Mobiilivarmennetta voidaan käyttää henkilön sähköiseen tunnistamiseen, viestinnän salaamiseen ja sähköiseen allekirjoitukseen sen mukaisesti, kuin teknistä alustaa koskien on määritelty varmennuskäytännössä. Mobiilivarmennetta voidaan käyttää käyttötarkoituksensa mukaisesti erilaisissa sovelluksissa ja palveluissa.

Varmenteen käyttöä ei ole rajoitettu muutoin kuin mitä seuraa varmenteen käyttötarkoituksesta (*keyUsage*). Palvelut, jotka käyttävät hyväkseen varmennetta, voivat asettaa käytölle omia rajoituksia tai estoja.

1.6 Osapuolten vastuut ja velvollisuudet

Mobiilivarmennuspalvelun luottamusverkoston muodostavat varmennuspalvelun tuottamisesta keskinäisen sopimuksen tehneet Varmentajat. Mobiilivarmennuspalvelun toiminta edellyttää, että eri osapuolille määritetyt vastuut ja velvollisuudet tulevat täytettyä. Tekemänsä sopimuksen perusteella varmentajat ovat sitoutuneet noudattamaan tätä varmennepolitiikkaa. Niiltä osin, kun varmentajat eivät itse toimi muissa määritellyissä rooleissa, ei varmennusorganisaation muita osapuolia voida velvoittaa noudattamaan tätä varmennepolitiikkaa.

Varmentajat ovat velvollisia muiden osapuolten kanssa tekemissään sopimuksissa edellyttämään näiltä varmennepolitiikassa ja omassa varmennuskäytännössään asetettuja käytäntöjä, vastuita ja velvollisuuksia. Varmennusorganisaation eri osapuoliin liittyvät vastuut ja velvollisuudet on kuvattu liitteessä 2 Varmennusorganisaation osapuolten vastuut ja velvollisuudet.

2 Yleiset ehdot

2.1 Tietojen julkaiseminen ja saatavuus

2.1.1 Varmentajan tietojen julkaiseminen

Varmentaja julkaisee sulkulistat yleisesti saatavilla olevalla palvelimella. Varmenteet julkaistaan varmentajien ja Mobiilivarmenteeseen luottavien palveluntarjoajien saataville sekä mahdollisesti yleisesti saatavilla olevassa hakemistossa. Varmentaja julkaisee varmennepolitiikan, varmennuskäytännöt, varmennekuvauksen (PDS) sekä muut julkiset varmennepalvelujen tuottamiseen liittyvät dokumentit www-sivuillaan.

2.1.2 Sulkulistojen julkaisutiheys

Sulkulistat julkaistaan tunnin välein ja ne ovat voimassa 24 tuntia julkaisuhetkestä eteenpäin. Sulkulista päivitetään aina viipymättä muutoksen jälkeen.

2.1.3 Tietojen saatavuus

Sulkulistat ovat kaikkien niitä tarvitsevien saatavilla. Varmenteet ovat julkisia sen mukaan mitä varmenteen omistajan kanssa on sovittu. Varmennepolitiikka ja varmentajien varmennuskäytännöt sekä varmennekuvaus (PDS) ovat julkisesti saatavilla olevia dokumentteja, jotka ovat jaossa varmentajien verkkosivuilla.

Varmenteet julkaistaan hakemistossa, jonne vain varmentajan järjestelmillä on pääsy. Osa varmenteista voidaan julkaista julkisessa hakemistossa (esim. julkisille puhelinnumeroille myönnetyt varmenteet).

2.1.4 Tietovarastot

Varmentajan julkaisemat tiedot ovat saatavilla varmentajan www-sivuilla. Varmenteet ovat talletettuina varmentajien luottamuksellisiin tietovarastoihin. Varmentajien tiedot arkistoidaan voimassaolevien arkistosäännösten mukaisesti. Varmentajat ovat laatineet myös henkilötietolain mukaisen rekisteriselosteen varmennejärjestelmän henkilötietojen käsittelyn osalta.

2.2 Auditointi

Varmentaja tarkastaa teknisten toimittajiensa ja rekisteröijiensä toimitilat, laitteet ja toiminnan tarkoituksenmukaisella tavalla. Varmentaja voi halutessaan tarkastuttaa oman toimintansa ulkoisella auditoijalla. Yksityiskohtainen tarkastusmenettely on kuvattu varmennuskäytännössä.

2.3 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 Varmentajien yksilöinti

Varmentajalla, joka myöntää tämän politiikan mukaisia varmenteita, on yksikäsitteinen X.501:n mukainen *Distinguished Name* (DN) - nimi, joka löytyy varmentajan varmenteesta *Subject*-kentästä, sekä kaikkien tämän Varmentajan myöntämien varmenteiden *Issuer* -kentästä.

3.1 Varmentajien nimeämiskäytäntö

Varmentajan nimi koostuu seuraavista attribuuteista:

Attribuutti	**Sisältö**
commonName (CN)	XXX CA
Organization (O)	DNA Oy/Elisa Oyj/TeliaSonera Oyj
Country (C)	FI

Varmentajan nimen tietosisältö on kuvattu yksityiskohtaisesti ao. varmennuskäytännössä.

4 Toiminnalliset vaatimukset

4.1 Varmenteen hakeminen

Mobiilivarmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa ja sen liitteenä olevissa ennen Mobiilivarmennehakemuksen allekirjoittamista hakijalle annettavissa varmentajan mobiilivarmennepalvelun sopimusehdoissa. Hakemusasiakirjassa ja mobiilivarmennuspalvelun sopimusehdoissa on tiedot kummankin osapuolen oikeuksista ja velvollisuuksista.

Mikäli varmentaja mahdollistaa palvelussaan varmenteesen liittyviä käyttörajoituksia, on varmenteen rekisteröinnin yhteydessä varmenteen hakijalle annettava mahdollisuus käyttörajoitusten määrittämiseen varmennehakemuksessa ja sopimuksessa.

Kun mobiilivarmenteen hakija hakee varmennetta, hän hyväksyy samalla varmenteen käyttöön liittyvät sopimusehdot ja varmentajan antamat toimintaohjeet, tarkistaa henkilötietojensa oikeellisuuden sekä hyväksyy tai kieltää varmenteensa julkaisun hakemistossa.

Sopimukseen liittyen hakija erityisesti sitoutuu huolehtimaan mobiilivarmenteeseen liittyvien tunnuslukujen säilyttämisestä huolellisesti sekä mahdollisen väärinkäytön tai varmenteiden tai liittymäkortin katoamisen ilmoittamisesta.

Mobiilivarmenteen yksityiskohtainen hakuprosessi kuvataan varmennuskäytännössä.

4.2 Varmenteen hakijan tunnistaminen

Mobiilivarmenteen hakija tunnistetaan joko käyttäen vahvaa sähköistä tunnistamista tai henkilökohtaisesti rekisteröijän asiointipisteessä.

4.2.1 Tunnistusvälineen toimittaminen

Tunnistusväline muodostuu liittymäkortista yksityisine avaimineen ja niihin liittyvistä tunnusluvuista. Liittymäkortti toimitetaan asiakkaalle ilman rekisteröityjä varmenteita. Tunnistusväline voidaan ottaa käyttöön onnistuneen rekisteröinnin jälkeen.

Kortin liikkeellelaskija varmistaa, että liittymäasiakkaalle toimitetaan Mobiilivarmenteen käytön kannalta oikeantyyppinen liittymäkortti. Liittymäkortti toimitetaan varmenteen hakijalle postitse tai henkilökohtaisesti asiointipisteessä operaattorin normaalin käytännön mukaisesti.

Yksityisten avainten tunnusluvut toimitetaan varmenteen hakijalle liittymäkortin mukana suojassa esimerkiksi raaputuspinnan alla siten, että vastaanottaja voi todeta luottamuksellisuuden säilyneen kuljetukseen ajan. Varmenteen hakijan tulee asettaa haluamansa tunnusluvut rekisteröinnin yhteydessä.

Prosessin yksityiskohdat on selostettu varmennuskäytännössä.

4.3 Varmenteen myöntäminen

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

4.4 Varmenteen luominen

Uusi Mobiilivarmenne luodaan rekisteröitymisen yhteydessä käyttäen aina uutta aiemmin käyttämätöntä avainmateriaalia. Mobiilivarmenne on käytettävissä onnistuneen rekisteröinnin jälkeen. Mobiilivarmenteen hakijalle korostetaan varmenteen luovutushetkellä, että yksityisistä avaimista ei ole eikä niistä voi myöhemminkään valmistaa kopiota.

4.5 Varmenteen voimassaolon päättyminen ja sulkeminen

4.5.1 Varmenteen sulkemisen edellytykset

Mobiilivarmenne on asetettava sulkulistalle, kun on syytä epäillä väärinkäyttöä esimerkiksi liittymäkortin katoamisen tai anastamisen vuoksi. Mobiilivarmenne voidaan sulkea soittamalla maksuttomaan sulkupalvelunumeroon tai rekisteröijän luona. Sulkupyyntö on tehtävä välittömästi sen jälkeen, kun epäilys väärinkäytön mahdollisuudesta on syntynyt.

Mobiilivarmenne on suljettava, mikäli sitä vastaava liittymä suljetaan. Suljettaessa liittymä tilapäisesti tehdään varmenteellekin tilapäinen sulku, ellei perusteltua syytä muuhun ole.

4.5.2 Sulkupyynnön tekijä

Mobiilivarmenteen sulkupyynnön tekee ensisijaisesti sen omistaja Sulkupyynnön voi tehdä myös varmentaja, kortin liikkeellelaskija tai viranomainen. Varmenteen sulkemista pyytäneen henkilön todentamiseen käytetty menetelmä kirjataan.
Varmenteen sulkemisen perusteet, ajankohta ja suorittajan tiedot talletetaan.

Sulkupyynnön tekijän tunnistaminen on kuvattu varmennuskäytännössä.

4.5.3 Sulkutapahtuma

Mobiilivarmenteen sulkupyyntö voidaan tehdä esimerkiksi seuraavilla tavoilla:

a) Puhelinsoitolla sulkupalveluun
b) Käymällä rekisteröijän luona, jos sulkeminen on mahdollista rekisteröijän toimipisteessä.

Varmenteen sulkeminen ja sen vaikutukset on kuvattu yksityiskohtaisesti varmennuskäytännössä. Tieto varmenteen sulkemisesta on julkisesti saatavilla välittömästi sen jälkeen, kun sulkupyyntö on todettu pätevästi ja hyväksytty.

Varmentaja sulkee varmenteet aina silloin, kun se on saanut tiedon varmenteen omistajan kuolemasta. ***Varmentaja tekee sulkemista koskevan ilmoituksen kuolleen varmenteen omistajan oikeudenomistajille.***

Varmentaja sulkee myöntämänsä varmenteet, mikäli varmenteiden tietosisällössä havaitaan virhe.

Varmentaja voi sulkea käyttämällään yksityisellä avaimellaan allekirjoitetut varmenteet, mikäli on syytä epäillä varmentajan yksityisten avainten paljastuneen tai joutuneen vääriin käsiin. Kaikki paljastuneella avaimella myönnetyt ja voimassa olevat varmenteet on suljettava yhdellä tai useammalla sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeisen suljetun varmenteen voimassaoloaika on päättynyt.

Mikäli varmentajan varmenteiden luonnissa käyttämä yksityinen avain tai muu tekninen menetelmä on paljastunut tai tullut muutoin käyttökelvottomaksi, Varmentajan on ilmoitettava tapahtuneesta varmenteen omistajille, palveluntarjoajille, Viestintävirastolle ja varmentajille asianmukaisella tavalla.

Varmentaja voi sulkea varmenteen erityisestä syystä, esimerkiksi kryptografisten hyökkäysmenetelmien kehityksestä johtuen.

4.5.4 Sulkutapahtuman ajoitus

Mobiilivarmenteen sulkeminen toteutetaan viipymättä sulkupyynnön yhteydessä.

4.5.5 Varmenteen sulkeminen tilapäisesti

Mobiilivarmenteen sulkeminen tilapäisesti tehdään muilta osin kuten pysyvä sulkeminen, mutta sulkemisen syykoodiksi merkitään mahdollisten muiden syykoodien lisäksi *certificateHold*.

4.5.6 Tilapäisen sulkupyynnön tekijä

Tilapäisen sulkupyynnön tekijää koskevat samat säännöt kuin pysyvän sulkupyynnön tekijää.

4.5.7 Tilapäisen sulkupyynnön tekemistapa

Tilapäistä sulkupyyntöä koskevat samat säännöt kuin pysyvää sulkupyyntöä.

4.5.8 Tilapäisen sulun aikarajoitukset

Tilapäinen sulku on voimassa kunnes se peruutetaan. Tilapäisen sulun purkupyynnön tekijää ja hänen tunnistamistansa koskevat samat säännöt kuin sulkupyynnön tekijää.

4.5.9 Varmenteen tilapäisen sulun purkaminen

Varmenteen tilapäisen sulun purkaja tunnistetaan joko käyttäen vahvaa sähköistä tunnistamista tai henkilökohtaisesti Rekisteröijän asiointipisteessä. Sulun purkajan tunnistaminen on kuvattu varmennuskäytännössä.

4.5.10 Sulkulistan julkaisutiheys

Tieto varmenteen viennistä sulkulistalle on julkisesti saatavilla viipymättä, kun sulkupyyntö on todettu päteväksi ja hyväksytty. Sulkulista on voimassa 24 tuntia. Sulkulista sisältää seuraavan sulkulistan julkaisuajankohdan.

Uusi sulkulista julkaistaan tunnin välein, kuitenkin viimeistään voimassaolevan sulkulistan voimassaolon päättymisajankohtaan mennessä.

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

4.5.11 Sulkulistan jakelupisteet

Sulkulista julkaistaan vähintään kahdessa erillisessä pisteessä, joista vähintään kahteen on viittaukset varmenteessa. Sulkulistan sijasta voidaan käyttää myös suorakäyttöistä varmenteen tilan tarkistamista OCSP-protokollalla.

4.5.12 Suorakäyttöinen varmenteen tilan tarkistaminen

Sulkulistan sijaan varmentaja voi käyttää OCSP-palvelua varmenteen tilan julkaisemiseen. Tätä kautta saatavan tiedon on oltava yhtäpitävää mahdollisesti tarjolla olevan sulkulistan kanssa.

4.6 Varmenteen uusiminen

Varmenteen uusiminen edellyttää aina avainmateriaalin vaihtamista käyttämättömään materiaaliin, ellei tässä varmennepolitiikassa erikseen muuta sanota.

4.6.1 Varmenteen uusiminen varmenteen vanhenemisen vuoksi

Varmenteen uusiminen vanhenemisen vuoksi johtaa uuden varmenteen rekisteröintiin. Liittymäkortilla luotavien avainten tapauksessa tapahtuma ei oleellisesti poikkea uuden varmenteen rekisteröinnistä. Yksityiskohdat on kuvattu tarkemmin varmennuskäytännössä.

Tehdasvalmisteisten avainten tapauksessa uusi varmenne rekisteröidään normaalisti käyttäen henkilön tunnistamiseen voimassa olevaa varmennetta. Näin ollen uusi varmenne rekisteröidään ennen kuin uusi liittymäkortti on kytketty verkkoon. Yksityiskohdat on kuvattu tarkemmin varmennuskäytännössä.

4.6.2 Varmenteen uusiminen nimenmuutoksen vuoksi

Kun varmenteen omistaja ilmoittaa nimenmuutoksesta varmentajalle, uusii varmentaja varmenteen halutessaan samalla avainmateriaalilla ja samalla voimassaolon päättymisajalla kuin voimassa oleva varmenne. Uusittu varmenne julkaistaan hakemistoissa samoin edellytyksin kuin alkuperäinen varmenne. Koska avainmateriaali ei muutu, voidaan varmenteen rekisteröinti tehdä ilman käyttäjän interaktiota. Uusi nimi tarkistetaan Väestötietojärjestelmästä samaan tapaan kuin uuden varmenteen rekisteröinnin yhteydessä.

4.6.3 Varmenteen uusiminen uuden ensitunnistamisen vuoksi

Varmentaja saa uusia varmenteen samalla avainmateriaalilla ja samalla voimassaolon päättymisajalla kuin voimassa oleva varmenne, mikäli varmentaja tekee uuden ensitunnistamisen kasvokkain. Tämän tarkoitus on mahdollistaa varmenteen tunnistustason nosto ja lyhentää ensitunnistusketjua saattamalla *identificationPathLength*-attribuutin arvo nollaksi. Uusimisen yhteydessä nimi tarkistetaan Väestötietojärjestelmästä samaan tapaan kuin uuden varmenteen rekisteröinnin yhteydessä.

4.6.4 Avainparin uusiminen varmenteen sulkemisen jälkeen

Avainparin uusiminen johtaa aina uuteen varmenteeseen uusilla avaimilla. Vanha varmenne ja avainpari pysyvät mitätöityinä.

4.7 Järjestelmän valvonta

Järjestelmän valvonta on kuvattu varmennuskäytännössä.

4.8 Varmenteisiin liittyvien tietojen arkistointi

4.8.1 Tallennettava aineisto

Varmentajan on tallennettava

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; sekä

4) varmenteen osalta varmenteen tietosisältö.

Edellä 1 kohdassa tarkoitetut tiedot on säilytettävä viisi vuotta tunnistustapahtumasta ja 2–4 kohdassa tarkoitetut tiedot viisi vuotta varmentajan ja varmenteen omistajan välisen asiakassuhteen päättymisestä.

Varmentajan arkistoimat tiedot, tallennusmenetelmä ja säilytysaika on kuvattu yksityiskohtaisesti varmennuskäytännössä.

4.8.2 Arkistojen suojaus

Arkistoitava tieto säilytetään korkean turvatason tiloissa, joissa on pääsynvalvonta.

4.8.3 Arkistojen varmistusmenettelyt

Varmuuskopiot varastoidaan fyysisesti erilliseen tilaan alkuperäisistä tiedoista.

4.8.4 Arkistotietojen hankinta- ja varmistusmenetelmät

Varmentaja varmistaa arkistojen tavoitettavuuden ja lukukelpoisuuden siinäkin tapauksessa, että varmentajan toiminta keskeytyy tai päättyy.

4.9 Varmentajan avainten uusiminen

Varmentajan avainten uusiminen on kuvattu varmennuskäytännössä.

4.10 Toiminnan jatkumisenhallinta ja poikkeustapausten käsittely

Varmentajalla on jatkuvuus- ja valmiussuunnitelma, joka mahdollistaa varmentajan toiminnan jatkuvuuden.

Poikkeustapauksiin varautuminen on kuvattu varmennuskäytännössä.

4.10.1 Varmentajan yksityinen avain on paljastunut tai varmentajan varmenne on suljettu

Varmentaja ilmoittaa jokaisessa varmennuskäytännössä ne toimenpiteet, joihin varmenteen omistajien, varmenteeseen luottavan osapuolen ja rekisteröijien ja varmentajan työntekijöiden on ryhdyttävä, mikäli varmentajan yksityinen avain on paljastunut tai tullut muutoin käyttökelvottomaksi.

4.10.2 Turvallisuuden vaarantuminen luonnonmullistuksen tai muun katastrofin seurauksena

Varmentaja on varautunut luonnonmullistukseen tai muuhun katastrofiin hajauttamalla varmennejärjestelmänsä hakemistopalvelut ja sulkulistajakelun maantieteellisesti useampaan eri paikkaan, jotta järjestelmän haavoittuvuus yhden pisteen vikaantumiselle olisi minimoitu.

4.11 Varmentajan toiminnan lakkauttaminen

Varmentajan lakkauttamisena pidetään tilannetta, jossa kaikki varmentajan varmenteen myöntämiseen liittyvät palvelut lakkautetaan pysyvästi. Varmentajan lakkauttamisella ei tarkoiteta tilannetta, jossa varmennepalvelu siirretään organisaatiolta toiselle.
Varmentaja ilmoittaa varmennepalveluiden lakkauttamisesta muille luottamusverkoston varmentajille ja asiakkailleen mahdollisimman pian, kuitenkin vähintään kuutta kuukautta ennen lakkauttamisen ajankohtaa.

Ennen varmentajan lakkauttamista suoritetaan vähintäänkin seuraavat toimenpiteet:

- 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 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.

5 Fyysiset, toiminnalliset ja henkilöstöturvallisuuteen liittyvät vaatimukset

5.1 Fyysinen turvallisuus

Varmentaja huolehtii varmennetuotannon turvallisuudesta ja toiminnasta asianmukaisella tavalla sen kaikilla osa-alueilla.

Yksityiskohtainen kuvaus turvallisuuteen liittyvistä järjestelyistä on varmennuskäytännössä.

5.1.1 Sijainti ja rakennusten ominaisuudet

Varmentajan järjestelmät sijaitsevat korkean turvatason konesalitiloissa ja täyttävät tietokonekeskuksille annetut turvallisuutta koskevat ohjeet ja määräykset.

Toimitilaturvallisuus on toteutettu siten, että asiattomien pääsy toimitiloihin on estetty.

5.1.2 Fyysinen pääsy toimitilaan

Toimitiloihin, joissa tehdään varmennejärjestelmän tuotannollisia tehtäviä, on valvottu pääsy. Kulunvalvontajärjestelmä havaitsee sekä luvallisen että luvattoman sisäänmenon. Konesalitiloihin vaaditaan henkilön tunnistautuminen, jolloin henkilö tunnistetaan ja pääsyoikeudet tarkistetaan sekä tapahtumat rekisteröidään. Konesalitiloja vartioidaan vuorokauden ympäri.

5.1.3 Varajärjestelyt

Laitteistoratkaisut on toteutettu hyvän tiedonhallintatavan mukaisesti siten, että järjestelmän pettäessä voidaan siirtyä käyttämään varajärjestelmää vaarantamatta järjestelmään sisältyvien tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä. Tärkeiden laitteiden varaosien saanti ja huolto on varmistettu.

5.2 Toiminnalliset vaatimukset

5.2.1 Vastuunjako

Varmentajan tehtävät on jaettu tehtävänmukaisiin vastuualueisiin, jotka on kuvattu yksityiskohtaisesti varmennuskäytännössä. Varmentajalla on oltava käytettävissä riittävät henkilöstöresurssit varmennetoimintaa varten.

5.2.2 Tehtäviin vaadittavien henkilöiden lukumäärä

Varmentajan yksityisen avaimen luominen, aktivointi, varmuuskopiointi ja palauttaminen suoritetaan valvotusti kahden järjestelmän ylläpitotehtäviin oikeutetun henkilön läsnä ollessa.

Varmentajan yksityisen avaimen peruuttaminen on mahdollista vain kahden oikeutetun henkilön valvonnassa.

Varmentajan yksityisen avaimen turvamoduulin alustuksessa on läsnä vähintään kaksi järjestelmän ylläpitotehtäviin oikeutettua henkilöä.

Järjestelmän käyttämiseen vaaditaan yhden tehtävään oikeutetun henkilön läsnäolo.

5.2.3 Tehtäväkohtainen tunnistaminen

Mobiilivarmenteen rekisteröijän, varmennejärjestelmän ylläpitäjän ja varmennejärjestelmän käyttäjän tunnistaminen ja tehtäväkuvaus on kuvattu yksityiskohtaisesti varmennuskäytännössä.

5.3 Henkilöturvallisuus

Varmentajat vastaavat kukin omasta varmennetoiminnastaan. Tekniset toimittajat toimivat varmentajan vastuulla ja lukuun.

Varmentaja kiinnittää erityistä huomioita sekä oman henkilökuntansa että teknisten toimittajien ja rekisteröijien luotettavuuteen ja tehtävien suorittamiseen tarvittaviin taitoihin.

5.3.1 Henkilökuntaa koskevan taustaselvityksen tekeminen

Varmentaja teettää omasta varmennepalveluhenkilöstöstään sekä edellyttää teknisiä toimittajia teettämään varmennetietojärjestelmän parissa työskentelevistä henkilöistään tarvittavat turvallisuus- ja taustaselvitykset.

5.3.2 Taustaselvityksen tekemisessä noudatettava menettely

Henkilökunnan työkokemus kartoitetaan työhönottovaiheessa. Henkilöön kohdistetaan turvallisuusselvitys antamiensa tietojen perusteella määrämuotoisella lomakkeella. Turvallisuusselvitysmenettely on kuvattu yksityiskohtaisesti varmennuskäytännössä.

5.3.3 Koulutukseen liittyvät vaatimukset

Varmentajan henkilökunnan on oltava koulutettu siten, että tehtävän hoitaminen on mahdollista.

5.3.4 Asiantuntemuksen ja osaamisen ylläpito

Henkilökunnan koulutus suunnitellaan ja toteutetaan siten, että 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 on ohjattava erityisen huolellisesti.

5.3.6 Henkilökunnan käyttöön annettavat asiakirjat

Henkilökunnalla on aina käytössään varmentajan laatu- ja turvallisuusohjeet.

6 Tekniset turvatoimet

Tekniset turvajärjestelyt on kuvattu yksityiskohtaisesti varmennuskäytännössä.

6.1 Avainparin luominen, tallettaminen ja käyttöönotto

6.1.1 Avainparin luominen

Varmentaja:

Varmentaja luo yksityiset allekirjoitusavaimensa ja yksityisiä allekirjoitusavaimiaan vastaavat julkiset avaimet. Varmentajan yksityistä avainta säilytetään turvamoduulissa.

Varmenteen omistaja:

Varmenteen omistajien yksityiset avaimet luodaan turvallisesti liittymäkortille. Yksityisistä avaimista ei tehdä kopioita niiden luontivaiheessa, eivätkä ne ole siirrettävissä tai kopioitavissa liittymäkortilta. Varmentajalla, kortin liikkeellelaskijalla ja kortinvalmistajalla ei ole pääsyä varmenteen omistajien yksityisiin avaimiin.

Tehdasvalmisteisten avainten tapauksessa varmenteen omistajan avainpari luodaan Mobiilivarmenteen myöntämiseen vaadittavalla tavalla suojatuissa turvatiloissa. Yksityisistä avaimista ei säilytetä kopiota. Tehdasvalmisteisten avainten luontivaiheessa avaimia ei ole vielä kohdistettu kenellekään henkilölle.

Liittymäkortilla tapahtuvan avaintenluonnin tapauksessa avaimet luodaan liittymäkortilla eikä yksityinen avain koskaan poistu sieltä.

Liittymäkortilla on aina vähintään 1024-bittinen RSA-avain.

6.1.2 Liittymäkortin luovuttaminen hakijalle

Liittymäkortin luovutusprosessi on kuvattu varmennuskäytännössä. Asiaa on käsitelty myös avainten toimituksen yhteydessä kohdassa 4.2.1.

6.1.3 Varmenteen hakijan julkisen avaimen toimittaminen varmentajalle

Tehtaalla luotujen avainten tapauksessa kortin liikkeellelaskija toimittaa julkiset avaimet ja niitä vastaavat liittymäkortin tiedot varmentajalle. Julkisten avainten eheys suojataan varmennukseen asti. Mobiilivarmenteen rekisteröinnin yhteydessä varmentaja tekee varmennepyyntöjä varmennejärjestelmään. Varmennepyyntö sisältää julkisen avaimen ja muut mobiilivarmenteen tiedot.

Kortilla luotujen avainten tapauksessa hakijan julkinen avain toimitetaan varmentajalle osana varmenteen hakuprosessia.

6.1.4 Varmentajan julkisen avaimen jakelu

Varmentajan varmenne sisältää varmentajan julkisen avaimen. Varmentajan varmenne talletetaan julkiseen hakemistoon, josta se on saatavilla.

6.1.5 Avainten pituudet

Mobiilivarmenteen allekirjoittamiseen käytetty varmentajan yksityinen avain sekä sitä vastaava julkinen avain ovat vallitsevan käsityksen mukaan riittävän pitkiä avaimia. Vuonna 2010 käytetty varmentajan avain on vähintään 2048-bittinen RSA-avain.

6.1.6 Avainten käyttötarkoitukset

Varmenteen tietosisällössä käyttötarkoituksen määräävä kenttä 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. Tunnistusavaimen käyttötarkoituksiin voidaan sisällyttää salaus.

6.2 Varmentajan yksityisten avainten suojaaminen

6.2.1 Turvamoduulia koskevat standardit

Varmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa.

Varmentaja huolehtii siitä, että varmentajan yksityiset avaimet on suojattu paljastumiselta ja luvattomalta käytöltä. Varmentajan yksityisistä avaimista otetaan varmuuskopio kriittisen tietoturvallisuuden edellyttämällä tavalla.

6.2.2 Varmentajan yksityisen avaimen käsittelyyn osallistuva henkilökunta

Varmentajan yksityisen avaimen luontiin ja käyttöön liittyvään ympäristöön vaaditaan vähintään kahden henkilön samanaikainen läsnäolo tai toiminnan aktivoiminen.

6.2.3 Yksityisen avaimen varmuuskopio

Varmentajan yksityiset avaimet ja niiden varmuuskopiot säilytetään vahvasti salattuina kriittisen tietoturvallisuuden vaatimukset täyttävissä laitteissa.

Varmenteen omistajan yksityisistä avaimista ei ole kopioita.

6.2.4 Yksityisen avaimen arkistointi

Varmentajan tai käyttäjän yksityisiä avaimia ei arkistoida.

6.2.5 Yksityisen avaimen hallinnointi turvamoduulissa

Varmentajan yksityiset allekirjoitusavaimet suojataan korkean luotettavuuden fyysisillä ja loogisilla turvatoimilla. Niitä käytetään vain turvalliseen ympäristöön sijoitetussa järjestelmässä.

6.3 Varmenteen omistajan avainten suojaaminen

6.3.1 Liittymäkorttia koskevat standardit

Liittymäkortin on oltava valmistettu GSMA-SAS -sertifioidussa tehtaassa.

6.3.2 Yksityisen avaimen luovutus luotetun osapuolen huostaan

Varmenteen omistajan yksityistä avainta ei luovuteta kenellekään muulle kuin sen hakijalle. Toisaalta, korttitehtaalta lähtiessään kortit eivät ole kohdistettuja kenellekään erityisesti, joten yksityiselle avaimelle tulee omistaja vasta, kun sen sisältävä liittymäkortti toimitetaan varmenteen hakijalle.

6.3.3 Yksityisen avaimen varmuuskopio

Mobiilivarmenteeseen liittyvistä yksityisistä avaimista ei ole kopioita.

6.3.4 Yksityisen avaimen arkistointi

Mobiilivarmenteeseen liittyvää 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 lyhyempikin, 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.

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. Varmentaja määrittää oman menettelynsä tunnuslukujen käyttöön omassa varmennuskäytännössään.

6.5.2 Tunnusluvun suojaus

Tunnusluvut on suojattu niin, ettei niitä voi lukea tai kopioida kortilta.
Yksityiskohtainen menettely on kuvattu varmennuskäytännössä.

6.6 Varmennejärjestelmän laitteiden käyttöön ja pääsyyn liittyvät turvallisuusvaatimukset

6.6.1 Laitteistoturvallisuus

Varmennejärjestelmän laitteistoina käytetään vain käyttötarkoitukseensa sopivia laitteistoja.
Yksityiskohtainen menettely on kuvattu varmennuskäytännössä.

6.7 Varmennejärjestelmän elinkaaren hallinta

6.7.1 Varmennejärjestelmän kehittämiseen liittyvä valvonta

Järjestelmän kehitys ja testaus tapahtuu erillisessä testiympäristössä. Ainoastaan testatut, toimivat ja hyväksytyt ratkaisut siirretään tuotantojärjestelmään.

6.7.2 Turvallisuuden hallinta

Varmentajan tietoturvallisuutta hallitaan varmentajan tietoturvapolitiikan mukaisesti.

6.8 Tietoverkon turvallisuus

Tietoliikenneturvallisuus on toteutettu siten, että varmennejärjestelmän tietoverkko on yhtenäinen kokonaisuus, joka on eriytetty muista tietoverkoista ja jonka kriittiset osat on toteutettu korkean saatavuuden menetelmillä.

Tarkempi kuvaus tietoverkon turvallisuudesta on kuvattu varmennuskäytännössä.

6.9 Turvamoduulin käytön valvonta

Varmentaja huolehtii siitä, että varmentajan yksityiset avaimet on suojattu paljastumista ja luvatonta käyttöä vastaan. Varmentajan yksityisistä avaimista otetaan varmuuskopio kriittisen tietoturvallisuuden edellyttämällä tavalla.

Yksityiskohtainen menettely on kuvattu varmennuskäytännössä.

7 Varmenne- ja sulkulistaprofiilit

7.1 Varmenteiden tekniset tiedot

7.1.1 Yhteiset attribuutit

Varmenteen tietosisältö muodostuu yhteisistä attribuuteista ja mahdollisista varmentajakohtaisista attribuuteista. Mobiilivarmenne noudattaa yleistä X.509 v.3 suositusta ja sisältö on normaalin käytännön mukainen. Erityisesti kannattaa huomata, että käyttäjän sähköinen asiointitunnus talletetaan *Subject*-kenttään *SerialNumber*-attribuuttiin ja liittymäkortin ICCID talletetaan *eidSmartCardSerialNumber*-attribuuttiin. Lisäksi varmenteen myönnön yhteydessä tehdyn ensitunnistuksen mahdollisen ketjutuspolun pituus on talletettu attribuuttiin *identificationPathLength*, jonka arvo on nolla, jos henkilöllisyys on todettu henkilökohtaisesti kirjallisista asiakirjoista. Muussa tapauksessa sen arvo kertoo ensitunnistuksen tunnistusketjun pituuden. Varmenteen tietosisältö on kuvattu liitteessä 1.

7.1.2 Varmentajakohtaiset attribuutit

Varmentaja voi lisätä varmenteeseen tarpeelliseksi katsomiaan RFC-5280:n mukaisia kenttiä, joista kerrotaan erikseen varmennuskäytännössä. Toiminnallisen yhteensopivuuden varmistamiseksi kyseiset laajennuskentät eivät ole kriittisiä.

7.2 Sulkulistaprofiili

Sulkulistaprofiili on kuvattu varmennuskäytännössä.

8 Varmennepolitiikan hallinnointi

8.1 Varmennepolitiikan muutosmenettely

Varmentajat voivat yhteisellä kirjallisella päätöksellä muuttaa määrityksiä lainsäädännöllisten tai toiminnallisten vaatimusten vuoksi. Määritysten muutokset on kirjattava varmennepolitiikkaan ja varmennuskäytäntöön seuraavassa kuvatulla tavalla.

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

Kohtia, jotka varmentajien mielestä eivät merkittävästi vaikuta varmenteiden omistajiin ja luottaviin osapuoliin, voidaan muuttaa ilmoittamalla niistä käyttäjille ja palveluntarjoajille 14 päivää aikaisemmin. Varmennuskäytännön uudistuminen ei vaadi tiedonantoa.

Uusien osapuolien liittyminen luottamusverkostoon ei sellaisenaan anna aihetta varmennepolitiikan muuttamiseen.

8.1.2 Kohdat, joiden muutos vaatii tiedonannon käyttäjille ja palveluntarjoajille

Kaikkia varmennepolitiikan ja varmennuskäytännön kohtia voidaan muuttaa ilmoittamalla tulevista pääasiallisista muutoksista käyttäjille ja palveluntarjoajille vähintään 60 päivää ennen muutosten voimaan astumista.

8.1.3 Muutokset, joiden johdosta täytyy laatia uusi varmennepolitiikka

Varmennepolitiikka on uusittava, mikäli halutaan myöntää varmenteita, jotka eivät ole voimassa olevan politiikan mukaisia. Jokainen uusi politiikka saa uuden OID:n, myös luvun 8.1.1 mukaisten muutosten johdosta poislukien kuitenkin oikeinkirjoitusvirheiden korjaukset. Varmennepolitiikan uudistuminen ei välttämättä edellytä uuden varmennuskäytännön julkaisemista. Varmennuskäytännön uudistuminen ei edellytä uuden politiikan laatimista.

8.2 Julkaiseminen ja tiedottaminen

Varmentajat julkaisevat varmennepolitiikan ja varmennuskäytännön, jotka ovat saatavilla varmentajien Internet-sivuilta.

Varmentaja pitää asiakirjoista versionhallintaa sekä arkistoi kaikki varmennepolitiikka- ja varmennuskäytäntöversiot.

8.3 Varmennepolitiikan muutos- ja hyväksymismenettely

8.3.1 Varmennepolitiikan hallitsija

Varmennepolitiikkaa hallinnoi ja sen kehitystä ohjaa luottamusverkoston varmentajien yhteisesti nimeämä Mobiilivarmennejohtoryhmä. Varmentajat sopivat keskenään johtoryhmän vahvuuden ja toimintatavat. Varmentajat nimeävät oman tai omat edustajansa johtoryhmään.

8.3.2 Muutosmenettely

Varmennuspolitiikkaan tehtäviä muutoksia tekee muodostettava työryhmä, johon varmentajat nimeävät omat edustajansa. Työryhmä esittelee ehdotuksen varmennepolitiikan muutoksista

Mobiilivarmennejohtoryhmälle, joka kirjallisesti hyväksyy muutokset, minkä jälkeen uudistettu varmennepolitiikka astuu voimaan.

8.4 Versionhallinta

Varmentajat arkistoivat kaikki hyväksymänsä varmennepolitiikkaversiot ja ne ovat pyydettäessä saatavilla.

Versio	Päiväys	Kuvaus
1.0	1.10.2010	Ensimmäinen hyväksytty ja julkaistu versio
1.1	15.4.2011	Poistettu suostumuspalvelun määrittely sanastosta ja viittaukset tällaiseen palveluun puhuttaessa avainten käyttötarkoituksesta. Määritelty testivarmenteessa käytettävän henkilöllisyyden profiili.

Viiteluettelo

[RFC3647] S. Chokhani, W. Ford., R. Sabett, C. Merrill, S. Wu. “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”. IETF RFC3647,November 2003. URL http://tools.ietf.org/html/rfc3647.

[RFC5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk. “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. IETF RFC5280,May 2008. URL http://tools.ietf.org/html/rfc5280.

[X.509] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8:1997, "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework."

Liite 1: Varmenteen tietosisältö

Varmenteen sisältämä tekstisisältö talletetaan käyttäen UTF-8 merkistökoodausta, jotta kaikki hankalammatkin merkit saataisiin esitetyksi mielekkäällä ja yhtenäisellä tavalla. Varmenteen tietosisältöön otetaan mukaan vain minimimäärä tietoja henkilöstä, jotta tarvetta uusia varmenne ei syntyisi niin helposti. Varmenteen tietosisältöön otetaan henkilöön sidottuja tietoja ainoastaan kaksi: henkilön virallinen nimi ja hänen sähköinen asiointitunnuksensa. Näin estetään esimerkiksi henkilön nimen ja puhelinnumeron välisen kytkennän rakentaminen Mobiilivarmennehakemiston avulla.

Varmenteen tietosisältöön tulee liittymäkortin ICCID, jotta varmenteen yksikäsitteinen kytkeminen annettuun puhelinnumeroon olisi mahdollista. Tämä tekee myös sen, että liittymän MSISDN:n vaihtaminen on ainakin teoriassa mahdollista uusimatta varmennetta, koska MSISDN ei vaikuta varmenteen sisältöön mitenkään.

Mobiilivarmenne noudattaa yleistä X.509 v.3 suositusta ja sisältö on normaalin käytännön mukainen.

Kenttä	**Sisältö**	**Kommentit**
Version	V3	
Serial number		Varmenteen sarjanumero
Signature algorithm	sha512RSA tai sha256RSA	
Signature value	Varmentajan allekirjoitus	
Issuer		
Valid from		
Valid to		
Subject	SerialNumber = SaTu CN = Sukunimi Etunimet SaTu G = Etunimet SN = Sukunimi	
Public key		
Key usage	*digitalSignature* ja *keyEncipherment* tai pelkästään *nonRepudiation*.	*Kriittinen*, tunnistus- ja allekirjoitusvarmenteelle on eri käyttötarkoitukset.
Extended key usage		*Ei-kriittinen*, ei käytössä yhteisessä tietosisällössä
eidSmartCardSerialNumber		ICCID
identificationPathLength	0, 1, 2 …	*Ei-kriittinen*, ensitunnistuspolun pituus
Authority key identifier		*Ei-kriittinen*, myöntöön käytetyn avainparin julkisen avaimen yksilöivä tieto.
Subject key identifier		*Ei-kriittinen*, julkisen avaimen SHA-1 -tiiviste.
CRL distribution points	CRL distribution point	*Ei-kriittinen*, mikäli käytössä
Authority Information Access	OCSP responder address	*Ei-kriittinen*, mikäli käytössä
Authority Information Access	CA Issuers	*Ei-kriittinen*, URI, josta varmentajan varmenne on haettavissa
Basic constraints / CA	False	*Kriittinen*, varmennetta ei voi käyttää varmentajan varmenteena
Certificate policies	Policy Identifier	*Kriittinen*, 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	URI	*Ei-kriittinen*, URI: http://oper-

id.operator.fi/eid/SATU,
yksityiskohtainen sisältö on
varmentajan päätettävissä.

Varmenteen tietosisällössä on muutama harvemmin käytetty attribuutti. Niiden yksilöivät tunnisteet (OID:it), viittaukset kyseisten attribuuttien määrittelyihin sekä tietojen tallennuksessa käytetty esitysmuoto ovat seuraavat:

Kenttä / Attribuutti	**OID / viite ja tallennuksessa käytetty esitysmuoto**
SerialNumber	2.5.4.5, id-at-serialNumber, http://www.alvestrand.no/objectid/2.5.4.5.html, *PrintableString*
eidSmartCardSerialNumber	1.2.752.34.2.1, SEIS Private Extension Arc, http://www.alvestrand.no/objectid/1.2.752.34.2.html, *PrintableString*
identificationPathLength	1.2.246.277.1.5.4.106 Elisan OID-avaruus, *Integer*

Liite 2: Varmennusorganisaation osapuolten vastuut ja velvollisuudet

M = Pakollinen (Mandatory)
R = Suositeltava (Recommendation)
O = Valinnainen (Optional)

Osapuolet ja velvoitteet	M/R/O	Selitykset ja tarkennukset
Varmentaja		
Kokonaisvastuu varmennepalvelun tuottamisesta.	M	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.	M	Varmentajan toimintaa sääntelee • Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009) • Varmennepolitiikka • Varmentajan omat varmennuskäytäntö-dokumentit (CPS)
Varmennepalvelun tuottaminen varmennuskäytäntö-dokumentin (CPS) mukaisesti.	M	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	R	Varmentajat yhdessä huolehtivat varmennepolitiikan kehittämisestä ja ylläpidosta.
Varmenteen hakijan tunnistaminen luotettavasti ja sopimuksen tekeminen.	M	Varmenteen hakijan tunnistamisessa noudatetaan mitä laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009) on määrätty. Hakijan kanssa tehtävä sopimus täyttää lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (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.	M	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.	M	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.	M	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	M	Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009)

mukaisesti.		
Varmentaja on huolehtinut riittävistä järjestelyistä, joiden avulla se pystyy hoitamaan toiminnastaan koituvat vastuut.	M	Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009)
Varmentaja on taloudellisesti vakavarainen ja sillä on riittävät taloudelliset voimavarat toimia tämän politiikan mukaisesti.	M	Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009)
Varmentajalla on varmennepalveluiden tarjoamiseen riittävä määrä työntekijöitä, joilla on tarvittava koulutus, tekninen osaaminen ja kokemus, ottaen huomioon varmennepalveluiden luonne, kattavuus ja volyymi.	M	Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009)
Varmenteen luomiseen ja peruuttamiseen liittyviä tehtäviä hoitavien varmentajan organisaation osien rakenteen tulee olla dokumentoitu.	M	Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (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.	M	Asianmukaisen ja täydellisen varmennepyynnön toimittaminen varmentajalle ensimmäistä varmennetta haettaessa, varmennetta uusittaessa ja avainpareja uusittaessa. Laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista on määritetty varmenteen hakijan tunnistamiseen kelpaavat asiakirjat seuraavasti: • Voimassa olevasta Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämästä passista tai henkilökortista • Euroopan talousalueen jäsenvaltion viranomaisen 1 päivän lokakuuta 1990 jälkeen myöntämästä voimassa olevasta ajokortista • Vahvalla sähköisellä tunnistusmenetelmällä Mobiilivarmenne voidaan myöntää Suomen kansalaiselle tai kotikuntalain (201/1994) mukaisesti Suomessa vakinaisesti asuvalle ulkomaalaiselle, jonka henkilötiedot on talletettu Väestörekisterikeskuksen Väestötietojärjestelmään. 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.	M	Kortilla luotavien avainten tapauksessa kortin liikkeellelaskija vastaa kortilla olevan alustan turvallisuudesta avaintenluontiohjelman ajamista varten, avaintenluontisovelluksesta, kortin turvamoduulin luotettavuudesta ja yksityisen avaimen luottamuksellisuudesta. Tehdasvalmisteisten avainten tapauksessa kortin liikkeellelaskija vastaa avainparien luonnista, liittymäkorttien ja tunnuslukujen luottamuksellisesta luomisesta ja jakelusta asiakkailleen, julkisen avaimen varmentamiseen tarvittavien julkisen avaimen ja korttitietojen toimittamisesta varmentajalle ja varmenteen rekisteröinnissä mahdollisesti tarvittavien liittymäasiakkuus- ja korttitietojen toimittamisesta liittymäasiakkaalle.
Varmenteen omistaja		
Antaa tarkat ja täydelliset henkilötiedot varmentajalle tai tämän edustajalle tämän politiikan mukaisesti rekisteröinnin yhteydessä.	M	Rekisteröijä varmistaa omalta osaltaan, että varmenteen hakijan antamat tiedot ovat täydelliset ja virheettömät. Varmenteen hakija vahvistaa hakemuksen allekirjoituksella antamansa tiedot oikeiksi.
Ilmoitettava varmentajalle nimen vaihdoksesta enintään kolmen kuukauden kuluessa muutoksesta.	M	Käyttäjä velvoitettava tähän Varmentajan ja Varmenteen omistajan välisessä sopimuksessa.
Säilyttää tunnistusvälinettä ja siihen liittyviä tunnuslukuja huolellisesti estääkseen mobiilivarmenteen luvattoman käytön.	M	Määritetty varmenteen haltijan velvollisuudeksi laissa vahvasta sähköisestä tunnistamisesta ja allekirjoituksista (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	M	Määritetty varmenteen haltijan velvollisuudeksi laissa vahvasta sähköisestä tunnistamisesta ja allekirjoituksista (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	M	Varmenteeseen luottavan osapuolen tulee tarkistaa varmenteen voimassaolo seuraavasti: • Tarkistettava varmenteen voimassaoloajan kattavuus varmenteen omista tiedoista. • 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.	R	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.

Liite 3: Testikäyttöön myönnettävän varmenteen näennäinen henkilöllisyys

Mobiilivarmennusjärjestelmän teknistä testaamista varten varmentaja voi myöntää varmenteita, joissa ei ole varmennepolitiikan tunnistetta (*Policy Identifier*) ja näin ollen varmenne ei ole tämän politiikan tarkoittama luonnolliselle henkilölle myönnetty varmenne. Samassa yhteydessä varmenteesta jäävät puuttumaan varmennepolitiikan lisätiedot (*Policy Qualifier Info*). Tällaisen varmenteen perustana käytetään jotakin alla määritellyistä näennäisistä henkilöllisyyksistä

Täysi-ikäinen mies

Etunimi	Timoteus TESTI
Sukunimi	TESTIVARMENNE
SATU	10000000Z
HETU	111111-999Z
Sukupuoli	Mies
Sähköposti	testi-1@posti.laatikko
Osoite	Testitie 1, 00100 Helsinki

Täysi-ikäinen nainen

Etunimi	Tellervo TESTI
Sukunimi	TESTIVARMENNE
SATU	20000000Z
HETU	111111-888Z
Sukupuoli	Nainen
Sähköposti	testi-2@posti.laatikko
Osoite	Testitie 2, 00100 Helsinki

Alaikäinen poika

Etunimi	Timppa TESTI
Sukunimi	TESTIVARMENNE
SATU	30000000Z
HETU	110111A999Z
Sukupuoli	Mies
Sähköposti	testi-3@posti.laatikko
Osoite	Testitie 3, 00100 Helsinki

Alaikäinen tyttö

Etunimi	Tea TESTI
Sukunimi	TESTIVARMENNE
SATU	40000000Z
HETU	110111A888Z
Sukupuoli	Nainen
Sähköposti	testi-4@posti.laatikko
Osoite	Testitie 4, 00100 Helsinki

Käytetyt henkilötunnukset ja sähköiset asiointitunnukset ovat keinotekoisia ja niiden tarkistusmerkki "Z" on tarkoituksellisesti valittu siten, että tarkistusmerkin oikeellisuuden tarkistus ei voi onnistua, koska Z-kirjain ei kuulu sallittujen tarkistusmerkkien joukkoon.