Elisa Varmenne

Elisa Oyj

VARMENNUSKÄYTÄNTÖ

Elisa Mobile-Id varmentajan varmenne

Versio 1.2
Voimassa 1.10.2014 lähtien

Versionhallinta

Muutoshistoria		
Versio	**Päivämäärä**	**Kuvaus**
1.0	1.10.2010	Asiointivarmentajan varmennuskäytännön ensimmäinen versio
1.1	1.1.2011	Poistettu henkilökunnan perusmuotoinen turvallisuusselvitys ja liittymän omistussuhteen pakottama varmenteen sulku sekä täsmennetty roolitusta.
1.2	15.9.2014	Täsmennetty sopimusarkistoinnin kuvausta, varmenteen elinkaaren hallintaa ja sulkupalvelun yhteystiedot. Ajantasaistettu suostumuspalvelun kuvaus.

SISÄLLYSLUETTELO

Käsitteet

Tässä dokumentissa käytetty suomenkielinen termi	**Englanninkielinen vastine**	**Selitys**
Aktivointitieto, Tunnusluku	Activation Data	Yksityisen avaimen käyttöä suojaava PIN-koodi tai salasana joka syöttämällä aktivoidaan yksityinen avain.
Alivarmentaja, operatiivinen varmentaja	Subordinate CA	Varmentaja jonka varmenteen juurivarmentaja on allekirjoittanut ja joka myöntää varmenteita määrittelemilleen loppukäyttäjille
Digitaalinen allekirjoitus	Digital Signature	Sähköinen allekirjoitus, joka on tehty asiakirjan tai viestin laatijan tai lähettäjän yksityisellä avaimella julkisen avaimen menetelmän mukaisesti. Käytännössä salattu tiiviste viestistä.
Hakemistopalvelu	Directory Service	Julkisen avaimen järjestelmässä palvelu, joka sisältää käyttäjien varmenteita ja sulkulistoja sisältäviä hakemistoja.
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 tuottaa käyttäjille avainparit, varmentaa ne digitaalisella allekirjoituksellaan ja jakaa ne 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.
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 vaadittavat tunnusluvut.
Luottava osapuoli	Relying Party	Sähköisiä palveluja varmenteiden loppukäyttäjille tarjoava taho. Luottava osapuoli toimii luottaen varmenteeseen ja/tai todentaa digitaalisen allekirjoituksen varmenteen avulla.
Mobiilivarmenne	Mobile Certificate	Varmenne, johon liittyvä yksityinen avain on tallennettu varmenteen omistajan mobiilipäätteen liittymäkortille.
Rekisteröijä	Registration Authority (RA)	Varmenteen hakijan tunnistamisesta ja varmennehakemukseen rekisteröitävien tietojen tarkistamisesta vastaava osapuoli. Rekisteröijä toimii varmentajan valtuuttamana varmenneorganisaation osana.
RSA	RSA	Epäsymmetrinen salausalgoritmi, jota käytetään epäsymmetrisen avainparin luontiin. Lyhenne tulee keksijöidensä sukunimistä; Rivest, Shamir ja Adleman.
Sulkulista	Certificate Revocation List (CRL)	Julkisen avaimen järjestelmässä käytöstä poistettujen varmenteiden luettelo. Varmentaja julkaisee sulkulistan hakemistopalvelussa.
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.
Todentaminen	Authentication; Verification	Järjestelmän käyttäjän (henkilön, organisaation tai laitteen) tai viestinnässä toisen osapuolen tunnistuksen varmistaminen.
Toimikortti	Smart Card, Integrated Circuit Card, Chipcard	Suorittimen ja muistia sisältävä kortti. Tiedot on talletettu kortilla olevaan muistiin. Korttiin liittyvän tekniikan avulla voidaan toteuttaa riittävän turvallisesti mm. osapuolten tunnistus, sähköinen allekirjoitus, salakirjoittaminen ja asioinnin kiistämättömyys.
Varmenne	Certificate	Varmenne on henkilön julkisesta avaimesta, nimitiedoista, sekä muista 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 sulkulista-palvelujen tuottajat sekä muut palvelun tuottajat, joiden palveluja varmentaja käyttää.
Varmennepolitiikka	Certificate Policy (CP)	Nimetty joukko sääntöjä, jotka ilmaisevat varmenteen soveltuvuuden tiettyyn kokonaisuuteen ja yleiset turvallisuus- ja muut vaatimukset.
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.
Varmentaja	Certification Authority (CA)	Varmenneorganisaation osapuoli, joka myöntää varmenteita allekirjoittamalla varmennetiedot omalla yksityisellä avaimellaan.
Varmennuskäytäntö, toimintamalli	Certification Practice Statement (CPS)	Yksityiskohtainen selostus menettelytavoista, joita varmenneorganisaatio käyttää myöntäessään ja hallinnoidessaan varmenteita.
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.

Lyhenneluettelo

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	Certificate Revocation List	Sulkulista
HSM	Hardware Secure Module	Varmentajien avainten luontiin ja säilytykseen käytettävä turvamoduuli
ICCID	Integrated Circuit Card Identifier	Liittymäkortin yksilöllinen sarjanumero
MSSP	Mobile Signature Service Provider	Mobiiliverkon ja kiinteän verkon välillä toimiva mobiiliallekirjoitusten 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, liittymän ominaisuus, ei varmenteen
RA	Registration Authority	Rekisteröijä
RSA	Rivest, Shamir ja Adleman	Salausalgoritmi
X.509	-	Varmenteen ja sulkulistan rakenteen määrittelevä standardi

Roolit

Liittymän Tilaaja	Vastaa laskujen maksusta. Luonnollinen henkilö tai yritys, joka sallii liittymän palvelut. Voi olla sama kuin Liittymän Käyttäjä.
Liittymän Käyttäjä	Liittymän ja palveluiden käyttäjä, luonnollinen henkilö, joka on merkitty liittymän haltijaksi. Käyttäjä voi olla sama kuin Liittymän Tilaaja

Varmenteen Hakija	Aina sama luonnollinen henkilö kuin Liittymän Käyttäjä. Liittymän haltijaksi on oltava merkittynä Varmenteen Hakija.
Varmenteen Omistaja	Luonnollinen henkilö, jolle on myönnetty Asiointivarmenne. Aina sama luonnollinen henkilö kuin Varmenteen Hakija eli Liittymän Käyttäjä.

1 Johdanto

Varmennepolitiikka (engl. *Certificate Policy, CP*) kuvaa varmennepalvelun soveltuvuuden käyttötarkoitukseensa ja periaatteet, joita varmentaja noudattaa myöntäessään ja hallinnoidessaan varmenteita. Varmennepolitiikka määrittelee keskeiset ominaisuudet, joiden perusteella varmenteen luotettavuus ja turvallisuus on arvioitavissa.

Asiointivarmenne on varmenne, josta on säädetty laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista. Asiointivarmenne ei ole laissa mainittu laatuvarmenne.

Varmennuskäytäntö (engl. *Certification Practice Statement, CPS*) 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.

Tämä varmennuskäytäntö kuvaa Elisa Oyj:n käytännöt ja toimintatavat varmentajana teleoperaattoreiden yhteisen asiointivarmenteen politiikan "**Mobiiliasiointivarmenne - Varmennepolitiikka - Operaattoreiden mobiiliasiointivarmennetta varten**" toteuttamiseksi.

1.1 Yleistä

Tämä varmennuskäytäntö kuvaa toimintatavat ja menetelmät, joita Elisa Oyj:n Elisa Mobile-Id varmentaja noudattaa myöntäessään ja hallinnoidessaan loppukäyttäjien asiointivarmenteita mobiilipäätelaitteisiin.

Elisa Oyj:n myöntämiä asiointivarmenteita voidaan käyttää tunnistamiseen, salaamiseen sekä tiedon tai tapahtuman eheyden, luottamuksellisuuden ja kiistämättömyyden varmistamiseen. Henkilövarmenteet myönnetään mobiilipäätelaitteilla käytettävillä liittymäkorteilla sijaitseville avainpareille. Varmennepolitiikan mukaisesti Elisa Mobile-Id varmentaja voi myöntää oman toimintansa vaatimille palveluille kuten esimerkiksi suorakäyttöiselle varmenteen tilan tarkistuspalvelulle (OCSP) varmenteen, jolla allekirjoittaa OCSP-kyselyjen vastaukset. Näiden lisäksi varmentaja voi myöntää varmennepolitiikassa määritellyille näennäisille testihenkilöllisyyksille varmenteita, joista puuttuu varmennepolitiikan tunniste (*Policy Identifier*), jotta ne voisi tunnistaa testivarmenteiksi. Kaikki muut Elisa Mobile-Id varmentajan myöntämät varmenteet ovat mobiilipäätelaitteisiin myönnettyjä henkilövarmenteita.

Tätä varmennuskäytäntöä sovelletaan varmenteisiin, jotka on myöntänyt Elisa Mobile-Id CA, jota tässä dokumentissa kutsutaan myös lyhyemmällä nimellä Asiointivarmentaja.

1.2 Varmennuskäytännön tunnisteet

Tämän varmennuskäytännön nimi on " **Elisa Varmenne – Elisa Oyj – Varmennuskäytäntö – Elisa Mobile-Id varmentajan varmenne ".**

Varmennuskäytännön tunniste (*Object Identifier*) on: **1.2.246.277.1.11.4.2.2.3**

ISO(1).MemberBody(2).Suomi(246).HPY(277).Services(1).caService(11).MobileCertificates(4).
CertificationPracticeStatements(2).Elisa-ID CA(2).Serial no(3)

Tätä varmennuskäytäntöä vastaava **varmennepolitiikka** on nimeltään **" 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)

Varmennepolitiikka on saatavissa osoitteesta http://mobile-id.elisa.fi/cps/.

Tämä varmennuskäytäntö viittaa seuraaviin Elisa Oyj:n juurivarmentajan (Elisa Corporation Root CA) dokumentteihin:

- Elisa Oyj – Varmennepolitiikka – Juurivarmentajan varmenne (OID 1.2.246.277.1.11.4.1.1.1)
- Elisa Oyj – Varmennuskäytäntö – Juurivarmentajan varmenne (OID 1.2.246.277.1.11.4.2.1.1)

1.3 Varmennusorganisaatio ja varmenteiden soveltuvuus

Elisa Oyj toimii juurivarmentajana tuottaen varmennepalvelut tämän varmennuskäytännön mukaisesti toimien. Juurivarmentaja vastaa varmennejärjestelmän toimivuudesta kokonaisuudessaan, myös käyttämiensä alihankkijoiden ja teknisten toimittajien osalta.

Juurivarmentaja noudattaa toiminnassaan voimassaolevaa Suomen lainsäädäntöä.

1.3.1 Varmentaja

Elisa Oyj toimii varmentajana. Varmentaja myöntää harkintansa mukaan hakijoille varmenteet ja vastaa myöntämiensä varmenteiden tietosisällön virheettömyydestä.

Varmentaja voi ulkoistaa toimintojaan tai käyttää toimintojensa toteuttamiseen alihankkijoita. Varmentajan käyttämät alihankkijat sitoutuvat noudattamaan voimassaolevan varmennepolitiikan ja varmennuskäytännön määräyksiä.

Varmentaja allekirjoittaa varmentajan varmenteessa sijaitsevaa julkista avainta vastaavalla yksityisellä avaimella myöntämänsä asiointivarmenteet ja julkaisemansa asiointivarmenteiden sulkulistan (*CRL*). Varmentajan yksilöivät tiedot näkyvät varmentajan myöntämän asiointivarmenteen ja varmentajan julkaiseman sulkulistan myöntäjä (*Issuer*) –kentässä.

Juurivarmentaja noudattaa toiminnassaan varmennepolitiikkaa ja varmennuskäytännön määräyksiä.

1.3.2 Rekisteröijä

Rekisteröijällä tarkoitetaan tahoa, joka toimii varmentajan toimeksiannosta ja vastuulla ja hoitaa varmennehakemusten käsittelyyn liittyvää käytännön työtä noudattaen tätä varmennuskäytäntöä ja vastaavaa varmennepolitiikkaa. Asiointivarmenteen rekisteröijinä toimivat varmentajan paikalliset asiointipisteet sekä muut varmentajan kanssa rekisteröintiä koskevan sopimuksen tehneet organisaatiot. Itsepalvelurekisteröitymisessä rekisteröijäksi katsotaan varmenteen myöntäjä.

1.3.3 Varmenteen mitätöijä

Varmenteiden mitätöijinä voivat toimia varmentajan organisaatioon kuuluvat, varmenteiden mitätöintiin valtuutetut henkilöt tai muut varmentajan valtuuttamat henkilöt, joiden kanssa varmentaja on tehnyt sopimuksen varmenteiden mitätöintitoimenpiteiden suorittamisesta.

Valtuutettujen varmenteiden mitätöijien toimintaan pätevät seuraavat ehdot:
- Valtuutettu varmenteiden mitätöijä sitoutuu noudattamaan varmennepolitiikkaa ja varmennuskäytäntöä.
- Varmenteiden mitätöijä todentaa varmenteen mitätöintipyynnön tekijän henkilöllisyyden.
- Varmenteen mitätöijä noudattaa varmentajan kanssa varmenteiden mitätöinnistä sovittuja menettelytapoja ja ohjeita.

1.3.4 Varmenteen Sulkupalvelu

Varmenteen Sulkupalvelu on organisaatio, jonka palveluksessa on yksi tai useampia varmenteen mitätöijä. Sen tehtävä on tarjota yleisölle asiointirajapinta, jonka kautta oman varmenteen voi sulkea. Käytännössä Rekisteröintipisteiden yhteydessä toimii yleensä myös Sulkupalvelu.

1.3.5 Varmenteen omistaja

Varmentaja myöntää asiointivarmenteita matkapuhelinliittymäasiakkaidensa käyttöön. Asiointivarmenteita myönnetään vain luonnollisille henkilöille, joilla on Väestörekisterikeskuksen myöntämä suomalainen henkilötunnus.

Asiointivarmenteen omistajan tulee noudattaa varmenteen käytössä ja hallinnassa varmentajan varmennepolitiikkaa ja varmennuskäytäntöä sekä hyväksyä näissä kuvatut ehdot ja toimintatavat.

1.3.6 Varmenteeseen luottava osapuoli

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

teeseen luottavan osapuolen vastuut ja velvollisuudet on selostettu varmennepolitiikassa.

1.3.7 Soveltaminen

Tätä varmennuskäytäntöä sovelletaan Elisa Oyj:n varmennetoimintaan, sen varmennetoiminnassa mahdollisesti käyttämiin alihankkijoihin kuten tietoteknisiin toimittajiin, kortin valmistajiin, yksilöijiin ja rekisteröijiin.

Varmennuskäytäntöä sovelletaan varmenteiden omistajiin ja varmenteisiin luottaviin osapuoliin.

Tämän varmennuskäytännön mukaisesti myönnetyn liittymäkortilla sijaitsevan asiointivarmenteen käyttötarkoitukset ovat:

- Varmenteen omistajan tunnistaminen
- Digitaalisen allekirjoituksen kiistämättömyyden muodostaminen ja todentaminen
- Sähköisessä muodossa olevan tiedon todentaminen
- Sähköisessä muodossa olevan tiedon luottamuksellisuuden varmistaminen

Mahdollisille Asiointivarmentajan auktorisoiduille OCSP-vastauspalveluille (*Authorized Responder*) myönnettyihin varmenteisiin merkitään käyttötarkoitukseksi vain laajennettu käyttötarkoitus *id-kp-OCSPSigning* RFC 2560:n mukaisesti [RFC2560].

Varmenteeseen luottavan osapuolen tulee huomioida varmenteessa oleva varmennepolitiikan tunniste ja avaimen käyttötarkoitus sekä noudattaa em. kenttien määrittelemiä käyttötarkoitusta koskevia määräyksiä.

Elisa Oyj:n juurivarmentajan varmenne ja Asiointivarmentajan varmenne ovat yleiskäyttöisiä varmenteita. Varmenteiden käyttöä ei ole rajattu erikseen määriteltyihin palveluihin tai sovelluksiin. Sovellusten tai palveluiden tulee olla voimassaolevan lainsäädännön ja määräysten sekä hyvän tavan ja käytäntöjen mukaisia.

Elisa Oyj:n juurivarmentajan varmenteen ja Asiointivarmentajan varmenteiden käyttö lain tai hyvän tavan vastaisiin palveluihin tai sovelluksiin on kielletty.

1.4 Yhteystiedot

1.4.1 Varmennuskäytäntöä hallinnoiva organisaatio

Tämän varmennuskäytännön on rekisteröinyt Elisa Oyj. Varmennuskäytännön hallinnoinnista ja päivityksestä vastaa Elisa Oyj.

Elisa Oyj
Käyntiosoite: Ratavartijankatu 5, Helsinki
Postiosoite: PL 1, 00061 ELISA

Puhelin (vaihde): 010 26 000

2 Yleiset ehdot

Tässä osassa kuvataan vaatimukset, jotka koskevat varmentajan, rekisteröijän, varmenteen omistajan ja varmenteeseen luottavan osapuolen velvollisuuksia ja vastuita.

2.1 Velvollisuudet

2.1.1 Varmentajan velvollisuudet

Varmentajan velvollisuudet on määritelty varmennepolitiikassa. Alla on tiivistetty lista keskeisimmistä varmentajan velvollisuuksista:

- Varmentaja laatii ja ylläpitää toimintaansa kuvaavan varmennepolitiikan ja varmennuskäytännön.
- Varmentaja noudattaa toiminnassaan varmennepolitiikassa ja varmennuskäytännössä asetettuja vaatimuksia.
- Varmentaja tarjoaa varmennepolitiikan mukaiset varmenne- ja hakemistopalvelut.
- Varmentaja asettaa varmennepolitiikkansa ja varmennuskäytäntönsä julkisesti saataville.
- Varmentajalla on palveluksessaan riittävä määrä työntekijöitä, joilla on tarvittava asiantuntijuus, tekninen osaaminen ja kokemus varmennepalveluiden tuottamiseksi.
- Varmentaja on taloudellisesti vakavarainen ja sillä on riittävät taloudelliset voimavarat toimia varmennepolitiikan ja varmennuskäytännön mukaisesti.
- Varmentaja vastaa varmennetoiminnasta kokonaisuudessaan, myös juurivarmentajan apunaan käyttämien alihankkijoiden, teknisten toimittajien ja henkilöiden tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta.
- Varmentaja huolehtii tietojen luottamuksellisesta ja huolellisesta käsittelystä.
- Varmentaja noudattaa toiminnassaan voimassaolevaa lainsäädäntöä.
- Varmentaja ilmoittaa Varmenteen omistajalle varmenteen peruuttamisesta mahdollisuuksien ja parhaan kykynsä mukaisesti ensi tilassa.

2.1.2 Rekisteröijän velvollisuudet

Rekisteröijän velvollisuudet on määritelty varmennepolitiikassa. Rekisteröijän keskeisin tehtävä on tunnistaa Varmenteen hakijan varmentajan puolesta luotettavasti joko

henkilökohtaisesti tai sähköisessä asiointikanavassa varmennepolitiikassa esitetyin tavoin.

2.1.3 Varmenteen mitätöijän ja Sulkupalvelun velvollisuudet

Varmenteen Sulkupalvelu ottaa vastaan varmenteen sulkupyynnön varmenteen omistajalta tai muulta varmenteen sulkemiseen oikeutetulta taholta ja todentaa sulkupyynnön tekijän henkilöllisyyden jollakin seuraavista tavoista:

- Passilla, henkilöllisyystodistuksella tai ajokortilla
- Vahvalla sähköisellä tunnistusmenetelmällä
- Suljettavan varmenteen omistajan henkilötunnuksen loppuosan tietäminen
- Soittajan numeron ja siihen liittyvän ei-ilmeisen tiedon tietäminen

Mikäli mikään tunnistustavoista ei tuota tulosta, on sulkupalvelun koetettava varmistua siitä, ettei kyseessä ole ilkivaltainen varmenteen sulkupyyntö. Epävarmoissa tapauksissa on varmenne suljettava.

Saatuaan asianmukaisen varmenteensulkupyynnön Sulkupalvelun on asetettava varmenne sulkulistalle. Mikäli sulkupyynnön teki joku muu kuin varmenteen omistaja, on Sulkupalvelun ilmoitettava sulkemisesta varmenteen omistajalle viivyttelemättä. Varmenteen mitätöijän on kirjattava muistiin sulkupyynnön tekijän henkilöllisyys, sen toteamistapa, pyynnön tekoaika ja pyynnön peruste.

Sulkupalvelun on suljettava varmenne pysyvästi ilman erillistä pyyntöä seuraavissa tapauksissa:

- Liittymän haltija vaihtuu
- Liittymän haltija kuolee
- Liittymä irtisanotaan
- Sulkupalvelun tietoon tulee, että varmenteen omistajan nimi on muuttunut, eikä hän ole ilmoittanut muutoksesta kolmen kuukauden kuluessa.

Sulkupalvelun on suljettava varmenne tilapäisesti tai pysyvästi ilman erillistä pyyntöä seuraavissa tapauksissa:

- Liittymän haltija ilmoittaa kadottaneensa puhelimensa ja pyytää sulkemaan liittymän
- On ilmennyt perusteltu syy epäillä, että varmenne on joutunut väärinkäytöksen kohteeksi.

2.1.4 Varmenteen omistajan velvollisuudet

Varmenteen omistajan velvollisuudet on kuvattu varmennepolitiikassa.

2.1.5 Varmenteeseen luottavan osapuolen velvollisuudet

Varmenteeseen luottavan osapuolen velvollisuudet on kuvattu varmennepolitiikassa.

2.1.6 Hakemistopalveluun liittyvät velvollisuudet

Varmentajien varmenteet ja varmentajien julkaisemat sulkulistat julkaistaan julkisessa hakemistossa, josta ne ovat yleisesti saatavilla 24 tuntia päivässä, seitsemänä päivänä viikossa lukuun ottamatta mahdollisia huoltokatkoksia.

Hakemistopalvelussa voidaan julkaista käyttäjien varmenteita, mikäli varmenteen omistaja niin haluaa.

2.2 Vastuut

Eri osapuolten vastuut on määritelty varmennepolitiikassa. Tässä luodaan näihin asioihin vain ylimalkainen katsaus.

2.2.1 Varmentajan vastuut

Varmentaja vastaa varmennepalveluista ja varmennejärjestelmän turvallisuudesta sekä ulkoistamistaan tai alihankkijoidensa tuottamista palveluista kohdan 2.2.7 mukaisin rajoituksin.

2.2.2 Rekisteröijän vastuut

Varmentaja vastaa kohdan 2.2.7 mukaisin rajoituksin varmenteen omistajia ja varmenteeseen luottavia tahoja kohtaan varmentajan valtuuttamien rekisteröijien varmentajan toimeksiannosta suorittamista palveluista.

Rekisteröijän ja varmentajan väliset vastuut määritellään tarkemmin osapuolten välisissä sopimuksissa.

2.2.3 Varmenteen Sulkupalvelun vastuut

Varmentaja vastaa kohdan 2.2.7 mukaisin rajoituksin varmenteen haltijoita ja varmenteeseen luottavia tahoja kohtaan Sulkupalvelun toiminnasta.

2.2.4 Varmenteen omistajan vastuut

Varmenteen omistajan vastuut on selostettu varmennepolitiikassa.

2.2.5 Varmenteeseen luottavan osapuolen vastuut

Varmenteeseen luottavan osapuolen vastuut on selostettu varmennepolitiikassa.

Mikäli luottava osapuoli lyö laimin varmenteen käyttötarkoitukseen, eheyteen tai voimassaoloon liittyvän tarkastuksen, niin luottava osapuoli vastaa tästä mahdollisesti aiheutuvista vahingoista.

2.2.6 Taloudelliset vastuut

Varmentajalla on taloudellinen vastuu varmennepalveluiden tuottamisesta, ylläpidosta ja kehittämisestä, sekä omalta osaltaan, että alihankkijoidensa puolesta varmennepolitiikan, varmennuskäytännön ja sopimusehtojen mukaisesti.

Varmentaja ei vastaa varmennetta käytettäessä syntyneistä taloudellisista sitoumuksista.

2.2.7 Vastuiden rajoitukset

Varmentajan vastuiden rajoitukset on selostettu varmennepolitiikassa sekä varmentajan ja asiakkaan välisissä sopimusehdoissa. Asiakkaita ovat sekä loppukäyttäjät että palveluntarjoajat.

2.3 Tulkinta ja täytäntöönpano

2.3.1 Sovellettava lainsäädäntö

Tähän varmennuskäytäntöön sovelletaan Suomen lakia.

2.3.2 Erimielisyyksien ratkaiseminen

Sopimuksesta tai sen tulkinnasta johtuvat erimielisyydet ratkaistaan ensisijaisesti Osapuolten välisin neuvotteluin. Jos neuvotteluissa ei päästä yksimielisyyteen, erimielisyydet ratkaistaan käräjäoikeudessa.

2.4 Maksut

Varmennepalvelusta perittävät maksut perustuvat varmentajan ja varmenteen omistajan välisiin sopimuksiin.

2.5 Tietojen julkaiseminen ja tietovarastot

2.5.1 Tietojen julkaiseminen

Varmentajan toimintaa kuvaavat ajan tasalla olevat tiedot, kuten varmennepolitiikka, varmennuskäytäntö ja muut julkiset varmennepalveluihin liittyvät asiakirjat ovat saatavilla varmentajan verkkosivuilta.

Kaikki varmentajien varmenteet ja sulkulistat julkaistaan juurivarmentajan hakemistopalvelussa. Loppukäyttäjien varmenteet julkaistaan varmentajan hakemistopalvelussa varmenteen omistajan luvalla.

2.5.2 Tietojen julkaisutiheys

Varmentajan tiedot päivitetään www-palveluun viipymättä, mikäli niissä tapahtuu varmenteeseen luottamisen kannalta oleellisia muutoksia.

Juurivarmentajan ja varmentajan varmenteet julkaistaan hakemistoon niiden luonnin jälkeen ja ne ovat saatavilla hakemistosta koko niiden voimassaoloajan.

Juurivarmentaja julkaisee varmentajien varmenteiden sulkulistan (*ARL*) juurivarmentajan varmennuskäytännön mukaisesti.

Varmentaja julkaisee kokonaisen sulkulistan suljetuista loppukäyttäjän asiointivarmenteista 60 minuutin määräajoin sekä uuden varmenteen sulkemisen tapahduttua. Sulkulista on voimassa 24 tuntia sulkulistan julkaisemisesta. Täydellisen sulkulistan lisäksi varmentaja julkaisee ositettuja sulkulistoja luvussa 7.2.3 esitetyllä tavalla.

2.5.3 Pääsynvalvonta

Juurivarmentajan, varmentajan ja Asiointivarmenteiden varmennepolitiikka, varmennuskäytäntö ja muut varmennepalveluihin liittyvät julkiset asiakirjat ovat julkisesti saatavilla varmentajan verkkosivuilta.

Varmentajan varmenne ja sulkulista ovat julkisesti saatavilla varmentajan hakemistopalvelusta.

Asiointivarmenteet ovat saatavilla rajoitetusti hakemistopalvelusta. Niiden julkaisemiseen pyydetään varmenteen omistajan lupa.

Hakemiston ja www-palvelun päivitysoikeudet ovat vain nimetyillä henkilöillä sekä varmennejärjestelmällä yksilöityjen käyttäjätunnusten kautta.

2.5.4 Tietovarastot

Varmentajan varmennepalveluun liittyvät julkiset tiedot ovat saatavilla varmentajan verkkosivuilta. Varmennepalveluun liittyvät tiedot, jotka eivät ole julkisia, ovat talletettuina varmentajan tietovarastoihin voimassaolevien arkistointisääntöjen mukaan.

2.6 Toiminnan tarkastukset

2.6.1 Sisäiset tarkastukset

Varmentaja valvoo varmennejärjestelmänsä ja varmennetoimintansa eri osa-alueiden tietoturvallisuutta sisäisin tarkastuksin. Sisäinen tarkastus suoritetaan tarkoituksenmukaisessa laajuudessaan vähintään kerran vuodessa ja aina kun toimintaan liittyviin prosesseihin, laitteistoihin tai organisaatioon on kohdistunut merkittäviä muutoksia.

2.6.2 Ulkoisen auditoijan suorittamat tarkastukset

Ulkopuolinen auditoija tarkastaa varmentajan toiminnan. Tarkastuksen kohteena on Elisa varmennepalvelun tietoturvallisuuden hallintajärjestelmä, joka kattaa kyseisen palvelun kehitys-, tuotanto- ja asiakaspalveluprosessit.

Ulkopuolinen auditointi noudattaa arvioinnissaan ISO/IEC 27001:2005 tietoturvastandardin tai vastaavan mukaisia menettelytapoja.

2.6.3 Tarkastuksien suorittajat

Varmennetoiminnan sisäisestä tarkastuksesta vastaavat Elisa Oyj:n nimeämät tahot.

Ulkoisen auditoinnin suorittaa ISO/IEC 27001:2005 –tietoturvasertifikaatin tai vastaavan myöntämiseen valtuutettu taho.

2.6.4 Toimenpiteet poikkeamatapauksissa

Mikäli sisäisessä tai ulkoisessa auditoinnissa havaitaan poikkeamia, ryhtyy varmentaja toimenpiteisiin niiden korjaamiseksi. Poikkeamien korjaamiseksi laaditaan toimenpidesuunnitelma, joka priorisoidaan ja aikataulutetaan poikkeamien vakavuuden perusteella.

Mikäli poikkeamista aiheutuu muutoksia varmennepolitiikkaan tai varmennuskäytäntöön, suoritetaan muutokset näihin dokumenttien muutoskäytäntöjen mukaisesti.

2.6.5 Tarkastuksen tuloksesta tiedottaminen

Tarkastuksista syntyvät raportit ovat tarkoitettuja varmentajan organisaation sisäiseen käyttöön. Varmentaja voi tiedottaa tarkastuksien tuloksista tai

julkaista tarkastusraportit osittain tai kokonaan viranomaisia tai kolmansia osapuolia varten tarvittaessa.

2.7 Luottamuksellisuus

2.7.1 Luottamukselliset tiedot

Varmentaja käsittelee kaikki varmenteen omistajaa koskevat tiedot luottamuksellisina. Varmenteen omistaja päättää itse omien tietojensa julkaisemisesta. Varmentamiensa loppukäyttäjien varmenteiden julkaisemisesta sovitaan erikseen varmenteen omistajan kanssa.

Varmenteen käyttöön ja sulkulistan tarkastamiseen liittyvät lokitiedot ovat luottamuksellisia. Luottamuksellisia tietoja ovat myös kaikki varmennepalvelussa käytettävät yksityiset avaimet ja tunnusluvut.

2.7.2 Julkiset tiedot

Varmentajan varmenteen ja sulkulistan sisältämät tiedot ovat julkisia tietoja.

2.7.3 Tietojen luovuttaminen viranomaisille

Viranomaisille luovutetaan tietoja vain lakien, asetusten taikka niiden nojalla annettujen määräysten tai muiden viranomaismääräysten perusteella.

2.7.4 Tietojen luovuttaminen varmenteen omistajan pyynnöstä

Varmenteen omistajalla on oikeus saada käyttöönsä itseään koskevat tiedot mm. henkilötietolain perusteella.

2.8 Omistus- ja immateriaalioikeudet

Elisa Oyj omistaa seuraavien tietojen immateriaalioikeudet:

- Kaikki varmennepalveluiden yhteydessä käytettävät tavaramerkit ja nimet
- Juurivarmentajan varmennepolitiikka ja varmennuskäytäntö, sekä tämä varmennuskäytäntö
- Asiointivarmenteen varmennepolitiikan immateriaalioikeudet ovat sen laatijoiden eli Elisa Oyj:n, TeliaSonera Finland Oyj:n ja DNA Oy:n yhteistä omaisuutta.
- Muut varmennepalveluun liittyvät juurivarmentajan tuottamat dokumentit

- Varmennejärjestelmän luomat varmenteet ja sulkulistat poislukien asiointivarmenteen hakijoille luodut varmenteet

- Varmennejärjestelmän luomat ja käyttämät sekä haltijoille toimitetut avainparit poislukien asiointivarmenteiden avainparit

- Varmennepalvelun tekijänoikeudet, patentit, ideat ja tietotaidon.

3 Varmenteen hakijan tunnistaminen

3.1 Varmenteiden nimeämiskäytäntö

Asiointivarmenteessa käytetään varmentajan yksilöivänä yksikäsitteisenä nimenä X.501–määritysten mukaista *Distinguished Name* (DN) –nimeä. Tämä yksilöivä nimi löytyy Asiointivarmentajan varmenteen *subject*–kentästä sekä kaikkien Asiointivarmentajan myöntämien varmenteiden *issuer* –kentästä.

Asiointivarmentajan yksilöivä *Distinguished Name* (DN) –nimi on:

CN = Elisa Mobile-Id CA Rev-1
O = Elisa Oyj
C = FI

Asiointivarmentajan *commonName* (CN) sisältää lopussa revisionumeron, jota kasvatetaan varmenteen uusimisen yhteydessä. Juurivarmentajan yksikäsitteinen *Distinguished Name* (DN) –nimi on:

CN = Elisa Corporation Root CA Rev-1
O = Elisa Oyj
C = FI

Juurivarmentajan *commonName* sisältää lopussa revisionumeron aivan samoin kuin varmentajan varmenne.

3.2 Varmenteen omistajan rekisteröinti

3.2.1 Nimeämiskäytäntö

Varmenteen omistaja nimetään yksikäsitteisesti varmenteen *subject* –kentässä käyttäen X.501–määritysten mukaista *Distinguished Name* (DN) –nimeä. Se koostuu seuraavan taulukon mukaisista varmennepolitiikan määräämistä pakollisista attribuuteista.

Attribuutti	**Sisällön kuvaus**
SerialNumber	SaTu (Sähköinen asiointitunnus)
commonName (CN)	Sukunimi Etunimet SaTu
givenName (G)	Etunimet
Surname (S)	Sukunimi

Esimerkki varmenteen nimeämisestä:

SerialNumber = 123456789
CN = Meikäläinen Matti Niilo 123456789
G = Matti Niilo
S = Meikäläinen

Elisa Oyj ei varmentajana lisää varmenteen tietosisältöön politiikan sallimia varmentajakohtaisia attribuutteja.

3.2.2 Nimivaatimukset ja tulkinta

Varmenteen *subject* –kentän sisällöstä tulee kyetä yksilöimään varmenteen omistaja. Mikään kentän attribuuteista ei saa sisältää pseudonyymejä, vaan nimeämiset tulee tehdä merkityksellisillä nimillä. Varmenteen omistajan nimeksi kirjataan se, minkä Väestötietojärjestelmä ilmoittaa henkilön nimeksi.

3.2.3 Nimien yksikäsitteisyys

Varmenteen *eidSmartCardSerialNumber*-kentän sisällön tulee olla yksikäsitteinen varmentajan allekirjoittamien tunnistus- ja allekirjoitusvarmenneparien kesken. Varmentaja ei myönnä useita varmennepareja, joissa on identtiset *eidSmartCardSerialNumber* –kentän arvot. Mikäli kortille luodaan uudet avaimet OBKG-tekniikalla tai varmennepari uusitaan nimenmuutoksen vuoksi, uudet varmenteet laitetaan hakemistoon vanhojen tilalle. Vanha varmennepari säilytetään arkistossa.

3.2.4 Nimiepäselvyyksien ratkaiseminen

Mikäli nimiepäselvyyksiä ilmenee, on varmentajan järjestelmiin päätynyt virheellistä tietoa ja varmentajan on ryhdyttävä välittömiin korjaustoimenpiteisiin. Nimiepäselvyyksiä ei tule, koska *eidSmartCardSerialNumber* on kortin sarjanumero eli ICCID, joka on määritelmän mukaan yksikäsitteinen.

3.2.5 Hakijan tunnistaminen ja liittymän ominaisuudet

Varmennetta hakeva henkilö tunnistetaan sähköisessä asiointikanavassa vahvalla sähköisellä tunnistusmenetelmällä käyttäen hakijan henkilökohtaisia pankkitunnuksia. Kasvokkainrekisteröinnissä henkilö tunnistetaan hyödyntäen jotakin seuraavista henkilöllisyyden osoittavista asiakirjoista:

1. suomalainen passi
2. suomalainen henkilökortti
3. suomalaisen poliisin myöntämä, Suomessa vakinaisesti asuvan ulkomaalaisen henkilökortti
4. 1.10.1990 jälkeen myönnetty suomalainen ajokortti.

Kaikkien henkilöllisyyden osoittavien asiakirjojen tulee olla hyväkuntoisia, voimassa olevia ja rekisteröintiä suorittavan henkilön täytyy kyetä kohtuudella tunnistamaan varmennetta hakeva henkilö asiakirjassa olevasta valokuvas-

ta. Käytettäessä ajokorttia henkilöllisyyden osoittavana asiakirjana, tulee ajokortin olla alun perin suomalaisen viranomaisen myöntämä - suomalaiseksi vaihdettua, alun perin ulkomailla myönnettyä ajokorttia ei hyväksytä.

Hakijalla on oltava oikeus maksullisten lisäpalveluiden käyttöönottoon, mikä siis vaatii liittymän omistajan luvan. Liittymän tiedoista tarkistetaan, että liittymäkortti on PKI-kykyinen.

On huomattava, että varmenteen hakijan sähköinen asiointitunnus haetaan Väestörekisterikeskuksen väestötietojärjestelmästä hänen henkilötunnuksensa perusteella. Kyselyyn saatava vastaus pitää sisällään hakijan henkilötunnuksen, joka voi olla eri kuin se, millä tietoja kysyttiin. Tämä tarkoittaa, että hakijan henkilötunnus on muuttunut ja näin ollen se tulee ensi tilassa korjata myös asiakastietojärjestelmiin.

3.2.6 Salaisen avaimen hallussapidon osoittaminen

Kortin liikkeellelaskija tallettaa liittymäkorttia vastaavan julkisen avaimen hakemistoonsa varmenteen rekisteröintiä varten. Itsepalvelurekisteröinnissä varmennehakemusta ei allekirjoiteta, eli *Proof of posession* -viestiä ei tässä muodossa käytetä. Sen sijaan varmenteen hakija pakotetaan asettamaan yksityisten avaintensa tunnusluvut, millä varmistetaan, että vain tunnistettu liittymän haltija kykenee käyttämään liittymäkortilla olevia yksityisiä avaimia. Lisäksi oikean päätelaitteen hallussapito tarkistetaan kertakäyttöisellä SMS-salasanalla, joka varmenteen hakijan tulee vastaanottaa puhelimeensa ja kopioida sieltä rekisteröintikäyttöliittymään.

Myymälärekisteröinnissä oikean päätelaitteen halussapito tarkistetaan samalla tavalla, kuin itsepalvelussa, minkä jälkeen hakijalle annetaan uusi liittymäkortti ja sen mukana yksityisten avainten tunnusluvut tulostettuna liittymäkortin kantaosalle suojattuina raaputuspinnan alla, jotta hakija voisi itse todeta luottamuksellisuuden säilyneen kuljetuksen ajan. Mikäli hakijalla kuitenkin on entuudestaan hallussaan sopiva SIM-kortti , ei sen vaihtaminen ole välttämätöntä, koska tällöin hakija ohjataan käymään PIN-reset -palvelussa asettamassa haluamansa tunnusluvun avaimilleen.

3.3 Varmenteen avainparin ja varmenteen uusiminen

3.3.1 Varmenteen uusiminen nimenmuutoksen vuoksi

Varmenne tulee uusia, kun varmenteen elinkaari on siinä pisteessä, että varmenteen voimassaoloaikaa on jäljellä enintään yksi kuukausi tai varmenteen omistajan nimi on muuttunut. Varmenteen uusiminen tapahtuu siten, että vanha suljetaan, SIM-kortti vaihdetaan ja luodaan uusi varmenne luvun 3.2 mukaisesti. Tässä yhteydessä nimi tarkistetaan Väestötietojärjestelmästä normaaliin tapaan.

3.3.2 Varmenteen uusiminen varmenteen vanhenemisen vuoksi

Varmenteen uusiminen vanhenemisen vuoksi johtaa uuden varmenteen rekisteröintiin uudella avainmateriaalilla. Liittymäkortilla luotavien avainten

tapauksessa uudet avaimet ja uusi varmenne luodaan aivan kuin alkuperäisen varmenteen luomisen yhteydessä. Ero on se, että henkilön tunnistaminen sähköisessä kanavassa tehdään asiointivarmenteella TUPAS-tunnusten sijaan.

Tehdasvalmisteisten avainten tapauksessa rekisteröidään uusi varmenne käyttäen alkuperäistä varmennetta henkilön tunnistamiseen sähköisessä asiointikanavassa. Tunnistamisen jälkeen tehdään normaali henkilötietokysely VTJ:stä. Uusien avainten hallinta varmistetaan pyytämällä käyttäjää kopioimaan uuden liittymäkorttinsa ICCID:n (sarjanumeron) viimeiset 6 numeroa.

3.3.3 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. Tällä tavoin voidaan varmenteen tunnistustasoa nostaa ja lyhentää ensitunnistusketjua saattamalla *identificationPathLength*-attribuutin arvo nollaksi. Uusimisen yhteydessä nimi tarkistetaan Väestötietojärjestelmästä samaan tapaan kuin uuden varmenteen rekisteröinnin yhteydessä. Mikäli samassa yhteydessä halutaan uudelle varmenteelle täysi viiden vuoden elinikä, on avainmateriaali uusittava ja toimitaan kohdan 3.3.2 mukaisesti. Elisa ei uusi varmennetta vanhalla avainmateriaalilla, vaan avainmateriaali vaihdetaan aina, minkä jälkeen luodaan täysin uusi varmenne.

3.4 Avainparin uusiminen mitätöinnin jälkeen

Avainparin ja varmenteen uusiminen mitätöinnin jälkeen edellyttää uuden varmennehakemuksen tekemistä. Avainparin ja varmenteiden myönnössä noudatetaan tällöin samaa prosessia kuin haettaessa varmennetta ensimmäistä kertaa.

3.5 Varmenteen sulkupyynnön tekeminen

Varmenne voidaan sulkea tilapäisesti tai kokonaan ennen varmenteen voimassaoloajan päättymistä. Varmenteen sulkupyynnön tekee ensisijaisesti varmenteen omistaja. Sulkupyynnön voi omistajan sijasta tehdä myös viranomainen, varmentaja tai varmenteen omistajan valtuuttama henkilö. Tässä luvussa näitä vaihtoehtoja ei erotella vaan kaikki tapaukset kuvataan varmenteen omistajan kannalta.

Jos varmenteen käytön mahdollistavan mobiilipäätelaitteen epäillään tilapäisesti kadonneen, varmenteen omistajan täytyy välittömästi pyytää varmenteiden tilapäistä sulkemista.

Kun on epäilys tai tieto, että varmenteen julkista avainta vastaava yksityinen avain on kadonnut, paljastunut tai otettu luvattomasti käyttöön, tai yksityisen avaimen käytön mahdollistava tunnusluku on kadonnut tai paljastunut, tulee varmenteen omistajan tehdä varmenteen sulkupyyntö.

Varmenne asetetaan pääsääntöisesti ensin tilapäiseen sulkuun (*certificateHold*) odottamaan varmenteen omistajan pyyntöä varmenteen täydelli-

sestä sulkemisesta. Varmenne suljetaan pysyvästi mikäli henkilön varmenteeseen liittyvä puhelinliittymä suljetaan pysyvästi, liittymän haltija vaihtuu tai liittymäkortti vaihdetaan.

Varmenteen sulkupyyntö tehdään henkilökohtaisesti puhelimitse Elisa Oyj:n asiakaspalveluun 01019 0240, joka palvelee 24 tuntia vuorokaudessa seitsemänä päivänä viikossa. Sulkupalvelun on tehtävä parhaansa tunnistaakseen sulkupyynnön tekijän, mutta epäselvissäkin tilanteissa on varmenne suljettava, ellei ole ilmeistä, että kyseessä on ilkivaltainen sulkupyyntö. Luvussa 2.1.3 on käsitelty yksityiskohtaisemmin tapoja, joilla sulkupyynnön tekijä voidaan tunnistaa.

Varmenteen sulkupyyntö, sulkupyynnön tekijän tiedot, sulkupyynnön tekoaika ja -tapa ja sulkupyyntöä seuranneet varmentajan toimenpiteet kirjataan ylös.

3.6 Varmenteen tilapäisen sulun purkaminen

Jos varmenne on ollut tilapäisesti suljettuna, voidaan se palauttaa takaisin käyttöön. Varmenteen palautuksen käyttöön tilapäisestä sulusta suorittaa Rekisteröijä.

Varmenteen palautuspyyntö tehdään henkilökohtaisesti rekisteröintipisteessä. Palautuspyynnön tekijä tunnistetaan samoin menetelmin kuin ensitunnistamisen yhteydessä.

Varmenteen palautuspyyntö, palautuspyynnön tekijän tiedot, palautuspyynnön tekoaika ja tapa ja palautuspyyntöä seuranneet varmentajan toimenpiteet kirjataan ylös.

4 Toiminnalliset vaatimukset

4.1 Varmenteen hakeminen

Varmentajan ja varmenteen hakijan välillä luodaan sopimus asiointivarmennepalvelun lisäämisestä liittymään. Sopimus voidaan luoda sähköisessä asiointikanavassa esimerkiksi OmaElisassa tai kasvokkain Elisan asiointipisteessä. Sähköisessä asiointikanavassa sopimus syntyy, kun liittymän haltija tilaa itselleen asiointivarmenteen. Tilauksen jälkeen asiakkaalle toimitetaan tarvittaessa sopiva liittymäkortti.

Henkilö, joka hakee varmennetta, ilmaisee varmennetta hakiessaan, että hän hyväksyy varmennepolitiikan ja varmenteen hallintaan ja käyttöön liittyvät ehdot.

Varmennehakemus tehdään kortin liikkeellelaskijan verkkopalvelussa, kun uusi SIM-kortti on saatu haltuun ja kytketty verkkoon. Varmenteen hakija kirjautuu verkkopalveluun ja siirtyy rekisteröimään varmennetta. Tämä kuvataan luvussa 4.2 . Kasvokkain asioitaessa erillistä hakemusta ei tarvitse tehdä, mutta hakijan tiedot kirjataan järjestelmään.

Riippumatta asiointitavasta hakijan viralliset henkilötiedot eli koko nimi ja sähköinen asiointitunnus haetaan Väestötietojärjestelmästä hakijan henkilötunnuksen perusteella. Sähköisessä asiointikanavassa henkilön on täytynyt tunnistautua vahvalla säköisellä tunnistautumismenetelmällä, jolla saadaan hakijan henkilötunnus. Asioitaessa kasvokkain henkilö tunnistetaan varmennepolitiikan ja luvun 2.1.2 mukaisella tavalla.

4.2 Varmenteen myöntäminen

Mikäli varmenteen myöntämisen ehdot toteutuvat, varmentajan valtuuttama rekisteröintioperaattori tai kortin liikkeellelaskijan järjestelmä välittää varmennepyynnön varmentajan varmennejärjestelmään, joka myöntää varmenteen ja julkaisee sen hakemistopalveluun hakijan luvalla.

Asiointivarmenteen myöntäminen edellyttää sopivaa liittymätyppiä ja -korttia.

4.3 Varmenteen hyväksyminen

Varmenteen omistajan katsotaan hyväksyneen varmenteen, kun varmenteessa sijaitsevaa julkista avainta vastaavaa yksityistä avainta on käytetty.

4.4 Varmenteen mitätöinti ja varmenteen voimassaolon keskeyttäminen

4.4.1 Olosuhteet varmenteen mitätöimiseksi

Varmenne täytyy sulkea kokonaan seuraavissa olosuhteissa:

- Varmenteen julkista avainta vastaavan yksityisen avaimen tiedetään tai epäillään olevan kadonnut, varastettu tai paljastunut
- Yksityisen avaimen sisältävä mobiilipäätelaitteen liittymäkortti on kadonnut
- Varmenteen omistaja irtisanoo liittymäsopimuksen
- Liittymäkortti vaihdetaan tai liittymän haltija vaihtuu
- Varmenteen omistaja tai sulkemiseen oikeutettu taho näin pyytää
- Varmenteen omistaja on kuollut.

Varmentajalla on oikeus sulkea varmenne seuraavissa olosuhteissa:

- Varmenteen julkista avainta vastaavaa yksityistä avainta tiedetään tai epäillään käytettävän luvattomasti
- Varmennetta ei käytetä varmenteen käyttötarkoituksen, varmennepolitiikan tai varmennuskäytännön mukaisesti
- Varmenteen omistaja rikkoo varmentajan kanssa tehtyä sopimusta tai lakia
- Varmenteen tiedot ovat epätarkkoja tai muuttuneet
- Varmenteen sulkemiseen tai jäädyttämiseen on olemassa jokin muu erityinen syy.

4.4.2 Oikeus varmenteen mitätöintiin

Varmenteen mitätöintipyynnön tekijää koskevat samat säännöt kuin varmenteen sulkupyynnön tekijää luvussa 3.5 .

Varmentaja voi suorittaa varmentajan varmenteen mitätöinnin, mikäli sillä on perusteltu epäilys että kappaleen 4.4.1 mukaiset olosuhteet varmenteen sulkemiseksi ovat täyttyneet.

4.4.3 Mitätöintipyyntö ja sen käsittely

Varmenteen mitätöintipyyntö on sama kuin varmenteen sulkupyyntö, joka on kuvattu luvussa 3.5 .

Varmenteen mitätöintipyynnöt, mitätöinnin perusteet, mitätöinnin pyytäjän tunnistustapa ja pyyntöä seuranneet varmentajan toimenpiteet kirjataan ylös ja arkistoidaan.

4.4.4 Olosuhteet varmenteen sulkemiseksi tilapäisesti

Varmenne suljetaan pääsääntöisesti ensin tilapäisesti.

4.4.5 Oikeus varmenteen tilapäiseen sulkemiseen

Oikeus varmenteen tilapäiseen sulkemiseen määritellään kappaleen 4.4.2 mukaisesti.

4.4.6 Menettelytapa varmenteen sulkemiseksi tilapäisesti

Varmenteen tilapäistä sulkua varten käytetään samoja menettelytapoja kuin varmenteen sulkemisessa.

4.4.7 Tilapäisesti suljetun varmenteen avaaminen

Mikäli varmenne on tilapäisesti suljettu, voidaan se palauttaa käyttöön perustellusta syystä. Tämä tapahtuma on kuvattu luvussa 3.6 .

4.4.8 Sulkulistan julkaisutiheys

Varmennepolitiikassa on määritelty sulkulistan julkaisutiheys. Varmentaja julkaisee täydellisen sulkulistan tunnin välein. Sulkulista on voimassa 24 tuntia sulkulistan julkaisemisesta. Lisäksi varmentaja julkaisee ositetun sulkulistan luvun 7.2.3 mukaisesti.

4.4.9 Sulkulistan tarkistusvaatimukset

Sulkulistan tarkistusvaatimukset on selostettu varmennepolitiikassa.

4.5 Turvatarkastusmenettelyt

Turvallisuuden tarkastuksen menettelytavat sitovat kaikkia laitteisto- ja järjestelmäkokonaisuuksia, jotka ovat yhteydessä varmenteiden tilaus- ja myöntöprosessiin pois lukien varmentajan avainten säilytysmoduuli (nShield Connect units).

Juurivarmentajan varmennepalveluiden tietoturvallisuuden hallintajärjestelmä, joka kattaa kyseisen palvelun kehitys-, tuotanto- ja asiakaspalveluprosessin, on sertifioitu ISO/IEC 27001:2005 tietoturvallisuusstandardin mukaisesti.

4.5.1 Tallennettavat tapahtumat

Varmentaja tallentaa turvallisuustarkistuksia varten varmennejärjestelmän lokitiedot, käyttöoikeuksien hallintaan liittyvät tapahtumat, tiedot laitteiden ja ohjelmistojen asennuksista ja päivityksistä, tiedot varmistuksista ja niiden palauttamisesta, tiedot järjestelmän sulkemisesta ja käynnistämisestä sekä hyökkäystun-

nistimien ja pääsynvalvonnan lokitiedot. Myös lokitietojen tyhjentämisajankohdat kirjataan.

4.5.2 Haavoittuvuusarvio

Elisa Oyj on arvioinut ja dokumentoinut hallinnoimiensa varmennepalvelukomponenttien ja ympäristönsä haavoittuvuudet ja minimoinut riskit sekä tehnyt erillisen riskienhallintasuunnitelman sisältäen toipumissuunnitelman (Turvakuvaus).

4.6 Varmennetietojen arkistointi

Varmennetoimintaan liittyvistä henkilörekistereistä tehdään Henkilötietolain (523/99) 10 §:n mukainen rekisteriseloste.

4.6.1 Arkistoitava aineisto

Elisa Oyj:n varmennetoimintaan liittyvä aineisto arkistoidaan mukaan luettuna:

- Varmennetilaukset ja tilauksiin liittyvät Elisa Oyj:n ja rekisteröijän, asiakkaan tai hakemistopalvelun väliset viestit
- Kopio tunnistusasiakirjasta digitoituna sähköiseen muotoon tai sitä vastaavasta vahvan sähköisen tunnistuspalvelun vastausviestistä
- Varmenne- tai muun tilauksen allekirjoitetut hyväksynnät. Allekirjoituksesta ilmenee hyväksynnästä vastuussa oleva henkilö
- Varmennepalvelusopimukset
- Varmenteen sulkupyynnöt ja kaikki sulkupyynnön alkuunpanijan ja/tai loppukäyttäjän viestit
- Varmentajan julkaisemat varmenteiden sulkemiseen liittyvät tiedot
- Turvakuvaukset
- Tarkastuspöytäkirjat mukaan luettuna varmennusperiaatteiden ja soveltamisohjeen vuosittaisen tarkastuksen pöytäkirjat
- Voimassaolevat ja edelliset varmennepolitiikat ja niihin liittyvät soveltamisohjeet.

Digitaalisesti allekirjoitetusta asiakirjasta tulee käydä ilmi asiakirjasta vastuussa oleva henkilö mahdollista myöhempää tarkistusta varten.

4.6.2 Asiakirjojen säilytysaika

Asiakirjat säilytetään 5 vuotta.

4.6.3 Arkistojen suojaus

Allekirjoitetut asiakirjat, tiedostot ja muut mediat säilytetään paloturvallisessa, kulunvalvonnalla varustetussa tilassa, johon vain valtuutetuilla henkilöillä on pääsy.

4.6.4 Arkistotietojen varmistusmenettelyt

Arkistoitavat asiakirjat ja tiedostot varmuuskopioidaan. Alkuperäiset asiakirjat talletetaan kassakaappiin. Varmuuskopiot varastoidaan turvallisiin tiloihin fyysisesti erilleen alkuperäisistä.

4.6.5 Arkistoissa olevien tietojen saaminen ja tarkistaminen

- Elisa Oyj toimii tietosuojavaatimusten ja tietosuojalainsäädännön mukaisesti.
- Yksityiset, henkilökohtaiset asiakirjat voidaan luovuttaa osallisena olevien kokonaisuuksien tai heidän valtuutettujen edustajiensa pyynnöstä.
- Elisa Oyj voi periä käsittelymaksun arkistoissa olevien tietojen toimittamisesta.
- Elisa Oyj varmistaa arkistojen käytettävyyden ja luettavuuden koko säilytysjakson ajan.
- Elisa Oyj tiedottaa loppukäyttäjille tiedotussuunnitelman mukaisesti varmennepalvelutoimintansa keskeyttämisestä tai lakkauttamisesta.

4.7 Varmentajan avainten uusiminen

Juurivarmentajan ja tämän varmentamien alivarmentajien avainparit ja varmenteet uusitaan loppukäyttäjien varmenteiden pisimmän voimassaoloajan mittaista ajanjaksoa ennen varmentajien varmenteiden vanhenemista. Sekä uudet että vanhat juurivarmentajan ja tämän varmentamien alivarmentajien varmenteet ovat saatavilla juurivarmentajan hakemistopalvelusta.

Varmentajien varmenteiden vaihdon yhteydessä luodaan juuri- ja alivarmentajille uusi varmentajan varmennepalvelun yksilöivä yhteisnimi.

Uuden juurivarmentajan avainparin ja varmenteen tullessa käyttöön myönnetään kaikki uudet alivarmentajien varmenteet tätä varmennetta käyttäen. Vanhaa juurivarmentajan yksityistä avainta ja varmennetta käytetään tämän jälkeen varmentajien varmenteiden sulkulistan allekirjoitukseen ja allekirjoituksen todentamiseen.

Juurivarmentajan avainparin ja varmenteen vaihdon yhteydessä luodaan ja julkaistaan hakemistoon seuraavat varmenteet:

- Juurivarmentajan uudella yksityisellä avaimella itse allekirjoitettu juurivarmenne.
- Juurivarmentajan uudella yksityisellä avaimella allekirjoitettu varmenne juurivarmentajan vanhalle julkiselle avaimelle.
- Juurivarmentajan vanhalla yksityisellä avaimella allekirjoitettu varmenne juurivarmentajan uudelle julkiselle avaimelle.

4.8 Ongelma- ja katastrofitilanteista selviäminen

Varmentaja vastaa, että ongelma- ja katastrofitilanteissa varmennetoiminta palautetaan normaaliksi niin nopeasti kuin mahdollista. Varmennepalvelusta on olemassa jatkuvuus- ja valmiussuunnitelma, joka mahdollistaa toiminnan häiriöttömän jatkumisen ja varmentajan järjestelmien toipumisen normaali- ja poikkeusoloissa.

4.8.1 Laitteisto- ja ohjelmistovaurioista tai tiedon korruptoitumisesta toipuminen

Varmennejärjestelmän kriittiset komponentit on kahdennettu. Laitteisto- tai ohjelmistovaurion sattuessa tuotanto siirtyy automaattisesti toimimaan kahdennuksen toiseen laiteosapuoleen. Rikkoutuneen laite- tai ohjelmistokomponentin korjaus suoritetaan valmiussuunnitelman mukaisesti.

Tiedon korruptoituessa palautetaan viimeisimmät eheät tiedot varmennejärjestelmään varmistusnauhoilta. Koko varmennejärjestelmä varmistetaan kerran kuukaudessa ja kriittinen tuotantodata varmistetaan kerran vuorokaudessa. Varmistukset testataan säännöllisesti.

Laajemman varmennejärjestelmän laitteisto- tai ohjelmistorikon tapahtuessa aiheutuu tuotantoon katkos siksi aikaa, kunnes tuotanto kyetään palauttamaan tilapäiseen tuotantojärjestelmään.

4.8.2 Varmentajan yksityisen avaimen paljastuminen

Varmentajan yksityisen avaimen paljastuessa noudatetaan tästä määriteltyä toipumissuunnitelmaa.

Seuraavat toimenpiteet tulee suorittaa varmentajan yksityisen avaimen paljastuessa:

- Varmentaja tiedottaa yksityisen avaimen paljastumisesta ja sen edellyttämistä toimenpiteistä asiakkaitaan välittömästi yksityisen avaimen paljastumisen tultua esiin.
- Luottamus varmentajan varmenteeseen sekä varmentajan avainparin käyttö loppuu. Varmentajan varmenne ja varmentajan var-

mentamat varmenteet suljetaan.

- Toiminnan jatkamiseksi luodaan varmentajalle uudet avainparit ja varmenteet. Loppukäyttäjien varmenteet on rekisteröitävä uudelleen normaalein menettelyin.

4.8.3 Luonnon- tai muun katastrofin jälkeinen toiminnan toipuminen

Varmennejärjestelmä on sijoitettu turvallisiin tiloihin näiden maantieteellisen sijainnin riskit huomioon ottaen. Varmennejärjestelmä on suojattu vesivahinkojen, tulipalon ja tunkeutumisen varalta ja sen komponenttien sijoittelu on hajautettu useampaan tilaan.

Mahdollisen luonnon- tai muun katastrofin tapahtuessa toimitaan tästä määritellyn toipumissuunnitelman mukaan.

4.9 Varmentajan toiminnan lakkauttaminen

Varmentajan lakkauttaminen on tilanne, jossa varmenneorganisaatio lakkautetaan pysyvästi. Varmentajan lakkauttamiseksi ei katsota tilannetta, jossa varmentajan palvelut siirtyvät organisaatiolta toiselle tai jossa varmennepalvelut siirretään vanhalta varmentajan avainparilta uudelle avainparille

Mikäli Elisa Oyj lakkauttaa varmennepalvelutoimintansa, suoritetaan seuraavat toimenpiteet:

- Tilanteesta tiedotetaan osapuolia, joiden kanssa Elisa Oyj on solminut varmennepalveluja koskevia sopimuksia sekä muita sopimusosapuolia, vähintään kuusi (6) kuukautta ennen lakkauttamista.

- Varmentaja asettaa julkisesti saataville tietoa varmennepalvelutoiminnan lakkauttamisesta vähintään kolme (3) kuukautta ennen lakkauttamista.

- Varmentaja mitätöi kaikki myöntämänsä varmenteet ja julkaisee yhden tai useamman sulkulistan, jonka voimassaolo ei lakkaa ennen kuin viimeisen varmentajan myöntämän varmenteen voimassaolo on päättynyt.

- Varmentajan varmenne mitätöidään juurivarmentajan toimesta ja julkaistaan juurivarmentajan sulkulistalla.

- Varmentaja lakkauttaa varmenneorganisaation toiminnot.

5 Turvatoimenpiteet

5.1 Fyysinen turvallisuus

Varmentajien yksityiset avaimet, joilla allekirjoitetaan varmenteet ja sulkulistat, on suojattu avainmoduuleihin (FIPS 140-2 standardin mukaisesti) siten, ettei niitä voi paljastaa loogisella tai fyysisellä murtautumisella.

Varmennepalvelun laitteistot ja tilat on sijoitettu ympäristöön, jonka riskit on analysoitu ja minimoitu. Tilat ja laitteistot tarkastetaan vähintään kerran vuorokaudessa.

Varmentajalla on arkistotila, jossa säilytetään varmennejärjestelmään liittyvää dokumentaatiota, varmuuskopioita ja muita tallennusvälineitä siten, että luvattomalla henkilöllä ei ole mahdollisuutta päästä käsiksi tallennettuun tietoon ja että tietojen varastaminen, luvaton muuttaminen ja tuhoaminen on mahdotonta.

Arkistotila sijaitsee erillään varmennepalvelun laitetiloista.

5.1.1 Toimitilan sijainti ja rakenne

Varmennepalvelun tekninen ympäristö ja muut varmennepalveluun liittyvät laitteistot ja tilat on sijoitettu ympäristöön, jonka riskit on analysoitu ja minimoitu.

5.1.2 Fyysinen pääsynvalvonta

Varmennejärjestelmän laitteistot ja tilat on sijoitettu vartioinnilla, kamera- ja kulunvalvonnalla ja hälytysjärjestelmillä suojattuun ympäristöön.

Pääsy tiloihin, joissa varmennejärjestelmä, sen hallintatyöasemat ja testijärjestelmä sijaitsevat on rajoitettu kulunvalvonnalla vain varmennejärjestelmän hallinnointiin valtuutetuille henkilöille. Henkilöt, joilla ei ole pysyvää kulkuoikeutta tiloihin, saavat liikkua tiloissa vain varmennejärjestelmän hallinnoinnista vastaavien henkilöiden seurassa.

Varmenteiden rekisteröinti- ja sulkupisteiden tulee sijaita tiloissa, joihin pääsyä voidaan valvoa ja jotka on suojattu hälytysjärjestelmällä ja vartioinnilla.

5.1.3 Sähkönsyöttö ja ilmastointi

Varmennejärjestelmän virransyöttö on varmistettu katkeamattoman virransyöttöjärjestelmän ja varavoimalaitteiston avulla.

Varmennejärjestelmä on sijoitettu tilaan, joka on varustettu ilmastointijärjestelmällä. Tilan lämpötilaa ja kosteutta monitoroidaan jatkuvasti.

5.1.4 Paloturvallisuus

Konesalitilat, joissa varmennejärjestelmän komponentit sijaitsevat, on varustettu tarpeellisin ilmaisimin ja automaattisin sammutusjärjestelmin. Muut tilat ovat automaattisen paloilmoitusjärjestelmän piirissä sekä varustettu käsisammuttimin.

5.1.5 Vesivahingoilta suojautuminen

Konesalitilat, joissa varmennejärjestelmän komponentit sijaitsevat, on varustettu kosteusilmaisimin.

5.1.6 Tietomateriaalin säilytys

Varmennepalveluun liittyvät dokumentit, arkistoitavat materiaalit ja varmuuskopiot säilytetään maantieteellisesti eri paikassa kuin varmennejärjestelmän laitteistot. Materiaalin säilytys on toteutettu siten, että materiaali on suojattu tulipalon ja vesivahinkojen varalta sekä häviämiseltä ja luvattomalta käytöltä. Pääsy tiloihin joissa materiaalia säilytetään, on kulkuoikeuksin rajattu vain asianosaisille henkilöille.

5.1.7 Jätteiden hävittäminen

Varmennepalveluun liittyvä luottamuksellinen materiaali hävitetään tuhoamalla.

5.2 Toiminnalliset kontrollit

5.2.1 Luotetut työtehtävät

Asiointivarmentajan ja juurivarmentajan työtehtävät on jaettu siten, että väärinkäytösmahdollisuudet on minimoitu ja mahdolliset väärinkäytökset voidaan jäljittää järjestelmän turvakontrollien ja lokien perusteella. Juurivarmentajan luotetut työtehtävät ovat:

- Rekisteröijä (Registration Operator): Varmentajan varmenteiden ja avainparien luontiin ja jakeluun liittyvien toimenpiteiden suorittaminen.

- Varmenteiden mitätöijä (Revocation Operator): Varmentajan varmenteiden mitätöintipyyntöjen vastaanotto ja varmenteiden mitätöintien tekeminen.

- Järjestelmän pääkäyttäjä (System Administrator): Varmennejärjestelmän operointi, varmistaminen, valvonta ja järjestelmän muutostyöt sekä varmentajien avainten, varmenteiden ja proseduurien luonti ja hallinta.

- Järjestelmän omistaja (System Owner): Järjestelmän käyttöoikeuksien tarkastus ja hyväksyntä, varmentajien varmenteiden teon hyväksyntä ja prosessointi ja kokonaisvastuu järjestelmän turvallisuudesta ja toiminnasta.

- Turvallisuusauditoija (Security Auditor): Järjestelmän turvallisuuskäytäntöjen toteutuksen ja hallinnan tarkastus.

Asiointivarmentajan luotettuja tehtäviä ovat:

- Rekisteröijä: Loppukäyttäjien varmenteiden rekisteröinti rekisteröintijärjestelmää käyttäen

- Varmenteiden mitätöijä: Loppukäyttäjien varmenteiden mitätöintipyyntöjen vastaanotto ja täytäntöönpano

- Päärekisteröijä: Rekisteröintijärjestelmän tunnushallinta

Luotetuissa työtehtävissä toimivat henkilöt sitoutuvat noudattamaan tätä varmennuskäytäntöä ja siihen liittyvää varmennepolitiikkaa.

5.2.2 Tehtäviin vaadittavien henkilöiden lukumäärät

Seuraavat tehtävät vaativat yhden henkilön paikallaoloa:

- Loppukäyttäjien varmenteiden rekisteröinti
- Loppukäyttäjien varmenteiden sulku
- Rekisteröintijärjestelmän rekisteröijien ja mitätöijien oikeuksien määrittely ja sulkeminen.

Seuraavat tehtävät vaativat vähintään kahden henkilön yhtäaikaista läsnäoloa:

- Varmentajien avainparien, varmenteiden ja varmenneproseduurien luonti ja sulku

- Varmentajien avainparien, varmenteiden ja varmenneproseduurien palautus varmuuskopioilta

- Varmennejärjestelmän rekisteröijien, mitätöijien ja pääkäyttäjien oikeuksien määrittely ja sulkeminen.

Varmentajien avainten, varmenteiden ja varmenneproseduurien ja luotetuissa työtehtävissä toimivien henkilöiden oikeuksien luonti vaativat varmennejärjestelmän omistajan hyväksynnän. Varmennejärjestelmän muutostoimenpiteet vaativat järjestelmän omistajan hyväksynnän.

5.2.3 Luotettujen toimenhaltijoiden tunnistaminen ja todentaminen

Juurivarmentajan luotetuissa työtehtävissä toimivilla henkilöillä on hallussaan tunnusluvulla suojattu henkilökohtainen toimikortti, joka sisältää varmennejärjestelmän käyttöön oikeuttavat avainparit ja varmenteet. Henkilön oikeus käyttää varmennejärjestelmää tai muita varmentamiseen liittyviä järjestelmiä määritellään ja todetaan toimikortin sisältämien avainparien ja varmenteiden avulla. Sähköiset dokumentit allekirjoitetaan toimikorttia käyttäen.

Asiointivarmentajan luotetuissa tehtävissä toimivat henkilöt tunnistautuvat rekisteröintijärjestelmiin käyttäjätunnus-salasana -parilla tai toimikortilla.

5.3 Henkilöturvallisuus

5.3.1 Pätevyysvaatimukset

Henkilön, joka toimii varmentajan luotetussa työtehtävässä, tulee olla lojaali, huolellinen, luotettava ja rehellinen sekä ymmärtää turvallisuuden merkitys jokapäiväisessä työssä.

Henkilöillä on työtehtävien edellyttämä ammatillinen pätevyys ja mahdollisuus lisäkoulutukseen tarvittaessa. Asiointivarmenteen myöntöoikeus edellyttää vaaditun koulutuksen hyväksyttyä suorittamista.

Elisa Oyj:n työntekijät ovat ammattitaitoisen työhönottotarkastuksen läpikäyneitä ja sitoutuneet noudattamaan Elisa Oyj:n salassapitomääräyksiä ja yritysturvallisuusperiaatteita.

5.3.2 Taustatietojen tarkistusmenettely

Varmentaja valitsee henkilökuntansa erityisesti luotettavuutta silmälläpitäen.

Varmennejärjestelmän pääkäyttäjän, prosessikehittäjän tai RA:n tehtävissä työskentelevien henkilöiden tausta on tarkistettu. Henkilöt, joiden taustatiedot eivät ole moitteettomat, eivät voi toimia näissä tehtävissä.

Varmentaja voi tarkastaa myös muissa luotetuissa työtehtävissä toimivien taustat harkintansa mukaan. Varmentaja voi uusia taustojen tarkistuksen harkintansa mukaan.

Elisa Oyj edellyttää alihankkijoidensa tarkistavan henkilöstönsä luotettavuuden vastaavin menettelyin kuin Elisa Oyj:n henkilöstön.

5.3.3 Seuraukset luvattomista toimenpiteistä

Mikäli varmentaja huomaa varmennetoimintaan liittyviä väärinkäytöksiä, väärinkäytöksiin syyllistyneen henkilön kaikki oikeudet varmennejärjestelmään ja –ohjelmistoihin lakkautetaan. Tämän jälkeen suoritetaan tutkinta väärinkäytösten aiheuttamista haitoista ja pyritään normalisoimaan tilanne mahdollisimman pian.

Alihankkijoiden väärinkäytöstilanteissa noudatetaan alihankintasopimuksessa sovittuja menettelyjä.

5.3.4 Henkilöstölle tarjottava dokumentaatio

Varmentaja tarjoaa luotetuissa työtehtävissä toimiville henkilöille ohjeet käytännöistä ja ohjelmien käytöstä työtehtävän mukaan.

Varmentaja antaa luotetuissa työtehtävissä toimiville henkilöille pääsyoikeuden varmennetoimintaan liittyviin sähköisiin dokumentteihin. Ohjeistusta on myös saatavilla työtehtävien suorittamiseen käytettyjen ohjelmistojen käytön yhteydessä.

6 Tekniset turvatoimet

Juurivarmentajan noudattamat tekniset turvatoimet on kerrottu Elisa Oyj:n juurivarmentajan varmennepolitiikassa ja –käytännössä.

6.1 Varmentajan avainparin luominen ja käyttöönotto

6.1.1 Avainparin luominen

Loppukäyttäjien avainten luonti tapahtuu valvotuissa olosuhteissa ja fyysisesti turvallisessa ympäristössä korttitehtaalla. Kaikissa tapauksissa varmentaja vastaa avainparin luontiin liittyvien ehtojen täyttymistä.

Varmentajan alihankkijana toimiva korttivalmistaja huolehtii turvallisesta avainparien generoinnista mobiilipäätelaitteiden liittymäkorteille. Liittymäkorteilla sijaitsevat avaimet ovat yksilöllisiä, ja ne luodaan joko kortin sisäisin menetelmin tai erillisessä järjestelmässä. Avaimet luodaan siten, että avainparien yksityiset avaimet tallennetaan ainoastaan korteille, eikä niistä jää kopioita kortin ulkopuolelle. Liittymäkortille luodaan ainakin kolme avainparia, joista kahta käytetään asiointivarmenteeseen ja yksi jää vapaaksi käytettäväksi.

6.1.2 Yksityisen avaimen toimittaminen loppukäyttäjälle

Korttitoimittaja toimittaa avainparit sisältävät liittymäkortit ja korttien tunnusluvut varmentajalle varmentajan määrittelemän turvallisen prosessin mukaisesti. Varmentaja toimittaa liittymäkortin ja korttiin liittyvät tunnusluvut varmenteen hakijalle kortin mukana. Varmenteen sähköisessä rekisteröinnissä varmenteen hakija pakotetaan asettamaan tunnusluvut haluamikseen ja näin varmistetaan, että tunnusluvut ovat vain oikealla henkilöllä tiedossa.

6.1.3 Julkisen avaimen toimittaminen varmentajalle

Korttitoimittaja luo avainparit liittymäkorteille ja toimittaa julkiset avaimet ja niitä vastaavat liittymäkorttien tiedot salatussa tiedostossa varmentajalle mobiilivarmenteiden rekisteröintisovellukseen syötettäväksi. Mobiilivarmenteen rekisteröintiprosessissa varmenteen hakijan julkinen avain toimitetaan rekisteröintisovelluksesta sähköisesti allekirjoitettuna varmennejärjestelmään.

6.1.4 Avainten pituudet ja algoritmi

Varmenteiden avainparit ovat varmennepolitiikan mukaisia vähintään 1024–bittisiä RSA–avaimia.

6.1.5 Avainten käyttöikä

Mobiilipäätelaitteen liittymäkortilla sijaitsevien avainten enimmäiskäyttöikä on viisi (5) vuotta. Avainpituudesta johtuen voidaan avainten käytölle asettaa takaraja, joka on riippumaton käyttöiästä.

6.1.6 Avainten käyttötarkoitus

Varmenteen *keyUsage* –kenttä määrittelee varmenteisiin liittyvien julkisten avainten ja näitä vastaavien yksityisten avainten käyttötarkoitukset.

Avainten käyttötarkoitukset ovat:

Tunnistusavainpari:
- Varmenteen omistajan tunnistaminen
- Sähköisessä muodossa olevan tiedon salaus

Allekirjoitusavainpari:
- Sähköisessä muodossa olevan tiedon eheyden ja kiistämättömyyden todentaminen sekä suostumus

6.1.7 Varmentajan julkisen avaimen toimittaminen käyttäjille

Varmentajan julkinen avain on varmentajan varmenteessa, joka on saatavilla varmentajan www-palvelun ja hakemistopalvelun kautta.

Asiointivarmentajan hakemistopalvelun osoite varmentajan varmenteelle on ldap://ldap.elisa.fi/cn=Elisa%20Mobile-Id%20CA%20Rev-1,ou=ca,o=elisa,c=fi?caCertificate;binary. Asiointivarmentajan voimassa oleva varmenne on saatavilla myös www-selaimella osoitteesta https://mobile-id.elisa.fi/cps/elisa-mobile-id-ca-rev-1.crt.

6.2 Yksityisen avaimen suojaaminen

6.2.1 Varmenteen omistajan yksityisten avainten suojaaminen

Yksityiset avaimet on tallennettu liittymäkortille, joka on ISO 7816 –standardin sekä ETSI:n TS GSM 11.11 –standardin mukainen. Yksityisten avainten käyttö suojataan tunnusluvuin.

6.2.2 Yksityisten avainten tallettaminen (key escrow)

Loppukäyttäjien yksityisistä avaimista ei talleteta *key escrow* –tyyppistä kopiota.

6.2.3 Yksityisten avainten varmuuskopiointi

Loppukäyttäjien yksityisistä avaimista ei oteta varmuuskopioita.

6.2.4 Yksityisten avainten arkistointi

Yksityisiä avaimia ei arkistoida.

6.2.5 Yksityisen avaimen aktivointi

Loppukäyttäjän yksityinen avain tulee aktivoida tunnusluvulla ennen jokaista käyttökertaa.

6.2.6 Henkilökohtaisen avaimen lukkiutuminen ja avaaminen

Yksityinen avain lukkiutuu, mikäli siihen liittyvä tunnusluku syötetään viisi kertaa peräkkäin väärin. Lukkiutunut avain voidaan palauttaa takaisin käyttöön Elisa Oyj:n Palvelun hallinta -osiossa. Tässä yhteydessä varmenteen omistajan henkilöllisyys todetaan vahvalla sähköisellä tunnistusmenetelmällä.

6.3 Muut avainparin hallintaan liittyvät seikat

6.3.1 Julkisten avainten arkistointi

Julkiset avaimet arkistoidaan varmenteina hakemistopalveluun vähintään varmenteen voimassaolon ajaksi. Varmenteet arkistoidaan varmentajan varmennejärjestelmän tietokantaan vähintään 5 vuoden ajaksi varmenteen voimassaolon päättymisestä.

6.4 Aktivointitieto

6.4.1 Aktivointitiedon luominen ja käyttöönotto

Liittymäkortin valmistaja luo tunnusluvun samalla, kun liittymäkortin avainparit luodaan.

Liittymäkortin valmistaja suojaa aktivointitiedon turvapinnoitteella ja pakkaa liittymäkortin ja aktivointitiedon suojattuun pakkaukseen.

6.4.2 Aktivointitiedon suojaaminen

Yksityisiä avaimia suojaava aktivointitieto tulostetaan suojattuna siten, että tietoa ei voi saada haltuun poistamatta suojausta. Vastaanottaessaan aktivointitiedot tulee varmenteen omistajan varmistua, että aktivointitiedon suojaus on ehjä.

Varmenteen omistajalla on velvollisuus säilyttää saamaansa aktivointitietoa huolellisesti siten, ettei aktivointitieto joudu ulkopuolisen haltuun.

Liittymäkortilla sijaitsevat tunnusluvut on suojattu kortin sisäisin mekanismein siten, että ne eivät ole luettavissa kortilta.

6.5 Tietoteknisten järjestelmien turvatoimenpiteet

Varmentajan järjestelmät on suunniteltu ja toteutettu korkean tietoturvallisuuden mahdollistavien vaatimusten mukaisesti.

- Varmennejärjestelmä tarjoaa pääsynvalvonnan ja jäljitettävyyden jokaisen varmentajan henkilökohtaiseen avaimeen liittyvän toimenpiteen osalta yksilötasolle asti.
- varmentajan järjestelmät ja tietoliikenneyhteydet on eristetty julkisista verkoista.
- Järjestelmien kriittiset osat on suojattu palomuurilla ja suodatuslistojen avulla.
- Tietoliikenteen turvallisuus on varmistettu vahvan salauksen tai yksityisen verkon tietoliikenneyhteyksien avulla.
- Järjestelmän resurssien riittävyyttä ja käyttöä valvotaan jatkuvasti automaattisen valvonnan avulla, joka antaa hälytyksen asetettujen arvojen ylittyessä.
- Varmennejärjestelmän laitteistojen fyysinen turvallisuus on varmistettu sijoittamalla laitteistot erillisiin lukittuihin kulunvalvonnalla varustettuihin tiloihin.
- Turvatehtävissä toimivat henkilöt tunnistetaan varmentajan järjestelmissä toimikortin avulla ja toimenpiteet varmistetaan sähköisellä allekirjoituksella.

Varmenteiden rekisteröijän ja sulkijan työasemat eivät tarvitse erillistä sertifiointia, mutta niiden tulee tukea pääsynvalvontaa, toimikortilla tapahtuvaa käyttäjän tunnistamista ja lokitiedon keräämistä.

6.6 Elinkaaren hallinnan turvatoimenpiteet

6.6.1 Järjestelmäkehityksen turvatoimenpiteet

Järjestelmäkehitys tapahtuu turvallisessa ympäristössä. Järjestelmäkehitystä ei suoriteta tuotantojärjestelmässä, vaan kehitystä varten on varattu palvelimia, jotka on sijoitettu fyysisesti turvallisiin tiloihin ja joiden tietoliikenne on rajattu omaan sisäverkkoon.

Varmennejärjestelmän muutokset suunnitellaan, dokumentoidaan ja testataan huolellisesti, ja ainoastaan dokumentoidut, testatut ja hyväksytyt muutokset viedään hallitusti tuotantojärjestelmään.

6.6.2 Tietoturvallisuuden hallinta

Järjestelmän tietoturvallisuuden hallinnassa noudatetaan Elisa Oyj:n tietoturvallisuus-periaatteita.

Tietoturvallisuuden hallinta perustuu muun muassa:

- työtehtävien ja käyttöoikeuksien tarveperustaiseen jakoon
- turvallisuuden seurantaan
- säännöllisiin turvatarkastuksiin
- teknisiin turvaratkaisuihin ja –menetelmiin
- muutosten hyväksymismenettelyyn

6.7 Tietoliikenneverkon turvatoimenpiteet

Varmennejärjestelmän käyttämät tietoliikenneverkot on erotettu julkisista verkoista palomuurein ja järjestelmien väliset tietoliikenneyhteydet on suojattu salaamalla tai erottamalla tietoliikenneyhteys julkisesta verkosta. Tietoliikenteen salaukseen käytetään vahvaa salausta, vähintään SSL-protokollaa 128-bittisellä avaimella. Verkon kriittiset osat on erotettu julkisesta verkosta useammalla kuin yhdellä palomuurilla.

7 Varmenne ja sulkulistaprofiilit

7.1 Varmenneprofiili

Kaikki varmenteet ovat X.509 v3 -varmenteita [X.509]. Varmenneprofiili asiointivarmenteelle on esitetty varmennepolitiikassa.

7.2 Sulkulistaprofiili

7.2.1 Sulkulistan yleiset ominaisuudet

Elisa Oyj:n Varmennepalveluiden julkaisemat sulkulistat ovat X.509 v2:n [X.509] ja RFC 5280 [RFC5280] mukaisia sulkulistoja. Niiden tietosisältö koostuu seuraavista osista:

- Sulkulistan versionumero (*version*) = *V2*

  Kaikki Elisan varmennejärjestelmän julkaisemat sulkulistat ovat versiota kaksi.

- Sulkulistan allekirjoituksen muodostusalgoritmin tunniste (*signatureAlgorithm* = *signature*) = *sha512WithRSAEncryption*

  Allekirjoituksen muodostusalgoritmin tunniste kertoo mitä algoritmia varmentaja on käyttänyt sulkulistan allekirjoituksessa. Elisan varmennejärjestelmässä käytetään em. algoritmia.

- Sulkulistan allekirjoitus (*signatureValue*)

  Kyseisen sulkulistan allekirjoituksen arvo

- Sulkulistan julkaisijan identiteetin yksilöintitiedot (*issuer*) = sulkulistan julkaisijan varmenteen *Subject*-kentän arvo

  Sulkulistan julkaisija -kenttä yksilöi sulkulistan julkaisijan ja allekirjoittajan.

- Sulkulistan luontiajankohta (*thisUpdate*)

- Seuraavan sulkulistan julkaisuajankohta (*nextUpdate*)

- Lista suljetuista varmenteista (*revokedCertificates*)

  Lista, jolla on yksilöity jokaisesta suljetusta varmenteesta:

  - Varmenteen sarjanumero (*userCertificate*)
  - Sulkuajankohta (*revocationDate*)
  - Mahdolliset sulkutiedon laajennukset (*crlEntryExtensions*)

Sulkutietolaajennukset ovat vapaavalintaisia ja pitävät sisällään:

- Sulkusyyn (*reasonCode*)

  Sulkusyy voi olla esim. määrittelemätön (*unspecified*), avaimen paljastuminen (*keyCompromise*) tai tilapäinen sulku (*certificateHold*).

- Mitättömäksituloajankohta (*invalidityDate*), eli hetki, jolloin epäillään, että varmenteeseen liittyvä yksityinen avain on tullut mitättömäksi. Tämä voi olla aiempi kuin sulkuajankohta, koska sulkuajankohta on hetki, jolloin varmentaja on käsitellyt sulkupyynnön.

- Sulkulistan julkaisijan avaimen tunniste (*authorityKeyIdentifier*)

  Tunniste, jonka avulla voidaan yksilöidä sulkulistan allekirjoitukseen käytetty avainpari. Tunnisteena käytetään varmentajan *subjectKeyIdentifier*-kenttää.

- Sulkulistan sarjanumero (*crlNumber*)

  Monotonisesti kasvava sarjanumero, jolla kaikki sulkulistat voidaan järjestää aikajärjestykseen. Jos täydellinen ja ositettu sulkulista julkaistaan samalla hetkellä, niillä on oltava sama sarjanumero ja sama sulkutietosisältö.

- Sulkulistan tyyppi (*deltaCRLIndicator*)

  Sulkulista voi olla täydellinen (*Complete*) tai ositettu (*delta CRL*). Tämä kriittinen laajennus on läsnä vain ositetussa sulkulistassa ja sen arvo on referenssinä käytettävän täydellisen sulkulistan sarjanumero (*BaseCRLNumber*).

- Ositetun sulkulistan jakelupiste (*Freshest CRL*)

  Täydellisen sulkulistan sisältämä viittaus paikkaan, josta on jatkossa saatavilla täydentäviä ositettuja sulkulistoja.

- Viittaus julkaisijan varmenteeseen (*Authority Information Access*)

  Osoite, josta sulkulistan julkaisijan varmenne on saatavilla (*CA Issuers*) = URI:http://mobile-id.elisa.fi/elisa-mobile-id-ca-rev-1.crt.

7.2.2 Elisa Mobile-Id CA:n julkaisema täydellinen sulkulista

Elisa Mobile-Id CA:n julkaisemalla sulkulistalla suljetaan Elisa Mobile-Id CA:n myöntämiä asiointivarmenteita. Sulkulistan profiili noudattelee edellä kohdassa 7.2.1 määriteltyä profiilia seuraavin lisäyksin ja täsmennyksin:

- Täydellinen sulkulista on voimassa 24 tuntia julkaisuhetkestään eteenpäin.

- Elisa Mobile-Id CA julkaisee uuden täydellisen sulkulista normaalisti tunnin välein.

- Täydellinen sulkulista pitää sisällään viittauksen ositettuun sulkulistaan (*FreshestCRL*) = ldap://ldap.elisa.fi/cn=Elisa%20Mobile-IdD%20CA%20Rev-1,ou=ca,o=elisa,c=fi?deltaRevocationList;binary.

- Täydellinen sulkulista ei sisällä viittausta täydelliseen sulkulistaan (*BaseCRL-Number*).

7.2.3 Elisa Mobile-Id CA:n julkaisema ositettu sulkulista

Elisa Mobile-Id CA:n julkaisemalla ositetulla sulkulistalla täydennetään kohdan 7.2.2 mukaista täydellistä sulkulistaa. Sulkulistan profiili noudattelee edellä kohdassa 7.2.1 määriteltyä profiilia seuraavin lisäyksin ja täsmennyksin:

- Ei sisällä viittausta ositettuun sulkulistaan (*FreshestCRL*)

- Elisa Mobile-Id CA julkaisee uuden päivitetyn sulkulistan, eli ositetun sulkulistan, viiden (5) minuutin välein tai aina sulkiessaan uuden varmenteen. Ositettu sulkulista on voimassa tunnin.

- Uusi ositettu sulkulista julkaistaan aina, kun julkaistaan täydellinen sulkulista, ja se viittaa edelliseen julkaistuun täydelliseen sulkulistaan. Toisin sanoen "aktiivinen" täydellinen sulkulista (*BaseCRLNumber*) on niin pitkään kuin mahdollista askeleen perässä.

7.2.4 Elisa Corporation Root CA:n julkaisema täydellinen sulkulista

Elisa Corporation Root CA:n julkaisemalla sulkulistalla suljetaan Elisa Corporation Root CA:n myöntämiä varmentajan varmenteita. Sulkulistan profiili noudattelee edellä kohdassa 7.2.1 määriteltyä profiilia. Yksityiskohtainen sulkulistaprofiili on esitetty Elisa Oyj Juurivarmentajan varmenteen varmennuskäytännössä.

8 Varmennuskäytännön hallinnointi

8.1 Varmennuskäytännön muutosmenettely

Varmentaja voi muuttaa varmennuskäytäntöä lainsäädännöllisten, toiminnallisten tai toimituksellisten vaatimuksien vuoksi. Muutokset kirjataan ylös varmennuskäytännön versionhallintaan.

Varmentaja voi julkaista varmennuskäytännöstä käännöksiä eri kielelle ilman erillistä ilmoitusta.

8.2 Julkaisu- ja tiedottamiskäytäntö

Varmennuskäytännön ja varmennepolitiikan lisäksi varmentajan toimintaan liittyvät seuraavat dokumentit, jotka eivät ole julkisesti saatavilla:

- varmennejärjestelmän tekninen kuvaus
- varmenneorganisaation työtehtävien prosessikuvaukset ja ohjeet
- varmenneorganisaation sisäisten varmenteiden rekisteröinti- ja hallintaohje
- varmenneprofiilit luotetuissa työtehtävissä käytettävien ja muiden varmennejärjestelmässä tarvittavien varmenteiden osalta
- salassapitomääräykset
- yritysturvallisuusperiaatteet
- muut luottamukselliset dokumentit

Ajantasainen varmennepolitiikka on saatavissa sähköisessä muodossa verkosta osoitteesta http://mobile-id.elisa.fi/cps/ tai Elisa Oyj:ltä pyydettäessä.

8.3 Varmennuskäytännön hyväksymismenettely

Varmennuskäytäntö on varmentajan sisäisin menettelyin hyväksymä.

Viiteluettelo

[Tekninen kuvaus]	ELISA Varmentajana – Tekninen kuvaus, version 0.1, September 2005.
[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 RFC 5280,May 2008. URL http://tools.ietf.org/html/rfc5280.
[RFC3647]	S. Chokhani, W. Ford., R. Sabett, C. Merrill, S. Wu. “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”. IETF RFC 3647, November, 2003. URL http://tools.ietf.org/html/rfc3647
[RFC2560]	M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams. "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP". IETF RFC 2560, June 1999. URL http://tools.ietf.org/html/rfc2560.
[X.509]	ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8:1997, "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework."