OP RYHMÄ
VARMENNEPOLITIIKKA

LIIKETOIMINTAPALVELUIDEN JUURIVARMENTAJA

OP-Pohjola Root CA

Versio 3.0
Voimassa 6.3.2017 lähtien

OID: 1.3.6.1.4.1.11374.1.1.1.1.3

SISÄLTÖ

JOHDANTO

Varmennepolitiikka (CP, *Certificate Policy*) kuvaa ne menettelyt ja periaatteet, joiden mukaisesti Varmentaja myöntää Varmenteita. Varmennekäytäntö (CPS, *Certification Practice Statement*) puolestaan kuvaa Varmennepolitiikkaa yksityiskohtaisemmin Varmentajan toimintaa.

Varmennepolitiikka määrittelee toimintaan liittyvät vastuuorganisaatiot, niiden roolit ja vastuut. Lisäksi Varmennepolitiikka määrittelee fyysiset, toiminnalliset, henkilöstöön liittyvät ja tekniset turvavaatimukset, joita Varmentaja toiminnassaan noudattaa.

Tunnistetiedot:

OP Ryhmä, Varmennepolitiikka, Liiketoimintapalvelujen Juurivarmentaja

OID: 1.3.6.1.4.1.11374.1.1.1.1.3

1 SOVELTAMISALA

Tämä Varmennepolitiikka koskee OP Ryhmän Varmentajaa (CA, *Certification Authority*), joka on dedikoitu Juurivarmentaja. Toisin sanoen Varmentaja ei ole toisen Juurivarmentajan alainen tai Alivarmentaja. Tämä Varmentaja myöntää Varmenteita ainoastaan toisille Varmentajille.

Tämä politiikka määrittää perusvaatimukset liiketoimintapalveluiden Juurivarmentajan alaisen Julkisen avaimen järjestelmän (*Public Key Infrastructure, PKI*) liiketoiminnallisille ja teknisille ratkaisuille. Lisäksi politiikka kirjaa perusedellytykset PKI-pohjaisten varmenteiden turvalliselle hallinnoinnille ja käytölle. Politiikka pohjautuu vahvasti standardiin *Policy requirements for certification authorities issuing public key certificates (*ETSI TS 102 042 v2.1.1, 2009) ja sen määrittelemään Normalisoituun Varmennepolitiikkaan (NCP, *normalized certificate policy*). Tämä Varmennepolitiikka noudattaa jossain määrin myös luvussa 2 ”Viitteet” listattuja asiakirjoja.

Tämä Varmentaja myöntää Alivarmenteita seuraaville osapuolille:

- OP Ryhmän liiketoimintapalveluita ja ICT-palveluita tuottavat tai hallinnoivat osastot ja toiminnot.

2 VIITTEET

ETSI042	**ETSI TS 102 042** v2.1.1 (2009) Policy requirements for certification authorities issuing public key certificates.
ETSI176-1	**ETSI TS 102 176-1** v2.0.0 (2007) Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
FIPS PUB 140-2	**FIPS PUB 140-2** Security requirements for cryptographic modules
ISO 21188	**ISO 21188** (2006) Public key infrastructure for financial services – Practices and policy framework

3 MÄÄRITELMÄT JA LYHENTEET

3.1 Määritelmät

Alivarmenne (Subordinate CA Certificate): Alivarmentajalle myönnetty Varmenne.

Alivarmentaja (Subordinate CA): Varmentaja, joka ei ole Juurivarmentaja. Alivarmentajan Varmenne on Juurivarmentajan allekirjoittama. (katso Varmentaja ja Juurivarmentaja).

Asiakas (End-entity): Tässä yhteydessä: Taho, joka on tehnyt sopimuksen varmennepalveluiden käytöstä ja on allekirjoittanut Varmenteen tilaajan sopimuksen.

Asiakasvarmenne (End-entity Certificate): Varmentajan Asiakkaalle myöntämä Varmenne. Asiakasvarmennetta voidaan käyttää erilaisiin käyttötarkoituksiin, mutta se ei kuitenkaan koskaan ole Varmentajan Varmenne. Asiakasvarmenteen Avainparista Yksityinen avain on Asiakkaan hallussa.

Audit trail: Katkeamaton kirjausketju. Vaatimus siitä, että lokimerkinnät tehdään siten, että järjestelmässä tehdyt toiminnot voidaan jäljittää tarkasti.

Avaimen käyttö -kenttä (Key usage): Varmenteen tekninen parametri, jolla määritellään Varmenteen sallitut käyttökohteet yleisellä tasolla.

Avainpari (Key Pair): Julkisen avaimen menetelmissä käytetään kahta toisiinsa liittyvää avainta, joista toinen on julkinen ja toinen yksityinen. Yhdessä ne luovat Avainparin. Avainten käyttötarkoitus on määritelty Varmenteessa, jota puolestaan määrittää Varmennepolitiikka.

CDP (CRL Distribution Point): Sulkulistan julkaisupaikka.

HSM-laite (Hardware Security Module): Yksityisten avainten suojaamisen käytetty erikoislaite.

Julkinen avain (Public Key): Julkisen avaimen järjestelmässä epäsymmetrisessä salauksessa käytettävän Avainparin julkinen osa. Julkisella avaimella salattu tieto (esim. RSA-algoritmissa) voidaan purkaa vain Avainparin Yksityisellä avaimella. Kun Julkisen avaimen haltija on tiedossa, sitä vastaavalla Yksityisellä avaimella tehty sähköinen allekirjoitus voidaan tarkistaa. Julkisen avaimen haltija voidaan luotettavasti tunnistaa Varmenteen avulla.

Julkisen avaimen järjestelmä (PKI, Public Key Infrastructure): Teknisten ja hallinnollisten ratkaisujen kokonaisuus, jonka avulla luodaan, hallinnoidaan, jaetaan, käytetään, varastoidaan ja lakkautetaan Julkisen avaimen Varmenteita. Järjestelmä myös asettaa kontrollit ja standardit, joita Varmentajien tulee noudattaa toiminnassaan varmistaakseen sähköisten Varmenteiden yhteensopivuus, tunnistettavuus ja saatavuus. PKI perustuu Julkisen avaimen salausalgoritmiin.

Julkisen avaimen salaus (Public Key Cryptography): Julkisen avaimen salausmenetelmässä on kaksi yhteen liittyvää avainta: Julkinen avain ja Yksityinen avain, jotka yhdessä muodostavat Avainparin. Julkisella avaimella salattu tieto voidaan yleensä purkaa vain Avainparin Yksityisellä avaimella. RSA-algoritmi toimii myös päinvastoin: Yksityisellä avaimella salattu tieto voidaan purkaa vain Julkisella avaimella. Sähköiset allekirjoitukset perustuvat tähän RSA:n ja muutaman muun algoritmin erityisominaisuuteen.

Juurivarmenne (Root Certificate): Juurivarmenne on Juurivarmentajan itselleen myöntämä Varmenne ja varmennehierarkian ylin taso (ns. luottamusankkuri).

Juurivarmentaja (Root Certification Authority; Root CA): Hierarkkisen PKI:n varmenneketjun luotetuin ja ensimmäinen taho. Juurivarmentaja määrää Varmennepolitiikat sekä tekniset ja operatiiviset normit.

Kaksoiskäyttö (Dual Control): Periaate, jonka mukaan tiettyjen toimintojen suorittamiseen on aina osallistuttava vähintään kaksi henkilöä. Tällä estetään yksittäisten henkilöiden väärinkäytökset turvallisuutta vaativissa toiminnoissa.

Key escrow (Vara-avain järjestelmä): Turvamekanismi, jossa salausavain annetaan kolmannen osapuolen säilytettäväksi siten, että se olisi tietyissä olosuhteissa kolmannen osapuolen käytettävissä. Key Escrow liittyy yleensä salauksessa käytettyihin avaimiin, ei allekirjoitus- tai tunnistautumisavaimiin. Jos Key Escrow -menetelmää käytetään PKI:ssa, se täytyy mainita asiaankuuluvassa Varmentajan Varmennepolitiikassa.

Luottava taho (Relying Party): Varmenteen vastaanottava taho, joka luottaa Varmenteen tai siihen pohjautuvan sähköisen allekirjoituksen tietoihin ja käyttää niitä toiminnassaan. Luottavia tahoja ovat esimerkiksi Alivarmentaja, Alivarmentajan Varmenteen haltija (Loppuasiakas), OP Ryhmän Varmenteita käyttävä liiketoimintapalvelu tai muu kolmas osapuoli.

Luottavan tahon sopimus (RPA, Relying Party Agreement): Varmentajan ja Luottavan tahon välinen sopimus, jossa määritellään yleensä molempien osapuolten Varmenteen käyttöä, kuten esimerkiksi sähköisen allekirjoituksen varmistamista, koskevat velvollisuudet ja vastuut.

Pienimpien tarvittavien oikeuksien periaate (Principle of Least Privilege): Käyttöoikeuksien hallintaperiaate, jonka mukaan työntekijälle annetaan vain työtehtävän hoitamisen kannalta välttämättömät käyttöoikeudet. Käyttöoikeudet poistetaan, kun niitä ei enää tarvita.

Rekisteröijä (RA, Registration Authority): Rekisteröijä vastaa yleisesti mm. seuraavista toiminnoista:

1) Tunnistaa (varmistaa henkilöllisyyden) Varmenteen tilaajan (esim. yritys) ja mahdollisen edustajan (esim. yrityksen edustaja).

2) Hyväksyy/hylkää varmennehakemukset.

3) Käynnistää tarvittaessa Varmenteen sulkemis- tai käytönestoprosessin.

4) Voi käsitellä Varmenteen haltijan Varmenteen käytönesto- tai sulkemispyynnön. Hyväksyy tai hylkää Varmenteen uudistamispyynnöt ja pyynnöt saada uusi avain olemassa olevalle Varmenteelle.

Rekisteröijä ei kuitenkaan allekirjoita tai myönnä Varmenteita. Rekisteröijä hoitaa vain Varmentajan sille delegoimat tehtävät.

Seremonia (Ceremony): Varmentajan hyväksymä määrämuotoinen operaatio, jonka suorittamiseen tarvitaan enemmän kuin kaksi läsnä olevaa henkilöä ja jolle valitaan puheenjohtaja.

Yleensä seremonioita käytetään lähinnä avainoperaatioissa, kuten Varmentajan avaimen luonnissa.

Sulkulista (CRL, Certificate Revocation List): Varmenteiden sulkulista (CRL, Certificate Revocation List). Varmentajan sähköisesti allekirjoittama lista, joka sisältää käytöstä poistettujen Varmenteiden sarjanumerot ja käytöstä poiston syykoodin.

Sulkupalvelu (Revocation Service): Varmenteiden sulkemisesta ja jäädyttämisestä (tilapäisestä sulkemisesta) vastaava Varmentajan palvelu.

Sulkutietopalvelu (VA, Validation Authority): Sulkutietopalvelu on Varmenteisiin luottavan tahon käytössä oleva palvelu, jonka avulla Varmenteen voimassaolo voidaan tarkistaa luottamuspäätöksen tekemisen yhteydessä. Käytännössä sulkutietopalvelu tarkoittaa suljettujen Varmenteiden luetteloa.

Sulkutietopalvelu voi tarjota sulkulistatiedostoa eri protokollilla tai kyselypalvelua OCSP-protokollalla.

Sähköinen allekirjoitus (Digital Signature): Matemaattisen laskennan tulos, jolla todennetaan viestin lähettäjän tai asiakirjan allekirjoittajan henkilöllisyys ja sisällön eheys. Toisin sanottuna sähköinen allekirjoitus yhdistää viestin ja lähettäjän. Termillä tarkoitetaan tässä yhteydessä sähköisen allekirjoituksen teknistä menetelmää kaikissa käyttötapauksissa, ei sähköistä allekirjoitusta sellaisena kuin se on määritelty Laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista.

Tilaaja: ks. Varmenteen tilaaja.

Työtehtävien eriyttäminen (Segregation/Separation of Duties): Käytäntö, jossa tiettyyn toimintoon kuuluvat tehtävät on jaettu useammalle henkilölle, jotta kukaan ei pystyisi yksinään väärinkäyttämään prosessia.

Varmenne (Certificate): Tietorakenne, joka liittää Julkisen avaimen sen haltijan tietoihin ja joka on allekirjoitettu Varmenteen myöntäjän (CA) Yksityisellä avaimella.

Varmenneketju (Certificate Chain): Varmenneketjun avulla voidaan, Juurivarmenteeseen luottamalla, tarkistaa ketjun varmenteet sekä tehdä luottamuspäätös loppukäyttäjän varmenteesta.

Varmenneketju alkaa Juurivarmenteesta ja päättyy loppukäyttäjän Varmenteeseen. Varmenneketjussa ylempi Varmentaja vahvistaa alemman Varmentajan allekirjoittamalla tämän Varmenteen. Ylimmän tason Varmentajan (Juurivarmentaja) Varmenne on itseallekirjoitettu.

Varmennekuvaus (PDS, PKI Disclosure Statement): Varmennepolitiikkaa tai Varmennekäytäntöä täydentävä asiakirja, joka sisältää keskeiset tiedot Varmentajan politiikoista ja käytännöistä. Varmennekuvauksessa voidaan nostaa esiin ja korostaa sellaisia tietoja, jotka on yleensä kirjattu yksityiskohtaisesti Varmennepolitiikkaan ja/tai Varmennekäytäntöön. Varmennekuvaus ei korvaa kumpaakaan niistä vaan on niiden tiivistelmä.

Varmennekäytäntö (CPS, Certification Practice Statement): Kuvaus Varmentajan teknisestä ja toiminnallisesta ympäristöstä sekä vastuiden ja velvollisuuksien jakautumisesta osapuolten kesken. Varmennekäytäntö noudattaa Varmennepolitiikassa kuvattuja periaatteita.

Varmennepolitiikka (CP, Certificate Policy): Kuvaus Varmenteiden myöntämisperiaatteista sekä Varmenteisiin luottavien osapuolten vastuista.

Varmenneprofiili (Certificate Profile): Yksityiskohtainen kuvaus Varmenteen teknisistä parametreistä.

Varmennetuotanto: Prosessi, joka tuottaa Varmenteita ja ylläpitää niiden sulkutietoa.

Varmentaja (CA, Certification Authority): Varmenteita myöntävä organisaatio, joka vastaa mm. Varmenteiden tuottamisesta ja laatii toimintaansa kuvaavan Varmennepolitiikan ja Varmennekäytännön.

Varmentajan yksityinen avain (CA Private Key): Yksityinen avain, jota Varmentaja käyttää Varmenteiden myöntämiseen ja julkaisemiensa Sulkulistojen allekirjoittamiseen.

Varmentajan yksityisen avaimen varmuuskopiointi (CA Key Backup): Järjestely, jolla taataan mahdollisuus palauttaa Varmentajan Yksityinen avain, mikäli se tuhoutuu.

Varmenteen avaimen uusiminen (Certificate Rekey): Tilanne, jossa Varmenne uusitaan niin, että Avainpari vaihtuu, mutta Varmenteen tietosisältö säilyy ennallaan. Varmenteen voimassaoloaika voi muuttua.

Varmenteen haltija (Certificate Subject): Taho, joka käyttää Varmenteeseen liittyvää Yksityistä avainta. Varmenteen subject-kenttä yksilöi Varmenteen haltijan. Haltijana voi toimia esimerkiksi tietty palvelu tai liiketoimintaorganisaatio.

Varmenteen tilaaja (Subscriber): Taho, joka hakee Varmennetta ja jonka vastuulla myönnetty Varmenne on. Tilaajayrityksellä on yleensä edustaja, joka hakee Varmennetta yrityksen nimissä.

Varmenteen tilaajan sopimus (Subscriber Agreement, varmentajatoiminnassa): Varmentajan ja Varmenteen tilaajan välinen sopimus, joka määrittelee osapuolten oikeudet ja vastuut Varmenteen myöntämisen ja hallinnoinnin osalta.

Varmenteen jäädyttäminen (Certficate Suspension): Varmenteen tilapäinen asettaminen sulkulistalle.

Varmenteen päivittäminen (Certificate Modification): Tilanne, jossa Varmenteen tietosisältö muuttuu, mutta Avainpari ja viimeinen voimassaoloaika pysyvät samana.

Varmenteen sulkeminen (Certificate Revocation): Varmenteen pysyvä kuolettaminen asettamalla Varmenne Sulkulistalle.

Varmenteen uusiminen (Certificate Renewal): Tilanne, jossa Varmenne uusitaan, mutta Avainpari ja Varmenteen tietosisältö säilyvät ennallaan. Varmenteen voimassaoloaika voi muuttua.

Yksityinen avain (Private Key): Julkisen avaimen järjestelmässä epäsymmetrisessä salauksessa käytettävän Avainparin yksityinen osa. Tämä avain on määritelty yksikäsitteisesti tietylle taholle, joten sillä voidaan esimerkiksi luoda sähköinen allekirjoitus. Yksityisellä avaimella voidaan purkaa tietoa, joka on salattu Avainparin Julkisella avaimella. Lisäksi sitä voidaan käyttää jaetun salaisuuden luomiseen. Tietyissä Julkisen avaimen algoritmeissa Yksityisellä avaimella salatun tiedon voi purkaa Avainparin Julkisella avaimella. Tällainen algoritmi on esimerkiksi tämän Varmentajan käyttämä RSA.

X.509: Yleisimmin käytetty ITU (International Telecommunication Union) -standardi Julkisen avaimen järjestelmälle (PKI). X.509:ssä määritellään Julkisen avaimen Varmenteiden, Sulkulistojen, attribuuttivarmenteiden ja Varmenteiden varmennepolkujen standardiformaatti. X.509 on ITU:n suositus, minkä vuoksi PKI-toimittajat ovat toteuttaneet standardeja eri tavoin.

3.2 Lyhenteet

CA, Certification Authority	Varmentaja
CP, Certificate Policy	Varmennepolitiikka
CPS, Certification Practice Statement	Varmennekäytäntö
CRL, Certificate Revocation List	Sulkulista
ETSI, European Telecommunications Standards Institute	
HSM, Hardware Security Module	Fyysinen turvalaite yksityisten avainten suojaamiseen
ITU, International Telecommunication Union	
NCP, Normalized Certificate Policy	Normalisoitu Varmennepolitiikka
OCSP, Online Certificate Status Protocol	Ajantasainen Varmenteen tilatiedon palauttava palvelu
OID, Object Identifier	Yksilöivä tunnus
PDS, PKI Disclosure Statement	Tiivistelmä Varmennepolitiikasta
PKI, Public Key Infrastructure	Julkisen avaimen järjestelmä
RA, Registration Authority	Rekisteröijä
RSA, Rivest Shamir Adleman	Eräs laajasti käytetty julkisen avaimen salausalgoritmi

3.3 Merkintätapa

Ei käytössä

4 YLEISET TOIMINTAMALLIT

Varmentaja toimii käyttäjien (Luottavat tahot) luotettuna kolmantena osapuolena Varmenteiden luomiseen, myöntämiseen ja käyttämiseen liittyvissä asioissa. Varmentaja merkitään niiden Varmenteiden myöntäjäksi, jotka on allekirjoitettu Varmentajan yksityisellä avaimella. Varmentaja vastaa mahdollisten alihankkijoidensa toiminnasta kuten omastaan.

4.1 Varmentaja

Tämän Juurivarmennepolitiikan Juurivarmentajana toimii OP Osuuskunta (jäljempänä Juurivarmentaja). Termillä Varmentaja tarkoitetaan tässä asiakirjassa sekä Juurivarmentajaa että Alivarmentajaa.

Varmentajan tehtäviä ovat:

1. Varmentajan varmennepalvelun hallinto.
2. Varmentajan varmennepalveluun liittyvän rekisteröintipalvelun toteutus ja hallinto.
3. Varmentaa hyväksymiensä Alivarmenteiden Julkiset avaimet.
4. Varmistaa, että tässä asiakirjassa kuvatut Varmentajan palvelut ovat Luottavien tahojen käytettävissä.

4.2 Varmennepalvelut

Varmennepalveluihin kuuluvat seuraavat palvelut:

1. Rekisteröintipalvelut: Varmenteen Tilaajan ja/tai edustajan tunnistaminen ja valtuutuksen varmistaminen.

2. Varmennetuotantopalvelut: Varmenteen luominen ja allekirjoittaminen rekisteröintipalveluissa tunnistetun identiteetin ja muiden varmistettujen Tilaajan tietojen perusteella.

3. Sulkupalvelu: Sulkupyyntöjen ja niihin liittyvien raporttien käsittely ja päätöksenteko tarvittavista toimenpiteistä.

4. Sulkutietopalvelu: Ilmoitus Luottaville tahoille suljetuista Varmenteista. Tämä palvelu voi olla ajantasainen tai tiedot voidaan toimittaa tai julkaista sovituin väliajoin.

4.3 Varmennepolitiikka ja Varmennekäytäntö

4.3.1 Tarkoitus

Yleisesti ottaen Varmennepolitiikka vastaa kysymykseen ”Mitä?”, kun taas Varmennekäytäntö vastaa kysymykseen ”Miten?”.

Varmennepolitiikka määrittelee PKI-toiminnan edellyttämät vaatimukset ja standardit eri osa-alueilla. Varmennekäytäntö puolestaan kertoo, millaisia menettelytapoja ja kontrolleja Varmentajan ja muiden tahojen tulee ottaa käyttöön täyttääkseen Varmennepolitiikan asettamat vaatimukset. Täten Varmennekäytännön tarkoitus on kuvata se, miten eri tahot suorittavat toimintojaan ja kontrolloivat prosessejaan.

4.3.2 Yksityiskohtaisuus

Varmennepolitiikka kuvaa yleiset vaatimukset Varmentajan toiminnalle. Varmennekäytäntö puolestaan kirjaa yksityiskohtaisemmin ne toiminnot, joilla Varmennepolitiikan vaatimukset täytetään.

4.3.3 Lähestymistapa

Varmennepolitiikka ei ole sidottu tiettyyn teknologiaan tai malliin. Sen on tarkoitus olla yleisluontoinen ja antaa perusteet luotettavalle PKI-järjestelmälle.

Varmennekäytäntö puolestaan on tarkempi kuvaus, joten se on sidottu tiettyyn kohteeseen.

4.3.4 Muut Varmentajan käytännöt

Varmennepolitiikan ja Varmennekäytännön lisäksi Varmentaja voi julkaista muuta PKI:hin liittyvää dokumentaatiota, kuten Varmennekuvauksen, Varmenteen tilaajan sopimuksen, Luottavien tahojen sopimuksia ym.

4.4 Varmenteen tilaaja ja Varmenteen haltija

Tässä asiakirjassa käytetään kahta eri termiä erottamaan kaksi Varmenteisiin liittyvää roolia.

1. Varmenteen tilaaja on vastuutaho, joka hakee Varmennetta Varmentajalta.

2. Varmenteen haltija on taho, joka Varmenteessa yksilöidään.

Rekisteröinnin yhteydessä Varmenteen tilaajaorganisaatiota edustaa organisaation valtuuttama henkilö.

Tämän politiikan puitteissa Varmenteen haltija voi olla OP Ryhmän liiketoiminta- tai ICT-palveluita tuottava tai hallinnoiva osasto tai toiminto tai muu Juurivarmentajan hyväksymä taho. Varmenteen haltija käyttää Yksityistä avainta Varmenteen tilaajan lukuun ja Tilaajan vastuulla.

5 VARMENNEPOLITIIKAN ESITTELY

5.1 Yleiskatsaus

Varmennepolitiikka on joukko sääntöjä, jotka osoittavat Varmenteen soveltuvuuden nimettyyn yhteisöön ja määrittelevät siihen liittyvät yhteiset tietoturvavaatimukset. Tämän politiikan mukaisesti myönnetyt Varmenteet sisältävät tunnistetiedon, jonka avulla Luottavat tahot voivat arvioida Varmenteen soveltuvuuden ja luotettavuuden tarvittavaan käyttöön.

5.2 Tunnistaminen

Tätä Varmennepolitiikkaa käytetään ainoastaan OP Ryhmän tarjoamien tai valtuuttamien palveluiden yhteydessä. Varmenneketjun määräävimpänä asiakirjana tämä Varmennepolitiikka on koko palvelun lallisten ja teknisten vaatimusten perusta.

Tämän Varmennepolitiikan tunniste (OID) on 1.3.6.1.4.1.11374.1.1.1.1.3.

5.3 Varmenteiden käyttöala

Tämän Juurivarmentajan myöntämiä Varmenteita käytetään Alivarmenteina OP Ryhmän palveluissa.

Juurivarmentajan myöntämiä Varmenteita käytetään myös muihin Juurivarmentajan erikseen määrittämiin tarkoituksiin.

Varmenteiden käyttö muihin tarkoituksiin on kielletty.

Varmenteiden myöntäjäksi merkitään OP-Pohjola Root CA.

5.4 Vaatimustenmukaisuus

5.4.1 Yleistä

Varmentaja tuottaa varmennepalvelua Varmennepolitiikassa mainituin ehdoin ja vastaa varmennepalvelun toimivuudesta Varmenteen haltijalle. Varmentaja vastaa koko varmennejärjestelmän toimivuudesta, myös mahdollisesti käyttämiensä alihankkijoiden osalta.

Palvelun vaatimustenmukaisuudesta voi varmistua vertaamalla politiikkaa käytäntöön Varmentajan toiminnan aikana sekä prosessien ja dokumentaation merkittävien muutosten jälkeen.

5.4.2 Vaatimukset

Varmentaja täyttää luvussa 6 kuvatut velvollisuudet ja noudattaa luvussa 7 määriteltyjä käytäntöjä. Kaikkien tähän Juurivarmenteeseen liittyvien tahojen on noudatettava tätä Varmennepolitiikkaa.

5.4.3 Muut ehdot

Tästä asiakirjasta voidaan tehdä käännöksiä muille kielille. Mikäli käännöksien ja suomenkielisen asiakirjan välillä ilmenee ristiriitoja, noudatetaan suomenkielistä versiota.

6 VASTUUT JA VELVOLLISUUDET

6.1 Juurivarmentajan velvollisuudet

1. Juurivarmentajan velvollisuus on huolehtia siitä, että kaikki vaatimukset, jotka on kirjattu luvussa 7, toteutetaan tämän Varmennepolitiikan mukaisesti.

2. Juurivarmentaja on velvollinen varmistamaan, että kaikki sen tarjoamat varmennepalvelut ovat voimassa olevan Varmennekäytännön mukaisia.

6.2 Alivarmentajan velvollisuudet

Alivarmenteen Tilaaja ja haltija voivat olla samoja. Varmenteen tilaaja on vastuussa myös Varmenteen haltijan velvoitteista. Juurivarmentaja sitoo sopimuksella Alivarmentajan noudattamaan seuraavia ehtoja:

1. Tämän politiikan mukaisuus: Alivarmentajalla on velvollisuus huolehtia siitä, että kaikki vaatimukset, jotka on kirjattu luvussa 7, on toteutettu Varmennepolitiikan mukaisesti.

2. Virheettömät ja täydelliset tiedot: Alivarmentaja on velvollinen toimittamaan varmennehakemuksen yhteydessä virheettömät ja täydelliset tiedot.

3. Huolellisuus: Alivarmenteen haltija on velvollinen käsittelemään Yksityistä avaintaan huolellisesti väärinkäytösten ehkäisemiseksi.

4. Varmenteen haltijan avainten pituus: Alivarmentajan velvollisuus on valita avainten pituudet niin, että ne ovat riittäviä tässä Varmennepolitiikassa määriteltyihin Varmenteen käyttötarkoituksiin sen määriteltynä voimassaoloaikana.

5. Avainten luonti: Alivarmentaja on velvollinen luomaan Avainparinsa algoritmilla, jonka yleisesti (esimerkiksi standardin NIST SP800-57 mukaan) katsotaan olevan riittävän vahva tässä Varmennepolitiikassa määriteltyihin Varmenteen käyttötarkoituksiin. Alivarmentaja on velvollinen luomaan avaimet HSM-laitteessa, joka on validoitu vähintään standardin FIPS PUB 140-2 tasolle 3.

6. Avainten pääsynhallinta: Vain Varmenteen haltijan valtuuttamalla taholla on oikeus käyttää Varmentajan yksityistä avainta. Avainta säilytetään ja käytetään OP Osuuskunnan Alivarmentajien käyttöön dedikoidussa HSM-laitteessa.

7. Tiedoksiantovaatimus: Alivarmentaja on velvollinen ilmoittamaan Juurivarmentajalle viipymättä, jos jokin seuraavista tapahtuu tai epäillään tapahtuneen ennen Varmenteen vanhenemista:

    i. Varmenteen haltijan Yksityinen avain katoaa, varastetaan tai sen luotettavuus vaarantuu.

    ii. Kontrolli Varmenteen haltijan Yksityisestä avaimesta menetetään esim. hallinnointikorttien kadotessa.

    iii. Varmenteen sisällössä havaitaan epäkohtia tai muutostarpeita.

    iv. Varmenteen myöntämisen edellytykset ovat muuttuneet.

8. Varmentajan avaimen vaarantuminen: Alivarmentajalla on velvollisuus poistaa välittömästi käytöstä vaarantunut Alivarmenteen haltijan Yksityinen avain ja kaikki siihen pohjautuvat Varmenteet sekä toimittaa Alivarmentajan Varmenteen sulkupyyntö Juurivarmentajalle.

9. Alivarmentaja on velvollinen noudattamaan tätä Varmennepolitiikkaa, Juurivarmentajan Varmennekäytäntöä sekä omaa Varmennepolitiikkaansa ja Varmennekäytäntöään. Ristiriitatapauksessa tämä Varmennepolitiikka on määräävä.

10. Alivarmentaja on velvollinen noudattamaan Alivarmentajan toimialaa koskevaa ja voimassa olevaa Suomen lainsäädäntöä.

11. Alivarmentaja on velvollinen viipymättä päivittämään oma Varmennepolitiikkansa ja Varmennekäytäntönsä, mikäli Alivarmentajan toiminnassa tapahtuu sellaisia muutoksia, jotka edellyttävät kyseisten asiakirjojen muuttamista tai mikäli Juurivarmentajan Varmennepolitiikkaan tai Varmennekäytäntöön tulee sellaisia muutoksia, jotka edellyttävät Alivarmentajan vastaavien asiakirjojen muuttamista.

12. Alivarmentajalla on velvollisuus sisällyttää luvussa 6.3 kuvatut Varmenteeseen luottavien tahojen velvollisuudet Varmenteen tilaajan sopimuksiinsa.

13. Alivarmentajalla on velvollisuus säilyttää Varmenteisiin liittyviä oleellisia tietoja vähintään 10 vuotta tapahtumahetkestä.

14. Alivarmentaja on velvollinen julkaisemaan nimensä ja yhteystietonsa siten, että ne ovat Luottavien tahojen saatavilla.

6.3 Varmenteeseen luottavien tahojen velvollisuudet

Luottamalla Varmenteeseen Luottava taho ilmaisee hyväksyneensä tämän Varmennepolitiikan ehdot.

Varmenteeseen Luottavan tahon velvollisuutena on varmistaa seuraavat asiat koko Varmenneketjun osalta

1. tarkastaa Varmenteen voimassaolo sekä mahdolliset sulkemiset ja käytön estot Sulkutietopalvelusta sekä varmistaa sulkutiedon oikeellisuus ja eheys

2. noudattaa Varmenteessa tai ehdoissa Luottaville tahoille ilmoitettuja Varmenteen käytön rajoitteita

3. noudattaa kaikkia varotoimenpiteitä, jotka on mainittu sopimuksissa tai muissa Varmenteeseen liittyvissä asiakirjoissa

4. hyväksyä Varmenne vain Varmennepolitiikassa määriteltyihin käyttötarkoituksiin. Lisäksi on arvioitava, soveltuuko Varmennepolitiikassa kuvattu Varmentajan tarjoama luottamustaso Luottavan tahon tarkoituksiin.

6.4 Juurivarmentajan vastuut

1. Juurivarmentaja vastaa tässä Varmennepolitiikassa kuvattujen menettelyjen ja toimintatapojen noudattamisesta Varmennepalveluissaan, ellei noudattamatta jättäminen johdu ylivoimaisesta esteestä.

2. Juurivarmentajalla on vastuu noudattaa voimassa olevaa Suomen lainsäädäntöä.

3. Juurivarmentaja vastaa Alivarmentajien tunnistamisesta ja valtuutuksen varmistamisesta.

4. Juurivarmentaja vastaa oman toimintansa lisäksi siitä, että myös kaikki juurivarmennepalvelun tuottamiseen osallistuvat osapuolet toimivat tämän Varmennepolitiikan mukaisesti.

5. Juurivarmentaja vastaa siitä, että Juurivarmentajan hyväksymät Alivarmentajien Varmennepolitiikat ja Varmennekäytännöt ovat tämän politiikan mukaisia.

6. Juurivarmentaja ei ole millään tavalla vastuussa vahingoista, jotka aiheutuvat Alivarmentajan myöntämien Varmenteiden käytöstä, mikäli vahingot eivät johdu siitä, että Juurivarmentaja olisi toiminut tämän Varmennepolitiikan vastaisesti.

7. Juurivarmentaja ei vastaa tämän Varmennepolitiikan mukaisesti myönnettyjen Varmenteiden tai niihin liittyvien avainten käytöstä silloin, kun niitä käytetään tämän Varmennepolitiikan vastaisesti.

8. Juurivarmentaja ei vastaa tavaramerkkien käytöstä Alivarmentajan myöntämissä Varmenteissa.

6.5 Alivarmentajan vastuut

Juurivarmentaja myöntää Alivarmenteita vain Alivarmentajille, jotka ovat sopimuksella sitoutuneet seuraaviin vastuisiin:

1. Alivarmentaja vastaa siitä, että se noudattaa tätä Varmennepolitiikkaa sekä voimassa olevaa omaa Varmennepolitiikkaansa ja Varmennekäytäntöänsä.

2. Alivarmentaja vastaa siitä, että sen yksityistä avainta käytetään ainoastaan Alivarmentajan varmennepolitiikassa määriteltyihin käyttötarkoituksiin. Määritellyt käyttötarkoitukset voivat olla Tilaajavarmenteen allekirjoittaminen, OCSP-varmenteen myöntö, Sulkulistan allekirjoittaminen, sekä muut Varmentajan allekirjoitustarkoitukset, kuten Varmentajan lokitietojen allekirjoittaminen.

3. Alivarmentaja vastaa myöntämiensä Varmenteiden tilaajien tunnistamisesta ja valtuutuksen varmistamisesta.

4. Alivarmentaja vastaa siitä, että omistaa käytössään olevat nimet ja tavaramerkit, jotka mainitaan alivarmennehakemuksessa tai Varmenteen tietokentissä, tai oikeuden niiden käyttöön.

6.6 Varmenteeseen Luottavien tahojen vastuut

Luottamalla Varmenteeseen Luottava taho ilmaisee hyväksyneensä Varmennepolitiikan ehdot.

Varmenteeseen Luottava taho vastaa itse muista tapahtuman valtuuttamiseen tai hyväksymiseen tarvittavista toimista Varmenteen tarkistuksen lisäksi.

7 VARMENTAJAN NOUDATTAMAT KÄYTÄNNÖT

Tässä luvussa kuvataan Juurivarmentajan toimintaa ja asetetaan vaatimuksia Alivarmentajan toiminnalle, mikäli toisin ei ole mainittu.

7.1 Varmennekäytäntö

Kontrollitavoite: Varmentaja kuvaa käytäntönsä ja toimintatapansa Varmennekäytännössä.

1. Varmentajalla on Varmennekäytäntö, johon on kirjattu ne käytännöt ja toimintatavat, joilla vastataan Varmennepolitiikassa esitettyihin vaatimuksiin.

2. Varmennekäytäntö kuvaa Varmennetuotannon osapuolten vastuut ja käytännöt.

3. Varmentaja päättää erikseen Varmennekäytännön julkaisusta.

4. Varmentaja hyväksyy Varmennepolitiikan ja Varmennekäytännön.

5. Varmentaja katselmoi Varmennekäytännön vähintään kahden vuoden välein ja päättää tarvittavista toimenpiteistä, kuten esimerkiksi auditointien suorittamisesta.

7.2 PKI-avainten elinkaaren hallinta

7.2.1 Varmentajan avainten luonti ja hallinnointi

Kontrollitavoite: Varmenteiden luonti ja hallinnointi – Varmentaja varmistaa, että Varmentajan Varmenteen avaimet luodaan valvotuissa olosuhteissa etukäteen laaditun Juurivarmentajan hyväksymän ohjeistuksen mukaisesti.

1. Varmentajan avaimet luodaan fyysisesti turvallisissa tiloissa (ks. luku 7.4.4). Avainten luomisen hoitavat asianmukaiset henkilöt (ks. luku 7.4.3) kaksoiskäyttömenettelyä noudattaen. Tarkemmat menettelyt on kuvattu Varmennekäytännössä.

2. Varmentajan avainten luonti suoritetaan HSM-laitteessa, joka täyttää luvun 6.2 alakohdassa 5 mainitut vaatimukset.

3. Juurivarmentaja on ns. offline-varmentaja, eli sen teknisestä ympäristöstä ei ole verkkoyhteyksiä ulkopuolelle. Kaikki tässä ympäristössä suoritetut toiminnot ovat manuaalisia.

4. Varmentajan avainten luonti suoritetaan algoritmilla, jonka yleisesti katsotaan olevan riittävän vahva Varmentajan käyttöön. Avaimen parametrit, erityisesti avaimen pituus, valitaan siten, että ne ovat riittävän vahvoja Varmentajan allekirjoitustarkoitukseen. Algoritmit, avainten pituudet ja muut parametrit ovat standardin NIST SP800-57 tai sitä uudempien soveltuvien suositusten mukaisia. Yksityiskohtaisemmat kuvaukset löytyvät Varmennekäytännöstä.

5. Varmentajan avainoperaatioihin osallistuva henkilöstö on luetteloitu ja heille on määritelty nimetyt, luotetut roolit (ks. luku 7.4.3), ja kaikki avainoperaatioiden tehtävät suoritetaan aina kaksoiskäyttömenettelyä noudattaen. Varmentajan yksityiseen avaimeen ja sen laiteympäristöön liittyvät toiminnot kirjataan aina lokiin.

6. Kun henkilö ei toimi enää luotetussa roolissa, hänen luotettuun rooliin liittyvät käyttöoikeutensa peruutetaan välittömästi, ja avainoperaatioihin liittyvät hallinnointikortit luovutetaan seuraavalle roolin haltijalle.

7. Ennen Varmentajan yksityisen avaimen vanhenemista Varmentaja luo uuden Varmenteiden Avainparin. Uuden Varmentajan Varmenteen jakelumenettely ei poikkea vanhan Varmenteen jakelutavasta. Näin taataan Varmentajan Avainparista riippuvien toimintojen häiriötön jatkuvuus. Uusi Avainpari luodaan ja uusi Julkinen avain jaellaan tämän Varmennepolitiikan mukaisesti.

7.2.2 Varmentajan avainten säilyttäminen, varmuuskopiointi ja palautus

Kontrollitavoite: Varmentaja varmistaa, että Varmentajan yksityiset avaimet pysyvät luottamuksellisina ja eheinä koko elinkaarensa ajan.

1. Varmentajan Yksityinen avain suojataan HSM-laitteella. Juurivarmentajan Yksityinen avain suojataan ainoastaan OP Osuuskunnan Juurivarmentajien käyttöön dedikoidulla HSM-laitteella.

2. Varmentajan yksityisen avaimen varmuuskopioinnin, säilytyksen ja palautuksen saavat tehdä vain nimetyt henkilöt (ks. luku 7.4.3) fyysisesti turvatussa ympäristössä (ks. luku 7.4.4) siten, että läsnä on aina vähintään kaksi tehtävään nimettyä ja valtuutettua henkilöä.

3. Varmentajan yksityisen avaimen varmuuskopiot suojataan samalla menettelyllä kuin tuotantokäytössä oleva avain.

4. Menettelytavat on kuvattu tarkemmin Varmennekäytännössä.

7.2.3 Varmentajan Julkisen avaimen jakelu

Kontrollitavoite: Varmentaja varmistaa, että Varmentajan Julkinen avain säilyttää eheytensä ja aitoutensa, kun se siirretään tai jaetaan Luottavien tahojen käyttöön.

Juurivarmentajan Varmenne julkaistaan osoitteessa: https://www.op.fi/varmennepalvelu. Sivusto on suojattu organisaatiovarmennetulla palveluvarmenteella. Samassa web-palvelussa julkaistaan myös Varmenteen sormenjälki (fingerprint) ja sarjanumero.

7.2.4 Key escrow

Key escrow ei ole käytössä Varmentajien avaimille.

7.2.5 Varmentajan avainten käyttö

Kontrollitavoite: Varmentaja varmistaa, että Varmentajan yksityisiä avaimia käytetään asianmukaisesti.

1. Juurivarmentajan Yksityistä avainta käytetään sekä Juurivarmentajan Varmenteen allekirjoittamiseen että OP Ryhmän tarvitsemien Alivarmenteiden (ks. luku 7.3.3) ja Sulkulistojen allekirjoittamiseen. Juurivarmentajan Yksityistä avainta ei käytetä mihinkään muuhun tarkoitukseen.

2. Juurivarmentajan avaimen aktivoi vähintään kaksi luotettuun rooliin nimettyä henkilöä, jotka ovat paikalla niin kauan kuin Juurivarmentajan avain on aktivoituna.

7.2.6 Varmentajan avainten elinkaaren päättyminen

Kontrollitavoite: Varmentaja varmistaa, että Varmentajan yksityisiä avaimia ei käytetä niiden elinkaaren päätyttyä.

Kaikki kopiot Varmentajan yksityisestä avaimesta tuhotaan tai poistetaan käytöstä viipymättä sen jälkeen, kun niiden käyttöaika on umpeutunut. Näin estetään niiden luvun 7.2.5 mukainen käyttö vanhentumisen jälkeen.

7.2.7 HSM-laitteen elinkaaren hallinta

Kontrollitavoite: Varmentaja varmistaa HSM-laitteidensa turvallisuuden koko niiden elinkaaren ajan.

1. Varmentajan HSM-laitteet suojataan luvattomalta käsittelyltä kuljetuksen aikana. Vähintään kaksi nimettyä ja valtuutettua henkilöä tarkastaa HSM-laitteen sen asennuksen yhteydessä. Tarkastuksessa todetaan, ettei HSM-laitetta ole luvattomasti käsitelty kuljetuksen aikana, ja että se on turvallisuusstandardien mukainen (ks. luku 7.2.2).

2. HSM-laite suojataan luvattomalta käsittelyltä varastoinnin aikana.

3. HSM-laitteen käyttöönottoon, alustukseen ja käyttöön tarvitaan vähintään kaksi valtuutettua henkilöä.

4. Kun HSM-laite poistetaan käytöstä, se tuhotaan tai tyhjennetään valmistajan ohjeiden mukaisesti.

7.2.8 Varmentajan tarjoamien Varmenteen haltijan avainpalveluiden hallinta

Kontrollitavoite: Varmentajan yksityinen avain on vain sen itsensä hallinnassa.

1. Alivarmentaja luo itse Alivarmenteen Avainparin.

2. Varmennepyyntö toimitetaan Juurivarmentajalle allekirjoitettavaksi manuaalisella menettelyllä.

3. Alivarmentajan Yksityinen avain pysyy koko ajan Alivarmentajan hallinnassa HSM-laitteella suojattuna.

7.3 Varmenteiden elinkaaren hallinta

7.3.1 Alivarmentajan Varmenteen rekisteröinti

Kontrollitavoite: Juurivarmentaja varmistaa, että Alivarmenteen Tilaajan nimi ja muut tiedot on annettu oikein. Lisäksi Juurivarmentaja varmistaa, että varmennepyynnöt ovat virheettömiä, valtuutettuja ja perusteellisia.

1. Juurivarmentaja hyväksyy Alivarmentajaksi vain suomalaisia OP Ryhmän yhteisöjä.

2. Varmenteen tilaaja sitoutuu rekisteröinnin yhteydessä noudattamaan tätä Varmennepolitiikkaa. Varmenteen tilaaja hyväksyy tilaajasopimuksen ja mahdolliset muut asiaan liittyvät sopimukset.

3. Juurivarmentaja varmistaa Alivarmenteen Tilaajan identiteetin ja valtuutuksen toimia Alivarmentajan puolesta.

4. Alivarmentaja toimittaa Varmennepolitiikkansa ja Varmennekäytäntönsä Juurivarmentajalle, joka tarkastaa, että ne eivät ole ristiriidassa tämän Varmennepolitiikan eikä Juurivarmentajan Varmennekäytännön kanssa. On suositeltavaa, että Alivarmentajat noudattavat Varmennepolitiikassaan samoja standardeja ja rakennetta kuin Juurivarmentaja.

5. Juurivarmentaja hyväksyy tai hylkää kaikki alivarmennehakemukset omalla päätöksellään.

6. Juurivarmentaja arkistoi Alivarmenteen Tilaajan edustajan kanssa allekirjoitetun sopimuksen.

7. Juurivarmentaja säilyttää rekisteröintitietoja kymmenen vuoden ajan Juurivarmentajan toiminnan päättymisen jälkeen.

8. Alivarmentajan tekninen varmennepyyntö luodaan ja siirretään Juurivarmentajalle Juurivarmentajan määrittelemällä tavalla. Teknisen varmennepyynnön toimituksessa varmistetaan varmennepyynnön muuttumattomuus varmennepyynnön luontihetkestä Varmenteen luontiin asti.

9. Juurivarmentaja varmistaa, että Alivarmentajalla on hallussaan varmennepyyntöä vastaava Yksityinen avain ja että varmennepyyntö on Alivarmentajan toimittama.

7.3.2 Varmenteiden uusiminen, päivitys ja avainten uusiminen

Kontrollitavoite: Alivarmentajan uudet Alivarmenteet käsitellään samoin kuin uuden Varmentajan tilaukset. Juurivarmentaja varmistaa lisäksi, että Varmennetta ei myönnetä aiemmin käytetyille avaimille.

1. Varmenteiden uusimispyynnöt käsitellään aina kuten uuden Varmenteen tilaus.

2. Juurivarmentaja voi myöntää uuden Alivarmenteen olemassa olevan tilaajasopimuksen puitteissa.

3. Juurivarmentaja ei myönnä Varmennetta käytössä olevalle Avainparille vaan vaatii aina uuden Avainparin luonnin.

7.3.3 Varmenteiden luominen

Kontrollitavoite: Juurivarmentaja varmistaa, että Juurivarmentajan ja Alivarmentajan Varmenteiden myöntöprosessi on turvallinen, jotta Varmenteiden luotettavuus säilyy.

Varmentajien avaimet luodaan aina turvatuissa olosuhteissa kaksoiskäyttömenettelyä noudattaen luvun 7.2.1 vaatimusten mukaisesti.

7.3.3.1 Juurivarmentajan Varmenteen luominen:

1. Juurivarmenteiden sisältö on käsitelty yksityiskohtaisesti Varmennekäytännössä.

2. Juurivarmenteen voimassaoloaika on 29 vuotta.

3. Juurivarmentajan Varmenne allekirjoitetaan Juurivarmentajan avaimen luonnin yhteydessä.

7.3.3.2 Alivarmentajan Varmenteen luominen:

1. Alivarmenteiden sisältövaatimukset kuvataan yksityiskohtaisesti Juurivarmentajan Varmennekäytännössä.

2. Alivarmenteiden voimassaoloaika on korkeintaan 7 vuotta.

3. Juurivarmentaja varmistaa, että se myöntää olemassaolonsa aikana ainoastaan yksikäsitteisiä sarjanumeroita Alivarmentajan Varmenteille.

4. Alivarmentajan Varmenteissa käytetään sellaisia Varmentajaa kuvaavia nimiä, että Varmenteisiin luottavat osapuolet voivat tunnistaa Alivarmentajana toimivan tahon.

5. Alivarmentajan Varmenne luodaan erillisessä, Juurivarmentajan hyväksymässä Varmenteen luontiseremoniassa.

7.3.4 Yleisten ehtojen jakelu

Kontrollitavoite: Varmentaja varmistaa, että Varmenteiden yleiset ehdot ovat Varmenteen tilaajien, Varmenteen haltijoiden ja Luottavien tahojen saatavilla.

Varmenneketjussa ylempi Varmentaja toimittaa Varmennekäytäntönsä Alivarmentajan käyttöön.

Varmentajien Varmennepolitiikat julkaistaan osoitteessa https://www.op.fi/varmennepalvelu.

Tilaajasopimuksien tulee olla Tilaajien saatavilla.

7.3.5 Varmenteiden jakelu

Kontrollitavoite: Varmentaja varmistaa Varmenteensa saatavuuden Luottaville tahoille.

1. Kun Alivarmentajan Varmenne on luotu, sen eheys tarkastetaan ennen toimitusta Varmenteen tilaajalle ja Varmenteen haltijalle.
2. Alivarmentaja vastaa Varmenteensa jakelusta.
3. Juurivarmenne on saatavissa luvun 7.2.3 mukaisesti.

7.3.6 Varmenteiden sulkeminen ja toiminnan esto

Kontrollitavoite: Varmenteet suljetaan niin nopeasti kuin mahdollista valtuutettujen ja varmistettujen Varmenteen sulkupyyntöjen perusteella.

7.3.6.1 Varmenteiden sulkemisen hallinta

1. Alivarmentajan Varmenteen sulkupyynnön voi tehdä Alivarmentajan edustaja tai Juurivarmentaja.
2. Alivarmenteiden sulkupyynnöt toimitetaan Juurivarmentajalle.
3. Sulkutieto on kaikkien Luottavien tahojen käytettävissä Sulkutietopalvelussa Varmennekäytännössä mainitulla tavalla.
4. Alivarmentajan Varmenne voidaan sulkea esimerkiksi seuraavissa tilanteissa:
    i. Alivarmenteen Yksityisen avaimen vaarantuminen.
    ii. Alivarmenteen Tilaajan sopimuksen tai sopimusvelvoitteiden rikkominen.
5. Sulkupyynnöt käsitellään viivyttelemättä.
6. Sulkupyynnöt todennetaan Varmennekäytännön mukaisesti.
7. Kun Varmenne on lopullisesti suljettu (revoked), sitä ei voida enää palauttaa käyttöön.

7.3.6.2 Sulkutieto

1. Käytettäessä Sulkulistoja sulkutiedon välitykseen
    i. Juurivarmentajan Sulkulistan voimassaoloaika on yksi vuosi ja se julkaistaan vähintään kaksi kertaa vuodessa
    ii. jokaisella Sulkulistalla ilmoitetaan Sulkulistan voimassaoloaika
    iii. uusi Sulkulista voidaan julkaista ennen seuraavan Sulkulistan etukäteen ilmoitettua julkistamisajankohtaa

iv. Sulkulista on Varmentajan allekirjoittama.

2. Sulkutieto voidaan julkaista myös reaaliaikapalveluna (OCSP).

3. Sulkutieto on saatavissa jatkuvasti Juurivarmenteen ollessa voimassa.

4. Sulkutieto sisältää suljettujen Varmenteiden tilatiedot vähintään niiden alkuperäisen voimassaolon ajan.

7.4 Varmentajan hallinnointi ja toiminta

7.4.1 Yleinen turvallisuushallinto

Kontrollitavoite: Varmentaja varmistaa, että sovelletut hallinto- ja johtamismenettelyt ovat riittäviä ja standardeja vastaavia.

1. Varmentaja suorittaa toiminnastaan riskikartoituksia ja määrittää tarvittavat turvallisuusvaatimukset ja toimintatavat.

2. Varmentaja vastaa mahdollisten alihankkijoidensa toiminnasta kuten omastaan.

3. Varmentaja toimii määrämuotoisten menettelytapojen mukaisesti laadun ja tietoturvallisuuden varmistamiseksi varmennepalvelun tuottamisessa.

4. Varmentaja ylläpitää aktiivisesti varmennetuotantoympäristöään erityisesti huomioiden tietoturvallisuuden ja siihen liittyvät vaatimukset.

5. Turvakontrollit ja toimintatavat Varmentajan varmennepalvelun toimitiloissa, järjestelmissä ja tietovarannoissa ovat dokumentoituja ja ylläpidettyjä. Varmennepalvelun tuottamisen säännöt, ohjeet ja prosessit ovat dokumentoituja ja hyväksyttyjä. Lisäksi Varmentajalla on toipumis- ja jatkuvuussuunnitelma häiriötilanteiden, onnettomuuksien ym. varalle.

7.4.2 Tiedon luokittelu ja hallinto

Kontrollitavoite: Varmentaja käsittelee tietoaineistojaan asianmukaisesti.

Varmentajalla on käytössään menettelyt ja ohjeet asiakirjojen ja tietojen luokittelulle, käsittelylle ja hävittämiselle.

7.4.3 Henkilöstöturvallisuus

Kontrollitavoite: Varmentaja varmistaa, että sen henkilöstöpolitiikka edistää ja tukee Varmentajan toiminnan luotettavuutta.

7.4.3.1 Yleiset henkilöstöturvallisuuteen liittyvät asiat

1. Varmentajalla on käytettävissä riittävä määrä henkilöstöä, joilla on vaadittava asiantuntemus, kokemus ja pätevyys tarjottaviin palveluihin sekä työtehtäviinsä.

2. OP Ryhmä on todennut henkilöiden luotettavuuden ja soveltuvuuden tehtäviinsä normaalein rekrytointimenettelyin.

3. Alihankkijoiden osalta luotettavuus ja tehtäviin soveltuvuus varmistetaan sopimuksin.

4. Varmentajan luotetut roolit kuvataan yksiselitteisesti.

5. Varmentajan henkilöstöllä (sekä määräaikaisella että vakituisella) on määritellyt toimenkuvat, jotka noudattavat sekä Tehtävien eriyttämisen (segregation of duties) että Pienimpien tarvittavien oikeuksien (least privilege) periaatteita.

7.4.3.2 Rekisteröinti, Varmenteen luominen, Varmenteiden sulkemisen hallinta

1. Varmentajaa hallinnoivilla henkilöillä on kokemusta ja koulutusta PKI-tekniikoista ja he ovat perehtyneet henkilöstön turvamenettelyihin tehtävissä, jotka sisältävät turvallisuusvastuita. Lisäksi heillä on riittävästi kokemusta tietoturvasta ja riskien arvioinnista.

2. Varmentajan luotettuja tehtäviä hoitavilla henkilöstön jäsenillä ei saa olla eturistiriitoja, jotka saattavat vaikuttaa Varmentajan toiminnan luotettavuuteen.

3. Luotetut roolit määritellään Varmennekäytännössä.

4. Luotettuihin rooleihin tai hallinnollisiin toimiin ei hyväksytä ketään sellaista henkilöä, joka on tuomittu vakavasta rikoksesta tai sellaisesta rikkomuksesta, joka vaikuttaa hänen soveltuvuuteensa tehtävään. Henkilöstöllä ei ole pääsyä luotettuihin tehtäviin ennen kuin tarvittavat taustaselvitykset on tehty. Taustaselvitykset tehdään lakien ja viranomaismääräysten sallimissa rajoissa.

7.4.4 Fyysinen turvallisuus

Kontrollitavoite: Varmentaja varmistaa, että fyysistä pääsyä kriittisiin palveluihin valvotaan ja että Varmentajan tietovarantoihin liittyvät fyysiset riskit minimoidaan.

7.4.4.1 Yleiset fyysiseen turvallisuuteen liittyvät asiat

1. Vain asianmukaisesti valtuutetut henkilöt pääsevät tiloihin, joissa tehdään Juuri- ja Alivarmenteiden luontiin ja sulkemiseen liittyviä toimenpiteitä.

2. Varmentaja määrittelee kontrollit, joilla estetään onnettomuudet, vahingot ja omaisuuden vaarantuminen sekä tietoihin ja tuotantotiloihin kohdistuvat vaarat ja varkaudet.

3. Kaikissa Juurivarmentajan laitteistoon kohdistuvissa toimenpiteissä noudatetaan kaksoiskäyttömenettelyä.

   i. Laitteen ollessa varastoituna varastointitilan pääsynvalvonta on kaksoiskäytön piirissä.

   ii. Laitetta operoidaan valvottuna erillisessä tilassa.

4. Kaikki Varmentajan laitteistoon liittyvät toimenpiteet dokumentoidaan.

7.4.4.2 Varmennetuotanto ja sulkutapahtumien hallinta

1. Työtilat, joissa tehdään Varmenteen luomiseen tai sulkemisen hallintaan liittyviä tehtäviä, on suojattu fyysisesti niin, ettei järjestelmiin tai tietoihin ole luvatonta pääsyä.

2. Fyysisesti suojatulla alueella ulkopuolisilla henkilöillä on saattaja eikä heitä jätetä ilman valtuutetun henkilön valvontaa.

3. Fyysisen turvallisuuden varmistamiseksi Varmentajalla on Varmenteiden luomiseen ja sulkemisen hallintaan liittyville tehtäville kulunvalvonnalla suojattu alue.

4. Varmentajan fyysisen turvallisuuden menettelyt ja ympäristön turvallisuusmenettelyt kattavat fyysisen pääsynhallinnan, luonnon katastrofeihin varautumisen, paloturvallisuustekijät, tukijärjestelmien häiriöt, rakennusten romahtamisen, vesi- ja muut putkivahingot, varkauksiin varautumisen, murrot sekä toipumissuunnitelmat.

5. Varmentajan laitteiden, tietojen, viestimien ja ohjelmistojen suojaamiseksi on käytössä kontrollit, joilla estetään niiden valtuuttamaton haltuunotto. Samalla suojatulla alueella voidaan suorittaa muitakin toimintoja edellyttäen, että alueelle pääsevät vain valtuutetut henkilöt.

7.4.5 Käytön hallinta

Kontrollitavoite: Varmentaja varmistaa, että sen järjestelmät ovat turvallisia ja, että niitä käytetään oikein minimoiden häiriöiden riskit.

7.4.5.1 Yleiset käytön hallintaan liittyvät asiat

1. Varmentaja suojaa varmennejärjestelmien eheyden ja tiedot viruksia, haittaohjelmia ja luvattomia ohjelmistoja vastaan.

2. Varmentaja minimoi tietoturvaloukkauksista ja toimintahäiriöistä aiheutuvat vahingot käyttämällä vaaratilanteiden ilmoitusmenettelyjä ja toimintasuunnitelmia.

3. Varmentaja käsittelee käyttämiään tallennusvälineitä turvallisesti niiden suojelemiseksi vahingon, varkauden ja luvattoman käytön varalta.

4. Varmentaja käyttää tallennusvälineiden hallintamenettelyitä, joilla estetään tallennusvälineiden vanhentuminen ja heikkeneminen asiakirjojen säilyttämisen aikana.

5. Varmentaja määrittelee formaalit toimintatavat, jotka koskevat kaikkia varmennepalvelujen tarjoamiseen liittyviä luotettuja ja hallinnollisia tehtäviä.

7.4.5.2 Tallennusvälineiden käsittely ja turvallisuus

Kaikkia tallennusvälineitä käsitellään turvallisesti ja tietojen luokitukseen perustuvien vaatimusten mukaisesti (ks. 7.4.2). Käytön päättyessä tallennusvälineet, jotka sisältävät arkaluonteisia tietoja, hävitetään turvallisesti.

7.4.5.3 Poikkeavista tapahtumista raportoiminen ja niihin reagoiminen

1. Varmentajan toimintaan osallistuvat henkilöt ilmoittavat kaikki käytön hallinnan poikkeamatilanteet mahdollisimman pian tapahtuman jälkeen Varmentajalle. Varmentaja reagoi poikkeamatilanteisiin nopeasti ja koordinoidusti poikkeamien vaikutusten rajoittamiseksi.

2. Luvun 7.4.11 mukaiset auditointilokiprosessit toimivat järjestelmän käynnistymisestä järjestelmän sammuttamiseen asti. HSM-laitteen fyysisen valvonnan osalta auditointilokiprosessit toimivat myös laitteen ollessa varastoituna.

7.4.6 Järjestelmän pääsynhallinta

Kontrollitavoite: Varmentaja varmistaa, että vain valtuutetuilla henkilöillä on pääsy Varmentajan järjestelmiin.

7.4.6.1 Yleiset järjestelmien pääsynhallintaan liittyvät asiat

1. Varmentajan käyttäjä- ja valtuushallintamenettelyt rajaavat pääsyn järjestelmään työtehtävien perusteella. Varmentaja varmistaa, että pääsy järjestelmän tietoihin ja toimintoihin rajoitetaan pääsynhallintapolitiikan mukaisesti.

2. Varmentajan henkilöstö tunnistetaan luotettavasti ennen kuin heille luovutetaan tunnisteita Varmenteiden hallinnalle kriittisiin sovelluksiin pääsemiseksi.

3. Varmentajan henkilöstö vastaa tekemistään toimenpiteistä. Tätä tukee tapahtumalokien säilytys (ks. luku 7.4.11).

7.4.6.2 Varmenteiden luonti

1. Juurivarmentaja varmistaa, että sen varmennetuotannossa käyttämät laitteet eivät ole missään vaiheessa kytkettynä tietoverkkoon.

2. Laitteiden konfiguraatio dokumentoidaan ja se on todennettavissa yleisen auditoinnin yhteydessä.

7.4.6.3 Sulkutieto

Sulkutietojärjestelmä on pääsynhallinnan piirissä.

7.4.7 Luotettavien järjestelmien käyttö ja ylläpito

Kontrollitavoite: Varmentaja käyttää luotettavia järjestelmiä ja tuotteita, jotka on suojattu valtuuttamattomalta muokkaamiselta.

7.4.7.1 Yleiset järjestelmien luotettavuuteen liittyvät asiat

1. Jokaisessa Varmentajan järjestelmän kehitysprojektissa analysoidaan järjestelmän turvallisuusvaatimukset järjestelmän suunnittelu- ja vaatimusmäärittelyvaiheessa. Analyysin perusteella toteutetuilla turvallisuusratkaisuilla varmistetaan, että turvallisuus on sisäänrakennettu järjestelmiin.

2. Julkaisuille, muokkauksille ja hätäpäivityksille, jotka koskevat operatiivisia ohjelmia, on olemassa muutoksenhallintaprosessit.

7.4.8 Liiketoiminnan jatkuvuus ja ongelmien hallinta

Kontrollitavoite: Varmentaja varmistaa, että katastrofitilanteissa, kuten Varmentajan yksityisen avaimen vaarantuessa, toiminta palautuu normaaliksi mahdollisimman nopeasti. Muita hätätilanteita ovat mm. laite- tai ohjelmakomponenttien kriittiset virheet.

7.4.8.1 Yleiset jatkuvuuteen liittyvät asiat

Varmentajalla on katastrofitilanteiden varalta jatkuvuussuunnitelma, jota ylläpidetään säännöllisesti.

7.4.8.2 Varmentajan järjestelmien varmuuskopiointi ja palautus

Varmentajalla on riittävät varmuuskopiointijärjestelmät, jotta voidaan varmistaa, että katastrofitilanteissa tai järjestelmän vikaantuessa kaikki oleelliset liiketoimintatiedot ja ohjelmistot voidaan palauttaa.

7.4.8.3 Varmentajan avaimen vaarantuminen

Varmentajan liiketoiminnan jatkuvuussuunnitelma (tai toipumissuunnitelma) kattaa Varmentajan yksityisen avaimen vaarantumiset tai oletetut vaarantumiset, ja niiden varalle on toimintasuunnitelma.

Varmentajan avaimen vaarannuttua toimitaan seuraavasti:

1. Tiedotetaan tapahtuneesta kaikille Varmenteiden tilaajille ja muille tahoille, joiden kanssa Varmentajalla on sopimuksia tai muunlaisia vakiintuneita yhteyksiä, kuten Luottaville tahoille ja muille Varmentajille.

2. Tiedotetaan edellä mainituille tahoille, että Varmenteet ja sulkutiedot, joiden myöntämisessä on käytetty nyt vaarantunutta avainta, eivät ole enää käyttökelpoisia.

7.4.8.4 Algoritmin vaarantuminen

Jos jokin Varmentajan käyttämä algoritmi tai siihen liittyvä parametri osoittautuu liian heikoksi käyttötarkoitukseensa, niin Varmentaja

1. tiedottaa asiasta kaikille Varmenteiden tilaajille ja Luottaville tahoille, joiden kanssa Varmentajalla on sopimuksia tai muunlaisia vakiintuneita yhteyksiä

2. sulkee harkintansa mukaan kaikki Varmenteet, joita vaarantuminen koskee.

7.4.9 Varmentajan toiminnan lopettaminen

Kontrollitavoite: Varmentajan toiminnan loppuessa varmistetaan että Varmentajan avaimen luottamuksellisuus säilyy. Lisäksi Varmentaja varmistaa mahdollisia tulevia viranomaistutkimuksia tai oikeudenkäyntejä varten tarvittavien asiakirjojen ylläpidon jatkumisen.

Varmentaja tekee vähintään seuraavat toimenpiteet ennen toimintansa lopettamista:

1. Varmentaja ilmoittaa toimintansa lopettamisesta seuraaville tahoille: kaikille Varmenteiden tilaajille ja Luottaville tahoille, joiden kanssa Varmentajalla on sopimuksia tai muunlaisia vakiintuneita yhteyksiä. Lisäksi toiminnan loppumisesta ilmoitetaan muille Luottaville tahoille.

2. Varmentaja peruuttaa kaikkien alihankkijoiden valtuudet toimia Varmentajan puolesta Varmenteiden myöntämiseen liittyvissä toiminnoissa.

3. Varmentaja tekee kaikki vaadittavat toimenpiteet siirtääkseen vastuun rekisteröintitietojen ylläpidosta (ks. 7.3.1), Sulkutietopalvelusta (ks. 7.3.6) ja tapahtumalokien arkistoinnista (ks. 7.4.11) ja varmistaakseen niiden saatavuuden Varmenteiden tilaajille ja Luottaville tahoille niin kauan, kuin on alun perin ilmoitettu.

4. Varmentaja tuhoaa tai poistaa käytöstä Yksityisen avaimensa, kuten on määritelty luvussa 7.2.6.

7.4.10 Sovellettava lainsäädäntö

Kontrollitavoite: Varmentaja varmistaa, että sen toiminta on voimassaolevan Suomen lainsäädännön mukaista.

Tähän Varmennepolitiikkaan ja Juurivarmentajan toimintaan sovelletaan Suomen lakia pois luettuna sen lainvalintasäännökset.

7.4.11 Tiedon tallettaminen

Kontrollitavoite: Varmentaja varmistaa, että kaikki Varmenteisiin liittyvä oleellinen tieto pidetään tallessa asianmukaisen ajan.

Varmenteisiin liittyvät tallenteet sisältävät rekisteröintitietoja (ks. 7.3.1) ja Varmentajan ympäristöön, avaintenhallintaan ja Varmenteiden hallintaan liittyviä tapahtumatietoja.

7.4.11.1 Yleiset tiedon tallettamiseen liittyvät asiat

Varmentaja

1. ylläpitää Varmenteisiin liittyvien tallenteiden luottamuksellisuutta ja eheyttä

2. varmistaa, että Varmenteisiin liittyvät tallenteet ovat täydellisiä ja luotettavasti arkistoituja

3. varmistaa Varmenteisiin liittyvien tallenteiden saatavuuden, mikäli ne sisältävät mahdollisia oikeustoimia varten tarvittavaa tietoa

4. tallentaa Varmentajan ympäristön, avainten ja Varmenteiden hallintatapahtumien tarkan kellonajan

5. säilyttää Juurivarmenteisiin liittyviä tallenteita vähintään 10 vuotta Juurivarmentajan toiminnan päättymisestä

6. kirjaa tapahtumat lokiin siten, että lokitietoja ei voi valtuuttamattomasti muuttaa tai tuhota

7. kuvaa dokumentoitavat tapahtumat yleisluontoisesti Varmennekäytännössä

8. varmistaa arkistojen tavoitettavuuden ja lukukelpoisuuden siinäkin tapauksessa, että Varmentajan toiminta keskeytyy tai päättyy

9. suojaa loki- ja arkistotiedot oikeudettomilta katseluilta, muutoksilta ja poistoilta, sekä säilyttää kaikkia varmuuskopioita varmennejärjestelmäympäristöstä erillään vähintään saman turvatason omaavassa paikassa ja testaa niiden käytettävyyttä.

7.4.11.2 Varmentaja

Varmentaja tallentaa toiminnastaan seuraavia tietoja:

1. Varmennepalvelua koskevat sopimukset ja palvelukuvaukset.

2. Tarkastusraportit ja pöytäkirjat, jotka sisältävät tiedot Varmentajan toiminnan tarkastuksista.

3. Voimassa oleva ja aikaisemmin julkaistut Varmennepolitiikat.

4. Sähköinen kirjausketju (audit trail) Varmentajan toiminnasta.

7.4.11.3 Varmennetuotanto

Varmentaja tallentaa varmennejärjestelmää koskevista toimenpiteistä seuraavat tiedot:

1. Varmentajan yksityisen avaimen luontiin ja uusintaan liittyvät tapahtumat, mukaan lukien avainten tiedot.

2. Käyttäjätunnusten luominen.

3. Toimenpidepyynnöt ja niitä koskevat tunnustiedot, pyynnön tyyppi, tieto siitä suoritettiinko toimenpide loppuun saakka vai ei ja mahdollisen keskeytyksen syy.

4. Uusien ohjelmien asennus tai käytössä olevien ohjelmien päivitys.

5. Varmuuskopiointien päiväys, aika ja muut tiedot.

6. Järjestelmän pysäytys- ja uudelleenkäynnistystiedot.

7. Kaikkien laitepäivitysten päivämäärä ja aika.

8. Lokitietojen syntymisen päiväys ja aika.

7.4.11.4 Rekisteröinti

Varmentaja varmistaa, että kaikki rekisteröintiin liittyvät tapahtumat kirjataan lokiin.

7.4.11.5 Varmenteiden luonti

1. Varmentaja kirjaa lokiin kaikki Varmentajan avainten elinkaareen liittyvät tapahtumat.

2. Varmentaja kirjaa lokiin kaikki Varmenteiden elinkaareen liittyvät tapahtumat.

3. Varmentaja kirjaa lokiin myös kaikki HSM-laitteeseen liittyvät tapahtumat.

7.4.11.6 Sulkupalvelun hallinta

Varmentaja varmistaa, että kaikki Sulkupalveluun liittyvät pyynnöt ja raportit, sekä niistä seuraavat toiminnot kirjataan lokiin.

7.5 Asiakirjan hallinta

Tämän Varmennepolitiikan omistaa ja sen ylläpidosta vastaa OP Osuuskunta.

7.5.1 Muutosten hallinta

Tämä asiakirja katselmoidaan vähintään kahden vuoden välein. Asiakirjaa voidaan päivittää, ja muutosten laadusta riippuen niistä tiedotetaan kaikille Varmenteisiin luottaville tahoille seuraavasti.

Luonteeltaan vähäiset muutokset, jotka eivät vaadi ilmoitusta:

- asiakirjan ulkoasu muuttuu
- asiakirjaan tehdään kieliopillisia korjauksia
- asiakirjasta tehdään käännös toiselle kielelle.

Varsinaiseen asiasisältöön vaikuttavat muutokset, jotka vaativat ilmoituksen:

- yhteyshenkilö, muut mainitut yhteystiedot tai informatiiviset verkko-osoitteet muuttuvat
- osapuolten välisiin sopimuksiin vaikuttavista muutoksista ilmoitetaan kyseisten sopimusehtojen mukaisesti
- mitä tahansa Varmennepolitiikan kohtaa voidaan muuttaa saattamalla muutos kaikkien Varmenteisiin luottavien osapuolten tietoon vähintään 60 päivää ennen muutoksen voimaan astumista.

Juurivarmentaja ilmoittaa muutoksista suoraan Alivarmentajille.

Juurivarmentaja voi yksipuolisella päätöksellä korvata tämän politiikan uudella politiikalla.

7.5.2 Versionhallinta

Juurivarmentaja arkistoi kaikki julkaistut ja hyväksytyt Varmennepolitiikat.

Versio	Pvm	Muutokset
1.0	6.2.2013	Ensimmäinen hyväksytty ja julkaistu versio.
2.0	15.9.2014	Päivitetty ja hyväksytty muutokset
3.0	6.3.2017	Päivitetty syksyllä 2016. Hyväksytty julkaistavaksi.

7.5.3 Yhteystiedot

Kysymyksiin Varmennepolitiikasta vastaa Juurivarmentajan yhteyshenkilö.

Postiosoite: OP / Jukka Ikäheimonen, PL 909, 00101 Helsinki

Puhelin: 010 252 010 (Jukka Ikäheimonen)