

# **PANKKIEN VARMENNEPALVELUN LAITEVARMENNEPERIAATTEET**

Versio 1.0

## MUUTOSLUETTELO

Versiotunnus

Luku-Sivu

Huom.

## HYVÄKSYMINEN

Versiotunnus  
V 1.0

Päivämäärä  
8.6.2005

Hyväksyjä  
CA-Neuvottelukunta

1	Johdanto.....	5
1.1	Yleiskuvaus.....	5
1.2	Dokumentin nimi ja yksilöintitiedot.....	5
1.3	Osapuolet.....	6
1.3.1	Juurivarmentaja.....	6
1.3.2	Laitevarmentaja.....	6
1.3.3	Rekisteröijä.....	6
1.3.4	Varmenteen haltija.....	6
1.3.5	Varmenteeseen luottava osapuoli.....	6
1.3.6	Sulkupalvelun tuottaja.....	7
1.3.7	Hakemistopalvelun tuottaja.....	7
1.4	Varmenteen käyttötarkoitus.....	7
1.5	Varmenneperiaatteita hallinnoiva organisaatio.....	7
1.5.1	Yhteystiedot.....	7
1.5.2	Yhteyshenkilö.....	7
1.6	Määritelmät ja lyhenteet.....	7
2	Tietojen julkaiseminen ja saatavuus.....	8
2.1	Varmentajan tietojen julkaiseminen.....	8
2.2	Julkaisutiheys.....	8
2.3	Tietojen saatavuus.....	8
2.4	Tietovarastot.....	8
3	Hakijan luotettava tunnistaminen.....	8
3.1	Nimeämiskäytäntö.....	8
3.2	Hakijan tunnistaminen.....	9
3.3	Tunnistaminen avainparia uusittaessa.....	9
3.4	Sulkupyynnön tekijän luotettava tunnistaminen.....	9
4	Varmenteen elinkaaren toiminnalliset vaatimukset.....	10
4.1	Varmenteen hakeminen.....	10
4.2	Varmennehakemuksen käsittely.....	10
4.3	Varmenteen myöntäminen.....	10
4.4	Varmenteen ja avainten vastaanottaminen.....	10
4.5	Avainparin ja varmenteen käyttö.....	10
4.6	Avainten uudelleen varmentaminen.....	10
4.7	Varmenteen ja avaimien uusiminen.....	11
4.8	Varmenteen muutoksenhallinta.....	11
4.9	Varmenteen sulkeminen pysyvästi tai väliaikaisesti.....	11
4.10	Sulkulistapalvelu.....	11
4.11	Varmenteen käyttöoikeuden päättyminen.....	11
4.12	Avaimen palautus.....	11
5	Hallinnolliset, fyysiset, toiminnalliset ja henkilöstöturvallisuuteen liittyvät vaatimukset.....	12
5.1	Fyysiseen turvallisuuteen liittyvät järjestelyt.....	12
5.2	Luotetut työtehtävät ja valvontakäytännöt.....	12
5.2.1	Luotetut työtehtävät.....	12
5.2.2	Luotettujen toimenhaltijoiden tunnistaminen ja todentaminen.....	13
5.3	Henkilöturvallisuus.....	13
5.3.1	Pätevyysvaatimukset.....	13
5.3.2	Taustatietojen tarkistusmenettely.....	13
5.4	Lokien käyttö.....	13
5.5	Lokitietojen arkistointi.....	14
5.6	Varmentajan avaimen uusiminen.....	14
5.7	Toiminnan jatkuvuuden hallinta ja poikkeustapauksien käsittely.....	14
5.8	Toiminnan lakkauttaminen.....	14

6	Tekniset turvajärjestelyt.....	14
6.1	Avainparien luominen ja käyttöönotto.....	14
6.1.1	Varmentajan avainpari.....	14
6.1.2	Laitteen avainpari.....	15
6.1.3	Avainten pituudet.....	15
6.1.4	Avainten käyttötarkoitus.....	15
6.1.5	Julkisen avaimen jakelu.....	15
6.1.6	Yksityisen avaimen luovuttaminen.....	15
6.2	Yksityisen avaimen suojaus.....	15
6.3	Muut avainten hallintaan liittyvät seikat.....	16
6.3.1	Julkisten avainten arkistointi.....	16
6.3.2	Julkisten ja yksityisten avainten käyttöaika.....	16
6.4	Aktivointitieto.....	16
6.5	Tietotekniset turvajärjestelyt.....	16
6.6	Varmennejärjestelmän elinkaaren hallinta.....	16
6.6.1	Järjestelmäkehitys.....	16
6.6.2	Tietoturvallisuuden hallinta.....	17
6.7	Tietoliikenneverkon turvajärjestelyt.....	17
6.8	Aikaleima.....	17
7	Varmenne- ja sulkulistaprofiili.....	17
7.1	Varmenneprofiili.....	17
7.2	Sulkulistaprofiili.....	17
8	Auditointi ja tarkistukset.....	17
9	Muut varmennepalveluun liittyvät asiat.....	17
9.1	Maksut.....	17
9.2	Taloudelliset vastuut.....	18
9.3	Tietojen luottamuksellisuus.....	18
9.4	Luottamuksellisten tietojen luovuttaminen.....	18
9.5	Immateriaalioikeudet.....	18
9.6	Vastuu varmenteen tiedoista.....	18
9.7	Vastuuvapaus.....	18
9.8	Vastuusrajoitukset.....	19
9.9	Vahingonkorvaus.....	19
9.10	Varmenneperiaatteiden voimassaolo.....	19
9.11	Osapuolten tiedonvaihto.....	19
9.12	Varmenneperiaatteiden hallinnointi.....	19
9.13	Erimielisyyksien ratkaiseminen.....	19
9.14	Sovellettavat lait.....	19
9.15	Ylivoimainen este.....	20
9.16	Muut ehdot.....	20
LIITE 1	KÄYTETYT KÄSITTEET.....	21
LIITE 2	LYHENNELUETTELO.....	24

## 1 Johdanto

Suomen Pankkiyhdistyksen CA-Neuvottelukunta ("Neuvottelukunta") on laatinut tämän säännösten, jota noudatetaan myönnettäessä varmenteita maksupääteljärjestelmän käyttöön. Tätä säännöstöä kutsutaan Pankkien Varmennepalvelun laitevarmenneperiaatteiksi, jäljempänä Varmenneperiaatteiksi.

Varmenneperiaatteet määrittelevät toimintaan liittyvät vastuuorganisaatiot, niiden roolit ja vastuut. Lisäksi Varmenneperiaatteet määrittelevät fyysiset, toiminnalliset, henkilöstöön liittyvät ja tekniset turvavaatimukset.

Näihin Varmenneperiaatteisiin liittyvät rekisteröijäkohtaiset Varmennekäytännöt, jotka kuvaavat, miten kukin rekisteröijä toteuttaa tämän dokumentin vaatimukset.

Varmenneperiaatteet ja Varmennekäytäntö sisältävät vaatimuksia, jotka koskevat varmentajan, rekisteröijän, varmenteen haltijan ja varmenteeseen luottavan osapuolen velvoitteita sekä lainsäädäntöön ja mahdollisten erimielisyyksien ratkaisuun liittyviä kysymyksiä.

Nämä Varmenneperiaatteet on laadittu RFC 3647:n mukaiseksi.

### 1.1 Yleiskuvaus

Pankkien Varmennepalvelun toiminnat ovat varmenteiden luominen, hakemisto- ja sulkupalveluiden tuottaminen sekä varmennehakemusten rekisteröinti.

Varmenneperiaatteiden mukaan myönnettyihin varmenteisiin pätee seuraava:

- Varmentaja noudattaa toiminnassaan Varmenneperiaatteita ja sen mukaiseksi laadittua omaa Varmennekäytäntöään
- Varmenteen haltijasta rekisteröidyt tiedot ovat varmenteessa tässä dokumentissa kuvatussa muodossa
- Varmenteen kohteen yksityisten avainten käyttöä suojaavat tunnusluvut on toimitettu ainoastaan varmenteen haltijalle.
- Varmenteen luontiin liittyvä Varmentajan yksityinen avain on talletettu turvallisesti.
- Varmenteet ja ajantasainen sulkuinformaatio ovat saatavissa Varmentajan hakemistopalvelusta.

### 1.2 Dokumentin nimi ja yksilöintitiedot

Varmenneperiaatteiden nimi on: "Pankkien Varmennepalvelun Laitevarmenneperiaatteet".

Tämän dokumentin OID- tunniste on 1.2.246.546.1.1.1.1

Varmenneperiaatteet ovat saatavilla osoitteesta <http://www.fba-ca-committee.fi>.

### **1.3 Osapuolet**

Varmennehierarkia on monitasoinen. Järjestelmän osapuolia ovat Juurivarmentaja, operatiiviset varmentajat, rekisteröijät, varmenteen haltijat, varmenteeseen luottavat tahot sekä hakemisto- ja sulkupalvelun tuottajat.

#### **1.3.1 Juurivarmentaja**

Neuvottelukunta on Juurivarmentaja, joka on varmennehierarkian ylin taso. Juurivarmentaja varmentaa operatiiviset varmentajat, kuten laitevarmentajan, joka myöntää varmenteet pankkipalveluihin liittyvien tietoliikennelaitteiden käyttöön.

#### **1.3.2 Laitevarmentaja**

Laitevarmentaja (jäljempänä Varmentaja) on yksi järjestelmään liittyvistä operatiivisista varmentajista. Se myöntää laitevarmenteet näiden Varmenneperiaatteiden mukaisesti. Varmentaja huolehtii sulk- ja hakemistopalvelun tarjoamisesta.

#### **1.3.3 Rekisteröijä**

Rekisteröijinä toimivat järjestelmään liittyneet pankit ja muut tahot, jotka Neuvottelukunta on tähän valtuuttanut. Rekisteröijä noudattaa Varmentajan Varmenneperiaatteita ja Varmennekäytäntöä.

Rekisteröijä tunnistaa varmenteen hakijan ja tarkistaa Varmennehakemuksen tietojen oikeellisuuden sekä tekee varmennepyynnön Varmentajalle.

Rekisteröijä toimii rekisteröijänä omien maksupääteasiakkaidensa maksupäätalveluun liittyville laitteille ja reitityspalveluille.

#### **1.3.4 Varmenteen haltija**

Varmenteen haltija on taho, jolle Varmentaja on myöntänyt laitevarmenteen.

Laitevarmenne voidaan myöntää osapuolelle, jolla on voimassaoleva maksupäätösopimus rekisteröijänä toimivan pankin kanssa, reitityspalvelusopimus Neuvottelukunnan tai sen valtuuttaman tahon kanssa. Laitevarmenne voidaan myöntää myös pankin maksupäätalveluun liittyvälle tietoliikennelaitteelle.

#### **1.3.5 Varmenteeseen luottava osapuoli**

Varmenteeseen luottava osapuoli on taho, joka luottaa varmenteen tietoihin ja käyttää varmennettä tietoliikenneyhteyden suojaamiseen.

Varmenteeseen luottavan osapuolen on tarkastettava, että luotetun osapuolen varmenne on oikeellinen ja voimassa.

### 1.3.6 Sulkupalvelun tuottaja

Varmenteiden sulkupalvelu sulkee varmenteet, jotka varmenteen Rekisteröijä ilmoittaa suljetta-  
vaksi. Suljetut varmenteet toimitetaan sulkulistalle.

### 1.3.7 Hakemistopalvelun tuottaja

Hakemistopalvelussa on saatavilla kaikki Varmentajan myöntämät varmenteet, Varmentajalle  
itselleen myönnetyt varmenteet sekä sulkulista.

Hakemisto on osoitteessa ldap://ldap.fba-ca-committee.fi.

## 1.4 Varmenteen käyttötarkoitus

Varmennetta käytetään maksupäätteen tietoliikenneyhteyden osapuolten todentamiseen sekä  
salakirjoitetun tietoliikenneyhteyden muodostamiseen.

Varmennetta voidaan käyttää myös tietoliikenneyhteyden kautta välitettävien sanomien suo-  
jaamiseen.

## 1.5 Varmenneperiaatteita hallinnoiva organisaatio

Neuvottelukunta on hyväksynyt nämä Varmenneperiaatteet, vastaa niiden hallinnoinnista, yllä-  
pidosta. Rekisteröijäkohtaiset Varmennekäytännöt noudattavat näitä Varmenneperiaatteita..

### 1.5.1 Yhteystiedot

Suomen Pankkiyhdistys  
CA-Neuvottelukunta  
PL 1009  
00101 Helsinki

Puhelin +358 9 4056 120  
Telekopio: +358 9 4056 1291  
S-posti: [ca-neuvottelukunta@pankkiyhdistys.fi](mailto:ca-neuvottelukunta@pankkiyhdistys.fi)

### 1.5.2 Yhteyshenkilö

Suomen Pankkiyhdistys  
CA-Neuvottelukunnan sihteeri

Puhelin: +358 9 4056 120  
Telekopio: +358 9 4056 1291  
S-posti: [ca-neuvottelukunta@pankkiyhdistys.fi](mailto:ca-neuvottelukunta@pankkiyhdistys.fi)

## 1.6 Määritelmät ja lyhenteet

Dokumentissa käytetyt määritelmät ja lyhenteet on esitetty liitteissä 1 ja 2.

## 2 Tietojen julkaiseminen ja saatavuus

### 2.1 Varmentajan tietojen julkaiseminen

Nämä Varmentajan toimintaa kuvaavat Varmenneperiaatteet sekä muut varmenteiden tuottamiseen liittyvät julkiset dokumentit ovat saatavissa osoitteessa [www.fba-ca-committee.fi](http://www.fba-ca-committee.fi). Mahdollisista muutoksista tai katkoista palvelussa tiedotetaan samassa osoitteessa.

Varmentajan myöntämät varmenteet ja sulkulistat ovat noudettavissa osoitteessa ldap.fba-ca-committee.fi.

### 2.2 Julkaisutiheys

Varmenne tallennetaan hakemistoon sen luonnin yhteydessä ja varmenteen sulkutieto sulkulistalle varmenteen sulkemisen yhteydessä. Sulkulista julkaistaan tunnin välein ja se on voimassa kolme vuorokautta.

Juurivarmentajan sulkulistan julkaisutiheys on 31 vuorokautta ja se on voimassa 93 vuorokautta.

### 2.3 Tietojen saatavuus

Sulkulistatiedot ovat julkisia.

Hakemistossa olevat varmenteet ovat vain rekisteröijien saatavilla.

### 2.4 Tietovarastot

Varmentajan palveluun liittyvät julkiset dokumentit ja muut tiedot ovat saatavilla osoitteessa [www.fba-ca-committee.fi](http://www.fba-ca-committee.fi). Varmennejärjestelmän luottamukselliset tiedot on tallennettu varmentajan omaan, luottamukselliseen tietovarastoon.

## 3 Hakijan luotettava tunnistaminen

Rekisteröijän täytyy tunnistaa Varmenteen hakijan henkilöllisyys luotettavasti. Pankkitoimintaa koskevien lakien ja asetusten mukaan asiakas on tunnistettava aina tilinkäyttövälineitä ja niiden tunnuslukuja luovutettaessa sekä sopimusasiakirjoja allekirjoitettaessa.

Rekisteröijän tulee noudattaa näitä vaatimuksia Varmenteen hakijan tunnistamisen yhteydessä.

### 3.1 Nimeämiskäytäntö

Laitevarmenteen yksilöintitietokenttien arvot muodostetaan seuraavasti:

Maatunnus (country, C)	= FI
Organisaation nimi (organisationName, O)	= Asiakkaan nimi
Organisaatioyksikön nimi (organisationalUnitName, OU)	= Asiakkaan yksikkö
Laitenumero (serialNumber, SN)	= LLLYYYYYYYYYYYYNNNM
Yhteisnimi (commonName, CN)	= LLLYYYYYYYYYYYYNNNM

Laitenumero rakentuu neljästä osasta:

- rekisteröijän liittymätunnus (LLL, kolme (3) numeroa, etunollatäyttö)
- hakijan maksupäätepalvelusopimuksen sopimustunnus (YYYYYYYYYYYY, 12 merkkiä)
- varmenteen yksilöivä tunnus (NNN, 3 numeroa, etunollatäyttö)
- laitetyypin yksilöivä tunnus (M, 1 numero)

Yhteisnimi rakentuu neljästä osasta:

- rekisteröijän liittymätunnus (LLL, kolme (3) numeroa, etunollatäyttö)
- hakijan maksupäätepalvelusopimuksen sopimustunnus (YYYYYYYYYYYY, 12 merkkiä)
- varmenteen yksilöivä tunnus (NNN, 3 numeroa, etunollatäyttö)
- laitetyypin yksilöivä tunnus (M, 1 numero)

Yhteisnimi (commonName, CN) on varmennekohtaisesti yksikäsitteinen.

### **3.2 Hakijan tunnistaminen**

Varmenteen hakijan tunnistamisessa noudatetaan pankkien asiakkaan tunnistamiseen liittyviä ohjeita ja viranomaismääräyksiä.

Suomen Pankkiyhdistyksen ylläpitämä ohje asiakastunnistamiseen hyväksytyistä tunnistusasia-kirjoista on järjestelmään liittyneiden rekisteröijien saatavilla.

Sähköisissä hakemuksissa asiakas tunnistetaan Neuvottelukunnan hyväksymillä tunnisteilla.

### **3.3 Tunnistaminen avainparia uusittaessa**

Avainparin uusimisessa noudatetaan samoja asiakkaan tunnistuskäytäntöjä kuin uuden varmenteen myöntämisessä.

### **3.4 Sulkupyynnön tekijän luotettava tunnistaminen**

Sulkupyynnön Sulkupalveluun saa tehdä se Rekisteröijä, jonka myöntämästä varmenteesta on kysymys. Sulkupyynnön tekijä tunnistetaan operaattorivarmenteella.

Varmenteen sulkemista Rekisteröijältä voi pyytää:

- varmenteen haltija
- varmennehakemuksen tehnyt tilikonttori
- katevarmennuskyselyjä vastaanottava taho, joita ovat Luottokunta ja järjestelmään liittyneet pankit.

Varmenteen sulkemista pyytävä osapuoli on tunnistettava luotettavasti noudattaen pankkien asiakkaan tunnistamiseen liittyviä ohjeita ja viranomaismääräyksiä.

## **4 Varmenteen elinkaaren toiminnalliset vaatimukset**

### **4.1 Varmenteen hakeminen**

Varmenne voidaan myöntää sille, jolla on voimassaoleva maksupäätepalvelusopimus Rekisteröijän kanssa, reitityspalvelusopimus Neuvottelukunnan kanssa tai on Neuvottelukunnan hyväksymä katevarmennustapahtumien vastaanottaja. Varmenne haetaan Hakijan tilipankista Varmennehakemuksella.

### **4.2 Varmennehakemuksen käsittely**

Varmennehakemus toimitetaan Rekisteröijälle, joka tekee Varmennepyynnön Varmennepalveluun. Samalle Hakijalle voidaan myöntää useita varmenteita, mutta kustakin varmenteesta täytyy olla erillinen varmennehakemus.

Rekisteröijä tarkistaa:

- Varmenteen myöntämisen perusteena olevan sopimuksen voimassaolon
- varmennehakemuksen tietojen oikeellisuuden
- mahdollisen PKCS#10 muotoisen sähköisen varmennepyynnön oikeellisuuden ja tekee siihen mahdollisesti tarvittavat täydennykset ja muutokset
- Hakijan yhteyshenkilön henkilöllisyyden ja valtuudet toimia hakijan edustajana tässä asiassa

### **4.3 Varmenteen myöntäminen**

Varmennepalvelu tunnistaa Rekisteröijän Operaattorivarmenteella.

Varmennepalvelu tarkistaa Varmennepyynnön virheettömyyden ja aitouden, luo tarvittaessa avaimet, luo varmenteen sekä toimittaa varmenteen turvallisesti Rekisteröijälle.

### **4.4 Varmenteen ja avainten vastaanottaminen**

Hakijan rekisteröinnin hoitanut Rekisteröijä ilmoittaa Hakijan yhteyshenkilölle, kun varmenne ja avaimet ovat noudettavissa.

Varmenne luovutetaan kuittausta vastaan Hakijan valtuuttamalle yhteyshenkilölle. Varmenteen luovutuksen yhteydessä vastaanottaja tunnistetaan luotettavasti. Kuittaus ja Hakijan tunnistaminen voidaan hoitaa myös sähköisesti.

Varmenteeseen liittyvä yksityinen avain on suojattu PIN-tunnuksella. Varmenne ja siihen mahdollisesti liittyvä yksityinen avain toimitetaan Rekisteröijäkohtaisella menettelyllä asiakkaalle.

### **4.5 Avainparin ja varmenteen käyttö**

Varmennetta ja siihen liittyvää yksityistä avainta käytetään maksupäätteen katevarmennukseen tai tapahtumien välitykseen liittyvän tietoliikenteen osapuolten luotettavaan tunnistamiseen, suojatun tietoliikenneyhteyden avaamiseen osapuolten välille sekä viestien suojaamiseen.

### **4.6 Avainten uudelleen varmentaminen**

Avaimia ei oletusarvoisesti uudelleen varmenneta. Uudelleen varmentaminen ei ole mahdollista toimikortilla oleville avaimille eikä varmennepalvelussa luoduille avaimille.

#### **4.7 Varmenteen ja avaimien uusiminen**

Uutta varmennetta voi hakea, kun varmenteen voimassaoloaikaa on jäljellä enintään kuusi kuukautta, varmenne on tuhoutunut tai se on joutunut sulkemaan. Uutta varmennetta varten luodaan aina uudet avaimet.

Varmenteen ja avaimien uusimisessa noudatetaan samoja periaatteita kuin uuden varmenteen hakemisessa.

#### **4.8 Varmenteen muutoksenhallinta**

Varmenteen tietojen muuttaminen vaatii aina varmenteen uusimisen.

#### **4.9 Varmenteen sulkeminen pysyvästi tai väliaikaisesti**

Varmenne suljetaan sulkupyynnön jälkeen väliaikaisesti. Varmenne suljetaan kaksi (2) viikkoa varmenteen väliaikaisen sulkemisen jälkeen lopullisesti, mikäli perusteltua palautustarvetta ei ole ilmennyt.

Varmenne suljetaan, kun sen myöntämisen perusteena oleva sopimus päättyy, varmenne on tuhoutunut tai varmenteeseen liittyvän yksityisen avaimen epäillään joutuneen sivullisen haltuun.

Varmenteen sulkemista voi pyytää Varmenteen haltija, varmenteen rekisteröinyt taho tai katevarmennuskyselyjä vastaanottava taho. Varmenteen sulkemista voidaan pyytää pankkien aukioaikana. Varmenne suljetaan mahdollisimman nopeasti.

Varmenteen sulkee sen myöntänyt Rekisteröijä. Rekisteröijä vahvistaa sulkupyynnön operaattorivarmenteella.

#### **4.10 Sulkulistapalvelu**

Sulkulista on aina varmenteeseen luottavien osapuolien noudettavissa hakemistosta paitsi järjestelmän huoltokatkojen aikana. Huoltokatkoista ilmoitetaan osoitteessa [www.fba-ca-committee.fi](http://www.fba-ca-committee.fi). Sulkulistojen nouto ei vaadi tunnistautumista hakemistopalveluun.

#### **4.11 Varmenteen käyttöoikeuden päättyminen**

Varmenteen käyttöoikeus päättyy, kun sen myöntämisen perusteena oleva sopimus päättyy. Varmenteen sulkee varmenteen myöntänyt Rekisteröijä.

#### **4.12 Avaimen palautus**

Tuhoutuneita avaimia ei voida palauttaa, koska Varmenteeseen liittyviä yksityisiä avaimia ei tallenneta varmentajan tietovarastoihin.

## **5 Hallinnolliset, fyysiset, toiminnalliset ja henkilöstöturvallisuuteen liittyvät vaatimukset**

Neuvottelukunta käyttää teknisiä toimittajia varmennepalvelun tietoteknisten tehtävien hoitamiseen. Neuvottelukunta määrittelee Varmennepalvelun turvallisuuteen ja toimintaan liittyvät vaatimukset toiminnan eri osa-alueilla.

Yksityiskohtainen kuvaus turvallisuuteen liittyvistä järjestelyistä on kunkin Rekisteröijän varmennekäytännössä.

Hallinnollisten, fyysisten, toiminnallisten ja henkilöstöturvallisuuteen liittyvien vaatimusten osalta noudatetaan kunkin osapuolen omia ohjeita.

### **5.1 Fyysiseen turvallisuuteen liittyvät järjestelyt**

Varmennepalvelun järjestelmät tulee sijaita korkean turvatason konesalituloissa, joiden riskit on kartoitettu.

Asiattomien pääsy turvattuihin toimitiloihin on estettävä. Varmennepalvelun toimijoiden laitteistot ja tilat on sijoitettava suojattuun ympäristöön.

Varmennepalvelun tekniset laitteistot ja tilat on oltava keskeytymättömän varavoiman ja ilmastoinnin piirissä.

Varmennepalvelun konesalitilat on varustettava ilmaisimin ja automaattisella sammutusjärjestelmällä. Muut tilat on oltava automaattisen paloilmoitusjärjestelmän piirissä.

Varmennepalvelun kriittiset tilat on varustettava kosteusilmaisimin.

Materiaali on suojattava häviämiseltä ja luvattomalta käytöltä. Hävitettävä ei-julkinen materiaali tehdään luku- ja käyttökelvottomaksi.

Varmennepalvelun varmuuskopiot on säilytettävä eri paikassa kuin varmennepalvelun laitteistot.

### **5.2 Luotetut työtehtävät ja valvontakäytännöt**

#### **5.2.1 Luotetut työtehtävät**

Varmennepalvelun tehtävät on jaettava eri henkilöille siten, että väärinkäytösmahdollisuuksia ei esiintyisi ja että niiden paljastumisriski olisi ilmeinen. Palvelun kriittisille toimintoille on määriteltävä minimimäärä henkilöitä, joiden pitää olla läsnä operaatiota tehtäessä. Tehtäväkuvaus on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Varmennepalvelun luotettuihin työtehtäviin kuuluvat:

- Hakijan Rekisteröinti
- Varmenteiden luonti ja sulku

Varmentajan yksityisen avaimen luominen, aktivointi, varmuuskopiointi ja palauttaminen on suoritettava valvotusti kahden järjestelmän ylläpitotehtäviin oikeutetun henkilön sekä vähintään kahden Neuvottelukunnan nimeämän edustajan läsnä ollessa.

Varmentajan yksityisen avaimen peruuttaminen on mahdollista vain vähintään kahden Neuvottelukunnan nimeämän edustajan ja kahden järjestelmän ylläpitoon oikeutetun henkilön valvon-  
nassa.

Laitevarmenteen rekisteröiminen tai sulkeminen vaatii yhden tehtävään oikeutetun henkilön läsnäolon.

Järjestelmän tekniseen ylläpitoon vaaditaan yhden tehtävään oikeutetun henkilön läsnäolo.

### **5.2.2 Luotettujen toimenhaltijoiden tunnistaminen ja todentaminen**

Varmentajan luotetuissa työtehtävässä toimivalla henkilöllä (Operaattori) on oltava tehtävään oikeuttava henkilövarmenne, joka on toimikortilla ja suojattu PIN-koodilla. Henkilön oikeus käyttää Varmennejärjestelmää tai muita varmentamiseen liittyviä järjestelmiä, todetaan näiden varmenteiden avulla. Työsuhteen päättyessä henkilöltä on poistettava välittömästi kaikki käyttöoikeudet järjestelmiin.

### **5.3 Henkilöturvallisuus**

Tietoturvallisuuden hallinnassa on oltava kirjalliset tietoturvaperiaatteet.

Tuotantojärjestelmän ylläpito on varmistettava riittävillä varahenkilöjärjestelyillä ja päivystys-  
resursseilla.

Uuden työntekijän on allekirjoitettava vaitiolositoumuksen työhönsä liittyvien asioiden osalta. Uuden työntekijän perehdyttämiseen on kuuluttava tietoturvakoulutus.

#### **5.3.1 Pätevyysvaatimukset**

Henkilöllä on oltava työtehtävien edellyttämä ammatillinen pätevyys ja kyky sekä mahdollisuus tarvittavaan lisäkoulutukseen.

Henkilö, joka toimii järjestelmän luotetuissa työtehtävissä, on oltava huolellinen, luotettava ja rehellinen ja hän ymmärtää turvallisuuden merkityksen työssään.

#### **5.3.2 Taustatietojen tarkistusmenettely**

Varmennejärjestelmän tehtävissä työskentelevien henkilöiden taustat on tarkistettava.

### **5.4 Lokien käyttö**

Varmennejärjestelmä on kerättävä tapahtumista lokeja. Käytönaikaisia lokitietoja ovat hakemiston sulkulistan noudot, Varmenteiden päivitykset hakemistoon, kaikki operattorien tekemät toiminnot Varmennepalvelussa. Ylläpidollisista tapahtumista lokeihin koottavia tietoja ovat kaikki palvelun ylläpitäjien tekemät operaatiot palvelun teknisiin laitteisiin.

Lokitiedot täytyy suojata siten, että ne ovat vain käyttöön oikeutettujen henkilöiden nähtävissä.

Lokitietoja saa käyttää vain ylläpitoon, vianselvitykseen tai muuhun perusteltuun käyttötarkoitukseen.

## **5.5 Lokitietojen arkistointi**

Lokitiedot on säilytettävä korkean turvatason tiloissa, joissa on kulunvalvonta. Lokitietojen varmuuskopiot on varastoitava fyysisesti erilliseen tilaan alkuperäisistä tiedoista.

## **5.6 Varmentajan avaimen uusiminen**

Varmentajan uusitun julkisen avaimen toimituksessa on noudatettava samoja periaatteita kuin uuden varmenteen toimituksessa.

Uusittu varmenne on julkaistava kaikkien luottavien tahojen saataville. Voimassa oleva varmenne on oltava noudettavissa osoitteessa [www.fba-ca-committee.fi](http://www.fba-ca-committee.fi)

## **5.7 Toiminnan jatkuvuuden hallinta ja poikkeustapauksien käsittely**

Varmennepalvelusta on oltava jatkuvuussuunnitelma, joka tarkastetaan määräajoin ja päivitetään tarvittaessa. Poikkeustilanteisiin varautuminen on kuvattava Varmennekäytännössä.

Varmentaja ilmoittaa Varmennekäytännössä ne toimenpiteet, joihin varmenteeseen luottavan osapuolen on ryhdyttävä, mikäli Varmentajan yksityinen avain on paljastunut tai tullut muutoin käyttökelttomaksi.

## **5.8 Toiminnan lakkauttaminen**

Varmennepalvelun toiminnan lopettamisesta päättää Neuvottelukunta. Toiminnan lopettamisesta on tiedotettava kunkin Rekisteröijän ja Varmennepalvelun verkkosivuilla. Rekisteröijän on ilmoitettava Varmennepalvelun lopettamisesta lisäksi kullekin Varmenteen haltijalle erikseen.

Kun joku Rekisteröijä irtautuu palvelusta ja lopettaa näiden Varmenneperiaatteiden mukaisen toiminnan, asiasta on tiedotettava sekä Varmennepalvelun että kyseisen Rekisteröijän verkkosivuilla. Rekisteröijän tulee tiedottaa asiasta lisäksi kullekin rekisteröimälleen varmenteen haltijalle.

Toiminnan päättymisen yhteydessä ko. Rekisteröijän myöntämät varmenteet on suljettava.

# **6 Tekniset turvajärjestelyt**

## **6.1 Avainparien luominen ja käyttöönotto**

### **6.1.1 Varmentajan avainpari**

Varmentajan avainpari on luotava, säilytettävä ja suojattava käytön aikana turvamoduuleilla.

Avainten luonnissa on oltava paikalla vähintään neljä henkilöä, joista ainakin kaksi on Neuvottelukunnan nimeämiä edustajia sekä kaksi varmennepalvelujärjestelmän turvaoperaattoria.

Avainparien luomisesta on tehtävä pöytäkirja, jonka läsnäolijat allekirjoittavat. Pöytäkirja on arkistoitava.

### **6.1.2 Laitteen avainpari**

Laitteen avainparin voi luoda rekisteröintiorganisaatio tai loppukäyttäjä. Avainpari voidaan luoda Rekisteröijän toimesta erillisellä sovelluksella, toimikortin sirulla tai Varmenteen hakijan toimesta hakijan päätelaitteessa, josta julkisen avaimen sisältävä varmennepyyntö toimitetaan rekisteröijälle.

### **6.1.3 Avainten pituudet**

Kaikki avaimet ovat RSA –avaimia. Juurivarmentajan avain on vähintään 2048 bitin pituinen. Tiedostomuotoinen avain on vähintään 2048 bitin pituinen. Toimikortilla oleva avain on vähintään 1024 bitin pituinen.

### **6.1.4 Avainten käyttötarkoitus**

Varmenteessa käyttötarkoituksen määräävä tietokenttä määrittelee varmenteeseen liittyvän avaimen käyttötarkoituksen.

Laitevarmenteeseen liittyvien avainten käyttötarkoitus on laitteen todentaminen ja suojatun tietoliikenneyhteyden muodostaminen varmenteiden avulla todennettujen osapuolten välillä.

### **6.1.5 Julkisen avaimen jakelu**

Varmentajan ja laitevarmenteen julkinen avain on toimitettava varmenteen haltijalle laitevarmenteen mukana. Varmentajan varmenne on oltava myös saatavilla Varmentajan www-palvelun, pankkien verkkosivujen ja hakemistopalvelun kautta.

Laitevarmenne on oltava hakemistopalvelussa rekisteröijien saatavilla.

### **6.1.6 Yksityisen avaimen luovuttaminen**

Yksityiset avaimet on suojattava toimitusprosessin aikana paljastumiselta ulkopuolisille. Ne luovutetaan nimetylle yhteyshenkilölle erillistä tunnistamista vastaan. Salaisten avainten toimitus Varmenteen haltijalle on varmistettava Audit Trail- periaatteella.

Rekisteröintioperaattorin toimesta luodut avainparit voidaan toimittaa joko toimikortilla tai tiedostomuodossa.

## **6.2 Yksityisen avaimen suojaus**

Varmentajan yksityiset avaimet on suojattava Varmennepalvelujärjestelmän turvamoduuleilla.

Toimikortilla olevat avaimet on suojattava PIN-koodilla. Tiedostomuotoiset varmenteet sekä avaimet on salakirjoitettava. Tiedostomuotoiset avaimet voidaan siirtää laitteiden massamuistoihin käytettäväksi. Toimikortilla olevia avaimia käytetään toimikortilla.

Laitteiden, jotka luovat itse avainparinsa, on säilytettävä ne turvallisesti.

### **6.3 Muut avainten hallintaan liittyvät seikat**

#### **6.3.1 Julkisten avainten arkistointi**

Varmentajan on arkistoitava kaikki varmentamansa julkiset avaimet.

#### **6.3.2 Julkisten ja yksityisten avainten käyttöaika**

Varmentajan varmenne on voimassa 10 vuotta ja laitevarmenne kolme (3) vuotta. Varmenteeseen liittyvät avaimet ovat käytettävissä saman ajan. Varmenne voidaan sulkea voimassaoloi- kana.

### **6.4 Aktivointitieto**

Avainten aktivointitiedot, joita voivat olla PIN-koodit tai salasanat, luodaan varmentajan järjes- telmässä ja tallennetaan turvallisesti.

PIN-koodi toimitetaan Varmenteen haltijalle suojatussa kuoressa, jonka sisältöä ei voi saada selville kuorta avaamatta eikä kuorta voi avata huomaamatta, tai sähköisessä muodossa sala- kirjoitettuna .

Rekisteröijän luomien salaisten avainten käyttö on suojattu vähintään nelinumeroisella PIN- koodilla.

Toimikortilla oleva yksityinen avain lukkiutuu, mikäli PIN-koodi syötetään 10 kertaa peräkkäin väärin. Kortin saa auki syöttämällä oikea PUK-koodi. Jos syöttää PUK-koodin 10 kertaa väärin, muuttuu kortti käyttökelvottomaksi. PUK-koodi sisältyy PIN-tulosteeseen.

### **6.5 Tietotekniset turvajärjestelyt**

Varmentajan järjestelmät on toteutettu korkean tietoturvallisuuden vaatimusten mukaisesti.

- Varmennejärjestelmä sisältää pääsynvalvonnan ja tarjoaa jäljitettävyyden jokaisen Varmentajan yksityiseen avaimeen liittyvän toimenpiteen osalta yksilötasolle asti.
- Varmentajan järjestelmät ja tietoliikenneyhteydet on eristetty julkisista verkoista.
- Tietoliikenteen turvallisuus on varmistettu vahvan salauksen tai yksityisen verkon tietolii- kenneyhteyksien avulla.
- Järjestelmien kriittiset osat on suojattu palomuurilla ja suodatuslistojen avulla.

Rekisteröintiyöasemien täytyy tukea pääsynvalvontaa, varmenteella tapahtuvaa käyttäjän tun- nistamista ja lokitiedon keräämistä.

### **6.6 Varmennejärjestelmän elinkaaren hallinta**

#### **6.6.1 Järjestelmäkehitys**

Varmennepalvelun järjestelmäkehitys tapahtuu erillisessä, turvallisessa ympäristössä. Ainoas- taan dokumentoidut, testatut ja hyväksytyt muutokset viedään hallitusti tuotantojärjestelmään.

### **6.6.2 Tietoturvallisuuden hallinta**

Varmennepalvelun tietoturvallisuutta hallitaan Pankkien tietoturvaperiaatteiden ja BS 7799 standardin mukaisesti.

### **6.7 Tietoliikenneverkon turvajärjestelyt**

Varmennejärjestelmän käyttämät tietoliikenneverkot on erotettu julkisista verkoista palomuurin ja järjestelmien väliset tietoliikenneyhteydet on suojattu salaamalla tai erottamalla tietoliikenneyhteys julkisesta verkosta. Tietoliikenteen salaukseen käytetään vahvaa salausta tai SSL-protokollaa vähintään 128-bittisellä avaimella. Verkon kriittiset osat on erotettu julkisesta verkosta palomuuereilla omiksi vyöhykkeikseen.

### **6.8 Aikaleima**

Varmennejärjestelmä käyttää yhtä aikaleimapalvelua. Järjestelmässä ei ole käytössä virallista aikaleimapalvelua.

## **7 Varmenne- ja sulkulistaprofiili**

### **7.1 Varmenneprofiili**

Kaikki varmenteet ovat X.509 v3 standardin mukaisia varmenteita [X.509].

Varmenteiden tietosisällöt on kuvattu dokumentissa Pankkien maksupäätelvelun varmenteen, hakemiston ja sulkulistan kuvaus. Kuvaus on varmenteen haltijoiden saatavilla.

### **7.2 Sulkulistaprofiili**

Varmentajan julkaisemien sulkulistojen tietosisällöt on kuvattu dokumentissa Pankkien maksupäätelvelun varmenteen, hakemiston ja sulkulistan kuvaus.

## **8 Auditointi ja tarkistukset**

Varmentaja tarkastaa teknisen ylläpitäjän toimitilat, laitteet ja toiminnan tarkoituksenmukaisella tavalla. Tarkastuksen tekee Varmentajan nimeämä tarkastaja. Varmentajaa valvova viranomais-omainen voi tarkastaa Varmentajan toiminnan erillisissä määräyksissä kuvatulla tavalla.

Tarkastuksessa verrataan Varmenneperiaatteita, Varmennekäytäntöä ja soveltamisohjeita Varmentajan ja järjestelmän toimintaan. Havaitut poikkeamat kirjataan tarkastusraporttiin ja niihin reagoidaan ja tiedotetaan osapuolten välisten sopimuksien edellyttämällä tavalla.

## **9 Muut varmennepalveluun liittyvät asiat**

### **9.1 Maksut**

Kukin Rekisteröijä päättää itsenäisesti Varmenteidensa luontiin ja käyttöön liittyvistä Varmennepalvelun haltijalta perittävistä maksuista.

## **9.2 Taloudelliset vastuut**

Osapuolilla voi olla erillisiä sopimuksia, joissa keskinäiset taloudelliset vastuut on määritelty.

## **9.3 Tietojen luottamuksellisuus**

Varmenteen haltijaa koskevat tiedot, jotka eivät ole varmenteessa tai joiden luovuttamiseen Varmenteen haltija ei ole antanut suostumustaan, käsitellään luottamuksellisina. Varmentajan Varmenteen sisältämät tiedot, sulkulista sekä Varmenneperiaatteet ja julkaistut määräykset katsotaan julkisiksi tiedoiksi. Sulkulista on kaikkien varmenteeseen luottavien osapuolien saatavilla. Sulkulista sisältää mitätöityjen varmenteiden sarjanumerot.

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

## **9.4 Luottamuksellisten tietojen luovuttaminen**

Varmenteen haltijalla on oikeus saada häntä koskevia tietoja voimassaolevan lainsäädännön mukaisesti.

Luottamuksellisia tietoja voidaan luovuttaa edelleen vain lakien, asetusten, niiden nojalla annettujen määräysten tai muiden viranomaismääräysten perusteella.

## **9.5 Immateriaalioikeudet**

Varmennepalveluihin liittyviin ohjelmistoihin, määräyksiin ja dokumentteihin kohdistuvat omistus- ja immateriaalioikeudet kuuluvat Varmentajalle, Rekisteröijälle, niiden toimittajille tai ali-hankkijoille näiden kanssa laadittujen sopimusten mukaisesti.

Varmenne on Varmentajan omaisuutta ja Varmenteen haltijalla on varmenteen käyttöoikeus näiden varmenneperiaatteiden mukaiseen toimintaan.

## **9.6 Vastuu varmenteen tiedoista**

Varmenteen hakija vastaa antamiensa tietojen oikeellisuudesta.

Rekisteröijä vastaa varmennehakemuksessa olevien tietojen ja varmenteeseen oikeuttavan sopimuksen voimassaolon tarkistamisesta.

Varmentaja vastaa Rekisteröijälle siitä että varmenteen tiedot ovat varmennepyynnön mukaiset.

## **9.7 Vastuuvapaus**

Varmentaja ei vastaa myöntämiensä varmenteiden avulla tehdyistä liiketoimista tai liiketoimien seurauksista.

Varmentaja ei vastaa Varmenteen hakijan mahdollisesti antamien väärin tietojen aiheuttamista seurauksista.

## 9.8 Vastuusrajoitukset

Osapuolet eivät ole näiden Varmenneperiaatteiden mukaan vastuussa toiselle osapuolelle aiheutuvista välillisistä vahingoista, kutensaamatta jääneistä tuotoista tai muuten vaikeasti ennakoitavasta vahingosta. Tämä rajoitus ei koske kuitenkaan sellaisia vahinkoja, jotka osapuoli aiheuttaa toiselle tahallaan tai törkeällä tuottamuksellaan.

## 9.9 Vahingonkorvaus

Vahingonkorvausvelvollisuuksista voidaan sopia osapuolten kesken erikseen.

## 9.10 Varmenneperiaatteiden voimassaolo

Nämä Varmenneperiaatteet ovat voimassa toistaiseksi.

Varmenteet myönnetään viimeisimmän voimassaolevan Varmenneperiaatteiden mukaisesti. Varmenneperiaatteet ovat voimassa niin kauan kuin sen mukaisia varmenteita on voimassa.

## 9.11 Osapuolten tiedonvaihto

Tiedonvaihtoon käytettävistä menetelmistä voidaan sopia osapuolten kesken erikseen.

## 9.12 Varmenneperiaatteiden hallinnointi

Neuvottelukunta hyväksyy Varmenneperiaatteet ja Vvarmennekäytännöt sekä ilmoittaa muutoksista hyvissä ajoin ennen niiden voimaantuloa.

Varmentaja voi muuttaa määräyksiä lainsäädännöllisten tai toiminnallisten vaatimusten vuoksi sisäisin hyväksymismenettelyin. Määritysten muutokset kirjataan Varmenneperiaate- ja Varmennekäytäntöasiakirjoihin.

Varmennekäytännöt hyväksyy Varmentaja. Näiden Varmenneperiaatteiden mukaiset Varmennekäytännöt tunnistetaan kohdan 1.2 mukaisesti.

Varmenneperiaatteet julkaistaan sähköisessä muodossa osoitteessa [www.fba-ca-committee.fi](http://www.fba-ca-committee.fi)

Varmenneperiaatteiden lisäksi Varmentajan toimintaan liittyvät seuraavat dokumentit, jotka eivät ole julkisesti saatavilla:

- Varmennekäytännöt
- varmenneorganisaation työtehtävien prosessikuvaukset ja ohjeet
- varmenneprofiilit luotetuissa työtehtävissä käytettävien ja muiden varmennejärjestelmässä tarvittavien varmenteiden osalta
- muut tarpeelliset luottamukselliset dokumentit

## 9.13 Erimielisyyksien ratkaiseminen

Mahdolliset erimielisyydet ratkaistaan osapuolten keskinäisten sopimuksien mukaan.

## 9.14 Sovellettavat lait

Näihin Varmenneperiaatteisiin ja sen mukaiseen varmennetoimintaan sovelletaan Suomen lakia.

### 9.15 Ylivoimainen este

Varmentaja ei vastaa vahingosta, joka aiheutuu ylivoimaisesta esteestä kuten

- Viranomaisen toimenpiteestä
- sodasta tai sen uhasta, kapinasta tai kansalaislevottomuudesta
- Rekisteröijästä riippumattomasta ja sen toimintaan olennaisesti vaikuttavasta häiriöstä posti- ja puhelinliikenteessä, muussa sähköisessä viestinnässä, tiedonsiirrossa, automaattisessa tietojenkäsittelyssä tai sähkövirran saannissa
- Tulipalon tai muun turman aiheuttamasta keskeytyksestä tai viivästyksestä varmentajan toiminnassa
- Varmentajan toimintaan oleellisesti vaikuttavasta työtaistelutoimesta kuten lakosta, sulusta, boikotista tai saarrosta riippumatta siitä, onko varmentaja siihen osallinen vai ei
- Muusta näihin verrattavasta ylivoimaisesta esteestä tai vastaavasta syystä johtuvasta toiminnan kohtuuttomasta vaikeutumisesta. Varmentaja ilmoittaa niin pian kuin mahdollista siitä kohdanneesta ylivoimaisesta esteestä.

### 9.16 Muut ehdot

Näiden Varmenneperiaatteiden tulkintaan liittyvät asiat ratkaistaan tarvittaessa Neuvottelukunnassa, joka on Varmennepalvelun hallintoelin.

Varmennepalvelun teknistä toimintaa seuraa ja ohjaa CA-Tekninen lautakunta, jolle voi osoittaa palvelun tekniseen toimintaan liittyvät kysymykset ja kehitystoivomukset.

Varmennepalvelun hakemistoissa olevat tiedot on tarkoitettu vain ja ainoastaan varmenteiden aitouden varmistamiseen ja voimassaolon tarkastukseen liittyviä toimenpiteitä varten. Tietoja ei saa käyttää markkinointitarkoituksiin eikä muuhunkaan käyttötarkoituksen vastaiseen toimintaan.

**LIITE 1 KÄYTETYT KÄSITTEET**

<b>Käsite</b>	<b>Englannin-kielinen vastine</b>	<b>Kuvaus</b>
Digitaalinen allekirjoitus	Digital Signature	Sähköinen allekirjoitus, joka on tehty varmenteen haltijan tunnistamiseksi, salatun yhteyden tai viestin salausavaimen välittämiseksi tai asiakirjan/viestin laatijan/lähettäjän yksityisellä avaimella julkisen avaimen menetelmän mukaisesti.
Hakemistopalvelu	Directory Service	Julkisen avaimen järjestelmässä palvelu, joka hallitsee käyttäjien varmenteita ja sulkulistoja sisältäviä hakemistoja.
Hakemuksen hyväksyjä		Henkilö, joka vahvistaa omalla nimikirjoituksellaan varmenteen hakijan organisaatio-, yhteys- ja henkilötiedot.  Hakemuksen hyväksyjä voi myös olla luotettu henkilö
Yksityinen avain	Private Key	Salassa pidettävä osa epäsymmetrisestä avainparista, jota käytetään julkisen avaimen salaustekniikoissa. Yksityistä avainta käytetään tyypillisesti digitaaliseen allekirjoittamiseen tai julkisella avaimella salatun viestin avaamiseen.
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 toimintaympäristö, 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/algorithm	Epäsymmetrinen salausmenetelmä, jossa kullakin salakirjoituksen käyttäjällä on kaksi toisiinsa liittyvää avainta. Toinen avainparin avaimista on julkinen ja 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.

Loppukäyttäjä	End Entity	Henkilö tai laite, joka käyttää varmennetta. Loppukäyttäjä ei kuitenkaan ole varmentaja tai rekisteröijä.
Luotettu henkilö	Trusted person Trusted agent Trusted proxy	Varmentajan luottama ja valtuuttama varmenne- ja korttihakemuksen käsittelijä ja hyväksyjä. Luotetun henkilön vastuulla on tarkistaa varmennehakemuksen tietosisällön oikeellisuus ja todentaa hakijan henkilöllisyys virallista henkilöllisyystodistusta vastaan. Varmentaja tallentaa luotetun henkilön henkilötiedot ja allekirjoitusnäytteen rekisteröintivaiheessa tapahtuvaa hakemuksen tarkistusta varten.
Luottava osapuoli	Relying Party	Sähköisiä palveluja varmenteiden loppukäyttäjille tarjoava taho. Luottava osapuoli toimii luottaen varmenteeseen ja/tai todentaa digitaalisen allekirjoituksen varmenteen avulla. Luottava osapuoli todentaa tapahtuman toisen osapuolen identiteetin varmentajan tunnistusinfrastruktuuria apuna käyttäen. Luottava osapuoli on vahvaa tunnistusta käyttävä henkilö, palvelu tai laite .
Rekisteröijä	Registration Authority (RA)	Varmenteen hakijan tunnistamisesta ja varmennehakemukseen rekisteröitävien tietojen tarkistamisesta vastaava osapuoli. Rekisteröijä toimii varmentajan valtuuttamana varmenneorganisaation osana.
RSA-algoritmi	RSA-algorithm	Epäsymmetrinen salausalgoritmi, jota käytetään epäsymmetrisen avainparin luontiin. Lyhenne tulee algoritmin määrittelijöiden sukunimistä; Rivest, Shamir ja Adleman.
Sulkulista	Certificate Revocation List (CRL)	Julkisen avaimen järjestelmässä käytöstä suljettujen varmenteiden luettelo. Varmentaja julkaisee sulkulistan hakemistopalvelussa.
Sähköinen allekirjoitus	Electronic signature	Tietokoneen luettavassa muodossa oleva henkilön nimikirjoitus tai sen vastine, joka todisteellisesti liittää nimikirjoitukseen liittyvän asiakirjan tai viestin yhteydestä tiettyyn henkilöön.
Todentaminen	Authentication; Verification	Henkilön, organisaation tai laitteen tunnistuksen luotettava 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.
Tunnusluku	Activation Data	Toimintoon liittyvä salainen PIN-koodi tai salasana, jolla toiminto voidaan aktivoida.
Varmennehakemus	Certificate	Varmennehakemus on varmenteen hakijan täyttämä varmenteen hakijan henkilö-, organisaatio ja yh-

CA-Neuvottelukunta

25.05.2005 / V1.0

	application	teystyötiedot sisältävä, hakemuksen hyväksyjän hyväksymä ja tarvittaessa luotetun henkilön allekirjoittama lomake.
Varmennepyyntö	Certificate Request	Varmennepyyntö on varmentajalle lähetettävä, rekisteröijän muodostama, loppukäyttäjän tekemän varmennehakemuksen perusteella tehty digitaalinen varmenteen muodostamis- ja julkaisupyyntö.
Varmenne	Certificate	Varmenne on henkilön salausavaimista, nimitiedoista, sekä muista tiedoista muodostuva kokonaisuus, jonka varmentaja on allekirjoittanut omalla yksityisellä avaimellaan. Varmenteen aitous on todennettävissä tarkistamalla varmentajan digitaalinen allekirjoitus.
Varmenneorganisaatio		Varmenneorganisaation osapuolia ovat varmentaja, rekisteröijä, kortinvalmistaja, hakemisto- ja sulku-listapalvelujen tuottajat sekä muut palvelun tuottajat, joiden palveluja varmentaja käyttää.
Varmennekäytäntö, toimintamalli	Certification Practise Statement (CPS)	Yksityiskohtainen selostus menettelytavoista, joita varmenneorganisaatio käyttää myöntäessään ja hallinnoidessaan varmenteita.
Varmenneperiaatteet	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 ketju, joka ulottuu loppukäyttäjän varmenteesta juurivarmentajan varmenteeseen.
Varmentaja	Certification Authority (CA)	Varmenneorganisaation osapuoli, joka myöntää varmenteita allekirjoittamalla varmennetiedot omalla yksityisellä avaimellaan.
Varmenteen haltija		Loppukäyttäjä, jolle varmentaja on myöntänyt varmenteen ja jolla on laillisesti hallussaan varmenteen sisältämää julkista avainta vastaava yksityinen avain ja sen käyttöön vaadittavat tunnusluvut.
Varmenteen uusiminen	Certificate Re-key	Varmenteen uusimisella tarkoitetaan tilannetta, jossa Varmenteen Haltijalle luodaan uutta varmennetta varten uudet avaimet.
Uudelleen varmentaminen	Certificate Renewal	Uudelleen varmentamisella tarkoitetaan tilannetta, jossa vanhaan varmenteeseen liittyvät avaimet varmennetaan toistamiseen.

**LIITE 2    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	Certification Policy	Varmenneperiaatteet
CPS	Certification Practice Statement	Varmennekäytäntö
CRL	Certification Revocation List	Sulkulista
OID	Object Identifier	Varmenneperiaatteiden tunnistetieto
PIN	Personal Identification Number	Tunnusluku, PIN-koodi
PKI	Public Key Infrastructure	Julkisen avaimen varmennejärjestelmä
PUK	Personal Unblocking Key	PUK-koodi
RA	Registration Authority	Rekisteröijä
RSA		- Rivest, Shamir ja Adleman, salausalgoritmi
X.509		- Varmenteen ja sulkulistan rakenteen sekä määrittelevä standardi