

# **MOBIILIASIOINTIVARMENNE**

## **VARMENNEPOLITIIKKA**

### **Operaattoreiden mobiiliasiointivarmenteitavarten**

Versio1.0

Voimassa1.10.2010lähtien

## Yhteystiedot

### Varmennepolitiikkaahallinnoivaorganisaatio

Tämän varmennepolitiikan vahvistamiseksi otettiin käyttöön otta-  
musverkkosopimuksen allekirjoittaneet varmentajat, jotka huolehtivat yh-  
dessä tämän varmennepolitiikan hallinnoinnista päivittyksistä.

Tämän varmennepolitiikan tekijänoikeudet kuuluvat mobiilivarmennuspalvelun  
luottamusverkoston jäsenille. Varmennepolitiikkaan liittyviä kysymyksiin vastaavat kaikki  
mobiilivarmennuspalvelun luottamusverkoston kuuluvat varmentajat. Varmentajaansaa  
yhteydensähköpostiosoitteella, josta löytyy osoite [www.mobiilivarmenne.fi](http://www.mobiilivarmenne.fi).

### Varmennepolitiikan tunnisteet

Tämän varmennepolitiikan nimio "MOBIILIASIOINTIVA RMENNE-VARMENNEPOLITIIKKA  
-Operaattoreiden mobiiliasiointivarmennepolitiikan".

Varmennepolitiikan tunniste (ObjectIdentifier) on :1.2.246.277.1.11.4.1.2.1

ISO(1).MemberBody(2).Suomi(246).HPY(277).Services(1).caService(11).MobileCertificates(4  
)CertificatePolicies(1).Elisa-IDCA(2).SerialNo(1 )

Varmennepolitiikan tunniste on sijoitettu varmennepolitiikan X.509v3-määrityksen [X.509]  
mukaiseen varmennepolitiikan tunnisteiden kenttään (PolicyOID). Tätä varmennepolitiikkaa  
tutkimalla varmentajien luottava osapuolivoivarmennepolitiikan tunnisteiden varmennepolitiikan  
sopivuudesta kyseessä olevaan käyttötarkoitukseen.

Yhteystiedot.....	2
Varmennepolitiikkaahallinnoivaorganisaatio.....	2
Varmennepolitiikantunnisteet.....	2
Käsitteitäjaaihepiiriinliittyväsanastoa.....	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 Liittymäkortinliikkeellelaskija.....	13
1.4.4 Sulkupalvelu.....	13
1.4.5 Hakemistopalvelu.....	13
1.4.6 Varmenteenomistaja.....	14
1.4.7 Varmenteeseenluottavaosapuoli.....	14
1.5 Varmenteenkäyttäminen.....	14
1.6 Osapuoltenvastuutjavelvollisuudet.....	14
2 Yleisetehdot.....	15
2.1 Tietojenjulkaiseminenjasaatavuus.....	15
2.1.1 Varmentajantietojenjulkaiseminen.....	15
2.1.2 Sulkulistenjulkaisutiheys.....	15
2.1.3 Tietojensaataavuus.....	15
2.1.4 Tietovarastot.....	15
2.2 Auditointi.....	15
2.3 Tietojenluottamuksellisuusjajulkisuus.....	15
3 Varmentajienyksilöinti.....	16
3.1 Varmentajiennimeämiskäytäntö.....	16
4 Toiminnallisetvaatimukset.....	17
4.1 Varmenteenhakeminen.....	17
4.2 Varmenteenhakijantunnistaminen.....	17
4.2.1 Tunnistusvälineentoimittaminen.....	17
4.3 Varmenteenmyöntäminen.....	17
4.4 Varmenteenluominen.....	17
4.5 Varmenteenvoimassaolonpäättyminenjasulkeminen.....	18
4.5.1 Varmenteensulkemisenedellytykset.....	18
4.5.2 Sulkupyynnöntehtäjä.....	18
4.5.3 Sulkutapahtuma.....	18
4.5.4 Sulkutapahtumanajoitus.....	18
4.5.5 Varmenteensulkeminentilapäisesti.....	19
4.5.6 Tilapäisensulkupyynnöntehtäjä.....	19
4.5.7 Tilapäisensulkupyynnöntehtämistapa.....	19
4.5.8 Tilapäisensulunajkarajoitukset.....	19
4.5.9 Varmenteentilapäisensulunpurkaminen.....	19
4.5.10 Sulkulistanjulkaisutiheys.....	19
4.5.11 Sulkulistanjakelupisteet.....	19
4.5.12 Suorakäyttöinenvarmenteentilantarkistaminen.....	19
4.6 Varmenteenuusiminen.....	19
4.6.1 Varmenteenuusiminenvarmenteenvanhenemisenvuoksi.....	20
4.6.2 Varmenteenuusiminenennimenmuutoksenvuoksi.....	20
4.6.3 Varmenteenuusiminenuudenensitunnistamisenvuoksi.....	20
4.6.4 Avainparinuusiminenvarmenteensulkemisenjälkeen.....	20
4.7 Järjestelmänvalvonta.....	20
4.8 Varmenteisiinliittyvientietojenarkistointi.....	20
4.8.1 Tallennettavaaineisto.....	20
4.8.2 Arkistojensuojaus.....	21
4.8.3 Arkistojenvarmistusmenettelyt.....	21

4.8.4	Arkistotietojenhankinta-javarmistusmenetelmät.....	21
4.9	Varmentajanavaintenusiminen.....	21
4.10	Toiminnanjakumisenhallintajapoikkeustapausten käsittely.....	21
4.10.1	Varmentajanyksityinenavainonpaljastunuttaivarmentajanvarmenneon suljettu 21	
4.10.2	Turvallisuudenvaarantumisenluonnonmullistuksenta imuunkatastrofin seurauksena.....	21
4.11	Varmentajatoiminnanlakkauttaminen.....	21
5	Fyysiset,toiminnallisetjahrenkilöstöturvallisuute enliittyvätvaatimukset.....	22
5.1	Fyysinenturvallisuus.....	22
5.1.1	Sijaintijarakennustenominaisuudet.....	22
5.1.2	Fyysinenpääsytoimitilaan.....	22
5.1.3	Varajärjestelyt.....	22
5.2	Toiminnallisetvaatimukset.....	22
5.2.1	Vastuunjako.....	22
5.2.2	Tehtäviinvaadittavienhenkilöidenlukumäärä.....	22
5.2.3	Tehtäväkohtaintunnistaminen.....	22
5.3	Henkilöturvallisuus.....	23
5.3.1	Henkilökuntaa koskevat taustaselvityksentekeminen.....	23
5.3.2	Taustaselvityksentekemisessä noudatettavamenettely.....	23
5.3.3	Koulutukseenliittyvätvaatimukset.....	23
5.3.4	Asiantuntemuksenjaosaamisenylläpito.....	23
5.3.5	Poikkeamistajohtuvatoimenpiteet.....	23
5.3.6	Henkilökunnankäyttöönannettavatasiakirjat.....	23
6	Teknisetturvatoimet.....	24
6.1	Avainparinluominen,tallettaminenjakäyttöönotto.....	24
6.1.1	Avainparinluominen.....	24
6.1.2	Liittymäkortinluovuttaminenhakijalle.....	24
6.1.3	Varmenteenhakijan julkisenavaimentoimittaminen varmentajalle.....	24
6.1.4	Varmentajan julkisenavaimenjakelu.....	24
6.1.5	Avaintenpituudet.....	24
6.1.6	Avaintenkäyttötarkoitukset.....	25
6.2	Varmentajanyksityistenavaintensuojaaminen.....	25
6.2.1	Turvamoduuliakoskevat standardit.....	25
6.2.2	Varmentajanyksityisenavaimenkäsittelyyn osallistuvahenkilökunta.....	25
6.2.3	Yksityisenavaimenvarmuuskopio.....	25
6.2.4	Yksityisenavaimenarkistointi.....	25
6.2.5	Yksityisenavaimenhallinnointiturvamoduulissa..	25
6.3	Varmenteenomistajanavaintensuojaaminen.....	25
6.3.1	Liittymäkorttiakoskevat standardit.....	25
6.3.2	Yksityisenavaimenluovutusluotetun osapuolenhuostaan.....	25
6.3.3	Yksityisenavaimenvarmuuskopio.....	26
6.3.4	Yksityisenavaimenarkistointi.....	26
6.3.5	Yksityisenavaimenhallinnointiliittymäkortilla.....	26
6.4	Muutavainparin hallintaan liittyvät seikat.....	26
6.4.1	Julkisenavaimenarkistointi.....	26
6.4.2	Julkisten jayksityistenavainten voimassaoloaika.....	26
6.5	Liittymäkortilla olevien yksityistenavainten tunnusluvut.....	26
6.5.1	Tunnusluvun luominen ja käyttöön otto.....	26
6.5.2	Tunnusluvun suojaus.....	26
6.6	Varmennejärjestelmän laitteiden käyttöönjapääsyyn 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.....	27
6.8	Tietoverkon turvallisuus.....	27
6.9	Turvamoduulinkäytön valvonta.....	27
7	Varmenne-jasulkulistaprofiilit.....	28
7.1	Varmenteiden tekniset tiedot.....	28

7.1.1	Yhteisettribuutit.....	28
7.1.2	Varmennojakohtaisettribuutit.....	28
7.2	Sulkulistaprofiili.....	28
8	Varmennepolitiikanhallinnointi.....	29
8.1	Varmennepolitiikanmuutosmenettely.....	29
8.1.1	Kohdat,joitavoimuuttaailmantiedonantoakäyttäjillejapalveluntarjoajille.....	29
8.1.2	Kohdat,joidenmuutosvaatiitiedonannonkäyttäjillejapalveluntarjoajille.....	29
8.1.3	Muutokset,joidenjohdostatäytyylaatiauusivarmennepolitiikka.....	29
8.2	Julkaiseminenjätiedottaminen.....	29
8.3	Varmennepolitiikanmuutos-jahyvaksymismenettely.....	29
8.3.1	Varmennepolitiikanhallitsija.....	29
8.3.2	Muutosmenettely.....	29
8.4	Versionhallinta.....	30
	Viiteluettelo.....	31
	Liite1:Varmennoentietosisältö.....	32
	Liite2:Varmennusorganisaationosapuoltenvastuutjavelvollisuudet.....	34

## Käsitteitä ja aihepiiriin liittyvää sanastoa

Tässä dokumentissa käytetty suomenkielinen termi	Yleisestikäytössä oleva englanninkielinen termi	Selitys
Aktivointitieto, Tunnusluku	ActivationData	Yksityisen avaimen käyttöä suojaava PIN-kooditaisalasanana, joka syöttämällä aktivoi yksityinen avain. Mobiiliasiointivarmenteen yksityiset avaimet sijaitsevat puhelimen SIM-kortilla.
Alivarmentaja, operatiivinen varmentaja	SubordinateCA	Varmentaja, jonka varmenteen juurivarmentaja on allekirjoittanut ja joka myöntää varmenteita määrittelemilleen loppukäyttäjille.
Allekirjoituksen luomistiedot	SignatureCreation Data	Allekirjoittajan sähköisen allekirjoituksen luomisessa käyttämä ainutkertainen tietokokonaisuus, kuten koodit ja yksityiset avaimet.
Asiointivarmenne		Asiointivarmenne on varmenne, jos taon säädetty laissavahvastasähköisestä tunnistamisesta sähköisistä allekirjoituksista (617/2009). Asiointivarmenne ei ole laissamainittu laatuvarmenne.
Digitaalinen allekirjoitus	DigitalSignature	Sähköinen allekirjoitus, joka on tehty asiakirjantaiviestin allekirjoittajan yksityisellä avaimella julkisen avaimen menetelmän mukaisesti. Yleensä allekirjoitus on salattuihin viesteihin.
Hakemistopalvelu	DirectoryService	Julkisen avaimen järjestelmässä palvelu, joka sisältää käyttäjien varmenteita ja niihin mahdollisesti liittyviä muutietoja sekä sulkulistoja sisältäviä hakemistoja. Yleensä varmentajan itsensä ylläpitämä.
Julkinen avain	PublicKey	Julkisen avaimen epäsymmetrisestä avainparista, jota käytetään julkisen avaimen salaustekniikoissa. Julkinen avain sisältyy varmenteeseen, jonka varmentaja julkaisee hakemistopalveluun.
Julkisen avaimen järjestelmä	PublicKey Infrastructure (PKI)	Julkisen avaimen menetelmän käytön mahdollistava järjestelmä, jossa varmentaja varmentaavainparin julkisen osan digitaalisella allekirjoituksellaan jakaa näitä varmenteita muille käyttäjille, ylläpitää julkisten avainten hakemistoja ja sulkulistaa sekä mahdollisesti antamuita järjestelmän käyttöön liittyviä palveluja.
Julkisen avaimen menetelmä	Publickeymethod	Epäsymmetrisen salaustekniikan menetelmä, jossa kullakin salakirjoituksen käyttäjällä on kaksi toisiinsa liittyvää avainta. Toinen avainparin

		avaimista on julkisessa hakemistossa julkaistuja julkisen avain, toinen on vain avainparin käyttäjän hallussa oleva yksityinen avain. Yksityisellä avaimella salakirjoitettua tietoa voidaan avata vain vastaavalla julkisella avaimella, ja päinvastoin.
Juurivarmentaja	RootCA	Julkisen avaimen järjestelmässä ylin luotettu taho, joka allekirjoittaa, jakelee ja tarvittaessa peruuttaa varmenteet alemman tason varmentajille.
Kiistämättömyys	NonRepudiation	Avaimen käyttö tarkoitus, jolla annetaan mainittua avainta käyttäen tehdylle kehittyneelle sähköiselle allekirjoitukselle sopimuksellisen sitovuuslainedessä. Kiistämättömyys avaimella on mahdollista allekirjoittaa sopimuksia.  Allekirjoitettaessa dokumentti kiistämättömyys avaimella saavutetaan mahdollisuudesta dokumentin eheys ja aitous käyttäen kyseistä avainta vastaavaa varmennettä. Katso <i>Sähköinen allekirjoitus</i> alla.
Liittymäkortti	Subscriber Identity Module	Kortti, johon puhelinliittymä on sidottu. Puhekielessä yleensä SIM-kortti.
Loppukäyttäjä, Varmenteen omistaja	EndEntity	Henkilö, jolle varmentaja on myöntänyt varmenteen. Loppukäyttäjä käyttää varmennettä jähänellä on laillisesti hallussaan varmenteensa sisältämää julkista avainta vastaava yksityinen avain jäsenn käyttöön tarvittavien tunnusluvut.
Luottava osapuoli	RelyingParty	Sähköisiä palveluja varmenteiden loppukäyttäjille tarjoava taho. Luottava osapuoli toimii luottaen varmenteeseen ja/tai todentaadigitaalisen allekirjoituksen varmenteen avulla.
Luotettu varmenne	TrustAnchor	Varmenne, jonka luottavien osapuolien määrittelevät varmennehierarkiassa huipuksi jona kaalapuolella olevat varmenteet 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 palveluissa.  Tässä varmennepolitiikassa luettavuuden

		helpottamiseksi käytetään termiä Mobiilivarmenneisollakirjoitettuna, ellei asiayhteys anna aiheittamuuhun.
Mobiilivarmenne	Mobile Certificate	Tässä dokumentissa käytetty termi Mobiiliasiointivarmenteelle
Rekisteröijä	Registration Authority (RA)	Varmenteen hakijantunnistamisesta ja varmennehakemukseen rekisteröitävien tietojen tarkistamisesta vastaava osapuoli. Rekisteröijä toimii varmentajan valtuuttaman varmenneorganisaation osana.
Sulkulista	Certificate Revocation List (CRL)	Julkisen avaimen järjestelmässä käytöstä poistettujen varmenteiden luettelo. Varmentajan julkaisee sulkulistan hakemistopalvelussa.
Suostumus	Consent	Tapahtuman taitoimenpiteen vahvistaminen käyttäen avainta, jonka käyttötarkoituksenä on <i>digital Signature</i> mutta ei <i>non Repudiation</i> .
Sähköinen allekirjoitus	Electronic signature	Tietokoneen luettavassa muodossa oleva henkilön nimikirjoitus tai sen vastine, esimerkiksi digitaalinen allekirjoitus, todisteena nimikirjoitukseen liittyvän asiakirjan taivestinyhteydestä tiettyyn henkilöön.  Puhekielessä sähköisellä allekirjoituksella tarkoitetaan yleensä digitaalista allekirjoitusta, jonka tekemiseen käytetyn avaimen käyttötarkoituksiin kuuluu <i>non Repudiation</i> .
Todentaminen	Authentication; Verification	Järjestelmän käyttäjän (henkilön, organisaation tai laitteen) taivestinnässä toisen osapuolen tunnistuksen varmistaminen.
Tunnistaminen	Identification	Asioinnissa toisen osapuolen identiteetin selvittäminen. Yksinkertaisimmillaan tapahtuma, jossa vastataan kysymykseen: "Kukasinä olet?"
Tunnistusväline		Liittymäkortti yksityksine avaimen ja niihin liittyvät tunnukset.
Vahvistaminen	Validation	Varmenteen, varmenteellat ehdyn operaation taiten lopputuotoksen oikeellisuuden toteaminen.
Varmenne	Certificate	Varmenne on henkilön julkisesta avaimesta, nimitiedoista, sekä muistavarmenteeseen sisällytettävistä tiedoista muodostuva kokonaisuus, jonka varmentajan allekirjoittanut omalla yksityisellä avaimellaan. Varmenteen aitouden todennettavissa tarkistamalla varmentajan digitaalinen allekirjoitus.
Varmennehakemus	Certificate Application	Varmennehakemusten 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, kortin valmistaja, hakemisto- ja sulku listapalveluntuottajat sekä muut palveluntuottajat, joiden palveluja varmentajakäyttää.
Varmennepalvelu		Varmennepalvelu on varmenteisiin perustuvaa tunnistus- ja allekirjoituspalvelua, 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 yleisellä turvallisuus- ja muu vaatimukset. <b>Varmennepolitiikka</b> (engl. <i>Certificate Policy, CP</i> ) on varmentajan laatimakuvaus menettelytavoista ja toimintaperiaatteista, joita varmenteita myönnettäessä noudatetaan. Varmennuskäytännön varmennepolitiikka yksityiskohtaisempi kuvaus varmentajan toiminnasta.
Varmennepolku	Certificate Path	Varmenteen alkuperän varmistamiseksi tarvittavien 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. <b>Varmennuskäytäntö</b> kuvaakin varmentajan toteuttamia varmennepolitiikkaan saajakuvaava yksityiskohtaisesta varmentajan noudattamien käytäntöjen toimintatavat. Varmennepolitiikan ja varmennuskäytännön rakennus noudattaa pääosin IETF RFC 3647:n [RFC 3647] mukaista jaottelua.
Varmentaja	Certification Authority (CA)	Varmenneorganisaation osapuoli, joka myöntää varmenteita allekirjoittamalla varmenne tiedot omalla yksityisellä avaimellaan.
Yksityinen avain, henkilökohtainen avain	PrivateKey	Salainen osa epäsymmetrisestä avainparista, jota käytetään julkisen avaimensa laustekniikoissa. Yksityistä avainta käytetään tyypillisesti digitaaliseen allekirjoittamiseen tai julkisella avaimella

		salatunviestinavaamiseen. Puhekielessä käytetään usein myös käsitettävä salainen avain. Varmenteen omistajanyksityiset avaimet on talletettui liittymäkorttien niiden suojaamiseksi oikeudettomalta käytöltä.
--	--	---

## Lyhenteet

Lyhenne	Selitys	Tässä dokumentissa käytetty merkitys
ARL	AuthorityRevocationList	Juurivarmentajan julkaisemasulkulista, joka sisältää tiedot käytöstä poistetuista varmentajien varmenteista
CA	CertificationAuthority	Varmentaja
CP	CertificatePolicy	Varmennepolitiikka
CPS	CertificationPracticeStatement	Varmennuskäytäntö
CRL	CertificationRevocationList	Sulkulista
HSM	HardwareSecureModule	Varmentajien avainten luontiin ja säilytykseen käytettävä turvamoduuli
ICCID	IntegratedCircuitCardIdentifier	Liittymäkortin yksilöllinen sarjanumero
IETF	InternetEngineeringTaskForce	Internetin teknistä kehitystä edistävä kansainvälinen yhteisö
MSISDN	MobileSubscriberISDNNumber	Matkapuhelimen puhelinnumero
MSSP	MobileSignatureServiceProvider	Matkapuhelimessa tehtävän allekirjoituksen ja tunnistamisen mahdollistava palvelualue.
OCSP	OnlineCertificateStatusProtocol	Reaaliaikainen varmenteiden sulkutietoprotokolla
OID	ObjectIdentifier	Varmennepolitiikan tunnistetieto
PDS	PKIDisclosureStatement	Yksinkertaistettu kuva usvarmenteen käytön ehdoista rajoituksista.
PIN	PersonalIdentificationNumber	Tunnusluku, PIN-koodi
PKI	PublicKeyInfrastructure	Julkisen avaimen varmennejärjestelmä
PKIX	-	IETF:n PKI-työryhmä
PUK	PersonalUnblockingKey	PUK-koodi
RA	RegistrationAuthority	Rekisteröijä
RSA	Rivest, Shamir ja Adleman,	Epäsymmetrisen salausalgoritmi, jota käytetään epäsymmetrisen avainparin luontiin. Lyhennetulle keksijöidensä sukunimistä Rivest, Shamir ja Adleman.
X.509	-	Varmenteen jäsulkulistan rakenteen määrittävä standardi

## Roolit

Liittymätilaaja	Vastaalaskujenmaksusta.Luonnol linenhenkilöta yritys,joka sallii liittymäpalvelut.Voi olla samakuin liitt ymänkäyttäjä.
Liittymänkäyttäjä	Liittymäpalveluidenkäyttäjä,luonnollinenhenkilö,joka on merkitty liittymänhaltijaksi.Käyttäjä voi olla samakuin liittymän tilaaja.
Varmenteenhakija	Aina samaluonnollinenhenkilöku in liittymänkäyttäjä.Liittymän haltijaksi on oltava merkittynä varmenteenhakija.
Varmenteenomistaja	Luonnollinenhenkilö,jolle on myönnetty Mobiilivarmenne.Aina samaluonnollinenhenkilökuin varmenteenhakija eli liittymän käyttäjä.

# 1 Johdanto

## 1.1 Mobiilivarmennepalvelu

SuomalaisetteleoperaattoritovatyhdessäluoneetMobiilivarmennepalvelun,jota matkapuhelimiakäyttävätkuluttajatvoivathyödyntääasioidessaanpalveluntuottajien erilaisissasähköisissäpalveluissa.Palvelutarjoajakuluttajillehelponjaturvallisentavan tunnistautuapalveluihinsekävarmistuaasioinninyhteydessätekemiensäsitoumusten sisällöstäjakiistämättömydestä.PalveluntarjoajilleMobiilivarmennepalvelumahdollistaa käyttäjienhenkilöllisyydenluotettavantunnistamis enjatodentamisensekäpalveluunliittyvien, asiakkaanhyväksyntäävaativien,tapahtumienvahvistamisenasiakkaansähköisellä allekirjoituksella.Mobiilivarmennepalvelutäyttävahvansähköisentunnistamisenkriteerit, jotkaonmääritettylaissavahvastasähköisestääntunnistamisesta.

## 1.2 Varmennepolitiikka

Tämävarmennepolitiikkakuvaoperaattoreidennoudattamatperiaatteetkäytännöniiden myöntäessämobiilivarmeneteitanihinasiakassuhteessaolevilleluonnollisillehenkilöille. Tähänonyksipoikkeus:Varmentajavoihalutessaanmyöntäävarmenteitaomantoimintansa vaatimillepalveluille.Nämävarmenteeteivätolemobiilivarmeneteita,eivätnoudatata tätä varmennepolitiikkaa,eivätkäsisällävarmennepolitiikantunnistetta,vaikkaneovatkin mobiilivarmenentajanmyöntämiä.

Varmenteidenmyöntövaatiiinasopimuksenvarmentajanvarmenteenhakijanvälille.

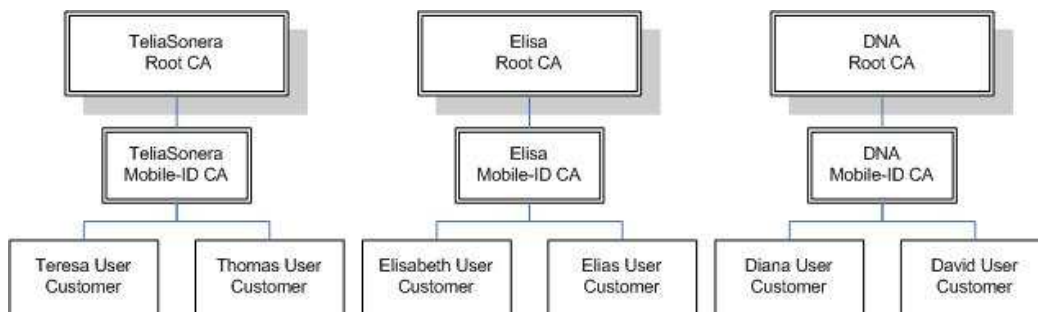
VarmennepolitiikkaonlaadittuETF:n suosituksenRFC-3647[RFC3647]mukaisestijasitä noudattaenmyönnettävätvarmenteetovatRFC-5280standardin[RFC5280]mukaisiaX.509 varmenteita[X.509].

## 1.3 Mobiilivarmenne

Mobiilivarmeneteitavoidaankäyttätunnistamiseen,salaamiseensekätiedontaitapahtuman eheyden,luottamuksellisuudenjakiistämättömyydenvarmistamiseen.Mobiilivarmeneteetovat mobiilipäätelaitteenliittymäkorteillasijaitseviin yksityisiinavaimiinperustuviavarmeneteita, jotkaonmyöntänytluottamusverkostoonkuuluvavarmenentaja.

Mobiilivarmeneteetmyöntäävarmentaja,jonkayksilöivättiedotlöytyvätjokaisenmyönnetyn varmenteenmyöntäjä( Issuer)–kentästä.Varmentajanvarmenteenonmyöntänytja allekirjoittanutyksityiselläavaimellaanvarmennepalvelunjuurivarmentaja.

Mobiilivarmeneteitäkäytetäänkuvan1 mukaisessahierarkiassa.Kaikkivarmentajatovat itsenäisiäjakullakintätäpolitiikkaakäyttävällävarmentajallaonomajuurivarmenteensa, johonvarmenteenkäyttäjätluottavat.



Kuva1: Mobiilivarmeneteisiinliittyvävarmennehierarkia.

Varmentajatakaa, että tämän varmennepolitiikan mukaisesti varmenteisiin pätevät seuraavat ominaisuudet:

- Varmentaja on myöntänyt varmenteen ja hallinnoinnit tämän varmennepolitiikan mukaisesti
- Loppukäyttäjän mobiilivarmenteen on myöntänyt luottamusverkoston kuuluva varmentaja. Varmentajan varmenteen on myöntänyt varmentajan varmennepalvelun juurivarmentaja.
- Varmenteen omistajasta rekisteröidyt tiedot ovat oikein varmenteessa.
- Varmentajan yksityiset avaimet on talletettu turvalliselle välilinjalle, josta niitä ei saa kopioituatoiselle välilinjalle.
- Varmentajan varmenne ja ajantasainen sulkuihin informoimista on saatavissa hakemistopalvelustavuoden jokaisen päivän äänivuoskautena ympäri.

Varmentajan kaikkien toiminnassaan noudatettavien voimassa olevien sääntöjen, varmennepolitiikka ja varmennuskäytäntöjen.

## 1.4 Varmennusorganisaatio

### 1.4.1 Varmentaja

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

### 1.4.2 Rekisteröijä

Rekisteröijällä tarkoitetaan tahoa, joka toimii varmentajatoimeksiannon vastuuhenkilönä hoitaen varmennehakemusten käsittelyyn liittyvää käytännön työtä noudattaen tätä varmennepolitiikkaa ja vastaavasti varmennuskäytäntöä. Mobiilivarmenteen rekisteröijinä toimivat varmentajan paikalliset asiointipisteet sekä kääntövarmentajankanssarekisteröintiä koskevat sopimukset neetorganisaatiot. Tarkempi menettelytapakuva on kyseessä oleva teknistä alustaa kuvaavassa varmennuskäytännössä. Itsepalvelurekisteröitymisessä rekisteröijäksikatsotaan varmenteen myöntäjä.

### 1.4.3 Liittymäkortin liikkeellelaskija

Liittymäkortin liikkeellelaskija toimii mobiilivarmenteeseen liittyvien avainparien ja aktivointitietojen osalta varmentajatoimeksiannon vastuuhenkilönä. Liittymäkortin liikkeellelaskija toimittaa mobiilivarmenteen rekisteröinnissä tarvittavat asiakkuus- ja korttitiedot liittymänkäyttäjälle varmentajalle.

### 1.4.4 Sulkupalvelu

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

### 1.4.5 Hakemistopalvelu

Hakemistopalvelu on *julkinen* Internet-palvelu, josta on saatavilla varmentajien varmenteet, sulkulistasekan mobiilivarmenteet, joiden julkaisemiseen on varmenteen omistajan suostumus.

#### 1.4.6 Varmenteenomistaja

Varmentajamyöntää Mobiilivarmenteenvarmenteenomistajalle varmennuskäytäntönsä mukaisesti.

#### 1.4.7 Varmenteeseen luottava osapuoli

Varmenteeseen luottava osapuolion henkilö tai organisaatio, joka luottaa varmenteen tietoihin ja joka käyttää varmennettavarmenteenomistajan henkilöllisyydentodentamiseksi tai varmenteenomistajan tekemänsä sähköisen allekirjoituksen todentamiseen. Tässä varmennepolitiikassa varmenteeseen luottavalla osapuolella tarkoitetaan luottamusverkoston sopimuksen allekirjoittanutta varmentajaa, joka on sopimussuhteessa sähköisiä palveluja loppukäyttäjälletuottavantahon kanssa.

#### 1.5 Varmenteenkäyttäminen

Tämän varmennepolitiikan mukaista Mobiilivarmennettavien henkilöiden sähköiseen tunnistamiseen, viestinnän salaamiseen ja sähköiseen allekirjoitukseen mukaisesti, kuin teknistä alustaa koskien määritelty varmennuskäytäntöissä. Mobiilivarmennettavien voidaan käyttää käyttöä tarkoituksensa mukaisesti erilaisissa sovelluksissa ja palveluissa.

Varmenteenkäyttöä ei ole rajoitettu muutoin kuin itse seuraavarmenteen käyttöä tarkoitukseltaan (*keyUsage*). Palvelut, jotka käyttäviä hyväksyen varmennetta, voivat asettaa käyttöleomiarajoituksia taieistoja.

#### 1.6 Osapuolten vastuut ja velvollisuudet

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

Varmentajat ovat velvollisia muiden osapuolten kanssa tekemissä sopimuksissa edellyttämäännäiltä varmennepolitiikassa ja omissa varmennuskäytännöissään asettuja käytäntöjä, vastuita ja velvollisuuksia. Varmennusorganisaation eriosapuoliin liittyvät vastuut ja velvollisuudet on kuvattu liitteessä 2 Varmennusorganisaation osapuolten vastuut ja velvollisuudet.

## 2 Yleiset ehdot

### 2.1 Tietojen julkaiseminen jasaatavuus

#### 2.1.1 Varmentajantietojen julkaiseminen

Varmentajajulkaiseesulkulistatyleisestisaatavillaolevalla palvelimella. Varmenteet julkaistaan varmentajien ja mobiilivarmenteeseen luottavien palveluntarjoajien saataville sekä mahdollisesti yleisestisaatavilla olevassa hakemistossa. Varmentajajulkaisee varmennepolitiikan, varmennuskäytännöt, varmennekuvausten (PDS) sekä muut julkiset varmennepalvelujen tuottamiseen liittyvät dokumentit www-sivuillaan.

#### 2.1.2 Sulkulistojen julkaisu tiheys

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

#### 2.1.3 Tietojensaataavuus

Sulkulistat ovat kaikkien tarvitseviensa saatavilla. Varmenteet ovat julkisiasen mukaan mitkä varmenteen omistajan kanssa sovittu. Varmennepolitiikka ja varmentajien varmennuskäytännöt sekä varmennekuvaus (PDS) ovat julkisestisaatavilla olevia dokumentteja, jotka ovat jaossa varmentajien verkko-sivuilla.

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

#### 2.1.4 Tietovarastot

Varmentajan julkaisemattia tietoja saatavilla varmentajan www-sivuilla. Varmenteet ovat talletettuina varmentajien luottamuksellisiin tietovarastoihin. Varmentajien tiedot tarkistetaan voimassa olevien arkistossääntösten mukaisesti. Varmentajat ovat laatineet myös henkilötietolain mukaisen rekisteriselosteen varmentajien järjestelmän henkilötietojen käsittelyn osalta.

### 2.2 Auditointi

Varmentajat tarkastetaan teknisten toimittajien ja rekisteröijien sätoimitilat, laitteet ja toiminnan tarkoituksen mukaisesti. Varmentajien avoimuudessa tarkastuttavaa toimintansa ulkoisella audittoijalla. Yksityiskohtainen tarkastusmenettely on kuvattu varmennuskäytännössä.

### 2.3 Tietojen luottamuksellisuus ja julkisuus

Varmennejärjestelmän tiedot ovat luottamuksellisia, elleivät ne perustu henkilötietolain, tai sähköisistä allekirjoituksista annetun lainsäädännön siintietojen luovuttamisesta tai varmennepolitiikassa määriteltyihin lainsäädännön tarkoituksiin. Viranomaisille luovutettavat tiedot määritellään voimassa olevan lainsäädännön mukaisesti. Varmennejärjestelmän tietoja ei luovuteta muuhunkin tarkoituksiin.

### 3 Varmentajienyksilöinti

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

#### 3.1 Varmentajien nimeämiskäytäntö

Varmentajanimikoostuuseuraavista attribuuteista :

Attribuutti	Sisältö
<i>commonName</i> (CN)	XXXCA
<i>Organization</i> (O)	DNAOy/ElisaOyj/TeliaSoneraOyj
<i>Country</i> (C)	FI

Varmentajanimientietosisältöön kuvattu yksityiskäytäntö on ohtaisestiao.varmennuskäytännössä.

## 4 Toiminnalliset vaatimukset

### 4.1 Varmenteenhakeminen

Mobiilivarmenteenhakijanoikeudet ja velvollisuudet on mainittu hakemusasiakirjassajsenen liitteenä olevissa ennen Mobiilivarmennehakemuksen allekirjoittamista hakijalle annettavissa varmentajan mobiilivarmenne palvelusopimusehdoissa. Hakemusasiakirjassaja mobiilivarmennus palvelusopimusehdoissa on tiedot kummankin osapuolen oikeuksista ja velvollisuuksista.

Mikäli varmentajamahdollista palvelussaan varmenteesen liittyviä käyttörajoituksia, on varmenteen rekisteröinnin yhteydessä varmenteen hakijalle annettavien mahdollisuus käyttörajoitusten määrittämiseen varmennehakemuksen sajasopimuksessa.

Kun mobiilivarmenteenhakijahakee varmenneä, hän hyväksyy samalla varmenteen käyttöön liittyvät sopimusehdot ja varmentajan antamat ohjeet, tarkistaa henkilötietojensa oikeellisuuden sekä hyväksyy tai kieltää varmenteensa julkaisun hakemistossa.

Sopimukseen liittyen hakija erityisesti sitoutuu huolehtimaan mobiilivarmenteeseen liittyvien tunnuslukujensa säilyttämisestä huolellisesti sekä mahdollisesta väärinkäytöstä varmenteiden tai liittämäkortin katoamisen ilmoittamisesta.

Mobiilivarmenteen yksityiskohtainen hakuprosessi kuvataan varmennuskäytännössä.

### 4.2 Varmenteenhakijan tunnistaminen

Mobiilivarmenteenhakijan tunnistetaan joko käyttäen vahva sähköistä tunnistamista tai henkilökohtaisesta rekisteröijänsiointipisteessä.

#### 4.2.1 Tunnistusvälineen toimittaminen

Tunnistusväline muodostuu liittämäkortista yksityisine avaimineen ja niihin liittyvistä tunnusluvuista. Liittämäkortti toimitetaan asiakkaalle ilman rekisteröityä varmenteita. Tunnistusväline voidaan ottaa käyttöön onnistuneen rekisteröinnin jälkeen.

Kortin liikkeellelaskijavarmistaa, että liittämäänsä iakkaalle toimitetaan Mobiilivarmenteen käytön kannalta oikeantyyppinen liittämäkortti. Liittämäkortti toimitetaan varmenteenhakijalle postitse tai henkilökohtaisesti siointipisteessä operaattorin normaalin käytännön mukaisesti.

Yksityisten avainten tunnusluvut toimitetaan varmenteenhakijalle liittämäkortin mukana suojaesimerkiksi raaputus pinnan alla siten, että västäänottajavoitodeta luottamuksellisuuden säilyneen kuljetukseen ajan. Varmenteenhakijantulee asettaa haluamansa tunnusluvut rekisteröinnin yhteydessä.

Prosessin yksityiskohtainen selostus varmennuskäytännössä.

### 4.3 Varmenteen myöntäminen

Varmentajamyoöntää mobiilivarmenteen hyväksyessään varmennehakemuksen. Varmentajavastaamyoöntäessään mobiilivarmenteen, esittäen tietosisältöön hakemuksen mukaisen sen luovuttamishetkellä.

### 4.4 Varmenteen luominen

Uusi Mobiilivarmenne luodaan rekisteröitymisen yhteydessä käyttäen aina uutta aiemmin käyttämätöntä avainmateriaalia. Mobiilivarmenne on käytettävissä onnistuneen rekisteröinnin jälkeen. Mobiilivarmenteenhakijalle korostetaan varmenteen luovutushetkellä, että yksityisistä avaimista ei ole eikä ikinä ole mahdollista kopioida.



#### 4.5.5 Varmenteensulkeminentilapäisesti

Mobiilivarmenteensulkeminentilapäisestitehdään uiltaosinkutenpysyvänsulkeminen, muttasulkemisyykoodiksiimerkitäänmahdollisten muidensyykoodienlisäksi *certificateHold*.

#### 4.5.6 Tilapäisensulkupyynnötekijä

Tilapäisensulkupyynnötekijääkoskevatsamatsään nōtkuinpysyvänsulkupyynnötekijää.

#### 4.5.7 Tilapäisensulkupyynnötekemistapa

Tilapäistäsulkupyntöökoskevatsamatsään nōtkuin pysyvääsulkupyntöä.

#### 4.5.8 Tilapäisensulunaikarajoitukset

Tilapäinensulkuonvoimassakunnesseperuutetaan. Tilapäisensulunpurkupyynnötekijää ja hānentunnistamistansakoskevatsamatsään nōtkuin insulkupyynnötekijää.

#### 4.5.9 Varmenteentilapäisensulunpurkaminen

Varmenteentilapäisensulunpurkajatunnistetaanjo kokäyttäen vahvaasähköistä tunnistamistatähenkilökohtaisesti Rekisteröijän asiointipisteessä. Sulunpurkajan tunnistaminenon kuvattu varmennuskäytännössä.

#### 4.5.10 Sulkulistan julkaisu tiheys

Tietovarmenteenviennistä sulkulistalle on julkise stisaatavillaviipymättä, kun sulkupyntöön todettupäteväksijahyväksyty. Sulkulista on voimassa 24 tuntia. Sulkulistasisältää seuraavansulkulistan julkaisu ajankohdan.

Uusisulkulista julkaistaan tunnin välein, kuitenkin nviimeistään voimassa olevansulkulistan voimassaolon päätty misajankohtaan mennessä.

Järjestelmä päivityksissä j amuis sapaikkeavissatil anteissavarmen taja voijulkaista sulkulista ja erijulkaisu tiheyksillä japidennetyil lävoimassa oloajoilla.

#### 4.5.11 Sulkulistan jakelupisteet

Sulkulista julkaistaan vähintään kahdessa erillisessä pisteessä, joista vähintään kahteen on viittaukset varmenteessa. Sulkulista sijastavoida an käyttää myös suora käyttöistä varmenteentilantarkistamista OCSP-protokollalla.

#### 4.5.12 Suorakäyttöinen varmenteentilantarkistaminen

Sulkulista nsijaan varmentaja voik käyttää OCSP-palvelu varmenteentilan julkaisemiseen. Tätä kautta saatavat tiedot on oltava yhtäpitävääm ahdollisestitarjolla olevansulkulistan kanssa.

#### 4.6 Varmenteenuusiminen

Varmenteenuusiminen edellyttää aina avain materiaalin vaihtamista käyttämättömään materiaaliin, ellei tässä varmennepoliitikassa erik seen muutasanota.

#### 4.6.1 Varmenteenusiminenvarmenteenvanhenemisen vuoksi

Varmenteenusiminenvanhenemisvuoksijohtaa uudet envarmenteenrekisteröintiin. Liittymäkortilla luotavien avaintapauksessa tapahtumaei oleellisesti poikkeavuuksien varmenteenrekisteröinnistä. Yksityiskohdaton kuva tutarkemmin varmennuskäytännössä.

Tehdasvalmisteisten avaintapauksessa uusivarmenteenrekisteröidään normaalisti käyttäen henkilöntunnistamiseen voimassa olevaa varmenteenrekisteröidään ennen kuin uusiliittymäkortin kytketty verkkoon. Yksityiskohdaton kuvattu tarkemmin varmennuskäytännössä.

#### 4.6.2 Varmenteenusiminennimenmuutoksen vuoksi

Kun varmenteen omistaja ilmoittaa nimenmuutoksesta varmentajalle, uusi varmentaja varmenteen halutessa ansamalla avainmateriaalilla ja samalla voimassaolon päättymisajalla kuin voimassa oleva varmenteenrekisteröidään. Uusittu varmenteenrekisteröidään edellytyksien mukaisesti. Koska avainmateriaali ei muutu, voidaan varmenteenrekisteröinti tehdä ilman käyttäjän nimen muutosta. Uusinimitarkistetaan Väestötietojärjestelmästä samaan tapaan kuin uuden varmenteenrekisteröinnin yhteydessä.

#### 4.6.3 Varmenteenusiminenuuden ensitunnistamisen vuoksi

Varmentajansa uusi avaimensa samalla avainmateriaalilla ja samalla voimassaolon päättymisajalla kuin voimassa oleva varmenteenrekisteröidään. Mikäli varmentajatekijän ensitunnistamisen kasvokkain. Tämä tarkoitus on mahdollista avaimen ensitunnistustason nostojäljentyä ensitunnistusketjuun saattamalla *identificationPathLength*-attribuutin arvo nolllaksi. Uusimisen yhteydessä nimitarkistetaan Väestötietojärjestelmästä samaan tapaan kuin uuden varmenteenrekisteröinnin yhteydessä.

#### 4.6.4 Avainparin uusiminenvarmenteen sulkemisen ja ilmeen

Avainparin uusiminen johtaa aina uuteen varmenteeseen uusilla avaimilla. Vanha varmenteenrekisteröinti jää avainparin pysyvästi mitätöitynä.

#### 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 sähköisenä tallennettavaksi kirjoittamiseksi tarvittavat tiedot;
- 2) tarvittavat tiedot hakijan ensitunnistamisesta yksinä käytetyistä asiakirjasta;
- 3) tiedot tunnistusvälineen käyttöön mahdollisesti liittyvästä estoistajakäyttörajoituksista; sekä
- 4) varmenteen osatavarmenteen tietosisältö.

Edellä 1 kohdassa tarkoitettujen tietojen säilytettäväksi vuosittain tunnistustapahtumasta 2–4 kuukauden ajan varmenteen omistajan välisen asiakassuhteen päättymisestä.

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

#### **4.8.2 Arkistojensuojaus**

Arkistoitavatietosäilytetään korkeanturvasottiloissa, joissa on pääsynvalvonta.

#### **4.8.3 Arkistojenvarmistusmenettelyt**

Varmuuskopiot varastoidaan fyysisesti erilliseen tilaan alkuperäisistä tiedoista.

#### **4.8.4 Arkistotietojenhankinta- ja varmistusmenettelyt**

Varmentajan varmistaa arkistojen tavoitettavuuden ja lukukelpoisuudensa inäkin tapauksessa, että varmentajan toimintakeskeytyä päättyy.

#### **4.9 Varmentajan avainten suojaaminen**

Varmentajan avainten suojaaminen on kuvattu varmennus käytännössä.

#### **4.10 Toiminnan jatkumisen hallintajapoikkeustapaus tarkastelu**

Varmentajalla on jatkuva ja valmiussuunnitelma, joka mahdollistaa varmentajan toiminnan jatkuvuuden.

Poikkeustapauksiin varautuminen on kuvattu varmennus käytännössä.

##### **4.10.1 Varmentajan yksityinen avain on paljastunut tai varmentajan varmenne on suljettu**

Varmentajailmoittaa jokaisessa varmennuskäytännössä avainten pitteet, joihin varmenteen omistajien, varmenteeseen luottavan osapuolen ja kisteröijien varmentajan työntekijöiden on ryhdyttävä, mikäli varmentajan yksityinen avain on paljastunut tai tulla muutoin käyttökelvottomaksi.

##### **4.10.2 Turvallisuuden vaarantuminen luonnonmullistuksen tai maanrakennuksen seurauksena**

Varmentajan varautunut luonnonmullistuksen tai maanrakennuksen seurauksena on kuvattu varmennus käytännössä.

#### **4.11 Varmentajan toiminnan lakkauttaminen**

Varmentajan lakkauttamisen apidetään tilannetta, jossa kaikkien varmentajan varmenteen myöntämiseen liittyvä palvelu lakkautetaan pysyvästi. Varmentajan lakkauttamisella ei tarkoiteta tilannetta, jossa varmennepalvelusiirre tää organisaatioltatoiselle.

Varmentajailmoittaa varmennepalveluiden lakkauttamisesta muille luottamusverkoston varmentajille ja asiakkaille mahdollisimman pian, kuitenkin vähintään kuuttakuukautta ennen lakkauttamisen ajankohtaa.

Ennen varmentajan lakkauttamista suoritetaan vähintäänkin seuraavat toimenpiteet:

- Kaikkien myönnettyjen avainmassa olevat varmenteet suljetaan yhdessä tai useammalla sulkuilla, joiden avainmassaoloaika ei lakkaa ennen kuin viimeistään suljetun varmenteen avainmassaoloaika on päättynyt.
- Varmentajan lakkauttaessa kaikkien sopimus kumppaniensa valtuutetuilla varmenteiden myöntämisprosessiin liittyviä tehtäviä varmentajan puolesta.
- Varmentajan varmistaa, että kohdassa 4.8 mainittu avainten suojaus varmentajan arkistoihin säilyy varmentajan lakkauttamisen jälkeenkin.
- Varmentajan huolehtii sähköisen allekirjoituslain mukaisesti tietojen arkistoinnista sekä noudattaamuotoinkin arkistolainsäätöä tietojen arkistoinninosalta.

## **5 Fyysiset, toiminnalliset ja henkilöstöturvallisuus teenliittyvät vaatimukset**

### **5.1 Fyysinenturvallisuus**

Varmentajahuolehtiivarmennetuotannon turvallisuus estajatoiminnasta asianmukaisella tavalla sen kaikkialla osa-alueilla.

Yksityiskohtainen kuvaus turvallisuuteen liittyvistä järjestelyistä on varmennuskäytännössä.

#### **5.1.1 Sijaintijarakennusten ominaisuudet**

Varmentajan järjestelmän sijaitsevat korkeat turvatason konesalitiloissa jätettävät tietokonekeskuksille annetut turvallisuutta koskevat ohjeet määräykset.

Toimitilaturvallisuus toteutettusiten, että asiattomien pääsy toimitiloihin on estetty.

#### **5.1.2 Fyysinen pääsytoimitilaan**

Toimitiloihin, joissa tehdään varmennejärjestelmän tuotannollisia tehtäviä, on valvottu pääsy. Kulunvalvontajärjestelmän havaitseminen kaluvallisen etäluvottoman sisäänmenon. Konesalitoihin vaaditaan henkilöntunnistautumisen, jolloin henkilötunnistetaan ja pääsyoikeudet tarkistetaan sekä tapahtumarekisteröidään. Konesalitojenvartioidaan vuorokauden ympäri.

#### **5.1.3 Varajärjestelyt**

Laitteistoratkaisut toteutettu hyvätiedonhallintatavan mukaisesti siten, että järjestelmän pettäessä voidaan siirtyä käyttämään varajärjestelmää vaarantamattajärjestelmään sisältyvien tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä. Tärkeiden laitteiden varaosiensaantijahuoltoon varmistettu.

### **5.2 Toiminnalliset vaatimukset**

#### **5.2.1 Vastuunjako**

Varmentajan tehtävät on jaettu tehtävien mukaisesti vastuualueisiin, jotka on kuvattu yksityiskohtaisesti varmennuskäytännössä. Varmentajalla on oltava käytettävissä riittävät henkilöstöresurssit varmennetoimintaavarten.

#### **5.2.2 Tehtäviin vaadittavien henkilöiden lukumäärä**

Varmentajan yksityisen avaimen luominen, aktivointi, varmuuskopiointijalauttaminen suoritetaan valvotusti kahden järjestelmän ylläpito tehtäviin oikeutetun henkilön läsnäollessa.

Varmentajan yksityisen avaimen peruuttaminen on mahdollistava kahden oikeutetun henkilön valvonnassa.

Varmentajan yksityisen avaimen turvamoduulinalustuksessa on läsnä vähintään kaksi järjestelmän ylläpito tehtäviin oikeutettua henkilöä.

Järjestelmän käyttämiseen vaaditaan yhden tehtävään oikeutetun henkilön läsnäolo.

#### **5.2.3 Tehtäväkohtainen tunnistaminen**

Mobiilivarmenteen rekisteröijän, varmennejärjestelmän ylläpitäjän ja varmennejärjestelmän käyttäjän tunnistaminen jatehtävää kuvauksen kuvattu yksityiskohtaisesti varmennuskäytännössä.

### **5.3 Henkilöturvallisuus**

Varmentajat vastaavat kukaan omaستavarmennetoiminnastaan. Tekniset toimittajat toimivat varmentajan vastuullajalukuun.

Varmentajakiinnittäerityistähuomioitasekäoman henkilökuntansaettäteknisten toimittajienjarekisteröijienluotettavuuteenjat ehtäviensuorittamiseentarvittaviintaitoihin.

#### **5.3.1 Henkilökuntaakoskevantaustaselvityksenteke minen**

Varmentajateettääomastavarmennepalveluhenkilöstö stäänsekäedellyttäätekniisiä toimittajateettämäänvarmennetietojärjestelmänparissatyöskentelevistähenkilöistäntarvittavaturvallisuus-jataustaselvitykset.

#### **5.3.2 Taustaselvityksenteke misessä noudatettavame nettely**

Henkilökunnantyökokemuskartoitetaantyöhönottovai heessa. Henkilöönkohdistetaan turvallisuusselvitysantamiensatiетоjenperusteell amäärämuotoisellalomakkeella. Turvallisuusselvityksenettelyonkuvattuyksityisko htaisesti varmennuskäytännössä.

#### **5.3.3 Koulutukseenliittyvät vaatimukset**

Varmentajan henkilökunnan on oltava koulutettusite n, että tehtävän hoitaminen on mahdollista.

#### **5.3.4 Asiantuntemuksen ja osaamisen ylläpito**

Henkilökunnankoulutussuunniteltaanjatoteutetaan siten, että tehtävän hoitamiseen liittyvä asiantuntemusonainatehtävänä edellyttämällä tasolla.

#### **5.3.5 Poikkeamista johtuvat toimenpiteet**

Poikkeustilanteissa voidaan varmentajatehtäviinottaaväliaikaisestiihenkilöstöä, jonka koulutuseioletäydellistä, mutta heidän työtänsä onohjattava erityisen huolellisesti.

#### **5.3.6 Henkilökunnankäyttöön annettavat asiakirjat**

Henkilökunnalla on aina käytössä varmentajan laat u-jaturvallisuusohjeet.

## 6 Teknisetturvatoimet

Teknisetturvajärjestelytonkuvattuyksityiskohtai sestivarmennuskäytännössä.

### 6.1 Avainparinluominen,tallettaminenjakäyttöön otto

#### 6.1.1 Avainparinluominen

##### Varmentaja:

Varmentajaluoksisetallekirjoitusavaimensaaja yksityisiäallekirjoitusavaimiaanvastaavat julkisetavaimet.Varmentajanyksityistäavaintasä ilytetäänturvamoduulissa.

##### Varmenteenomistaja:

Varmenteenomistajienyksityisetavaimetluodaantu rvallisestiliittymäkortille.Yksityisistä avaimistaehdäkopioitaniidenluontivaiheessa, eivätkäneolesiirrettävissätai kopioitavissaliittymäkortilta.Varmentajalla,kort inliikkeellelaskijallajakortinvalmistajalla ei ole pääsyävarmenteenomistajienyksityisiinavaimiin.

Tehdasvalmisteistenavaintentapauksessavarmenteen omistajanavainpariluodaan Mobiilivarmenteenmyöntämiseenvaadittavallatavall asuojatuissaturvatiloissa.Yksityisistä avaimistaeisäilytetätkopiota.Tehdasvalmisteisten avaintenluontivaiheessaavaimiaeiole vieläkohdistettukenenkäänhenkilölle.

Liittymäkortillatahtuvanavaintenluonnintapauks essaavaimetluodaanliittymäkortilla eiä yksityinenavainkoskaanpoistusieltä.

Liittymäkortillaonainavähintään1024-bittinenRSA-A-avain.

#### 6.1.2 Liittymäkortinluovuttaminenhakijalle

Liittymäkortinluovutusprosessionkuvattuvarmennu skäytännössä.Asiaaonkäsiteltymyös avaintentoimituksenyhteydessäkohdassa4.2.1.

#### 6.1.3 Varmenteenhakijanjulkisenavaimentoimittam inenvarmentajalle

Tehtaallaluotujenavaintentapauksessakortinliik keellelaskijatoimittajulkisetavaimetja niitävastaavatliittymäkortintiedotvarmentajalle .Julkistenavainteneheyssuojataan varmennukseenasti.Mobiilivarmenteenrekisteröinni nyhteydessävarmentajatekee varmennepyyntöjävarmennejärjestelmään.Varmennepyy ntösisältääjulkisenavaimenja muutmobiilivarmenteentiedot.

Kortillaluotujenavaintentapauksessahakijanjulk inenavaintoimitetaanvarmentajalleosana varmenteenhakuprosessia.

#### 6.1.4 Varmentajanjulkisenavaimenjakelu

Varmentajanvarmennesisältäävarmentajanjulkisen avaimen.Varmentajanvarmenne talletetaanjulkiseenhakemistoon,jostaseonsaat avilla.

#### 6.1.5 Avaintenpituudet

Mobiilivarmenteenallekirjoittamiseenkäytettyvarm entajanyksityinenavainsekäsitä vastaavajulkisenavainovatvallitsevankäsityksen mukaanriittävänpitkiäavaimia.Vuonna 2010käytettyvarmentajanavainonvähintään2048-b ittinRSA-A-avain.

## 6.1.6 Avaintenkäyttötarkoitukset

Varmenteentietosisällöissäkäyttötarkoituksenmäärä äväkenttämääritteleevarmenteisiin liittyvienavaintenkäyttötarkoituksen(esimerkiksi todentaminenjakiistämättömyys).Avainten käyttörajataanvainkäyttötarkoituksiinsa.Kiistäm ättömyystarkoitukseen tarkoitettuaavainta tuleesiiskäyttävaintähäntarkoitukseenikäes imerkiksi todentamiseen.

Varmenteenhakijankortilleluodaanavaimeteriksee nsähköistäallekirjoitustaeli kiistämättömyyttävartenjatunnistamistavarten.A siointivarmenteeseenliittyykaksi avainpariavastaavastikaksivarmennetta.Tunnis tusavaimenkäyttötarkoituksiinvoidaan sisällyttääsalaus.

Lain617/20094§mukaisestitunnistusvälineellävoi daantehdämyöskehittyneitäsähköisiä allekirjoituksia.Tämänmukaisesti todentamiskäyttö öntarkoitetunavaimenkäyttäminen suostumustarkoitukseenonsallittua.

## 6.2 Varmentajanyksityistenavaintensuojaaminen

### 6.2.1 Turvamoduuliakoskevatstandardit

Varmentajanyksityisiäavaimiasäilytetäänvarmenta janhallinnoimissaturvamoduuleissa.

Varmentajahuolehtiisiitä,ettävarmentajanyksity isetavaimetonsuojattupaljastumiseltaja luvattomaltakäytöltä.Varmentajanyksityisistäava imistaotetaanvarmuuskopiokriittisen tietoturvallisuudenedellyttämällätavalla.

### 6.2.2 Varmentajanyksityisenavaimenkäsittelyynos allistuvahenkilökunta

Varmentajanyksityisenavaimenluontiinjakäyttöön liittyvään ympäristöönvaaditaan vähintäänkahdenhenkilönsamanaikainenläsnäolota itoiminnanaktivoiminen.

### 6.2.3 Yksityisenavaimenvarmuuskopio

Varmentajanyksityisetavaimetjaniidenvarmuuskop iotsäilytetäänvahvastisalattuina kriittisentietoturvallisuudenvaatimuksettäyttävi ssälaitteissa.

Varmenteenomistajanyksityisistäavaimistaeiole kopioita.

### 6.2.4 Yksityisenavaimenarkistointi

Varmentajantaikäyttäjänyksityisiäavaimiaeiark istoida.

### 6.2.5 Yksityisenavaimenhallinnointiturvamoduulis sa

Varmentajanyksityisetallekirjoitusavaimetsuojata ankorkeanluotettavuudenfyysisilläja loogisillaturvatoimilla.Niitäkäytetäänvainturv alliseenympäristöön sijoitetussa järjestelmässä.

## 6.3 Varmenteenomistajanavaintensuojaaminen

### 6.3.1 Liittymäkorttiakoskevatstandardit

LiittymäkortinonoltavavalmistettuGSMA-SAS-sert ifioidussatehtaassa.

### 6.3.2 Yksityisenavaimenluovutusluotetunosapuole nhuostaan

Varmenteenomistajanyksityistäavaintaeiluovutet akenellekäänmuullekuinsenhakijalle. Toisaalta,korttitehtaaltalähtiessäänkortiteivät olekohdistettujakenellekään erityisesti,joten

yksityiselle avaimelle tuleomistajavasta, kun se sisältää liittymäkortti toimitetaan varmenteenhakijalle.

### **6.3.3 Yksityisen avaimen varmuuskopio**

Mobiilivarmenteeseen liittyvistä yksityisistä avaimista ei ole kopioita.

### **6.3.4 Yksityisen avaimen arkistointi**

Mobiilivarmenteeseen liittyviä yksityistä avainta ei arkistoida.

### **6.3.5 Yksityisen avaimen hallinnointiliittymäkortilla**

Yksityistä avainta ei hallinnoida erityisesti. Yksityinen avainonvainjaainoastaan liittymäkortilla.

## **6.4 Muutavainparin hallintaan liittyvät seikat**

### **6.4.1 Julkisen avaimen arkistointi**

Varmentaja arkistoi kaikki myöntämänsä varmenteet, joihin mukana julkinen avaintulee arkistoiduksi.

### **6.4.2 Julkisten jayksityisten avainten voimassaoloaika**

Mobiilivarmenteen voimassaoloaika on enintään viisi vuotta. Varmenteen voimassaoloaikavoimalla lyhyempikin, mikäli käytettävissä olevan avaimen pituudeneikatsotapysyvää turvallisena täyttävien vuodentaksoja. Varmenne voidaan sulkea avainten voimassaoloaikana. Varmenteen sulkutapahtuma on käsitelty enemmän kohdassa 4.5.

## **6.5 Liittymäkortilla olevien yksityisten avainten tunnukset**

### **6.5.1 Tunnusluvun luominen ja käyttöön otto**

Liittymäkortin yksityisten avainten käyttöön suojatut tunnukset, joita käytetään yksityisten avainten aktivointitietona. Varmentaja määrittää oman menettelynsä tunnuslukujen käyttöön omissa varmennuskäytännöissään.

### **6.5.2 Tunnusluvun suojaus**

Tunnusluvun suojaus on jätettävä, ettei niitä voi lukea tai kopioida kortilta. Yksityiskohtainen menettely on kuvattu varmennuskäytännöissä.

## **6.6 Varmennejärjestelmän laitteiden käyttöön jätettävät turvallisuusvaatimukset**

### **6.6.1 Laitteistoturvallisuus**

Varmennejärjestelmän laitteistoina käytetään vain käyttöä tarkoitukseen sopivia laitteistoja. Yksityiskohtainen menettely on kuvattu varmennuskäytännöissä.

## **6.7 Varmennejärjestelmän elinkaaren hallinta**

### **6.7.1 Varmennejärjestelmän kehittämiseen liittyvä alvonta**

Järjestelmän kehitys jätetään tapahtuessaan erillisessä testiympäristössä. Ainoastaan testatut, toimivat ja hyväksytyt ratkaisut siirretään tuotantoympäristöön.

### **6.7.2 Turvallisuudenhallinta**

Varmentajantietoturvaluottahallitaanvarmentaj antietoturvapoliikanmukaisesti.

### **6.8 Tietoverkonturvallisuus**

Tietoliikenneturvallisuuontoteutettusiten,että varmennejärjestelmäntietoverkkoon yhtenäinenkokonaisuus,jokaoneriytettymuistati etoverkoistajajonkakriittisetosaton toteutettukorkeansaataavuudenmenetelmillä.

Tarkempikuvaustietoverkonturvallisuudestaonkuv attuvarmennuskäytännössä.

### **6.9 Turvamoduulinkäytönvalvonta**

Varmentajahuolehtiisiitä,ettävarmentajanyksity isetavaimetonsuojattupaljastumistaja luvatontakäyttöävastaan.Varmentajanyksityisistä avaimistaotetaanvarmuuskopiokriittisen tietoturvalisuudenedellyttämälläätavalla.

Yksityiskohtainenmenettelyonkuvattuvarmennuskäy tännössä.

## 7 Varmenne-jasulkulistaprofiilit

### 7.1 Varmenteidentekniset tiedot

#### 7.1.1 Yhteiset attribuutit

Varmenteentietosisältömuodostuuyhteisistä attribuuteista ja mahdollisista varmentajakohtaisista attribuuteista. Mobiilivarmenneoudattaaleista X.509v.3 suositusta jasisältöön normaalikäytännön mukainen. Erityisesti kannattaa huomata, että käyttäjän sähköinen asiantuntijaprofiili tallennetaan *Subject*-kenttään *SerialNumber*-attribuuttiin ja liittymäkortin ICCID tallennetaan *eidSmartCardSerialNumber*-attribuuttiin. Lisäksi varmenteen myöntönyhteydessä tehdyn tunnistuksen mahdollisen ketjutuspituus on tallennettu attribuuttiin *identificationPathLength*, jonka arvolla, jos henkilö on todettu henkilökohteisesti kirjallisista asiakirjoista. Muut tapauksessa sen arvokerto on ensitunnistuksen tunnistusketjun pituus. Varmenteentietosisältöön kuvattuihin liitteisiin.

#### 7.1.2 Varmenajakohtaiset attribuutit

Varmenajavoiliasäätävien varmenteiden tarpeelliseksi katsomista RFC-5280:n mukaisesti, joista kerrotaan erikseen varmennuskäytännössä. Toiminnallisen yhteensopivuuden varmistamiseksi kyseiset laajennuskentät eivät ole kriittisiä.

### 7.2 Sulkulistaprofiili

Sulkulistaprofiili on kuvattu varmennuskäytännössä.

## 8 Varmennepolitiikanhallinnointi

### 8.1 Varmennepolitiikanmuutosmenettely

Varmentajatvoivat yhteisellä kirjallisella päätöksellä muuttaa määräyksiä lainsäädännöllisten taitoiminnallisten vaatimusten vuoksi. Määritysten muutokset on kirjattava varmennepolitiikkaan jarruvarmennuskäytäntöön seuraavassa kuvattavalla.

#### 8.1.1 Kohdat, joita voimuttamalla tiedonantajat ja palveluntarjoajat

Tähän dokumenttiin voidaan tehdä oikein kirjoitettuja julkaisukoasun liittyviä korjauksia sekä muutoksia yhteistietoihin ilman ilmoitusta käyttäjille ja palveluntarjoajille. Dokumentista voidaan julkaista käännöksiä erikielillä 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 muuttamalla ilmoittamalla niistä käyttäjille ja palveluntarjoajille 14 päivää aikaisemmin. Varmennuskäytännön uudistuminen ei vaadi tiedonantoa.

Uusien osapuolien liittyminen luottamusverkostoon ei aiheuta muutoksia varmennepolitiikan muuttamiseen.

#### 8.1.2 Kohdat, joiden muutosvaatitiedonannon käyttäjille ja palveluntarjoajille

Kaikki varmennepolitiikan jarruvarmennuskäytännön kohtia voidaan muuttamalla tulevista pääasiallisista muutoksista käyttäjille ja palveluntarjoajille vähintään 60 päivää ennen muutosten voimaantulua.

#### 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 politiikkasauuden OID:n, myösluvun 8.1.1 mukaisen muutosten johdosta pois lukien kuitteiden oikein kirjoitusvirheiden korjaukset. Varmennepolitiikan uudistuminen ei välttämättä edellytä uuden varmennuskäytännön julkaisemista. Varmennuskäytännön uudistuminen ei edellytä uuden politiikan laatimista.

### 8.2 Julkaiseminen ja tiedottaminen

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

Varmentajat pitävät asiakirjoistaversion hallintaasekään arkisto kaikkien varmennepolitiikka- ja varmennuskäytäntöversioita.

### 8.3 Varmennepolitiikanmuutos-jahyväksymismenettely

#### 8.3.1 Varmennepolitiikanhallitsija

Varmennepolitiikka hallinnoijajsen kehitysohja luottamusverkon varmentajien yhteisnimeä Mäbiilivarmennejohtoryhmä. Varmentajat osivat keskenään johtoryhmän vahvuuden jatoimintatavat. Varmentajat nimeävät omat aiomat dustajansa johtoryhmään.

#### 8.3.2 Muutosmenettely

Varmennepolitiikkaan tehtäviä muutoksia tekee muodostettavat työryhmä, johon varmentajat nimeävät omat dustajansa. Työryhmä esittelee ehdotuksensa varmennepolitiikan muutoksista.

Mobiilivarmennejohtoryhmälle,jokakirjallisestihy väksyymuutokset,minkäjälkeenuudistettu varmennepolitiikkaastuuvoimaan.

#### 8.4 Versionhallinta

Varmentajatarkistoivatkaikkihyväksymänsävarmenn epolitiikkaversiotjaneovat pyydettäessäsaatavilla.

<b>Versio</b>	<b>Päiväys</b>	<b>Kuvaus</b>
1.0	xx.yy.2010	Ensimmäinenhyväksytyyjulkaistu versio

## Viiteluettelo

- [RFC3647] S.Chokhani,W.Ford.,R.Sabett,C.Merrill,S.Wu."InternetX.509PublicKeyInfrastructureCertificatePolicyandCertificationPracticesFramework". IETF RFC3647,November2003.URL <http://tools.ietf.org/html/rfc3647>.
- [RFC5280] D.Cooper,S.Santesson,S.Farrell,S.Brodeur,R.Housley,W.Polk."InternetX.509PublicKeyInfrastructureCertificateandCertificateRevocationList(CRL)Profile".IETF RFC5280,May2008. 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."

## Liite1:Varmenteentietosisältö

Varmenteensisältämätekstisisältötalletetaan UTF-8merkistökoodausta, jotta kaikki hankalammatkin merkit saataisiin esitettyksi mielekkäällä jayhtenäisellä tavalla. Varmenteentietosisältöön otetaan mukaan vain minimimäärätietojaa inoastaan kaksi: henkilön virallinen nimi ja hänen sähköinen asiointitunnuksensa. Näin estetään esimerkiksi henkilön nimen ja puhelinnumeron välisen kytkennän rakentaminen mobiilivarmennehakemiston avulla.

Varmenteentietosisältöön tule liittymäkortin ICCID, jotta varmenteen yksikäsitteinen kytkeminen annettuun puhelinnumeroon olisi mahdollista. Tämä tekee myös sen, että liittymän MSISDN:n vaihtaminen on ainakin teoriassa mahdollista uusimattavarmennetta, koska MSISDN ei vaikuta varmenteensisältöön mitenkään.

Mobiilivarmenne noudattaa yleistä X.509v.3 suositusta jaisältöön normaalikäytännön mukainen.

Kenttä	Sisältö	Kommentit
Version	V3	
SerialNumber		Varmenteensarjanumero
SignatureAlgorithm	sha512RSAtai sha256RSA	
SignatureValue	Varmentajan allekirjoitus	
Issuer		
ValidFrom		
ValidTo		
Subject	SerialNumber=SaTu CN=Sukunimi Etunimet SaTu G=Etunimet SN=Sukunimi	
PublicKeyUsage	<i>digitalSignatureja keyEnciphermenttai pelkästään nonRepudiation.</i>	<i>Kriittinen, tunnistus- ja allekirjoitusvarmenteelle on eri käyttötarkoitukset.</i>
ExtendedKeyUsage		<i>Ei-kriittinen, eikä käytössä yhteisessä tietosisällössä</i>
eidSmartCardSerialNumber		ICCID
identificationPathLength	0,1,2...	<i>Ei-kriittinen, ensitunnistuspolut pituus</i>
AuthorityKeyIdentifier		<i>Ei-kriittinen, myöntöön käytetyn avainparin julkisen avaimen yksilöivä tieto.</i>
SubjectKeyIdentifier		<i>Ei-kriittinen, julkisen avaimen SHA-1 -tiiviste.</i>
CRLDistributionPoints	CRLDistributionPoint	<i>Ei-kriittinen, mikäli käytössä</i>
AuthorityInformationAccess	OCSPResponderAddress	<i>Ei-kriittinen, mikäli käytössä</i>
AuthorityInformationAccess	CAIssuers	<i>Ei-kriittinen, URI, josta varmentajan varmenne on haettava</i>
BasicConstraints/CA	False	<i>Kriittinen, varmennetta ei voida käyttää varmentajan varmenteena</i>
CertificatePolicies	PolicyIdentifier PolicyQualifierInfo	<i>Kriittinen, varmennepolitiikan OID PolicyQualifierId =CPS, Qualifier= Varmennuskäytännön URI</i>
	PolicyQualifierInfo	<i>PolicyQualifierId =UserNotice, NoticeText =Varmentajan info</i>
SubjectAlternativeName	URI	<i>Ei-kriittinen, URI: <a href="http://oper-">http://oper-</a></i>

[id.operator.fi/eid/SATU](http://id.operator.fi/eid/SATU),  
yksityiskohtainensisältöön  
varmentajanpäätettävissä.

Varmenteentietosisällöissäonmuutamaharvemminkä tetytribuutti.Niidenyksilöivät  
tunnisteet(OID:it),viittauksetkyseistenattribuu ttienmäärittelyihinsekätietojen  
tallennuksessakäytettyesitysmuotoovatseuraavat:

<b>Kenttä/Attribuutti</b>	<b>OID/viite jatallennuksessakäytettyesitysmuoto</b>
SerialNumber	2.5.4.5, <a href="http://www.alvestrand.no/objectid/2.5.4.5.html">id-at-serialNumber</a> , <a href="http://www.alvestrand.no/objectid/2.5.4.5.html">http://www.alvestrand.no/objectid/2.5.4.5.html</a> , <i>PrintableString</i>
eidSmartCardSerialNumber	1.2.752.34.2.1, <a href="http://www.alvestrand.no/objectid/1.2.752.34.2.html">SEISPrivateExtensionArc</a> , <a href="http://www.alvestrand.no/objectid/1.2.752.34.2.html">http://www.alvestrand.no/objectid/1.2.752.34.2.html</a> , <i>PrintableString</i>
identificationPathLength	1.2.246.277.1.5.4.106Elis anOID-avaruus, <i>Integer</i>

## Liite2: Varmennusorganisaation osapuolten vastuut ja velvollisuudet

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

Osapuolten jvelvoitteet	M/R/O	Selitykset ja tarkennukset
<b>Varmentaja</b>		
Kokonaisvastuuvarmennepalvelun tuottamisesta.	M	<p>Varmentajalla on asianmukaiset sopimukset jasopimussuhteiden palveluiden tuottamisesta, joihin liittyy ulkoistusta, alihankinta- ja muuta kolmansien osapuolten käyttöä.</p> <p>Varmentaja vastaa tämän politiikan vaatimusten täyttymisestä myös silloin, kun osavarmentajan toiminnosta on ulkoistettu alihankkijoille.</p>
Varmennepalvelun tuottamisessa siihen liittyvän lainsäädännön sekä varmentajien yhteisten ja varmentajan omien käytäntöjen noudattaminen.	M	<p>Varmentajan toiminta sääntele</p> <ul style="list-style-type: none"> <li>Lakivahvastasähköisestä tunnistamisesta jasähköisistä allekirjoituksista (617/2009)</li> <li>Varmennepolitiikka</li> <li>Varmentajan omat varmennuskäytäntö-dokumentit (CPS)</li> </ul>
Varmennepalvelun tuottaminen varmennuskäytäntö-dokumentin (CPS) mukaisesti.	M	<p>Varmentaja vastaa siitä, että Mobiilivarmenne on käytettävissä luovutushetkestä alkaen koko Mobiilivarmenne voimassaoloajan, ellei varmennetta ole asetettu sulkulistalle.</p> <p>Kortinliikkeelle laskijavoiirtisanoa liittymäsopimuksen esimerkiksi maksamattomien laskujen vuoksi, jolloin myös Mobiilivarmenne suljetaan.</p> <p>Varmentaja vastaa oman varmennejärjestelmän säturvallisuudesta.</p>
Varmennepolitiikan kehittäminen ja ylläpito	R	<p>Varmentajan tyhdessä huolehtivat varmennepolitiikan kehittämisestä ja ylläpidosta.</p>
Varmenteen hakijan tunnistaminen luotettavasti jasopimuksen tekeminen.	M	<p>Varmenteen hakijan tunnistamisessa noudatetaan mitä laissa vahvastasähköisestä tunnistamisesta jasähköisistä allekirjoituksista (617/2009) on määrätty.</p> <p>Hakijan kanssa tehtävä sopimus täyttää lain vahvastasähköisestä tunnistamisesta jasähköisistä allekirjoituksista (617/2009) vaatimukset.</p> <p>Varmentaja ilmoittaa hakijalle tai rekisteröijälle varmenteen myönnettäessä</p>

		<p>peruuttamisesta.</p> <p>Varmentajavastaamyössiitä, että Mobiilivarmenneonluovutettuhenkilölle, joka ontunnistettuMobiilivarmenteelta edellytettävällätavalla.</p> <p>Mikälihakijantunnistamisentekeeasiamies (Rekisteröijä), onvarmentajantämänkanssa tekemässäänsopimuksessaveloitettavalain mukainentoimintatapa.</p>
Huolehtiivarmenteidentietosisällön virheettömyydestä.	M	<p>Tarkistaavarmenteenhakijanhenkilötiedot Väestörekisterikeskuksen Väestötietojärjestelmästä.</p> <p>AllekirjoittaessaanMobiilivarmenteen yksityiselläavaimellaanvarmentajavakuuttaa tarkistaneensaMobiilivarmenteessaolevat henkilötiedotvarmennepolitiikassaja varmennuskäytännössäesitettyjen menettelyjenmukaisesti Väestötietojärjestelmästä.</p> <p>Varmentajavastaaainoastaanniistätiedoista, jotka on tallettanutMobiilivarmenteeseen.</p>
Huolehtiivarmenteiden sulkemisestajavarmenteiden sulkulistojenjulkaisemisesta.	M	<p>Kukinvarmentajaonvelvollinenjulkaisemaan varmenteetjasulkulistsiten, että ne ovat kaikkiennitatarvitsevientahojensaatavilla.</p> <p>Varmentajavastaasiitä, että sulkulistalle viedäänoikeaMobiilivarmennejaettäne ilmestyvässävarmennepolitiikassa mainitussaajassasulkulistalle.</p>
Noudattaavarmenteenomistajien henkilötietojenkäsittelyssä voimassaolevalainsäädäntöä, Viestintävirastonohjeistusta, hyvää tietosuojantasoasekähyvää tietojenkäsittelytapaa.	M	<p>Suojaahenkilötiedotriittäväillä teknisillä ja organisatorisilla toimenpiteillä laittomaltai luvattomaltakäytöltä.</p> <p>Suojaakaikkivarmennuspalveluunliittyvät tärkeät tiedot jätiedostothäviämiseltä, tuhoamiseltajaväärentämiseltä.</p> <p>Varmentajallaontietoturvallisuuden hallintajärjestelmä, joka on riittävä sen tarjoamille varmennepalveluille.</p> <p>Varmenteenhakijanvarmentajalle luovuttamaa henkilötietoaeiluovutetuille ilmanhakijansuostumusta, tuomioistuinpäätöstä taimuutalakiin perustuva vaatimustamuutoinkuin varmenteentietosisällönosana.</p> <p>Joitaintieto jasaatetaanmyöhemminjoutua palauttamaanoikeudellisistasyistä.</p>
Varmentajaonjuridinenhenkilö voimassaolevalainsäädännön	M	<p>Lakivahvastasähköisestä tunnistamisestaja sähköisistä allekirjoituksista (617/2009)</p>

mukaisesti.		
Varmentajaonhuolehtinut riittävistäjärjestelyistä, joiden avulla pystyy hoitamaan toiminnastaan koituvat vastuut.	M	Lakivahvastasähköisestä tunnistamisesta sähköisistä allekirjoituksista (617/2009)
Varmentaja on taloudellisesti vakavarainen ja sillä on riittävät taloudelliset voimavarat toimia tämän politiikan mukaisesti.	M	Lakivahvastasähköisestä tunnistamisesta 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 volyymit.	M	Lakivahvastasähköisestä tunnistamisesta sähköisistä allekirjoituksista (617/2009)
Varmenteen luomiseen ja peruuttamiseen liittyviä tehtäviä hoitavien varmentajan organisaation osien rakenteen tulee olla dokumentoitu.	M	Lakivahvastasähköisestä tunnistamisesta sähköisistä allekirjoituksista (617/2009).
<b>Rekisteröijä</b>		
Hoitaavien varmentajan puolesta varmenteen hakijan tunnistamisen varmennuskäytännön mukaisesti. Rekisteröijä toimii varmentajan lukuun ja vastuullasiten kuin varmentajan rekisteröijän välisessä sopimuksessa on sovittu.	M	<p>Asianmukaisen ja täydellisen varmennepyyntötoimittaminen varmentajalle ensimmistä varmennetta haettaessa, varmennetta uusittaessa ja avainpareja uusittaessa.</p> <p>Laissavahvastasähköisestä tunnistamisesta sähköisistä allekirjoituksista on määritetty varmenteen hakijan tunnistamiseen kelpaavat asiakirjat seuraavasti:</p> <ul style="list-style-type: none"> <li>• Voimassa olevasta Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämästä passista tai henkilökortista</li> <li>• Euroopan talousalueen jäsenvaltion viranomaisen 1 päivän lokakuuta 1990 jälkeen myöntämästä voimassa olevasta ajokortista</li> <li>• Vahvalla sähköisellä tunnistusmenetelmällä</li> </ul> <p>Mobiilivarmenne voidaan myöntää Suomen kansalaiselle taikotikuntalain (201/1994) mukaisesti Suomessa vakinaisesti asuvalle ulkomaalaiselle, jonka henkilötiedot on talletettu Väestörekisterikeskuksen Väestötietojärjestelmään.</p> <p>Varmistaa, että varmenteen hakijalle on toimitettu ennensopimuksen solmimista mobiilivarmenne käyttöön liittyvät</p>

		<p>käyttöohjeet.</p> <p>Liittymäntilaajan lupamaksullisen lisäpalvelun käyttöönottamiseksi, kun tämä on tarpeen.</p> <p>Edellä mainittu pätevyysinä tapauksessa, että varmentaja toimii rekisteröijänä.</p>
<b>Liittymäkortin liikkeellelaskija</b>		
Turvaallekirjoituksen luomistietojen luottamuksellisuuden eikätallennata jljennä varmenteen omistajalle luovutettuja allekirjoituksen luomistietoja.	M	<p>Kortilla luotavien avaintapauksessa kortin liikkeellelaskijavastaakortilla olevan alustan turvallisuudesta avaintenluontiohjelman ajamistavarten, avaintenluontisovelluksesta, kortin turvamoduulin luotettavuudesta ja yksityisen avaimen luottamuksellisuudesta.</p> <p>Tehdasvalmisteisten avaintapauksessa kortin liikkeellelaskijavastaavainparien luonnista, liittymäkorttien jätunnuksien luottamuksellisesta luomisesta jajakelusta asiakkailleen, julkisen avaimen varmentamiseen tarvittavien julkisen avaimen jakotietojen toimittamisesta varmentajalle javarmenteen rekisteröinnissä mahdollisesti tarvittavien liittymäasiakkuus-jakotietojen toimittamisesta liittymäasiakkaalle.</p>
<b>Varmenteen omistaja</b>		
Antaatakatjatäydelliset henkilötiedot varmentajalle tai tämän edustajalle tämän politiikan mukaisesti rekisteröinnin yhteydessä.	M	<p>Rekisteröijä varmistaa omalta osaltaan, että varmenteen hakijan antamat tiedot ovat täydelliset ja virheettömät.</p> <p>Varmenteen hakijavahvista hakemuksen allekirjoituksella antamansa tiedot oikeiksi.</p>
Ilmoitettavavarmmentajalle nimen vaihdoksesta enintään kolmen kuukauden kuluessa muutoksesta.	M	Käyttäjä veloitettavat hänen Varmentajan ja Varmenteen omistajan välisessä sopimuksessa.
Säilyttää tunnistusvälinettä ja siihen liittyviä tunnuslukuja huolellisesti ääkkseen mobiilivarmenteen luvattoman käytön.	M	<p>Määritetty varmenteen haltijan velvollisuudeksi laissa vahvasta sähköisestä tunnistamisesta ja allekirjoituksesta (617/2009).</p> <p>Varmentajan on Varmenteen omistajan kanssa tekemässään sopimuksessa otettava tämä huomioon.</p> <p>Varmenteen omistajan on käytettävä avaimensa suojaamiseen tunnuslukuja säilytettävän määrän huolellisesti.</p> <p>Mobiilivarmenteen omistajan sähköinen henkilöllisyys, eikä sitä tämän vuoksi saa luovuttaa toisen henkilön käytettäväksi. Mobiilivarmenteen omistaja on vastuussa</p>

		varmenteenkäytöstä, sillätekemistään oikeustoimistajaniidentaloudellisista seuraamuksista.
Varmenteenomistajantulee viipymättätehdävarmentajan Sulkupalveluunilmoitus	M	<p>Määritettyvarmenteenhaltijan velvollisuudeksi laissa vahvastasähköisestä tunnistamisesta ja allekirjoituksista (617/2009).</p> <p>Varmentajan on varmenteenomistajan kanssa tekemässään sopimuksessa otettava tämä huomioon.</p> <p>Ilmoituson tehtävä välittömästi kun:</p> <ul style="list-style-type: none"> <li>• Varmenteenomistajalla on syytä epäillä että hänen liittymäkorttinsa on kadonnut, varastettuja tietokoneita on käytetty,</li> <li>• Varmenteenomistaja on menettänyt yksityisen avaimensa hallinnan, koska sen aktivointitieto (ts. tunnusluku) on kadonnut tai joutunut väärin käsiin, tai jostain muustasyystä,</li> <li>• Varmenteenomistajalle on käynyt ilmi, että varmenteentiedoteivätenä päde tai etäniissä on epävarmuuksia.</li> </ul> <p>Mobiilivarmenteenomistajan vastuu varmenteenkäytöstä päättyy, kun hän on ilmoittanut sulkupalveluun tarvittavat tiedot sen sulkemiseksi. Tällöin vastuus siirtyy varmentajalle. Sulkuilmoituson tehtävä välittömästi, kun syy ilmoittamiseen on havaittu. Varmenteenomistajantulee säilyttää yksityisiä avaimiaan huolellisesti estääkseen yksityisten avaintensa eli käytännössä niihin liittyvien tunnuslukujen luvattoman käytön.</p>
<b>Varmenteeseen luottava osapuoli</b>		
Tarkistaaja varmistaa varmenteen voimassaolo varmenteenkäytön yhteydessä	M	<p>Varmenteeseen luottavan osapuolentulee tarkistaa varmenteen voimassaolo seuraavasti:</p> <ul style="list-style-type: none"> <li>• Tarkistettavavarmenteen voimassaolo ajankattavuus varmenteen omistatiedoista.</li> <li>• Varmistettavavarmenteen aitous ja eheys tarkistamalla sen myöntäjän sähköinen allekirjoitus käyttäen varmenteen myöntäjän julkista avainta.</li> <li>• Noudettavavarmennettakoskevat sulkutiedot vähintään yhdestä varmenteeseen tallennetusta osoitteesta.</li> <li>• Varmistettavavarmennettakoskevat sulkutiedot vähintään yhdestä varmenteeseen tallennetusta osoitteesta.</li> </ul>

		<p>tarkistamalla sen myöntäjän sähköinen allekirjoitus ja tähän käytetyn varmenteen voimassaolo.</p> <ul style="list-style-type: none"> <li>• Tarkistettavien sulkutiedon voimassaoloajankattavuus. Varmennetta ei pidä hyväksyä, mikäli ajantasaistaja voimassaoleva sulkutieto ei ole saatavilla. Kaikkien varmenteiden hyväksymiset ajantasaisesti puuttuessa tapahtuvat varmenteeseen luottavien osapuolien omalla riskillä.</li> <li>• Varmistettava, että käytettävä varmenne ei ole sulkutietojensa perusteella suljettu.</li> <li>• Tarkistettava, että myönnetty varmenne vastaakäyttöä tarkoitustansiinä oikeustoimessa, jossa sitä on käytetty.</li> </ul>
<p>Varmenteiden käyttöön liittyvien tietojen tallentaminen.</p>	<p>R</p>	<p>Luottavien osapuolien vastuulla on säilyttää ne tiedot, jotka hän tarvitsee mobiilivarmenteella tehtyjen toimienpiteiden varmentamiseksi myöhempänä ajankohtana. Tällaisia tietoja ovat käytetyt varmenteet ja sulkulistat sekä allekirjoituksen luontiajankohta, joka on myös syytä pitää mukana allekirjoitetussa tietosisällössä.</p>