OP-PALVELUT OY
VARMENNEPOLITIIKKA

OP WS CA

Versio 3.0
Voimassa 3.5.2021 lähtien

OID: 1.3.6.1.4.1.11374.1.2.1.1.1

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.

Tämä Varmennepolitiikka on OP-Palvelut Oy:n laatima säännöstö varmennepalvelun toteuttamiseen ja Varmenteiden myöntämiseen OP Ryhmän Yrityksen pankkiyhteys (Web Services) –kanavan käyttöön.

Tunnistetiedot:

OP-Palvelut Oy, Varmennepolitiikka, OP WS CA versio 3.0

OID: 1.3.6.1.4.1.11374.1.2.1.1.1

1 SOVELTAMISALA

Tämä Varmennepolitiikka koskee OP Ryhmän Varmentajaa OP WS CA (jäljempänä Varmentaja). Lisäksi Varmennepolitiikkaa sovelletaan tämän Varmentajan myöntämien Varmenteiden elinkaaren hallintaan liittyvissä toimissa. Varmennepolitiikka määrittää Varmentajan, Varmenteiden tilaajien, Varmenteisiin Luottavien tahojen sekä muiden Varmenteisiin liittyvien toimijoiden velvollisuudet ja vastuut.

OP WS CA myöntää Varmenteita OP Ryhmän Yrityksen pankkiyhteys (Web Services) –kanavan (jäljempänä WS-kanava) asiakkaille. Asiakkaat voivat myönnettyjen Varmenteiden avulla allekirjoittaa Yrityksen pankkiyhteyskanavan kautta välitettäviä palvelupyyntöjään.

Tämä Varmentaja on OP-Pohjola Root CA:n (jäljempänä Juurivarmentaja) Alivarmentaja. OP WS CA:n toiminnassa noudatetaan Juurivarmentajan Varmennepolitiikan määrittämiä periaatteita, vastuita ja velvollisuuksia.

Luottavien osapuolten tulee aina ennen Varmenteen hyväksymistä tarkastaa, että OP WS CA:n myöntämien Varmenteiden Varmentajien ketju ulottuu tämän Varmennepolitiikan mukaiseen Juurivarmentajaan tai sen yläpuolella olevaan, OP Ryhmän hyväksymään muuhun Juurivarmentajaan. Tämän Varmennepolitiikan mukainen Juurivarmentaja on kuitenkin aina oltava mukana varmennehierarkiassa. Muussa tapauksessa luottavien osapuolten tulee hylätä Varmenne.

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
NIST SP800-57	NIST Special Publication 800-57: Recommendation for Key Management
Juurivarmennepolitiikka	OP Ryhmä, Liiketoimintapalveluiden Juurivarmennepolitiikka OID: 1.3.6.1.4.1.11374.1.1.1.1.3

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.

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.

HSM-laite (Hardware Security Module): Yksityisten avainten suojaamiseen 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 Varmenteen haltija, 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 kuolettamisesta 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 sanoen 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 Juurivarmentajan itsensä allekirjoittama.

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 parametreista.

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 (Certificate 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): Avainparin yksityinen osa, jota käytetään Julkisen avaimen järjestelmässä epäsymmetrisessä salauksessa. 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. Koska X.509 on ITU:n suositus, 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 Varmennepolitiikan mukaisena Varmentajana toimii OP-Palvelut Oy. Varmentajan tehtäviä ovat:

1. Hallinnoida OP-Palvelut Oy WS-kanavan Varmentajaa.
2. Varmentajan varmennepalveluun liittyvän rekisteröintipalvelun toteutus ja hallinto.
3. Varmentaa hyväksymiensä asiakkaiden ja palveluiden 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. Rekisteröijinä toimivat OP Ryhmän toimihenkilöt.

2. Varmennetuotantopalvelut: Varmenteen luominen ja allekirjoittaminen rekisteröintipalveluissa tunnistetun identiteetin ja muiden attribuuttien perusteella. Varmennetuotantopalvelut tuottaa OP-Palvelut Oy.

3. Sulkupalvelu: Sulkupyyntöjen ja niihin liittyvien raporttien käsittely ja päätöksenteko tarvittavista toimenpiteistä. Sulkupalvelua hoitavat Osuuspankin konttorit aukioloaikoinaan sekä 24/7 puhelinpalvelu (ks. 7.5.3).

4. Sulkutietopalvelu: Ilmoitus Luottaville tahoille suljetuista Varmenteista. Sulkutietopalvelu toteutetaan säännöllisin väliajoin julkaistavan Sulkulistan muodossa. Varmentaja voi tarjota myös reaaliaikaista tilatiedon kyselypalvelua (OCSP).

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.

Varmenteen haltija käyttää Yksityistä avainta Varmenteen tilaajan lukuun ja Varmenteen tilaajan vastuulla. Jokainen Varmenteen haltija nimetään yksilöllisesti. Nimestä ei kuitenkaan käy ilmi tietoja, jotka voisivat yksilöidä Varmenteen haltijan OP Ryhmän ulkopuolisille tahoille.

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.

Tämä Varmennepolitiikka noudattaa OP Ryhmän Juurivarmentajan politiikkaa.

Tämän Varmennepolitiikan tunniste (OID) on 1.3.6.1.4.1.11374.1.2.1.1.1.

Juurivarmentajan Varmennepolitiikan tunniste (OID) on 1.3.6.1.4.1.11374.1.1.1.1.3.

5.3 Varmenteiden käyttöala

Tämän Varmennepolitiikan mukaan myönnettyjä Varmenteita voidaan käyttää varmistamaan tiedon alkuperä ja eheys WS-kanavan ja sen asiakkaiden välisessä asioinnissa. OP WS CA voi myöntää varmenteita myös OCSP-vastausten allekirjoittamiseen.

Varmenteiden käyttö muihin tarkoituksiin on kielletty.

Varmenteiden myöntäjäksi merkitään OP-Pohjola WS CA tai OP WS CA V2. Varmentajan nimen versionumeroa kasvatetaan Varmentajan avaimen uusimisen yhteydessä. OP-Pohjola WS CA –nimi korvautuu OP WS CA V2 –nimellä ensimmäisen avaimenvaihdon yhteydessä.

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 tässä asiakirjassa kuvattuun Varmentajan Varmenteeseen liittyvien tahojen on noudatettava tätä Varmennepolitiikkaa ja OP Ryhmän Juurivarmennepolitiikkaa.

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 Varmentajan velvollisuudet

1. Varmentajan velvollisuus on huolehtia siitä, että kaikki luvussa 7 kirjatut vaatimukset toteutetaan tämän Varmennepolitiikan mukaisesti.

2. Varmentaja on velvollinen varmistamaan, että kaikki sen tarjoamat varmennepalvelut (ks. 4.2) ovat voimassa olevan Varmennekäytännön mukaisia.

3. Varmentaja on velvollinen hyväksyttämään Varmennepolitiikkansa ja Varmennekäytäntönsä Juurivarmentajalla ja päivittämään niitä viipymättä, mikäli Varmentajan toiminnassa tapahtuu sellaisia muutoksia, jotka edellyttävät kyseisten asiakirjojen muuttamista tai mikäli Juurivarmentajan Varmennepolitiikkaan tai Varmennekäytäntöön tulee sellaisia muutoksia, jotka edellyttävät Varmentajan vastaavien menettelytapojen tai asiakirjojen muuttamista.

6.2 Varmenteen tilaajan velvollisuudet

Varmenteen tilaaja ja haltija voivat olla samoja. Varmenteen tilaaja on vastuussa myös Varmenteen haltijan velvoitteista. Varmentaja sitoo sopimuksella Varmenteen tilaajan noudattamaan seuraavia ehtoja:

1. Virheettömät ja täydelliset tiedot: Tilaaja on velvollinen toimittamaan varmennehakemuksen yhteydessä pyydetyt tiedot virheettöminä.

2. Varmenteiden käyttö: Tilaaja on velvollinen noudattamaan luvun 5.3 rajoitteita Varmenteiden käytössä.

3. Huolellisuus: Varmenteen haltija on velvollinen käsittelemään Yksityistä avaintaan huolellisesti.

4. Avainten luonti: Varmenteen haltija on velvollinen luomaan Avainparinsa algoritmilla, jonka yleisesti (esimerkiksi standardin NIST SP800-57 mukaan) katsotaan olevan riittävän vahva tässä Varmennepolitiikassa määriteltyihin Varmenteen käyttötarkoituksiin.

5. Avaimen pituus: Varmenteen haltija on velvollinen valitsemaan avainparin pituudeksi 2048 bittiä.

6. Avainten pääsynhallinta: Tilaajalla on velvollisuus varmistaa, ettei muilla kuin Varmenteen haltijalla ole mahdollisuutta käyttää Varmenteen Yksityistä avainta.

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

    i. Varmenteen haltijan Yksityinen avain tuhoutuu, katoaa, varastetaan tai sen luotettavuus vaarantuu muulla tavoin tai avain tulee muuten käyttökelvottomaksi.

    ii. Varmenteen sisällössä havaitaan epäkohtia tai muutostarpeita.

    iii. Varmenteen myöntämisen edellytykset ovat muuttuneet.

8. Tilaajalla on velvollisuus ilmoittaa WS-kanavan käyttäjätunnuksensa ja/tai Varmenteensa sarjanumero tehdessään Varmenteen sulkuilmoituksen. Näiden tietojen ilmoittaminen on Varmenteen sulkemisen edellytys.

6.3 Rekisteröijän velvollisuudet

Varmennepolitiikan mukaisia Varmenteita myöntävän Rekisteröijän velvollisuuksia ovat:

1. Tarkastaa Tilaajan henkilöllisyys ja valtuutus toimia edustamansa yrityksen nimissä.

2. Tilaajan sopimuksen solmiminen Tilaajan ja pankin välillä sekä sopimuksen arkistointi.

3. Varmenteen hakemisessa tarvittavien siirtoavainten toimitus Tilaajalle.

4. Tarvittavan dokumentaation toimittaminen Tilaajalle.

Lisäksi teknisen varmennepyynnön vastaanottavan järjestelmän on varmistettava, että Tilaajan varmennepyynnön allekirjoitus on tehty Varmenteen haltijan Yksityisellä avaimella ja että siirtoavain täsmää rekisteröijän toimittamaan siirtoavaimeen.

6.4 Varmenteeseen luottavien tahojen velvollisuudet

Luottamalla Varmenteeseen Luottava taho ilmaisee hyväksyneensä tämän Varmennepolitiikan ehdot.

Varmenteeseen Luottavan tahon velvollisuutena on koko Varmenneketjun osalta tarkastaa ennen Varmenteen hyväksymistä:

1. Varmenteiden voimassaolo.

2. Mahdolliset sulkemiset ja käytön estot Sulkutietopalvelusta sekä varmistaa sulkutiedon oikeellisuus ja eheys.

3. Varmenteen käyttötapaus vastaa Varmenteessa ilmoitettuja Varmenteen käyttötarkoituksia.

4. Varmenteen käyttötarkoitus vastaa tässä Varmennepolitiikassa määriteltyjä käyttötarkoituksia (ks. kohta 5.3). Lisäksi on arvioitava, soveltuuko Varmennepolitiikassa kuvattu Varmentajan tarjoama luottamustaso Luottavan tahon tarkoituksiin.

5. Että kaikkia varotoimenpiteitä, jotka on mainittu sopimuksissa tai muissa Varmenteeseen liittyvissä asiakirjoissa, noudatetaan.

6.5 Varmentajan vastuut

1. Varmentaja vastaa sekä Juurivarmentajan että tämän Varmennepolitiikan kuvaamien menettelyjen ja toimintatapojen noudattamisesta Varmennepalveluissaan, ellei noudattamatta jättäminen johdu ylivoimaisesta esteestä.

2. Varmentaja vastaa kaikista Yksityisellä avaimellaan tehdyistä toimista.

3. Varmentaja vastaa myöntämiensä Varmenteiden tilaajien tunnistamisesta ja valtuutuksen varmistamisesta. Kyseisiä tehtäviä hoitavat Varmentajan valtuuttamat Rekisteröijät.

4. Varmentaja vastaa siitä, että sen tarjoamat varmennepalvelut (ks. 4.2) noudattavat tätä Varmennepolitiikkaa.

5. Varmentaja ei ole millään tavalla vastuussa vahingoista, jotka aiheutuvat sen myöntämien Varmenteiden käytöstä, elleivät vahingot johdu siitä, että Varmentaja olisi toiminut tämän Varmennepolitiikan vastaisesti

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

6.6 Tilaajan vastuut

1. Tilaaja vastaa Yksityisen avaimensa käytöstä ja suojauksesta Varmenteen voimassaolon loppuun asti.

2. Tilaajan vastuu Yksityisen avaimen käytöstä kuitenkin päättyy, kun Varmentaja on vastaanottanut Varmenteesta sulkuilmoituksen.

6.7 Varmenteeseen luottavien tahojen vastuut

Luottamalla Varmenteeseen Luottava taho ilmaisee hyväksyneensä tämän Varmennepolitiikan ehdot.

1. Varmenteeseen luottavan tahon vastuulla on Varmenneketjun tarkastaminen.

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

6.8 Rekisteröijän vastuut

1. Rekisteröijä vastaa siitä, että Varmenteen tilaaja ja haltija on tunnistettu riittävällä huolellisuudella ja että Tilaajan edustajalla on valtuus toimia asiakkaan nimissä.

2. Rekisteröijä vastaa rekisteröintitapahtuman tietojen säilytyksestä ja arkistoinnista.

7 VARMENTAJAN NOUDATTAMAT KÄYTÄNNÖT

Myönnettäessä Varmenteita tämän Varmennepolitiikan mukaisesti, noudatetaan tässä kappaleessa esitettyjä menettelytapoja.

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 hyväksyy Varmennepolitiikan ja Varmennekäytännön.

4. Varmentaja katselmoi Varmennekäytännön säännöllisesti ja päättää tarvittavista toimenpiteistä, kuten esimerkiksi auditointien suorittamisesta.

5. Varmennekäytäntö ei ole julkinen asiakirja.

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 tehtävään nimetyt henkilöt (ks. luku 7.4.3) kaksoiskäyttömenettelyä noudattaen. Tarkemmat menettelyt on kuvattu Varmennekäytännössä.

2. Varmentajan avaimet luodaan HSM-laitteessa, joka on validoitu vähintään FIPS 140-2 tasolle 3 ja konfiguroitu tason 3 vaatimusten mukaisesti.

3. 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 suositusten mukaisia. Yksityiskohtaisemmat kuvaukset löytyvät Varmennekäytännöstä.

4. Varmentajan avainoperaatioihin osallistuva henkilöstö on luetteloitu ja heille on määritelty nimetyt, luotetut roolit (ks. luku 7.4.3). Lisäksi kaikki avainoperaatioiden tehtävät suoritetaan aina kaksoiskäyttömenettelyä noudattaen pois lukien Varmenteiden ja Sulkulistojen allekirjoitus varmennejärjestelmän sisäisenä toimintona sekä Varmentajan yksityisen avaimen aktivointi. Varmentajan yksityiseen avaimeen ja sen laiteympäristöön liittyvät toiminnot kirjataan aina lokiin.

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

6. Ennen Varmentajan yksityisen avaimen vanhenemista Varmentaja luo uuden Varmenteen 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 ainoastaan OP-palvelut Oy:n CA-palvelun 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.

Varmentajan Varmenne on asiakkaiden saatavilla WS-kanavan kautta. Varmentajan Varmenne sekä Juurivarmentajan Varmenne julkaistaan osoitteessa: https://www.op.fi/varmennepalvelu

7.2.4 Key escrow

Key escrow ei ole käytössä Varmentajan eikä Varmenteen haltijoiden Yksityisille avaimille.

7.2.5 Varmentajan avainten käyttö

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

1. Varmentajan yksityistä avainta käytetään ainoastaan WS-kanavan asiakkaiden Varmenteiden ja Varmenteita sisältävien Sulkulistojen allekirjoitukseen sekä OCSP-Varmenteiden myöntämiseen.

2. Varmentajan yksityisiä avaimia käytetään vain fyysisesti turvallisessa tilassa ja HSM-laitteessa.

3. Varmentajan avaimen aktivointitiedot ovat luotetussa roolissa olevan henkilön kontrollissa.

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 7.2.1. alakohta 2).

2. HSM-laite suojataan luvattomalta käsittelyltä varastoinnin aikana.

3. HSM-laitteen käyttöönottoon ja alustukseen 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 haltijan yksityinen avain on vain sen itsensä hallinnassa.

1. Varmentaja ei koskaan säilytä Varmenteen haltijoiden Yksityisiä avaimia (Ks. Kappale 7.2.4).

2. Varmenteen haltija generoi itse Varmenteen Avainparin.

7.2.9 Varmenteen haltijan Yksityisten avainten elinkaaren hallinta

Varmentajan toiminnassa ei käsitellä Varmenteen haltijoiden Yksityisiä avaimia.

7.3 Varmenteiden elinkaaren hallinta

7.3.1 Varmenteen tilaajan rekisteröinti

Kontrollitavoite: Varmentaja varmistaa, että Varmenteen tilaajan nimi ja muut tiedot on annettu oikein. Lisäksi Varmentaja varmistaa, että varmennepyynnöt ovat virheettömiä, valtuutettuja ja perusteellisia.

1. Rekisteröijä varmistaa, että Tilaajan edustaja on tunnistettu riittävällä huolellisuudella sekä sen, että Tilaajan edustajalla on oikeus toimia Tilaajan nimissä. Rekisteröinnin yhteydessä Rekisteröijä tallentaa Tilaajan ja Tilaajan edustajan tiedot sekä asiakirjojen todentamistiedot OP Ryhmän ohjeiden mukaisesti.

2. Tilaaja hyväksyy tilaajasopimuksen ja mahdolliset muut asiaan liittyvät palvelusopimukset.

3. Rekisteröijä arkistoi Tilaajan kanssa allekirjoitetun sopimuksen.

4. Rekisteröijä luovuttaa Tilaajan edustajalle Varmenteen teknisessä rekisteröinnissä tarvittavan kertakäyttöisen jaetun salaisuuden ensimmäisen osan.

5. Rekisteröintipalvelun järjestelmä lähettää jaetun salaisuuden toisen osan Tilaajan edustajan ilmoittamaan postiosoitteeseen, SMS-numeroon tai välittää sen suojatulla sähköpostilla.

6. Tilaaja lähettää teknisen varmennepyynnön WS-kanavan rekisteröintipalvelun järjestelmään, joka tunnistaa Tilaajan jaetun salaisuuden perusteella.

7. Rekisteröintipalvelun järjestelmä pyytää Varmennetta CA:lta ja toimittaa myönnetyn Varmenteen Tilaajalle.

8. Varmentaja säilyttää rekisteröintitietoja kymmenen vuotta rekisteröintitapahtumasta.

7.3.2 Varmenteiden uusiminen, päivitys ja avainten uusiminen

Uuden Varmenteen luonti edellyttää aina uuden Avainparin luontia. Myöskään Varmenteen päivitys ilman uuden Avainparin luontia ei ole mahdollista.

Varmenne voidaan uusia ilman tilaajasopimuksen uusimista ja henkilökohtaista tunnistusta niin kauan kuin vanha Varmenne on voimassa. Tällöin uusi varmennepyyntö allekirjoitetaan voimassa olevalla Yksityisellä avaimella. Varmenteen tilaaja voidaan tunnistaa myös muulla Varmentajan hyväksymällä luotettavalla menetelmällä. Muissa tapauksissa Tilaaja on aina tunnistettava henkilökohtaisesti ennen Varmenteen myöntämistä.

7.3.3 Varmenteiden luominen

Kontrollitavoite: Varmentaja varmistaa, että Varmenteiden myöntöprosessi on turvallinen, jotta Varmenteiden luotettavuus säilyy. Myöntöprosessi pitää sisällään seuraavia varmistuksia.

1. Tämän Varmentajan myöntämissä Varmenteissa käytetään ainoastaan yksikäsitteisiä sarjanumeroita ja Varmenteen haltijaan on liitetty yksiselitteinen yksilöivä tieto.

2. Varmentaja varmistaa, että Varmenteiden tietosisältö vastaa rekisteröinnin yhteydessä saatuja tietoja.

3. Varmennepyynnön yhteydessä Tilaaja osoittaa Varmentajan hyväksymällä menetelmällä, että sillä on hallinnassaan varmennepyyntöön liittyvää Julkista avainta vastaava Yksityinen avain.

4. Varmennejärjestelmä huolehtii Varmenteiden yhdenmukaisuudesta niiden kulloisenkin käyttötarkoituksen mukaisesti.

5. Myönnetyt Varmenteet ovat voimassa korkeintaan kaksi vuotta.

6. Varmenteiden myöntöprosessin voivat käynnistää ainoastaan valtuutetut Rekisteröijät, jotka tunnistetaan ennen Varmenteen luomista.

7. Varmentajan myöntämien Varmenteiden tietosisältö on kuvattu Varmennekäytännössä.

8. Rekisteröintitietojen eheys on suojattu, kun tietoja toimitetaan Varmenteen tilaajalle/haltijalle, tai siirretään Varmentajan tietojärjestelmien välillä.

7.3.4 Yleisten ehtojen jakelu

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

1. Tämä Varmennepolitiikka ja Juurivarmentajan Varmennepolitiikka ovat Tilaajan saatavilla osoitteessa: https://www.op.fi/varmennepalvelu

2. Tilaajan vastuut ja velvollisuudet on määritelty Varmenteen tilaajan sopimuksessa tämän Varmennepolitiikan mukaisesti.

7.3.5 Varmenteiden jakelu

Varmentaja ei julkaise Varmenteen haltijoiden Varmenteita.

Varmenteet toimitetaan Tilaajille WS-kanavan kautta.

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. Varmenteen sulkupyynnön voi tehdä Varmenteen haltija, Varmenteen tilaaja, Varmenteen tilaajan edustaja tai Varmentaja.

2. Varmenteiden sulkupyyntöjä voi tehdä pankin konttorissa henkilökohtaisesti tai puhelimitse tai soittamalla Sulkupalveluun.

3. Sulkupyynnön tekijän on sulkupyyntöä tehdessään ilmoitettava nimensä, edustamansa yritys ja puhelinnumeronsa sekä suljettavan varmenteen sarjanumero tai Yrityksen pankkiyhteys -kanavan käyttäjätunnus. Sulkupyyntö katsotaan vastaanotetuksi vain, jos nämä tiedot on ilmoitettu.

4. Sulkutieto on kaikkien Luottavien tahojen käytettävissä Sulkutietopalvelussa.

5. Sulkupalvelu käsittelee sulkupyynnöt viivyttelemättä.

6. Sulkupyynnöt todennetaan Varmennekäytännön mukaisesti.

7. Varmentaja voi tarjota myös mahdollisuuden Varmenteiden väliaikaiselle sululle (suspend). Varmentaja kuvaa Varmennekäytännössä tähän liittyvät menettelyt.

8. Kun Varmenne on lopullisesti suljettu (revoked), sitä ei voida enää palauttaa käyttöön.

7.3.6.2 Sulkutieto

1. Käytettäessä Sulkulistoja sulkutiedon välitykseen

   i. Sulkulistan voimassaoloaika on kolme vuorokautta ja se julkaistaan vähintään kerran vuorokaudessa sekä aina kun Varmenne suljetaan

   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.

4. Varmentaja tekee parhaansa pitääkseen Sulkutietopalvelun toimintakatkot Varmennekäytännössä kuvatuissa rajoissa.

5. 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 varmistaa, että sen tietoaineistot ja tiedot ovat asianmukaisesti luokiteltuja.

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

Rekisteröinti, sulkupalveluoperaattorina toimiminen, varmennejärjestelmien ylläpitotehtävät sekä Varmentajan hallinnolliset tehtävät ovat Varmentajan luotettuja tehtäviä.

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

2. Roolit, joiden haltijat suorittavat luotettuja tehtäviä, määritellään tarkemmin Varmennekäytännössä.

3. Luotettuja tehtäviä hoitaviin rooleihin 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 Suomen lain ja viranomaismääräysten sallimissa rajoissa.

4. Varmentajan luotetuissa tehtävissä toimivat henkilöt ovat koulutettuja tehtäviinsä ja he ovat perehtyneet henkilöstön turvamenettelyihin turvallisuusvastuita sisältävissä tehtävissä. Lisäksi heillä on riittävästi kokemusta tietoturvasta ja riskien arvioinnista.

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

2. Pääsy Varmentajan laitteistoon estetään valtuuttamattomilta henkilöiltä.

3. Kaikissa Varmentajan HSM-laitteistoon kohdistuvissa toimenpiteissä noudatetaan kaksoiskäyttömenettelyä lukuun ottamatta Varmentajan yksityisen avaimen aktivointia.

4. HSM-laitteen ollessa varastoituna varastointitilan pääsynvalvonta on kaksoiskäytön piirissä.

5. Kaikki Varmentajan laitteistoon liittyvät toimenpiteet dokumentoidaan.

7.4.4.2 Varmennetuotanto ja sulkutapahtumien hallinta

1. Tilat, joissa tehdään Varmenteen luomiseen tai sulkemisen hallintaan liittyviä tehtäviä tai joissa sijaitsee Varmentajan laitteistoja, on suojattu fyysisesti mm. kulunvalvonnalla niin, ettei järjestelmiin tai tietoihin ole luvatonta pääsyä.

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

3. 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.

4. 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

Kaikkia varmennejärjestelmään liitettyjä työasemia, palvelimia ja muita järjestelmän osia, jotka vaikuttavat toimintoihin, joilla tämän Varmennepolitiikan mukaisia Varmenteita myönnetään, julkaistaan ja saatetaan Sulkulistalle, koskevat seuraavat periaatteet ympäristön ollessa käytössä:

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

2. Varmentaja suojaa varmennejärjestelmään liittyvän tietoliikenneverkon luvattomalta pääsyltä, haittaohjelmilta, hyökkäyksiltä ja valtuuttamattomilta muutoksilta.

3. Varmentaja seuraa järjestelmien lokeja poikkeamien havaitsemiseksi.

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

5. Varmentaja monitoroi järjestelmää jatkuvasti sen kapasiteetin ja toimintavarmuuden varmistamiseksi.

6. Varmentaja suojaa käyttämänsä tallennusvälineet vahingon, varkauden ja luvattoman käytön varalta.

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

8. 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. luku 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, jotta poikkeamien vaikutuksia voidaan rajoittaa.

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, joiden avulla pääsee Varmenteiden hallinnalle kriittisiin sovelluksiin.

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

7.4.6.2 Varmenteiden luonti

Laitteiden konfiguraatio dokumentoidaan ja se on todennettavissa auditoinnin yhteydessä.

7.4.6.3 Sulkutieto

Sulkutietojen muokkausoikeudet on rajoitettu pääsynhallinnalla. Sulkutietokyselyihin ei kuitenkaan tarvita erillisiä pääsyoikeuksia.

7.4.7 Luotettavien järjestelmien käyttö ja ylläpito

Kontrollitavoite: Varmentaja käyttää luotettavia järjestelmiä ja tuotteita, jotka on suojattu 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 jatkuvuussuunnitelma, jota ylläpidetään ja testataan 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, Juurivarmentajalle ja muille Varmentajille.

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

3. Varmentaja toimittaa oman Varmenteensa sulkupyynnön Juurivarmentajalle

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, Juurivarmentajalle 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 vähintään 60 päivää ennen lakkauttamisen ajankohtaa seuraaville tahoille: kaikille Varmenteiden tilaajille ja Luottaville tahoille, joiden kanssa Varmentajalla on sopimuksia tai muunlaisia vakiintuneita yhteyksiä. Lisäksi toiminnan loppumisesta ilmoitetaan Juurivarmentajalle.

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) 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.

5. Varmentaja pyytää Varmenteensa sulkemista Juurivarmentajalta, mikäli Varmentajan toiminta lopetetaan ennen Varmentajan Varmenteen voimassaolon päättymistä.

7.4.10 Sovellettava lainsäädäntö

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

Tähän Varmennepolitiikkaan ja Varmentajan 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 Varmenteisiin liittyviä tallenteita vähintään 10 vuotta tallenteen syntymästä

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 Varmennepolitiikka 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-Palvelut Oy.

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.

Kaikki ilmoitusta vaativat muutokset julkaistaan osoitteessa: https://www.op.fi/varmennepalvelu

Varmentaja voi yksipuolisella päätöksellä korvata tämän politiikan uudella politiikalla.

7.5.2 Versionhallinta

Varmentaja arkistoi kaikki julkaistut ja hyväksytyt Varmennepolitiikat.

Versio	Pvm	Muutokset
1.0	9.4.2013	Ensimmäinen hyväksytty ja julkaistava versio
2.0	6.3.2017	Päivitetty syksyllä 2016. Hyväksytty julkaistavaksi
3.0	3.5.2021	Päivitetty ja hyväksytty julkaistavaksi.

7.5.3 Yhteystiedot

Ympärivuorokautisen sulkupalvelun puhelinnumero: 010 252 8470

Kysymyksiin Varmennepolitiikasta vastaa Varmentajan yhteyshenkilö.

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

Puhelin: 010 252 010 (Jukka Ikäheimonen)