Väestörekisterikeskus
Befolkningsregistercentralen

Varmennuskäytäntö terveydenhuollon ammattivarmennetta varten

OID: 1.2.246.517.1.10.7.1

SERTIFIOITU inspecta ORGANISAATIO ISO 9001

SERTIFIOITU inspecta ORGANISAATIO ISO/IEC 27001

Versiohistoria

Versio	Tekijä	Muutos	Päiväys
Versio 1.0	VRK	Hyväksytty versio 1.0	01.12.2010
Versio 1.1	VRK	Toimitukselliset muutokset	01.05.2011
Versio 1.2	VRK	ETSI TS 101 456 -varmennepolitiikkastandardin mukaisuus.	01.03.2012

Sisältö

1. Johdanto 8
1.1. Taustaa 8
1.2. Varmennuskäytännön tunnukset 9
1.3. Osapuolet ja soveltuvuus 9
1.3.1. Varmentaja 9
1.3.2. Rekisteröijä 10
1.3.3. Varmenteen haltija 11
1.3.4. Varmenteeseen luottava osapuoli 11
1.3.5. Muut osapuolet 11
1.4. Varmenteen käyttökohteet 11
1.4.1. Sallitut varmenteen käyttötarkoitukset 11
1.4.2. Kielletyt varmenteen käyttötarkoitukset 12
1.5. Yhteystiedot 12
1.5.1. Varmennuskäytännön hallintaorganisaatio 12
1.5.2. Yhteystiedot 12
1.5.3. Varmennuskäytäntöjen suhde varmennepolitiikkaan 12
1.5.4. Varmennuskäytäntöjen hyväksymismenettely 12
1.6. Määritelmät ja lyhenteet 12
2. Tietojen julkaiseminen 18
2.1. Julkinen hakemisto 18
2.2. Varmentajan julkaisemat tiedot 18
2.3. Julkaisutiheys 18
2.4. Pääsyoikeudet 18
3. Tunnistaminen ja todentaminen 19
3.1. Varmenteen haltijan nimeäminen 19
3.1.1. Nimeäminen 19
3.1.2. Nimeämisen merkitys 19
3.1.3. Anonyymit tai salanimet 19
3.1.4. Nimikenttien sisältö 19
3.1.5. Nimitietueen ainutkertaisuus 19
3.1.6. Tuotenimien käyttöoikeus 19
3.2. Henkilöllisyyden todentaminen 19
3.2.1. Menettelytapa yksityisen avaimen omistajuuden todistamiseksi 19
3.2.2. Varmenteen hakijan edustaman organisaation todentaminen 19
3.2.3. Henkilön tunnistaminen ja voimassaolevan ammattioikeuden todentaminen 20
3.2.4. Varmenteen hakijan tiedot, joita varmentaja ei tarkista 20
3.2.5. Varmenteen myöntämisen edellytykset 20
3.2.6. Varmentajien välisen yhteistyön edellytykset ja vaatimukset 20
3.3. Tunnistaminen ja todentaminen varmenteen uusimisessa 20
3.3.1. Tunnistaminen ja todentaminen varmenteen uusimisessa 20
3.3.2. Tunnistaminen ja todentaminen varmenteen sulkemisen jälkeen 20
3.4. Peruuttamispyynnön tekijän tunnistaminen 20
4. Varmenteen elinkaaren hallinnan toiminnalliset vaatimukset 22
4.1. Varmenteen hakeminen 22
4.1.1. Kuka voi tehdä varmennehakemuksen 22
4.1.2. Varmenteen myöntämisprosessi ja vastuut 22
4.2. Varmennehakemuksen käsittely 22
4.2.1. Tunnistamisen ja todentamisen toteuttaminen 22
4.2.2. Varmennehakemuksen hyväksyminen tai hylkääminen 23
4.2.3. Varmennehakemuksen käsittelyaika 23

4.3. Varmenteen myöntäminen 23
4.3.1. Varmenteen myöntämiseen liittyvät varmentajan tehtävät 23
4.3.2. Ilmoitus hakijalle varmenteen myöntämisestä 23
4.4. Myönnetyn varmenteen hyväksyminen 23
4.4.1. Myönnetyn varmenteen hyväksymismenettely varmenteen hakijan kannalta 23
4.4.2. Varmenteen julkaisu varmentajan toimesta 23
4.4.3. Ilmoitus muille osapuolille varmenteen myöntämisestä 23
4.5. Varmenteiden ja avainparien käyttö 24
4.5.1. Varmenteiden ja avainparien käyttö varmenteen haltijan toimesta 24
4.5.2. Varmenteiden ja julkisten avainten käyttö varmenteisiin luottavan osapuolen toimesta 24
4.6. Julkisen avaimen uudelleen varmentaminen 25
4.7. Varmenteen uusiminen 25
4.7.1. Varmenteen uusimisen syyt 25
4.7.2. Varmenteen uusimisen hakeminen 25
4.7.3. Varmenteen uusimispyynnön käsittely 25
4.7.4. Ilmoitus varmenteen hakijalle ammattikortin uusimisesta 25
4.7.5. Uusitun varmenteen hyväksymismenettely varmenteen haltijan kannalta 25
4.7.6. Uusitun varmenteen julkaisu 26
4.7.7. Ilmoitus uusitun varmenteen myöntämisestä muille osapuolille 26
4.8. Varmenteen muuttaminen 26
4.9. Varmenteen sulkeminen ja määräaikainen sulkeminen 26
4.9.1. Varmenteen sulkemisen edellytykset 26
4.9.2. Kuka voi vaatia varmenteen sulkemista 26
4.9.3. Varmenteen sulkemisprosessi 27
4.9.4. Varmenteen haltijan velvollisuus tehdä sulkupyyntö 27
4.9.5. Varmenteen sulkupyynnön käsittelyaika 27
4.9.6. Varmenteeseen luottavan osapuolen velvollisuus tarkistaa varmenteen voimassaolo 27
4.9.7. Sulkulistan julkaisutiheys 28
4.9.8. Sulkulistan voimassaolon enimmäisaika 28
4.9.9. Reaaliaikainen varmenteen tilan tarkistaminen 28
4.9.10. Vaatimukset varmenteen tilan reaaliaikaiselle tarkistamiselle 28
4.9.11. Muut varmenteen tilan tarkistamismenettelyt 28
4.9.12. Yksityisen avaimen paljastumisesta johtuva varmenteen sulkeminen 28
4.9.13. Varmenteen sulkeminen määräajaksi 28
4.9.14. Kuka voi vaatia varmenteen sulkemista määräajaksi 28
4.9.15. Menettelytavat varmenteen sulkemiseksi määräajaksi 28
4.9.16. Rajoitukset varmenteen määräaikaiselle sulkemiselle 28
4.10. Varmenteen tilan tarkistamismahdollisuus 28
4.11. Varmenteen voimassaolon päättyminen 29
4.12. Vara-avainjärjestelmä ja avainten palautus 29
5. Fyysisen, käyttö- ja henkilöstöturvallisuuden hallinta 30
5.1. Fyysisen turvallisuuden hallinta 30
5.1.1. Tilojen sijoittaminen ja rakenne 30
5.1.2. Fyysinen pääsynvalvonta 30
5.1.3. Sähkö ja ilmastointi 30
5.1.4. Vesivahinko 30
5.1.5. Tulipalo 30
5.1.6. Tietovälineiden säilytys 30
5.1.7. Tietovälineiden hävittäminen 30
5.1.8. Varmuuskopiointi verkon yli 31
5.2. Käyttöturvallisuuden hallinta 31
5.2.1. Työtehtäviin liittyvät roolit 31

5.2.2. Varmennetuotannon työtehtäviin tarvittavien henkilöiden määrä 31
5.2.3. Henkilöiden tunnistaminen ja todentaminen eri rooleihin 31
5.2.4. Tehtävien eriyttämistä vaativat roolit 31
5.3. Henkilöstöturvallisuuden hallinta 31
5.3.1. Tausta-, ansio-, kokemus- ja selvitysvaatimukset 31
5.3.2. Taustojen tarkistamisen menettelytapa 32
5.3.3. Koulutuksen tiheys ja vaatimukset 32
5.3.4. Jatkokoulutuksen tiheys ja vaatimukset 32
5.3.5. Työtehtävien kierrätyksen tiheys ja järjestys 32
5.3.6. Seuraukset luvattomista toimista 32
5.3.7. Alihankkijoiden henkilöstön vaatimukset 32
5.3.8. Asiakirjat, jotka toimitetaan henkilökunnalle 32
5.4. Varmennejärjestelmän turvallisuuden seuranta 32
5.4.1. Arkistoitavat tapahtumat 32
5.4.2. Lokitietojen analysointitiheys 33
5.4.3. Lokitietojen säilytysaika 33
5.4.4. Lokitietojen suojaaminen 33
5.4.5. Lokitietojen varmuuskopiointi 33
5.4.6. Lokitietojen keräysjärjestelmän toteuttaminen (sisäinen/ulkoinen) 33
5.4.7. Lokitapahtumasta ilmoittaminen 33
5.4.8. Haavoittuvuuksien arviointi 33
5.5. Arkistoitavat aineistot 33
5.5.1. Arkistoitavat asiakirjat, tiedostot ja mediat 33
5.5.2. Arkistojen säilytysaika 34
5.5.3. Arkistojen suojaaminen 34
5.5.4. Arkistojen varmuuskopiointimenettely 34
5.5.5. Arkistoitavien tietojen aikaleima 34
5.5.6. Arkistojen keräysjärjestelmä (sisäinen/ulkoinen) 34
5.5.7. Arkistoissa olevien tietojen saatavuus ja eheys 34
5.6. Varmentajan avainparin vaihto 34
5.7. Häiriötilanteisiin varautuminen 34
5.7.1. Suunnitelma toimintahäiriöiden ja toiminnan vaarantumisen varalta 34
5.7.2. Varmennejärjestelmän, ohjelmistojen tai tietojen vahingoittuminen 35
5.7.3. Toiminta varmenteen haltijan yksityisen avaimen paljastuessa 35
5.7.4. Toiminnan jatkuvuus häiriötilanteen jälkeen 35
5.8. Lakkauttaminen 35
5.8.1. Varmentajan toiminnan lakkauttaminen 35
5.8.2. Rekisteröijän toiminnan ja siihen liittyvien oikeuksien lakkauttaminen 35
6. Teknisen turvallisuuden hallinta 36
6.1. Avainparien luonti ja toimittaminen varmenteen haltijalle 36
6.1.1. Avainparien luonti 36
6.1.2. Yksityisen avaimen toimittaminen terveydenhuollon ammattihenkilölle 36
6.1.3. Varmenteen hakijan julkisen avaimen toimittaminen varmentajalle 36
6.1.4. Varmentajan julkisen avaimen toimittaminen luottaville osapuolille 36
6.1.5. Avainten pituus 36
6.1.6. Julkisen avaimen parametrien luonti ja laatu 36
6.1.7. Avainten käyttötarkoitukset 36
6.2. Yksityisen avaimen suojaaminen ja turvalaskentalaitteiston hallinta 37
6.2.1. Käytetyt standardit 37
6.2.2. Yksityinen avain usean henkilön hallinnassa 37
6.2.3. Yksityisten avainten vara-avainjärjestelmä 37
6.2.4. Yksityisen avaimen varmuuskopiointi 37
6.2.5. Yksityisten avainten arkistointi 37
6.2.6. Yksityisten avainten käsittely turvalaskentalaitteistossa 37

6.2.7. Yksityisten avainten säilyttäminen 38
6.2.8. Yksityisten avainten aktivointi 38
6.2.9. Yksityisten avainten käytön estäminen 38
6.2.10. Yksityisen avaimen tuhoaminen 38
6.2.11. Ammattikorttien ja turvalaskentalaitteistojen turvatason luokitus 38
6.3. Muita avainparin hallintaan vaikuttavia seikkoja 38
6.3.1. Julkisten avainten arkistointi 38
6.3.2. Varmenteiden ja avainten voimassaoloaika 39
6.4. Aktivointitiedot 39
6.4.1. Aktivointitiedon luonti 39
6.4.2. Aktivointitiedon suojaus 39
6.4.3. Muita huomioitavia seikkoja aktivointitiedosta 39
6.5. Tietokonelaitteistojen turvallisuuden hallinta 39
6.5.1. Erityisvaatimukset 39
6.5.2. Laitteistoturvallisuuden luokittelu 39
6.6. Elinkaaren turvallisuuden hallinta 39
6.6.1. Järjestelmien kehittämisen hallinta 39
6.6.2. Turvallisuuden hallinta 40
6.6.3. Elinkaaren turvallisuusluokittelu 40
6.7. Tietoverkon turvallisuuden hallinta 40
6.8. Aikaleima 40
7. Varmenteen ja sulkulistan profiili 41
7.1. Varmenteen profiili 41
7.2. Sulkulistan profiili 41
7.3. Reaaliaikainen sulkulistan tarkistus (OCSP) 41
8. Hyväksymistarkastus 42
8.1. Hyväksymistarkastusten suorittaminen 42
8.2. Tarkastaja 42
8.3. Tarkastuksen suorittajan suhde tarkastettavaan osapuoleen 42
8.4. Tarkastuksen kattavuus 42
8.5. Toimenpiteet, joihin ryhdytään poikkeamien esiintyessä 42
8.6. Tarkastuksen tuloksista tiedottaminen 42
9. Yleiset ehdot 43
9.1. Maksut ja muut palkkiot 43
9.1.1. Varmenteen myöntämismaksu 43
9.1.2. Varmenteen käyttömaksu 43
9.1.3. Varmenteen sulkumaksu tai tilan kyselymaksu 43
9.1.4. Maksut muista palveluista kuten neuvontapalvelusta 43
9.1.5. Hyvitykset 43
9.2. Taloudelliset velvollisuudet 43
9.3. Luottamuksellisuus ja tietosuoja 43
9.3.1. Yksityiset tiedot 43
9.3.2. Julkiset tiedot 44
9.3.3. Yksityisten tietojen suojaaminen 44
9.4. Yksityisyyden suoja 44
9.4.1. Yksityisten tietojen suojaamissuunnitelma 44
9.4.2. Varmentajan järjestelmissä käsiteltävät yksityiset tiedot 44
9.4.3. Varmentajan järjestelmissä käsiteltävät julkiset tiedot 44
9.4.4. Vastuu yksityisten tietojen suojaamisesta 44
9.4.5. Yksityisten tietojen käyttäminen tai julkistaminen varmenteen haltijan suostumuksella 44
9.4.6. Tietojen luovutus viranomaisille 44
9.4.7. Muut olosuhteet, joissa tiedot voidaan julkistaa 44
9.5. Immateriaalioikeudet 45

9.6. Osapuolten sitoumukset 45
9.6.1. Varmentajan sitoumukset 45
9.6.2. Rekisteröijän sitoumukset 45
9.6.3. Varmenteen haltijan sitoumukset 45
9.6.4. Varmenteisiin luottavien osapuolten sitoumukset 45
9.6.5. Muiden osapuolten sitoumukset 45
9.7. Vastuuvapauslauseke 45
9.8. Vastuunrajoitukset 45
9.9. Vahingonkorvaukset 46
9.10. Voimassaoloaika ja voimassaolon päättyminen 46
9.10.1. Varmennuskäytännön voimassaoloaika 46
9.10.2. Varmennuskäytännön voimassaolon päättyminen 46
9.10.3. Varmennuskäytännön voimassaolon päättymisen vaikutukset 46
9.11. Varmennepalvelun osapuolien keskinäinen viestintä 46
9.12. Varmennuskäytännön muutosten hallinta 47
9.12.1. Varmennuskäytännön muuttaminen 47
9.12.2. Muutoksista tiedottaminen 47
9.12.3. Varmennuskäytännön tunnistetiedon muuttaminen 47
9.13. Erimielisyyksien ratkaiseminen 47
9.14. Sovellettava laki 47
9.15. Lain noudattaminen 47
9.16. Muut järjestelyt 47
9.16.1. Sopimukset 47
9.16.2. Oikeudenluovutus 48
9.16.3. Pätemättömyys 48
9.16.4. Täytäntöönpano 48
9.16.5. Ylivoimainen este 48
9.17. Muut ehdot 48

1. JOHDANTO

Varmennepolitiikassa määritellään Väestörekisterikeskuksen – jatkossa varmentaja (Certification Authority) – julkisen avaimen menetelmän (Public Key Infrastructure; PKI) mukaisten varmentamistoimintojen edellytykset ja soveltuvuusalue sekä rajaukset. Tässä varmennuskäytännössä määritellään varmennepolitiikan sisältämät periaatteet käytännön tasolla.

Kaikkien tässä varmennuskäytännössä tarkoitettujen osapuolten tulee noudattaa varmennuskäytännön lisäksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007) ja laissa sähköisestä lääkemääräyksestä (61/2007) sekä niiden nojalla annetuissa säädöksissä ja niiden nojalla asetettuja vaatimuksia.

Tämän varmennuskäytännön tarkoituksena on kuvata menetelmät, jotka varmistavat Väestörekisterikeskuksen (jäljempänä VRK) myöntämien varmenteiden luotettavuuden. Tässä varmennuskäytännössä määritellään varmentajan ja varmenteiden käyttäjien toimintatavat ja yleiset turvallisuusvaatimukset, joiden avulla pyritään minimoimaan toiminnalliset, taloudelliset ja juridiset uhat ja riskit, jotka liittyvät julkisen avaimen järjestelmiin.

Varmenne sitoo yhteen julkisen avaimen ja joukon tietoja, jotka yksilöivät kohteen, kuten henkilön, organisaation, sivuston tai laitteen. Varmennetta käyttävät hyväkseen terveydenhuollon ammattihenkilö ja luottava osapuoli, joka luottaa varmenteen paikkansapitävyyteen ja tarvitsee varmennetta esimerkiksi sähköisen allekirjoituksen todentamiseen.

Tämä luku määrittelee varmennuskäytännön ja sen soveltuvuuden. Lisäksi luvussa määritellään varmennuskäytännön hallintaorganisaatio ja sen yhteystiedot.

1.1. Taustaa

VRK myöntää varmenteita terveydenhuollon ammattihenkilöistä annetussa laissa (559/1994) tarkoitetuille terveydenhuollon ammattihenkilöille.

Väestörekisterikeskus tarjoaa tietoturvallisuuden tasoltaan korkealaatuisia sähköisen allekirjoituksen ja tunnistamisen varmenteita ja niihin liittyviä palveluja julkiselle ja yksityiselle sektorille. Varmenteen avulla varmennetaan varmenteen haltijan henkilöllisyys sekä varmenteeseen sisältyvien tietojen oikeellisuus, eheys ja alkuperäisyys. Laatuvarmenteella tehty sähköinen allekirjoitus sekä vahvan sähköisten tunnistamisen välineen avulla tehty henkilön vahva sähköinen tunnistaminen antavat kansalaisille mahdollisuuden turvalliseen, ajasta ja paikasta riippumattomaan ja joustavaan verkkoasiointiin. Laatuvarmenteen ja vahvan sähköisen tunnistuspalvelun tarjoajia valvoo Suomessa Viestintävirasto.

Tämän varmennuskäytännön mukaisesti myönnetyt allekirjoitusvarmenteet täyttävät Euroopan parlamentin ja neuvoston direktiivin 1999/93/EY sähköisiä allekirjoituksia koskevista yhteisön puitteista, jäljempänä sähköallekirjoitusdirektiivin ja sen liitteiden tarkoittamat laatuvarmenteelle asetettavat vaatimukset. Laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009) on säädetty laatuvarmenteella tehdyistä sähköisistä allekirjoituksista.

Väestörekisterikeskus toimii 1.12.2010 alkaen terveydenhuollon lakisääteisenä varmentajana sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007), sähköisestä lääkemääräyksestä annetun lain (61/2007) sekä väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain (661/2009) nojalla.

VRK:n PKI:n perusteiden rakentamisessa on tukeuduttu seuraaviin säädöksiin, standardeihin ja ohjeisiin:

- Laki sähköisestä lääkemääräyksestä (61/2007)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Laki terveydenhuollon ammattihenkilöistä (559/1994)

- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Laki turvallisuusselvityksistä (177/2002)
- IETF RFC 3647 Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework (11/2003)
- IETF RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (4/2002)
- ETSI TS 101 456, v1.4.3: Policy requirements for certification authorities issuing qualified certificates (5/2007)
- ISO/IEC 17090-3: Health informatics - Digital Certificates in Healthcare - Part 3: Policy management of certification authority
- Viestintävirasto 8 C/2010 M - Määräys tunnistuspalvelun tarjoajien ja laatuvarmenteita tarjoavien varmentajien toiminnan luotettavuus- ja tietoturvavaatimuksista (20.10.2010)
- VAHTI 1/2002: Tietoteknisten laitetilojen turvallisuussuositus
- VAHTI 5/2004: Valtionhallinnon keskeisten tietojärjestelmien turvaaminen

Dokumentin tulkinnassa käytetään seuraavia periaatteita:

1. Varmennuskäytännön otsikot ja alaotsikot ovat pääasiassa kansainvälisen standardoinnin [RFC 3647] suomennettuja suosituksia. Dokumenttia tulkittaessa itse teksti on etusijalla otsikoihin nähden.
2. Yleisenä ehtona varmentajalle on tämän varmennuskäytännön kaikkien varmentajaa koskevien vaatimusten täyttäminen.
3. Merkki "—" tarkoittaa, ettei kyseiseen aiheeseen liity lisäehtoja, joita ei olisi muutoin varmennepolitiikassa määritelty.

1.2. Varmennuskäytännön tunnukset

Tämän varmennuskäytännön nimi on Varmennuskäytäntö terveydenhuollon ammattivarmennetta varten, jonka OID on 1.2.246.517.1.10.7.1.

Tämä varmennuskäytäntö viittaa Varmennepolitiikkaan terveydenhuollon ammattivarmennetta varten, OID 1.2.246.517.1.10.7. sekä ammattivarmenteen sisältämän sähköisen allekirjoituksen laatuvarmenteen politiikka-asiakirjan ETSI TS 101 456 mukaiseen laatuvarmennetyyppiin QCP public OID: 0.4.0.1456.1.2.

1.3. Osapuolet ja soveltuvuus

Tämä luku kuvaa osapuolet, jotka tuottavat varmenteita, hyödyntävät varmenteita tai ovat järjestelmän toimittajia.

1.3.1. Varmentaja

Varmentaja täyttää seuraavat ehdot:

- Varmentaja sitoutuu noudattamaan tämän varmennuskäytännön ehtoja.
- Varmentaja laatii varmennepolitiikan ja varmennuskäytännön sekä muita näitä dokumentteja täydentäviä menettelytapaohjeita.

- Varmentaja pitää yllä riittävät taloudelliset valmiudet turvatakseen tässä varmennuskäytännössä määritellyn toiminnan. Varmentaja vastaa varmennetoiminnasta ja siihen liittyvistä riskeistä ja edellyttää varmennejärjestelmän toimittajien suojautuvan toimintaan liittyviltä riskeiltä asianmukaisin riskienhallintakeinoin.
- Varmentaja pitää yllä rekisteriä hyväksymistään rekisteröijistä.
- Varmentaja päättää ristiinvarmentamisesta yhteistyössä toisten varmentajien kanssa.
- Varmentaja vastaa luomiensa avainparien elinkaaresta (luominen, tallennus, varmuuskopiointi, julkaiseminen ja käytöstä poistaminen).

Varmentaja sitoutuu:

1. tarjoamaan varmenne- ja hakemistopalveluja, jotka on määritelty tässä varmennuskäytännössä;
2. tarjoamaan tämän varmennuskäytännön luvuissa 4-6 kuvatut hallinta- ja seurantatoiminnot;
3. velvoittamaan rekisteröintipisteen suorittamaan tunnistamismenettelyn tämän varmennuskäytännön lukujen 3-4 mukaisesti;
4. myöntämään varmenteita yhdenmukaisesti tämän varmennuskäytännön kanssa;
5. noudattamaan voimassaolevia lakeja, asetuksia ja niiden nojalla annettuja määräyksiä ja ohjeita sekä tukemaan varmenteiden käyttäjien ja varmenteisiin luottavien osapuolten oikeuksia;
6. tarjoamaan sulkupalvelun tämän varmennuskäytännön lukujen 3-4 mukaisesti;
7. huolehtimaan siitä, että riittävät ja varmennuskäytännön mukaiset riippumattomat tarkastukset tulevat suoritetuiksi;
8. vastaamaan varmentajan toimivuudesta; ja
9. noudattamaan kaikkia tämän varmennuskäytännön sekä varmennepolitiikan ehtoja.

Varmentaja voi halutessaan tarjota varmennejärjestelmään liittyviä lisätoimintoja tai -palveluja.

Varmentaja vastaa, että varmenteen sisältämä informaatio on tämän varmennuskäytännön mukainen.

Varmentaja tarkastaa ja hyväksyy rekisteröijät sekä niiden henkilökunnan.

1.3.2. Rekisteröijä

Tämän varmennuskäytännön mukaisesti toimivan rekisteröijän on täytettävä seuraavat ehdot:

- Rekisteröijä sitoutuu noudattamaan tämän varmennuskäytännön vaatimuksia.
- Rekisteröijän on oltava varmentajan hyväksymä ja rekisteröimä.
- Rekisteröijä vastaa varmenteiden hakijoiden tunnistamisesta.
- Rekisteröijä vastaa rekisteröintipisteen henkilökunnan luotettavuudesta. Rekisteröijä hankkii palvelukseen otettavan henkilön luotettavuudesta varmentajan edellyttämät selvitykset sekä huolehtii valtuuttamansa henkilökunnan jatkuvasta luotettavuudesta. Varmentaja hyväksyy rekisteröintipisteen henkilökunnan rekisteröijän toimittamien selvitysten perusteella.

Tämän varmennuskäytännön mukaisen rekisteröijän tulee sitoutua:

1. noudattamaan voimassa olevaa lainsäädäntöä ja sen nojalla annettuja määräyksiä ja ohjeita;
2. tarjoamaan tämän varmennuskäytännön luvuissa 4-6 vaaditut hallinta- ja seurantatoiminnot;

3. suorittamaan varmenteen hakijan tunnistamismenettelyn tämän varmennuskäytännön lukujen 3-4;
4. täyttämään sovitut toimeksiannot ja tukemaan varmenteiden käyttäjien ja varmenteisiin luottavien osapuolten oikeuksia; ja
5. noudattamaan kaikkia tämän varmennuskäytännön rekisteröintipalveluun liittyviä ehtoja.

Rekisteröijä voi tarjota varmentajan hyväksymiä lisätoimintoja tai -palveluja.

Rekisteröijä kantaa vastuun kaikista antamistaan rekisteröintipalveluista.

1.3.3. Varmenteen haltija

Terveydenhuollon ammattivarmenteen haltijana voi olla terveydenhuollon ammattihenkilöiden keskusrekisteriin (Terhikki) merkitty terveydenhuollon ammattihenkilö.

Terveydenhuollon ammattihenkilön tulee todistaa henkilöllisyytensä varmennehakemusta tehdessään.

Varmennehakemuksen allekirjoittamalla terveydenhuollon ammattihenkilö sitoutuu noudattamaan varmenteen käyttöehtoja. Voimassaolevat käyttöehdot luovutetaan terveydenhuollon ammattihenkilölle varmenteen luovutuksen yhteydessä.

1.3.4. Varmenteeseen luottava osapuoli

Varmenteeseen luottava osapuoli voi olla sellaisen tietojärjestelmän omistaja, jonka tietojärjestelmän tietoturvamekanismit on rakennettu käyttämään hyväksi terveydenhuollon ammattivarmenteita.

Varmenteeseen luottava osapuoli on velvollinen noudattamaan tämän varmennuskäytännön luottavaa osapuolta koskevia velvoitteita.

Varmenteeseen luottava osapuoli sitoutuu toteuttamaan järjestelmäänsä kaikki varmennepolitiikassa ja varmennuskäytännössä vaadittavat osat (mm. sähköisten allekirjoitusten tarkistus, varmennepolun tarkistus, sulkulistan tarkistus) ja muuttamaan järjestelmänsä varmennepolitiikkaan ja varmennuskäytäntöön tehtävien päivitysten mukaiseksi.

1.3.5. Muut osapuolet

Varmentaja voi halutessaan käyttää varmennepalvelujen tuottamiseen Suomessa toimivia alihankkijoita ja yhteistyökumppaneita.

1.4. Varmenteen käyttökohteet

Tässä luvussa määritellään ne käyttökohteet, joihin varmennetta tyypillisesti käytetään ja joita varmennuskäytäntö tukee. Tämä varmennuskäytäntö koskee varmentajaa, rekisteröijiä, varmenteen haltijoita ja varmenteisiin luottavia osapuolia.

Varmenteiden pääasiallisista käyttökohteista on säädetty laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) ja laissa sähköisestä lääkkeen määräämisestä (61/2007). Lisäksi varmenteita voidaan käyttää terveydenhuollon ja apteekkilaitoksen muissa tietojärjestelmissä.

1.4.1. Sallitut varmenteen käyttötarkoitukset

Ammattivarmenne koostuu varmenneparista, jolla on kaksi toisistaan poikkeavaa käyttötarkoitusta. Todentamis- ja salausvarmenne täyttää vahvan sähköisen tunnistamisvälineen vaatimukset. Yksinomaan allekirjoituksen toteuttamiseen tarkoitettu allekirjoitusvarmenne täyttää laatu-

varmenteen vaatimukset. Varmenteen hakijan henkilöllisyyden oikeellisuuden takaa Väestörekisterikeskus.

Tämä varmennuskäytäntö kuvaa sähköisistä allekirjoituksista annettuun direktiiviin perustuvan, vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain mukaisen sähköisen allekirjoituksen laatuvarmenteen myöntämiseen, tuottamiseen ja vastuun jakoon liittyviä yksityiskohtaisia vaatimuksia.

Tämä asiakirja kuvaa myös ammattivarmenteeseen sisältyvän, vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain mukaisen vahvan sähköisen tunnistamisen välineenä tarjottavan tunnistusvarmenteen myöntämiseen, tuottamiseen ja tietojen tallentamiseen liittyviä ratkaisuja ja menettelytapoja laatuvarmenteen tuotantoympäristön vaatimuksia noudattaen.

1.4.2. Kielletyt varmenteen käyttötarkoitukset

Sosiaali- ja terveysministeriön tekemän päätöksen mukaisesti potilastietojen välittäminen sähköpostitse on kiellettyä. Terveydenhuollon ammattivarmenteiden hyödyntäminen potilastietoja sisältävien sähköpostien salaamisessa tai allekirjoittamisessa ei siten ole sallittua.

1.5. Yhteystiedot

1.5.1. Varmennuskäytännön hallintaorganisaatio

Tämän terveydenhuollon ammattivarmenteen myöntämistä kuvaavan varmennuskäytännön on rekisteröinyt Väestörekisterikeskus.

1.5.2. Yhteystiedot

Varmentajan yhteystiedot:

Väestörekisterikeskus (VRK)	www.fineid.fi
PL 70 (Tynnyrintekijänkatu 1 C)	vaestorekisterikeskus@vrk.fi
00581 Helsinki	Puh. (09) 229 161
Y-tunnus: 0245437-2	Fax. (09) 2291 6795

1.5.3. Varmennuskäytäntöjen suhde varmennepolitiikkaan

Varmennuskäytännöt pidetään varmennepolitiikan mukaisena. Varmennepolitiikan sisältö on aina ensisijaisesti ratkaiseva varmennuskäytäntöön nähden. Varmennepolitiikan ja varmennuskäytännön tarkastusrutiinit määritellään luvussa 8.

1.5.4. Varmennuskäytäntöjen hyväksymismenettely

VRK:n Varmennepalvelut määrittelee ja hyväksyy varmennuskäytäntöasiakirjat.

1.6. Määritelmät ja lyhenteet

Ammattioikeus	Ammattioikeudella tarkoitetaan tässä varmennuskäytännössä niitä rekisteröityjä laillistetun, luvan saaneen ja nimikesuojatun ammattihenkilön sekä terveydenhuollon opiskelijan ammatillisia oikeuksia, jotka henkilö voi saada terveydenhuollon ammattihenkilöistä annetun lain

	(559/1994) 2 §:n nojalla. Ammattioikeus voi olla rajoittamaton, rajoitettu tai kokonaan poistettu. Ammattioikeudet tallennetaan Sosiaali- ja terveysalan lupa- ja valvontaviraston ylläpitämään Terhikki-rekisteriin.
Avaimen palautus *(Key recovery)*	Key recoveryllä tarkoitetaan tilannetta, jossa yksityinen avain palautetaan ammattikortin hajottua tai hävitessä. Terveydenhuollon ammattikorttien yksityisiä avaimia ei voida palauttaa kortin hajottua tai hävitessä.
Avaintenhallinta (Key management)	Avaintenhallinnalla tarkoitetaan varmentajan avainten sekä varmenteen haltijan todentamis- ja allekirjoitusavainten hallintamenettelyjä ja -ratkaisuja niiden elinkaaren ajan. Elinkaaren vaiheita ovat avainten tilaaminen, luominen, jakelu, säilyttäminen, käyttö, sulkeminen, uusiminen, arkistointi ja tuhoaminen.
Eheys (*Integrity*)	1) Tietojen tai tietojärjestelmän aitous, väärentämättömyys, sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus 2) ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.
Julkisen avaimen järjestelmä *(PKI, Public Key Infrastructure)*	Julkisen avaimen järjestelmässä nimetty varmentaja tuottaa käyttäjille avainparit, varmentaa ne digitaalisella allekirjoituksellaan, takaa varmenteen haltijan henkilöllisyyden ja jakaa varmenteet käyttäjille, ylläpitää varmennehakemistoa ja sulkulistaa sekä mahdollisesti antaa muita järjestelmän käyttöön liittyviä palveluja. Julkisen avaimen järjestelmässä kullakin käyttäjällä on kaksi toisiinsa liittyvää avainta. Toinen avainparin avaimista on julkinen, toinen on vain avainparin käyttäjän hallussa oleva yksityinen avain. Yksityisellä avaimella sähköisesti allekirjoitettu tiedon aitous voidaan todentaa vain vastaavalla julkisella avaimella, ja vastaavasti tiedon välittämisessä vastaanottajan julkisella avaimella salattu tieto voidaan muuttaa selväkieliseen muotoon vain vastaanottajan yksityisellä avaimella.
Kiistämättömyys (*Non-repudiation*)	Kiistämättömyys tarkoittaa, että osapuolten osallisuus tapahtumaan tai tekoon voidaan jälkeenpäin todistaa. Kiistämättömyys varmistaa sen, ettei toinen osapuoli voi kieltää toimintaansa, esimerkiksi tekemäänsä sähköistä allekirjoitusta, jälkeenpäin. Kiistämättömyyden tavoitteena on juridinen sitovuus.
Käytettävyys (*Availability*)	Ominaisuus, joka ilmentää sitä, kuinka varmasti järjestelmä, laite, ohjelma tai palvelu on tarvittaessa käytettävissä.

Luottamuksellisuus (*Confidentiality*)	Tieto on vain valtuutettujen henkilöiden, organisaatioiden tai prosessien saatavissa.
Palvelujen antajien henkilötoimija	Terveydenhuollon alalla toimivan palvelujen antajan henkilö, joka ei ole terveydenhuollon ammattihenkilö tai terveydenhuollon muuta henkilöstöä. Kyseiseen henkilöstöryhmään kuuluvat muut valtakunnallisia tietojärjestelmiä käyttävät henkilöt ja erityisryhmät, kuten tietosuojavastaavat sekä tietojärjestelmätoimittajat, konsultit jne.
PIN *(Personal identification number)*	Ammattikortin avainparin käyttöoikeuden varmistamiseksi käytettävä tunnusluku. Terveydenhuollon ammattikortilla on kaksi tunnuslukua, toinen todentamista ja toinen sähköistä allekirjoitusta varten.
Prosessi (Process)	Tapahtumasarja, jolla on tietty suunta, tarkoitus, vaikutus tai tulos, esimerkiksi varmenteen myöntämisprosessi.
PUK (*Pin unblocking key*)	Avaustunnusluku, joka vapauttaa lukkiutuneen ammattikortin PIN-tunnusluvun tilanteessa, jossa PIN-tunnusluku on syötetty väärin liian monta kertaa peräkkäin.
Rekisteröijä *(RA, Registration Authority)*	Julkisen avaimen järjestelmässä luotettu taho, joka varmentajan valtuuttamana ja auditoimana toteuttaa rekisteröijän tehtäviä. Rekisteröijä ylläpitää varmentajan lukuun yhtä tai useampaa rekisteröintipistettä.
Rekisteröintinumero	Rekisteröintinumero on tekninen numerosarja, joka muodostuu kaikille terveydenhuollon ammattihenkilöille, jotka rekisteröityvät tai ovat jo rekisteröityneet terveydenhuollon ammattihenkilöiden keskusrekisteriin, Terhikkiin. Rekisteröintinumeroa käytetään muun muassa ammattihenkilöiden tunnisteena esimerkiksi sähköisissä lääkemääräyksissä.
Rekisteröintipiste	Palvelupiste, jossa tarkistetaan varmenteen hakijan henkilöllisyys ja terveydenhuollon ammattioikeudet ja joka vastaa ammattikorttien, varmenteiden ja PIN-/PUK-tunnuslukujen jakelusta käyttäjille varmennepolitiikan ja varmennuskäytännön mukaisesti.
Sosiaali- ja terveysalan lupa- ja valvontavirasto *(Valvira)*	Valvira on sosiaali- ja terveydenhuollon lupa- ja valvontaviranomainen. Valvira parantaa ohjauksen ja valvonnan keinoin elinympäristön terveysriskien hallintaa sekä oikeusturvan toteutumista ja palvelujen laatua sosiaali- ja terveydenhuollossa. Valviran tehtäviin kuuluu myös ter-

	veydenhuollon laitteiden ja tarvikkeiden vaatimustenmukaisuuden valvonta sekä turvallisen käytön edistäminen.
Sulkulista *(CRL, Certificate Revocation List)*	Sulkulista on luettelo suljetuista varmenteista. Varmenne suljetaan, kun varmenteen haltija pyytää sulkemista, menettää varmenteeseen merkityn ammattioikeuden, ammattikortti ja avaustunnusluku ovat kadonneet tai anastettu tai varmenteen haltija on kuollut.
Sulkupalvelu	Varmentajan palvelu, joka sulkee terveydenhuollon ammattivarmenteita tehtyjen sulkupyyntöjen perusteella.
Terveydenhuollon ammattihenkilö	Terveydenhuollon ammattihenkilöistä annetun lain (559/1994) 2 §:n 1 momentin mukaan terveydenhuollon ammattihenkilöllä tarkoitetaan henkilöä, joka lain nojalla on saanut ammatinharjoittamisoikeuden (laillistettu ammattihenkilö) tai ammatinharjoittamisluvan (luvan saanut ammattihenkilö) sekä henkilöä, jolla lain nojalla on oikeus käyttää asetuksella säädettyä terveydenhuollon ammattihenkilön ammattinimikettä (nimikesuojattu ammattihenkilö). Tässä varmennuskäytännössä terveydenhuollon ammattihenkilöllä tarkoitetaan myös terveydenhuollon ammattihenkilöistä annetun lain 2 §:n 3 momentissa tarkoitettua opiskelijaa.
Terveydenhuollon ammattikortti	Terveydenhuollon ammattihenkilölle myönnetty ammattivarmenteen sisältävä toimikortti.
Terveydenhuollon henkilöstökortti	Terveydenhuollon muulle henkilöstölle (muut kuin terveydenhuollon ammattihenkilöt) myönnetty varmenteen sisältävä toimikortti.
Terveydenhuollon muu henkilö	Muu terveydenhuollon toimintayksikössä työskentelevä taikka sen tehtäviä suorittava henkilö, joka ei ole terveydenhuollon ammattihenkilö.
Terveydenhuollon palvelujen antaja	Terveydenhuollon toimintayksikkö tai itsenäisenä ammatinharjoittajana toimiva terveydenhuollon ammattihenkilö.
Terveydenhuollon toimijakortti	Muulle terveydenhuollon toimijalle myönnetty varmenteen sisältävä toimikortti.
Terhikki-rekisteri	Terveydenhuollon ammattihenkilöistä annetun lain (559/1994) nojalla Valviran ylläpitämä valtakunnallinen rekisteri terveydenhuollon ammattihenkilöistä ja heidän ammatinharjoittamisoikeustiedoistaan.

Todentaminen (*Authentication*)	Järjestelmän käyttäjän (henkilön, organisaation, laitteen tai järjestelmän) tai viestinnässä toisen osapuolen aitouden varmistaminen. Yleisiä käyttäjän todennuksen menetelmiä ovat: 1) käyttäjä tietää ainutkertaisen asian, esimerkiksi salasanan 2) hänellä on hallussaan jokin ainutkertainen ominaisuus kuten sormenjälki 3) hänellä on hallussaan ainutkertainen väline, esimerkiksi terveydenhuollon ammattihenkilön ammattikortti.
Tunnistaminen *(Identification)*	Menettely, jolla yksilöidään esimerkiksi tietojärjestelmän käyttäjä. Tyypillisesti tunnistus tapahtuu tarkistamalla, onko esitetty tunnus tai muu tunniste hyväksyttävien tunnusten joukossa, esimerkiksi käyttäjäksi ilmoittautunut henkilö tietojärjestelmän valtuutettujen käyttäjien luettelossa.
Turvataso	Turvatasolla tarkoitetaan niiden turvatoimien tasoa, joilla varaudutaan siihen, että turvallisuutta uhkaavaa välikohtausta yritetään tai se tapahtuu. Tyypillisiä turvatason seurantakohteita ovat esimerkiksi tietoturvapoikkeamat.
Vara-avainjärjestelmä *(Key escrow)*	Key escrow on menetelmä, jossa todentamisavainten turvatalletus on pakollista ja turvatalletuksessa oleva avain on tietyissä tilanteissa käytettävissä ilman varmenteen haltijan suostumusta. Terveydenhuollon ammattikorttien yksityisiä avaimia ei turvatalleteta.
Varmenne *(Certificate)*	Julkisen avaimen järjestelmää käyttävän palveluverkon toimijan kuten terveydenhuollon ammattihenkilön tai palveluntuottajan julkisesta avaimesta ja tunnistetiedoista muodostettu tietokokonaisuus, jonka varmentaja on muodostanut ja allekirjoittanut yksityisellä avaimellaan. Varmenteen aitous on todennettavissa varmentajan julkisella avaimella (varmentajan varmenteella).
Varmennehakemisto	Varmennehakemisto on julkinen tietokanta, johon varmentaja tallettaa varmentajan varmenteet, terveydenhuollon ammattihenkilöiden todentamisvarmenteet sekä sulkulistat.
Varmennepolku	Varmenteiden ketju, joka tarvitaan, jotta yhteen varmennehallintoon kuuluva voi turvallisesti asioida toiseen varmennehallintoon kuuluvan kanssa. Tämä saadaan aikaan joko siten, että molemmilla varmentajilla on puolestaan yhteinen varmentaja, tai että varmentajat ovat sopineet vastavuoroisesti toistensa varmenteiden hyväksymisestä.
Varmennetietojärjestelmä (Vartti)	Varmennekorttien ja varmenteiden tilaus- ja hallinnointisovellus.

Varmentaja
(CA, Certification Authority)

Julkisen avaimen järjestelmässä luotettu taho, joka tuottaa järjestelmän käyttäjille avainparit ja tuottaa, allekirjoittaa, jakelee ja tarvittaessa sulkee varmenteet.

Väestötietojärjestelmä *(VTJ)*

Väestötietojärjestelmä on valtakunnallinen atk-rekisteri, jossa on perustiedot Suomen kansalaisista ja Suomessa vakinaisesti asuvista ulkomaalaisista. Järjestelmässä on tietoa myös rakennuksista, rakennushankkeista ja huoneistoista sekä kiinteistöistä. Väestötietojärjestelmää ylläpitävät Väestörekisterikeskus ja maistraatit. Tietojen rekisteröinti perustuu kansalaisten ja viranomaisten lakisääteisiin ilmoituksiin.

2. TIETOJEN JULKAISEMINEN

2.1. Julkinen hakemisto

Varmentaja vastaa varmennehakemiston ylläpidosta sekä luvussa 2.2 määritellyn informaation julkaisemisesta. Hakemiston tietosisältö ja rakenne noudattavat FINEID S5 - Directory Specification -määritystä.

Hakemiston ylläpitäjä vastaa hakemistoihin liittyvistä palveluista sopimuksen ja tämän varmennuskäytännön mukaisesti.

2.2. Varmentajan julkaisemat tiedot

Varmentaja vastaa siitä, että varmennepolitiikat, varmennuskäytännöt, varmennekuvaukset ja varmentajan varmenteet ovat julkisesti saatavilla osoitteesta www.fineid.fi. Hakemistopalvelu on julkinen Internet-palvelu, josta on saatavilla varmentajan myöntämät julkiseen hakemistoon tarkoitetut varmenteet ja varmentajan varmenteet sekä sulkulista. Hakemistopalvelu on saatavissa osoitteesta ldap://ldap.fineid.fi.

2.3. Julkaisutiheys

Varmentaja julkaisee varmennepolitiikan ja varmennuskäytännön. Muutoshallinta on kuvattu luvussa 9.12.

Todentamisvarmenteet sekä sulkulistat julkaistaan varmennehakemistoon heti, kun ne on luotu.

2.4. Pääsyoikeudet

Varmentajan julkaisemien tietojen saatavuutta ei rajoiteta pääsyoikeuksin.

3. TUNNISTAMINEN JA TODENTAMINEN

Tästä luvusta ilmenevät käytännöt ja menettelytavat, joiden mukaan henkilöt tunnistetaan ja todennetaan varmenteen tilausprosessissa.

3.1. Varmenteen haltijan nimeäminen

3.1.1. Nimeäminen

Terveydenhuollon ammattihenkilön nimeäminen todentamisvarmenteessa sekä allekirjoitusvarmenteessa on kuvattu määrityksessä THPKI - T2 - Väestörekisterikeskuksen CA-malli ja varmenteiden tietosisältö terveydenhuollossa.

3.1.2. Nimeämisen merkitys

Varmenteen haltijan nimeämisessä käytetään luonnollisen henkilön Terhikki-rekisteriin kirjattuja etu- ja sukunimiä.

Attribuuttien joukko, josta muodostuu varmenteeseen kohteen nimitietue, on ainutlaatuinen ja yksilöi asianomaisen terveydenhuollon ammattihenkilön. Rekisteröintinumeron antaa Terhikki-rekisteriä ylläpitävä Valvira. Kaikkien terveydenhuollon ammattihenkilöiden on toimittava omilla nimillään.

3.1.3. Anonyymit tai salanimet

Anonyymejä varmenteita ei myönnetä, eikä myöskään varmenteita sala-, taiteilija- tai lempinimille.

3.1.4. Nimikenttien sisältö

Nimikenttien sisältö on määritetty luvussa 3.1.1.

3.1.5. Nimitietueen ainutkertaisuus

Luvussa 3.1.1 määritelty nimitietue yksilöi rekisteröidyn terveydenhuollon ammattihenkilön. Henkilön tunnistetieto on terveydenhuollon ammattihenkilön ainutkertaisesti yksilöivä.

3.1.6. Tuotenimien käyttöoikeus

—

3.2. Henkilöllisyyden todentaminen

3.2.1. Menettelytapa yksityisen avaimen omistajuuden todistamiseksi

Terveydenhuollon ammattihenkilön yksityiset avaimet luodaan aina ammattikortin sirulla. Yksityiset avaimet sisältävä ammattikortti luovutetaan terveydenhuollon ammattihenkilölle sen jälkeen, kun hänen henkilöllisyytensä on luotettavasti todettu ja varmenne on rekisteröity ja luotu.

3.2.2. Varmenteen hakijan edustaman organisaation todentaminen

Terveydenhuollon ammattihenkilöiden osalta ei vaadita heidän edustamiensa organisaatioiden todentamista. Terveydenhuollon ammattihenkilöt voivat työskennellä useassa terveydenhuollon

toimintayksikössä, joten terveydenhuollon ammattivarmenne ja ammattikortti eivät ole organisaatiosidonnaisia.

3.2.3. Henkilön tunnistaminen ja voimassaolevan ammattioikeuden todentaminen

Varmennetta haettaessa henkilöllisyys tarkistetaan voimassa olevasta, poliisin myöntämästä henkilöllisyyden osoittavasta asiakirjasta, joita ovat henkilökortti ja passi, tai 1.10.1990 jälkeen myönnetystä ajokortista. Hyväksyttäviä tunnistamisasiakirjoja ovat myös Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä voimassa oleva passi tai henkilökortti, Euroopan talousalueen jäsenvaltion viranomaisen 1.10.1990 jälkeen myöntämä voimassa oleva ajokortti ja muun valtion viranomaisen myöntämä voimassa oleva passi. Jos hakijalla ei ole em. asiakirjoja, poliisi tunnistaa hakijan henkilöllisyyden muilla tavoin.

Terveydenhuollon ammattihenkilön ammattioikeuden voimassaolo tarkistetaan Valviran ylläpitämästä terveydenhuollon ammattihenkilöiden keskusrekisteristä (Terhikki). Terveydenhuollon ammattivarmenteeseen ja ammattikorttiin merkitään vain yksi hakijan valitsema ammattioikeus, mikäli hakijalla on useita voimassaolevia ammattioikeuksia. Jos varmenteen hakijalla ei ole voimassaolevaa Terhikki-rekisteriin merkittyä ammattioikeutta, varmennetta ei myönnetä.

Mikäli ammattihenkilön tietoja ei ole rekisteröity Terhikkiin, tulee henkilön ottaa yhteyttä Valviraan ammattioikeuksiensa rekisteröimiseksi.

3.2.4. Varmenteen hakijan tiedot, joita varmentaja ei tarkista

Kaikki terveydenhuollon ammattihenkilön varmennehakemuksessa tarvittavat henkilötiedot saadaan Terhikki-rekisteristä.

3.2.5. Varmenteen myöntämisen edellytykset

Vain Valviran rekisteröimällä terveydenhuollon ammattihenkilöllä on oikeus hakea ammattivarmennetta. Varmenteen hakijalla on oltava voimassaoleva terveydenhuollon ammattioikeus, jotta varmenne voidaan myöntää. Ammattioikeuteen liittyvät mahdolliset rajoitukset eivät estä varmenteen myöntämistä.

3.2.6. Varmentajien välisen yhteistyön edellytykset ja vaatimukset

Varmentajien välisen yhteistyön edellytykset ja vaatimukset määritellään juurivarmentajan varmennepolitiikassa.

3.3. Tunnistaminen ja todentaminen varmenteen uusimisessa

3.3.1. Tunnistaminen ja todentaminen varmenteen uusimisessa

Varmenteiden uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

3.3.2. Tunnistaminen ja todentaminen varmenteen sulkemisen jälkeen

Uuden varmenteen myöntämisessä noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

3.4. Peruuttamispyynnön tekijän tunnistaminen

Varmenteen sulkupyyntö voidaan tehdä puhelimitse sulkupalveluun tai kirjallisesti varmentajalle.

Kun sulkupyyntö tehdään puhelimitse tai kirjallisesti, ilmoittajan ja varmenteen haltijan tiedot kirjataan varmennetietojärjestelmään.

Jos sulkupyynnön tekijää ei saada tunnistettua riittävän luotettavasti ja on olemassa riski varmenteen väärinkäyttämisestä, varmentaja asettaa varmenteen sulkemisen etusijalle.

4. VARMENTEEN ELINKAAREN HALLINNAN TOIMINNALLISET VAATIMUKSET

Tämä luku kuvaa varmentajan, rekisteröijän ja terveydenhuollon ammattihenkilön toiminnalle asetetut vaatimukset. Luku sisältää myös varmenteiden sulkemisen.

4.1. Varmenteen hakeminen

Terveydenhuollon ammattivarmennetta haetaan henkilökohtaisesti rekisteröijänä toimivalta organisaatiolta.

Hakemuksen tiedot tallennetaan varmentajan varmennetietojärjestelmään.

Terveydenhuollon ammattivarmenteen hakeminen edellyttää, että hakija:

- osoittaa henkilöllisyytensä luvussa 3 esitetyllä tavalla
- esittää luvussa 3.2.3 kuvatun mukaisesti henkilötietonsa
- allekirjoittaa hakemuslomakkeen.

Rekisteröijä ilmoittaa hakijalle ammattikortin sekä tunnuslukukuoren toimitustavasta.

4.1.1. Kuka voi tehdä varmennehakemuksen

Varmennehakemuksen voi tehdä Valviran rekisteröimä terveydenhuollon ammattihenkilö.

4.1.2. Varmenteen myöntämisprosessi ja vastuut

Myönnettävän varmenteen tietojen ja niihin liittyvän ammattikortin rekisteröinti tapahtuu järjestelmällä, joka turvaa tietojen eheyden.

Varmentajan tietojärjestelmien väliset tietoliikenneyhteydet on suojattu. Varmennetietojärjestelmää käyttävät henkilöt tunnistetaan varmentajan myöntämillä varmennekorteilla. Varmenteen tietosisältö muodostuu hakemuslomakkeessa ilmoitetuista tiedoista.

Rekisteröijä myöntää varmenteen, kun rekisteröijä ja hakija ovat tarkistaneet ja hyväksyneet allekirjoituksellaan varmennehakemuksen tiedot.

Varmentaja toimittaa hakijalle hakijan tiedoilla yksilöidyn:

- ammattikortin, joka sisältää kortinhaltijan henkilökohtaiset avainparit ja varmenteet
- tunnuslukukuoren, joka sisältää ammattikortin käyttöön tarvittavat henkilökohtaiset PIN- ja PUK-tunnusluvut.

Lisäksi rekisteröijä toimittaa varmenteen hakijalle ammattikortin käyttöohjeen.

Varmenteen myöntämiseen liittyvät rekisteröijän vastuut on kuvattu luvussa 1.3.2.

4.2. Varmennehakemuksen käsittely

Varmennehakemus käsitellään rekisteröintipisteessä ilman aiheetonta viivytystä.

Rekisteröijä tallettaa varmenteen tilaustiedot varmentajan varmennetietojärjestelmään.

4.2.1. Tunnistamisen ja todentamisen toteuttaminen

Rekisteröijä tunnistaa varmenteen hakijan luvun 3 mukaisesti ja tarkistaa, että henkilöllä on Terhikki-rekisteriin merkittynä voimassa oleva tieto ammatinharjoittamisoikeudesta.

Hakemuslomakkeen tiedot saadaan Terhikki-rekisteristä ja Väestötietojärjestelmästä. Hakemuksessa on mainittu hakijan ilmoittama varmenteeseen talletettava kutsumanimi sekä Terhikki-rekisteriin merkitty ammattioikeus. Näiden lisäksi rekisteröijä täyttää lomakkeeseen varmenteen tuottamiseen ja toimittamiseen tarvittavia tietoja sekä tiedon hakijan tunnistamisessa käytetystä tunnistamisasiakirjasta.

4.2.2. Varmennehakemuksen hyväksyminen tai hylkääminen

Ammattivarmennehakemus hyväksytään myöntämällä varmenne. Mikäli edellytykset varmenteen myöntämiseksi puuttuvat hakijan osalta, varmennetta ei myönnetä ja hakemus hylätään. Päätöksestä ilmoitetaan viipymättä hakijalle, joka voi tehdä päätöksestä kirjallisen muutosvaatimuksen varmentajalle.

4.2.3. Varmennehakemuksen käsittelyaika

Varmennehakemus käsitellään ilman aiheetonta viivytystä rekisteröintipisteen aukioloaikana.

4.3. Varmenteen myöntäminen

4.3.1. Varmenteen myöntämiseen liittyvät varmentajan tehtävät

Rekisteröintipisteen virkailija käynnistää varmenteen myöntämisprosessin. Varmennejärjestelmän käyttö edellyttää virkailijan vahvaa tunnistamista. Virkailijan toimenpiteet tallentuvat varmentajan tietojärjestelmien lokitietoihin.

Varmenteen myöntämiseen liittyvät tehtävät on kuvattu luvuissa 4.1 ja 4.2.

4.3.2. Ilmoitus hakijalle varmenteen myöntämisestä

Erillistä ilmoitusta terveydenhuollon ammattivarmenteen myöntämisestä ei tehdä.

4.4. Myönnetyn varmenteen hyväksyminen

4.4.1. Myönnetyn varmenteen hyväksymismenettely varmenteen hakijan kannalta

Varmenteen haltijan edellytetään tarkistavan kortin ja varmenteen tietojen oikeellisuus. Myönnetyn varmenteen hyväksyminen ei edellytä varmenteen haltijalta muita toimenpiteitä. Ongelmatilanteissa varmenteen haltijan tulee ottaa yhteyttä rekisteröintipisteeseen tai tukipalvelupuhelimeen.

4.4.2. Varmenteen julkaisu varmentajan toimesta

Varmentaja julkaisee myönnetyt todentamisvarmenteet julkisessa tietoverkossa olevassa varmennehakemistossa luvussa 2.1 kuvatulla tavalla. Allekirjoitusvarmenteita ei julkaista hakemistossa.

4.4.3. Ilmoitus muille osapuolille varmenteen myöntämisestä

Erillistä ilmoitusta terveydenhuollon ammattivarmenteen myöntämisestä ei tehdä.

4.5. Varmenteiden ja avainparien käyttö

4.5.1. Varmenteiden ja avainparien käyttö varmenteen haltijan toimesta

Terveydenhuollon ammattivarmenteet ja niihin liittyvät avainparit on tarkoitettu käytettäväksi Suomen sosiaali- ja terveydenhuollon tietojärjestelmissä ja niihin liittyvissä palveluissa.

Terveydenhuollon ammattihenkilön tulee sitoutua toimimaan tämän varmennuskäytännön mukaisesti hakiessaan ja käyttäessään varmennetta.

Terveydenhuollon ammattihenkilö vastaa ensisijaisesti vahingosta, jonka hän aiheuttaa:

- voimassaolevan lain, asetuksen taikka niiden nojalla annetun määräyksen tai ohjeen vastaisella menettelyllä;
- varmennepolitiikan tai varmennuskäytännön vastaisella menettelyllä;
- hyväksymiensä varmenteen käyttöehtojen vastaisella menettelyllä;
- varmenteen muulla tahallisella tai huolimattomalla virheellisellä käytöllä.

Terveydenhuollon ammattihenkilön tulee säilyttää ja hallita huolellisesti omia varmenteitaan ja avainparejaan sekä niihin liittyviä tunnuslukuja ja ammattikorttiaan. Varmenteen haltijan tulee estää ammattikortin katoaminen sekä tunnuslukujen paljastuminen tai luvaton käyttö.

Kortinlukijassa olevaa omaa ammattikorttia ei saa jättää valvomatta eikä missään tilanteessa antaa kenenkään muun käyttöön.

Terveydenhuollon ammattihenkilön tulee ilmoittaa sulkupalveluun:

- ammattikortin katoaminen tai väärinkäyttöepäily.

Jos ammattikortti rikkoutuu, tulee kortinhaltijan sulkea rikkoutuneen kortin varmenteet ja hakea uusi ammattikortti rekisteröintipisteestä. Kortin uusimisessa noudatetaan samoja menettelyjä kuin korttia ja varmennetta ensi kertaa haettaessa.

PIN-tunnuslukuja, joita käytetään avainten aktivointiin, ei saa säilyttää samassa paikassa ammattikortin kanssa. Varmenteen haltijan on vaihdettava PIN-tunnusluvut, mikäli on epäiltävissä, että tunnusluvut ovat voineet joutua ulkopuolisten tietoon.

Jos tunnusluku on lukkiutunut ja sen avaamiseen tarvittava PUK-tunnusluku eli avaustunnusluku on kadonnut, tulee kortinhaltijan mennä rekisteröintipisteeseen saadakseen tietoonsa avaustunnusluvun. Avaustunnuslukua kysyttäessä kortinhaltija tunnistetaan voimassa olevasta poliisin myöntämästä virallisesta henkilöllisyysasiakirjasta. Rekisteröintipisteen virkailija tulostaa uuden tunnuslukukuoren, joka sisältää avaustunnusluvun. Avaustunnuslukua ei ilmoiteta puhelimitse tai kirjeitse tietoturvasyistä.

4.5.2. Varmenteiden ja julkisten avainten käyttö varmenteisiin luottavan osapuolen toimesta

Luottavan osapuolen vastuulla on omien tietojärjestelmiensä osalta varmistaa, että varmennetta käytetään tässä varmennuskäytännössä määriteltyyn tarkoitukseen. Varmenteen oikean käyttötarkoituksen varmistamisessa luottava osapuoli voi tukeutua varmenteen sisältämään viittaukseen tähän varmennuskäytäntöön.

Luottavan osapuolen tulee varmistaa, että käytettävät sovellukset täyttävät tämän varmennuskäytännön vaatimukset.

Luottavan osapuolen vastuulla on varmenteen tarkistaminen asianmukaisella tavalla koko varmennepolun läpi IETF RFC 3280 -määrityksen mukaisesti. Mikäli varmentajan ja luottavan organisaation välillä on sovittu varmenteen käyttöön liittyvistä lisäpalveluista, luottava osapuoli sitoutuu noudattamaan lisäpalveluja koskevia ehtoja.

Luottavan osapuolen vastuulla on tarkistaa ennen varmenteen hyväksymistä, että varmenne on voimassa eikä sitä ole suljettu.

Luottavan osapuolen vastuulla on voimassaolevan sulkulistan tarkistaminen. Varmenteeseen ei tule luottaa, ellei luottava osapuoli suorita suljettujen varmenteiden tarkistusta seuraavalla tavalla:

1. Luottavan osapuolen tulee tarkistaa sulkulistan varmennuspolku ja sulkulistan aitous varmentajan digitaalisesta allekirjoituksesta.
2. Luottavan osapuolen tulee tarkistaa sulkulistan kelpoisuusaika varmistuakseen, että sulkulista on voimassa.
3. Varmenteet (julkinen avain) voidaan tallettaa paikallisesti varmenteeseen luottavan osapuolen järjestelmään, mutta varmenteen voimassaolo tulee tarkistaa ennen varmenteen hyväksymistä.

Jos voimassaolevaa sulkulistaa ei ole saatavilla järjestelmän tai palvelun häiriön vuoksi, tämän varmennuskäytännön mukaisia varmenteita ei saa hyväksyä. Jos luottava osapuoli kuitenkin hyväksyy varmenteen, hyväksyminen tapahtuu luottavan osapuolen omalla vastuulla.

4.6. Julkisen avaimen uudelleen varmentaminen

Ammattivarmenteita ei myönnetä aiemmin varmennetuille julkisille avaimille.

4.7. Varmenteen uusiminen

4.7.1. Varmenteen uusimisen syyt

Terveydenhuollon ammattihenkilön varmenne voidaan uusia edellisen varmenteen voimassaolon päättyessä, mikäli luvussa 3.2.5 kuvatut varmenteen myöntämisen edellytykset ovat edelleen voimassa.

Varmenne voidaan uusia myös varmenteen tietosisältöön vaikuttavien ammattioikeus- tai muiden tietojen muuttuessa tai ammattikortin rikkoutuessa. Tällöin varmenteen haltijan tulee ottaa yhteyttä rekisteröintipisteeseen ja hakea uutta ammattikorttia ja ammattivarmennetta luvussa 4 kuvatulla tavalla.

4.7.2. Varmenteen uusimisen hakeminen

Varmenteen uusimista voi hakea vain varmenteen haltija.

4.7.3. Varmenteen uusimispyynnön käsittely

Varmenteiden uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

4.7.4. Ilmoitus varmenteen hakijalle ammattikortin uusimisesta

Erillistä ilmoitusta terveydenhuollon ammattivarmenteen uusimisesta ei tehdä.

4.7.5. Uusitun varmenteen hyväksymismenettely varmenteen haltijan kannalta

Uusittu varmenne hyväksytään kappaleessa 4.4.1 kuvatun menetelmän mukaisesti.

4.7.6. Uusitun varmenteen julkaisu

Varmenteet julkaistaan kappaleessa 4.4.2 kuvatun menetelmän mukaisesti.

4.7.7. Ilmoitus uusitun varmenteen myöntämisestä muille osapuolille

Erillistä ilmoitusta terveydenhuollon ammattivarmenteen uusimisesta ei tehdä.

4.8. Varmenteen muuttaminen

Varmenteen tietosisältöä ei voi muuttaa varmenteen luonnin jälkeen. Varmenteen tietosisältöön vaikuttavien tietojen muuttuessa varmenteen haltija voi hakea uutta ammattivarmennetta ja ammattikorttia luvun 4.7 mukaisesti.

4.9. Varmenteen sulkeminen ja määräaikainen sulkeminen

Varmentaja ylläpitää varmenteiden sulkupalvelua, joka on käytettävissä 24 tuntia vuorokaudessa 7 päivänä viikossa. Tiedot suljetuista varmenteista julkaistaan sulkulistan avulla, jonka varmentaja allekirjoittaa ja joka julkaistaan julkisessa hakemistossa. Varmennetta ei voi sulkea määräajaksi.

Varmentaja ilmoittaa terveydenhuollon ammattihenkilölle varmenteen sulkemisesta silloin, kun sulkeminen johtuu ammattioikeuden menettämisestä.

Varmenteen sulkeminen ei mitätöi kyseisellä varmenteella ennen sulkemisajankohtaa tehtyjä sähköisiä allekirjoituksia.

4.9.1. Varmenteen sulkemisen edellytykset

Varmenne suljetaan kun:

- varmenteen haltija pyytää sulkemista
- varmenteen haltija menettää jonkin rekisteröidyn ammattioikeuden
- ammattikortti on vahingoittunut, kadonnut tai anastettu
- avaustunnusluku sekä ammattikortti ovat kadonneet tai anastettu
- varmenteen haltija on kuollut.

Varmentaja voi sulkea terveydenhuollon ammattihenkilön varmenteen, mikäli varmennetta on käytetty tämän varmennuskäytännön, sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) tai sähköisestä lääkemääräyksestä (61/2007) annetun lain sekä niiden nojalla annettujen säädösten tai niiden nojalla asetettujen vaatimusten ja ohjeiden vastaisesti.

Varmennetta ei saa käyttää tai yrittää käyttää sen jälkeen, kun sitä koskeva sulkupyyntö on tehty.

4.9.2. Kuka voi vaatia varmenteen sulkemista

Varmenteen sulkemista voivat vaatia:

- terveydenhuollon ammattihenkilö tai hänen lakisääteinen edustajansa ammattihenkilön oman varmenteen osalta;
- varmentaja kohdan 4.9.1 edellytysten täyttyessä.

4.9.3. Varmenteen sulkemisprosessi

Varmenteen haltija esittää varmenteen sulkupyynnön sulkupalveluun tai varmentajalle. Ilmoitus tehdään:

1) Puhelimitse soittamalla maksuttomaan sulkupalveluun +358 800 162 622.
2) Kirjallisesti varmentajalle.

Varmenteen sulkupyynnön tekijä tunnistetaan luvussa 3.4 kuvatulla tavalla.

Varmentaja sulkee viran puolesta varmenteet:

- ammattioikeuden menettämisen perusteella tai
- varmenteen haltijan kuoleman perusteella.

Varmenteen sulkemisesta kirjataan seuraavat tiedot:

- suljettavan varmenteen haltijan käytettävissä olevat henkilötiedot
  - etunimet ja sukunimi
  - rekisteröintinumero, henkilötunnus
- sulkupyynnön tekijän henkilötiedot (jos eri kuin varmenteen haltija)
- sulkupyynnön tekijän tunnistamistapa
- sulkupyynnön ajankohta
- sulkupyynnön syy kirjataan, kun sulkupyynnön tekee muu kuin varmenteen haltija; varmenteen haltijan ei tarvitse ilmoittaa sulkupyyntönsä syytä
- sulkupyynnön vastaanottajan henkilötiedot
- mahdolliset muut varmenteen haltijan ilmoittamat lisätiedot
  - ammattikortin katoamisaika, varmenteen haltijan kuolinaika tms.
- varmenteen sulkijan henkilötiedot
- varmenteen sulkemisen ajankohta.

Varmentaja ei lähetä varmenteen haltijalle erillistä vahvistusta varmenteen sulkemisesta muutoin kuin siinä tapauksessa, että varmenteen sulkeminen johtuu ammattioikeuden menettämisestä. Varmenne suljetaan varmennejärjestelmän kautta ja varmenteen sulkemiseen liittyvät tiedot säilytetään 10 vuotta sulkemisajankohdasta.

4.9.4. Varmenteen haltijan velvollisuus tehdä sulkupyyntö

Varmenteen haltijan tulee viipymättä tehdä varmenteen sulkupyyntö sulkupalveluun, kun luvussa 4.9.1 kuvatut varmenteen sulkemisen edellytykset täyttyvät.

4.9.5. Varmenteen sulkupyynnön käsittelyaika

Sulkupalvelu käsittelee varmenteen sulkupyynnöt viipymättä.

4.9.6. Varmenteeseen luottavan osapuolen velvollisuus tarkistaa varmenteen voimassaolo

Luottavan osapuolen vastuulla on tarkistaa ennen varmenteen hyväksymistä, että varmenne on voimassa eikä sitä ole suljettu.

Luottavan osapuolen vastuulla on voimassaolevan sulkulistan tarkistaminen. Varmenteeseen ei tule luottaa, ellei luottava osapuoli ole suorittanut sulkulistan tarkistusta.

4.9.7. Sulkulistan julkaisutiheys

Päivitetty sulkulista julkaistaan tunnin välein.

Sulkulistasta ilmenee seuraavan sulkulistan suunnitelman mukainen julkaisuajankohta. Uusi sulkulista voidaan julkaista myös ennen suunnitelman mukaista julkaisuajankohtaa.

4.9.8. Sulkulistan voimassaolon enimmäisaika

Päivitetty sulkulista on voimassa enintään 72 tuntia. Jokaisessa sulkulistassa on mainittu voimassaolon päättymisajankohta.

4.9.9. Reaaliaikainen varmenteen tilan tarkistaminen

Reaaliaikainen varmenteen tilan tarkistaminen ei ole käytössä.

4.9.10. Vaatimukset varmenteen tilan reaaliaikaiselle tarkistamiselle

—

4.9.11. Muut varmenteen tilan tarkistamismenettelyt

—

4.9.12. Yksityisen avaimen paljastumisesta johtuva varmenteen sulkeminen

Yksityisen avaimen paljastumisesta johtuva varmenteen sulkeminen ei poikkea muilla perusteilla tapahtuvasta varmenteen sulkemisesta.

4.9.13. Varmenteen sulkeminen määräajaksi

Varmenteita ei suljeta määräajaksi.

4.9.14. Kuka voi vaatia varmenteen sulkemista määräajaksi

—

4.9.15. Menettelytavat varmenteen sulkemiseksi määräajaksi

—

4.9.16. Rajoitukset varmenteen määräaikaiselle sulkemiselle

—

4.10. Varmenteen tilan tarkistamismahdollisuus

Varmenteen tilan tarkistaminen tehdään sulkulistan avulla. Varmenteeseen luottavan osapuolen tulee myös tarkistaa, ettei varmenteen voimassaoloaika ole päättynyt.

4.11. Varmenteen voimassaolon päättyminen

Varmenne on voimassa joko yleisen voimassaoloajan, varmennekohtaisen määräajan tai kunnes se sulkemisedellytysten täytyttyä suljetaan.

4.12. Vara-avainjärjestelmä ja avainten palautus

Ammattihenkilöiden salausavaimia ei turvatalleteta. Varmenteita ei siten voida käyttää ilman varmenteen haltijan suostumusta eikä yksityisiä avaimia voida palauttaa kortin hajottua tai hävitessä.

5. FYYSISEN, KÄYTTÖ- JA HENKILÖSTÖTURVALLISUUDEN HALLINTA

Väestörekisterikeskuksen tietoturvallisuutta hallitaan Väestörekisterikeskuksen tietoturvapolitiikan ja standardin ISO 27001 mukaisesti.

5.1. Fyysisen turvallisuuden hallinta

Väestörekisterikeskus käyttää teknisiä toimittajia varmennepalvelun tietoteknisten tehtävien hoitamiseen. VRK vastaa varmentajana varmennetuotannon turvallisuudesta ja toiminnasta asianmukaisella tavalla sen kaikilla osa-alueilla.

5.1.1. Tilojen sijoittaminen ja rakenne

Varmentajan järjestelmät sijaitsevat korkean turvatason konesalitiloissa ja täyttävät tietokonekeskuksille annetut turvallisuutta koskevat ohjeet ja määräykset.

Toimitilaturvallisuus on toteutettu siten että asiattomien pääsy toimitiloihin on estetty.

5.1.2. Fyysinen pääsynvalvonta

Toimitiloihin, joissa tehdään varmennejärjestelmän tuotannollisia tehtäviä, on valvottu pääsy. Kulunvalvontajärjestelmä havaitsee sekä luvallisen että luvattoman sisäänmenon. Konesalitiloihin vaaditaan henkilön tunnistautuminen, jolloin henkilö tunnistetaan ja pääsyoikeudet tarkistetaan sekä tapahtumat rekisteröidään. Konesalitiloja vartioidaan vuorokauden ympäri.

5.1.3. Sähkö ja ilmastointi

Varmennetuotannon järjestelmät sijaitsevat konesalitiloissa, joissa on varavoimalaitteilla varmistettu sähkön saanti ja ilmastointi. Polttoaineen saannista poikkeustilanteissa tulee olla toimitussopimus.

5.1.4. Vesivahinko

Varmennetuotannon järjestelmät sijaitsevat konesalitiloissa, joissa on korotetut lattiat ja lattian alla kaapelikorokkeet sekä vesivahingot havaitseva valvontajärjestelmä.

5.1.5. Tulipalo

Varmennetuotannon järjestelmät sijaitsevat automaattisammutuksella varustetuissa konesalitiloissa.

5.1.6. Tietovälineiden säilytys

Rekisteröintipisteissä sekä varmennetuotannossa käytettäviä tietovälineitä kuten kiintolevyjä, levykkeitä, flash-muisteja ja optisia muisteja, joissa on salassa pidettävää tietoa, tulee käsitellä ja säilyttää samojen vaatimusten mukaisesti kuin salassa pidettävää paperiasiakirjaa. Tieto tai asiakirja on salassa pidettävä, jos niin on laissa viranomaisten toiminnan julkisuudesta (621/1999) säädetty.

5.1.7. Tietovälineiden hävittäminen

Rekisteröintipisteissä sekä varmennetuotannossa käytetyt salassa pidettävää tietoa sisältävät tietovälineet hävitetään tähän soveltuvassa alan yrityksessä. Tietovälineiden hävittämisestä saadut tuhoamistodistukset arkistoidaan.

5.1.8. Varmuuskopiointi verkon yli

Varmennetuotantojärjestelmän varmuuskopiointi tapahtuu varmennejärjestelmän sisäisessä tietoliikenneverkossa.

5.2. Käyttöturvallisuuden hallinta

Varmentaja kantaa kokonaisvastuun varmenteiden myöntämiseen ja sulkulistojen julkaisuun liittyvistä hallinnollisista ja logistisista toiminnoista. Toimintoja voi suorittaa toinen organisaatio varmentajan toimeksiannosta.

5.2.1. Työtehtäviin liittyvät roolit

Varmentajan ja varmentajan käyttämien alihankkijoiden työtehtävät on jaettu siten, että tiedon ja palveluiden tahattoman tai tahallisen väärinkäytön riskiä pienennetään. Varmennetoiminnan työtehtävät on roolitettu ja jokaisella on vain roolinsa mukaiset oikeudet järjestelmään.

Varmennetoiminnan rooleja ovat:

- järjestelmän pääkäyttäjä
- järjestelmän käyttäjä
- rekisteröijä ja
- auditoija.

5.2.2. Varmennetuotannon työtehtäviin tarvittavien henkilöiden määrä

Varmentajan lukuun toimivat nimetyt organisaatiot ja henkilöt.

Varmentajan avainparin luonnissa ja hallinnoinnissa on mukana vähintään kaksi henkilöä. Varmennejärjestelmään tehtäviin järjestelmätason muutoksiin vaaditaan vähintään kahden henkilön osallistuminen. Varmenteen hakijan tunnistamiseen ja rekisteröintiin vaaditaan yhden henkilön läsnäolo.

5.2.3. Henkilöiden tunnistaminen ja todentaminen eri rooleihin

Varmentajan työtehtävissä toimivilla henkilöillä, jotka toimivat luvussa 5.2.1 mainituissa tehtävissä, on käytössään PIN-tunnusluvulla suojattu henkilökohtainen hallintakortti. Henkilön oikeus käyttää varmennejärjestelmää tai muita varmentamiseen liittyviä järjestelmiä todennetaan näiden hallintakorttien avulla.

5.2.4. Tehtävien eriyttämistä vaativat roolit

Rekisteröijä ei voi toimia järjestelmän pääkäyttäjän roolissa.

5.3. Henkilöstöturvallisuuden hallinta

5.3.1. Tausta-, ansio-, kokemus- ja selvitysvaatimukset

Järjestelmän käyttäjien työtehtävät ovat turvallisuuden kannalta kriittisiä, koska he luovat ja hallitsevat varmenne- ja avaintietoja. Henkilön, joka toimii järjestelmän käyttäjän työtehtävässä, tulee olla työtehtäviin soveltuva ja ymmärtää turvallisuuden merkitys jokapäiväiselle työlleen. Varmentajan valtuuttamat organisaatiot huolehtivat henkilökuntansa jatkuvasta luotettavuudesta.

Varmentajan työtehtävissä toimivista henkilöistä tehdään turvallisuusselvitys.

5.3.2. Taustojen tarkistamisen menettelytapa

Varmentajan valtuuttamat organisaatiot huolehtivat ja vastaavat itse henkilökuntansa taustojen tarkistamisesta sekä luotettavuudesta.

5.3.3. Koulutuksen tiheys ja vaatimukset

Varmentaja ja varmentajan lukuun toimivat organisaatiot huolehtivat itse henkilökuntansa riittävästä koulutuksesta. Varmentaja järjestää koulutusta rekisteröintipisteissä toimiville rekisteröijille.

5.3.4. Jatkokoulutuksen tiheys ja vaatimukset

—

5.3.5. Työtehtävien kierrätyksen tiheys ja järjestys

—

5.3.6. Seuraukset luvattomista toimista

Lakisääteisten seurausten lisäksi ja ohella luvattomasti toiminut henkilö menettää pysyvästi varmentajan järjestelmien käyttöoikeudet.

5.3.7. Alihankkijoiden henkilöstön vaatimukset

Varmentajan valtuuttamien organisaatioiden henkilöstön tulee täyttää luvun 5.3.1 edellytykset.

5.3.8. Asiakirjat, jotka toimitetaan henkilökunnalle

Varmennetoimintaan osallistuvalla henkilökunnalla on käytössään tämän varmennuskäytännön lisäksi varmennepolitiikka ja tarvittavat toimintaohjeet.

5.4. Varmennejärjestelmän turvallisuuden seuranta

Tässä luvussa kuvatut turvallisuuden seurannan menettelytavat sitovat kaikkia laitteisto- ja järjestelmäkokonaisuuksia, jotka ovat yhteydessä varmenteiden tilaus- ja myöntämisprosessiin.

5.4.1. Arkistoitavat tapahtumat

Varmentaja säilyttää turvallisuusseurantaa varten seuraavat tiedot:

1. Järjestelmätasoisten käyttöoikeuksien luonnit ja valtuusrikkomusyritykset.
2. Järjestelmän päivitykseen ja ylläpitoon liittyvät toimenpidepyynnöt.
3. Uuden ohjelmiston asennus tai ohjelmiston päivitys.
4. Kaikkien varmistusten kellonaika ja päivämäärä sekä muut kuvaavat tiedot.
5. Varmennejärjestelmän sulkeminen, käynnistäminen ja sammuminen.
6. Kaikkien laitteiston päivitysten kellonaika ja päivämäärä.

Varmenteiden ja varmennejärjestelmän osalta varmentaja säilyttää:

1. Kaikki tapahtumat, jotka liittyvät varmenteiden, myös varmentajan toiminnassaan käyttämien varmenteiden, luomiseen ja sulkemiseen.
2. Kaikki tapahtumat, jotka liittyvät varmenteiden allekirjoitusavainten hallintaan.

3. Kaikki järjestelmän hallintaan liittymättömät viestit rekisteröintipalvelusta, varmenteiden jakelupalvelusta ja lisäpalveluista.
4. Lokijärjestelmän käynnistykset ja alasajot.
5. Lokijärjestelmän asetusten muutokset.

5.4.2. Lokitietojen analysointitiheys

Lokitietoja analysoidaan tarvittaessa.

5.4.3. Lokitietojen säilytysaika

Lokitiedot säilytetään voimassaolevien arkistosäännösten mukaisesti.

5.4.4. Lokitietojen suojaaminen

Lokitietoihin on pääsy vain erikseen oikeutetuilla henkilöillä.

Lokitiedot suojataan muuttamiselta, tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä.

5.4.5. Lokitietojen varmuuskopiointi

Lokitiedoista otetaan varmuuskopiot päivittäin.

5.4.6. Lokitietojen keräysjärjestelmän toteuttaminen (sisäinen/ulkoinen)

Varmentaja vastaa lokitietojen keräysjärjestelmästä.

5.4.7. Lokitapahtumasta ilmoittaminen

Järjestelmän käyttäjälle ei erikseen ilmoiteta lokitapahtumien syntymisestä.

Lokitietojen valvonnasta vastaaville henkilöille ilmoitetaan erikseen seuraavista tapahtumista:

- valtuusrikkomusyritykset;
- järjestelmän sulkeminen, käynnistäminen ja sammuminen;
- ohjelmiston asennus tai ohjelmiston päivitys.

5.4.8. Haavoittuvuuksien arviointi

Varmentaja arvioi ja seuraa riskianalyysin avulla varmennejärjestelmän ja tuotantoympäristön haavoittuvuutta ja pyrkii minimoimaan niihin liittyviä riskejä.

5.5. Arkistoitavat aineistot

5.5.1. Arkistoitavat asiakirjat, tiedostot ja mediat

Varmentaja arkistoi seuraavat tiedot:

- varmennehakemukset;
- varmenne- tai muun hakemuksen allekirjoitetut hyväksynnät;
- varmennepalvelusopimukset;
- myönnetyt varmenteet;

- ristiinvarmennusasiakirjat mukaanluettuna ristiinvarmennuksen perustelut ja päätökset sekä suoritetut toimet;
- varmenteen sulkupyynnöt;
- voimassaolevat ja edelliset varmennepolitiikat ja varmennuskäytännöt;
- varmentajan ja rekisteröintipisteiden väliset sopimukset; ja
- varmennejärjestelmän ylläpitoon, käyttöön ja hallintaan liittyvät sopimukset.

5.5.2. Arkistojen säilytysaika

Arkistoinnissa sovelletaan yleislakina arkistolain (831/1994) säännöksiä. Arkistoinnissa sovelletaan lisäksi, mitä laissa sähköisestä asioinnista viranomaistoiminnassa (13/2003) on arkistoinnista määrätty.

5.5.3. Arkistojen suojaaminen

Arkistotietoihin on pääsy vain erikseen tätä tarkoitusta varten oikeutetuilla henkilöillä. Asiakirjat, tiedostot ja muut mediat säilytetään paloturvallisessa, kulunvalvonnalla varustetussa tilassa, johon vain varmentajan valtuuttamilla henkilöillä on pääsy.

Arkistotiedot suojataan muuttamiselta, tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä.

5.5.4. Arkistojen varmuuskopiointimenettely

Vain sähköisessä muodossa olevista arkistotiedoista otetaan varmuuskopiot.

5.5.5. Arkistoitavien tietojen aikaleima

Arkistoitavat asiakirjat on päivätty. Aikaleimapalvelu ei ole toistaiseksi käytössä.

5.5.6. Arkistojen keräysjärjestelmä (sisäinen/ulkoinen)

Varmentajalla ei ole keskitettyä arkistojen keräysjärjestelmää.

5.5.7. Arkistoissa olevien tietojen saatavuus ja eheys

Arkistotietoihin on pääsy vain erikseen tätä tarkoitusta varten oikeutetuilla henkilöillä. Arkistotiedot suojataan muuttamiselta, tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä.

5.6. Varmentajan avainparin vaihto

Varmentaja luo uuden avainparin ja varmentajan varmenteen viimeistään viisi vuotta ja kolme kuukautta ennen edellisen varmentajan varmenteen voimassaoloajan päättymistä. Varmentajan varmenne toimitetaan julkiseen hakemistoon luvun 2 mukaisesti. Lisäksi varmentajan varmenne on tallennettu ammattikortin sirulle.

5.7. Häiriötilanteisiin varautuminen

5.7.1. Suunnitelma toimintahäiriöiden ja toiminnan vaarantumisen varalta

Varmentajalla on jatkuvuus- ja toipumissuunnitelma, joka mahdollistaa toiminnan häiriöttömän jatkumisen ja varmentajan järjestelmien toipumisen onnettomuuksista. Häiriö- ja poikkeustilanteita varten on selkeät vastuut, suunnitelmat ja toimintaohjeet.

5.7.2. Varmennejärjestelmän, ohjelmistojen tai tietojen vahingoittuminen

Poikkeustilanteissa varmentaja noudattaa jatkuvuus- ja toipumissuunnitelmaa.

5.7.3. Toiminta varmenteen haltijan yksityisen avaimen paljastuessa

Varmenteen haltijan yksityiset avaimet on suojattu fyysistä tunkeutumista ja avainten paljastumista vastaan. Mikäli varmenteen haltijan yksityinen avain on paljastunut, suljetaan siihen liittyvä varmenne. Varmenteen haltijalle tuotetaan uusi ammattikortti, jossa on uudet yksityiset avaimet.

5.7.4. Toiminnan jatkuvuus häiriötilanteen jälkeen

Varmentaja pyrkii häiriötilanteen jälkeen saattamaan järjestelmien ydintoiminnot toimintakuntoon viipymättä. Laitteistoratkaisut on toteutettu hyvän tiedonhallintatavan mukaisesti siten, että järjestelmän pettäessä voidaan siirtyä käyttämään varajärjestelmää vaarantamatta järjestelmään sisältyvien tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä.

Tärkeiden laitteiden varaosien saanti ja huolto on varmistettu.

5.8. Lakkauttaminen

5.8.1. Varmentajan toiminnan lakkauttaminen

Varmentajan toiminnan lakkauttaminen on tilanne, jossa varmentaja lakkautetaan pysyvästi. Varmentajan lakkauttamiseksi ei katsota tilannetta, jossa varmentajan palvelut siirtyvät organisaatiolta toiselle tai varmentaja myöntää uuden varmentajan varmenteen.

Ennen varmentajan lakkauttamista suoritetaan vähintään seuraavat toimenpiteet:

- Kaikki myönnetyt ja voimassa olevat varmenteet mitätöidään yhdellä tai useammalla sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeisen mitätöidyn varmenteen voimassaoloaika on päättynyt.
- Varmentaja lakkauttaa kaikki sopimuskumppaniensa valtuudet suorittaa varmenteiden elinkaaren hallintaan liittyviä tehtäviä varmentajan puolesta.
- Varmentaja varmistaa, että luvussa 5.5.7 mainittu saatavuus varmentajan arkistoihin säilyy varmentajan lakkauttamisen jälkeenkin.
- Sulkulistat ovat saatavilla ilmoitetuilla tavalla niiden voimassaolon ajan.

5.8.2. Rekisteröijän toiminnan ja siihen liittyvien oikeuksien lakkauttaminen

Rekisteröijän toiminnan ja siihen liittyvien oikeuksien lakkauttaminen on tilanne, jossa varmentajan terveydenhuollon organisaatiolle myöntämä oikeus rekisteröidä terveydenhuollon ammattivarmenteita suljetaan pysyvästi.

Rekisteröijän toiminnan lakkauttaminen tapahtuu rekisteröijän ja varmentajan välisen sopimuksen mukaisesti.

6. TEKNISEN TURVALLISUUDEN HALLINTA

Tässä luvussa käsitellään varmentajan, rekisteröijän ja terveydenhuollon ammattihenkilön julkisen ja yksityisen avaimen hallinnan ehdot ja vastaavat tekniset määritykset.

Terveydenhuollon ammattihenkilön avainparin voi luoda varmentaja tai toinen organisaatio varmentajan valtuutuksella. Kaikissa tapauksissa varmentaja seuraa avainparin luontiin liittyvien ehtojen täyttymistä ja vastaa osaltaan avainparin toimivuudesta.

6.1. Avainparien luonti ja toimittaminen varmenteen haltijalle

6.1.1. Avainparien luonti

Varmentajan avainpari luodaan ja säilytetään turvalaskentalaitteistossa, joka on Euroopan yhteisöjen komission vahvistamien ja Euroopan yhteisöjen virallisessa lehdessä julkaistujen yleisesti tunnustettujen standardien mukainen, kuten FIPS 140-1 tai 140-2 level 3 tasoinen hyväksyntä.

Varmenteen haltijan avainparit luodaan ammattikortin sirulla.

Avainparien turvallinen luomis- ja tallentamisprosessi estää avaimen paljastumisen avaimen luomiseen käytettävän laitteiston ulkopuolelle.

6.1.2. Yksityisen avaimen toimittaminen terveydenhuollon ammattihenkilölle

Yksityiset avaimet sisältävä ammattikortti ja sen käytön mahdollistavat tunnusluvut toimitetaan terveydenhuollon ammattihenkilölle siten, ettei ulkopuolisten ole mahdollista saada niitä haltuunsa.

6.1.3. Varmenteen hakijan julkisen avaimen toimittaminen varmentajalle

Varmenteen hakijan julkinen avain siirretään varmentajan järjestelmien välillä käyttäen turvallista tietoliikenneyhteyttä.

6.1.4. Varmentajan julkisen avaimen toimittaminen luottaville osapuolille

Varmentajan julkisen avaimen sisältävän varmentajan varmenteen voi hakea julkisesta hakemistosta tai varmentajan ylläpitämästä palvelusta. Varmentajan varmenne tallennetaan myös jokaiselle terveydenhuollon ammattikortille.

6.1.5. Avainten pituus

Varmentajan avaimet ovat 2048 bitin pituisia RSA-avaimia.

Terveydenhuollon ammattihenkilön allekirjoitusavaimet sekä todentamisavaimet ovat 2048 bitin pituisia RSA-avaimia.

6.1.6. Julkisen avaimen parametrien luonti ja laatu

Avainparien luonnissa käytetään standardoituja, korkeatasoisia, tunnettuja ja testattuja menetelmiä ja turvalaskentalaitteistoja.

6.1.7. Avainten käyttötarkoitukset

Varmentajan avainparin käyttötarkoitukset ovat varmenteen allekirjoitus ja sulkulistan allekirjoitus.

Terveydenhuollon ammattihenkilön avainparien käyttötarkoitukset ovat varmenteen haltijan todentaminen ja tiedon salaaminen sekä kehittynyt sähköinen allekirjoitus.

6.2. Yksityisen avaimen suojaaminen ja turvalaskentalaitteiston hallinta

6.2.1. Käytetyt standardit

Varmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa turvalaskentalaitteistoissa (HSM), jotka täyttävät FIPS 140-1 tai 140-2 level 3 asettamat vaatimukset. Varmentajan yksityiset avaimet on suojattu paljastumiselta ja luvattomalta käytöltä.

Varmentaja varmistaa, että terveydenhuollon ammattihenkilön yksityinen avain, joka on talletettu ammattikorttiin, toimitetaan terveydenhuollon ammattihenkilölle tämän varmennuskäytännön menettelytapojen mukaisesti.

Terveydenhuollon ammattihenkilön ammattikortti on kulloinkin voimassaolevien tarkoitukseen soveltuvien standardien mukainen, kuten ISO/IEC 7816 ja IAS ECC v1.01.

Ammattikortin siru ja sen käyttöjärjestelmä on turvasertifioitu. Hyväksyttyjä turvasertifiointeja ovat FIPS 140-1 tai 140-2 level 3 tai korkeampi, Common Criteria EAL4+ ja ISO/IEC 15408.

6.2.2. Yksityinen avain usean henkilön hallinnassa

Varmentajan yksityisten avainten hallintaan vaaditaan vähintään kahden avainten hallintaan oikeutetun henkilön läsnäolo.

Sekä rekisteröijän että terveydenhuollon ammattihenkilön yksityistä avainta voi hallita ja käyttää vain avaimen haltija itse.

6.2.3. Yksityisten avainten vara-avainjärjestelmä

Terveydenhuollon ammattikorttien vara-avainjärjestelmä ei ole käytössä.

6.2.4. Yksityisen avaimen varmuuskopiointi

Varmentajan yksityisestä avaimesta on varmuuskopio.

Varmentajan varmuuskopioidun yksityisen avaimen turvallisuusominaisuudet ja säilytys vastaavat varmentajan alkuperäisen yksityisen avaimen turvallisuusvaatimuksia kaikissa tilanteissa.

Terveydenhuollon ammattihenkilön yksityisistä avaimista ei oteta eikä säilytetä kopioita.

Terveydenhuollon ammattihenkilön yksityinen avain ei missään ammattikortin elinkaaren vaiheessa paljastu ulkopuoliselle henkilölle, eikä terveydenhuollon ammattihenkilön yksityisiä avaimia säilytetä muualla kuin terveydenhuollon ammattikortilla.

6.2.5. Yksityisten avainten arkistointi

Varmentajan yksityiset avaimet tuhotaan niiden voimassaoloajan päättymisen jälkeen.

Terveydenhuollon ammattihenkilön yksityisiä avaimia ei arkistoida. Varmentajalla ei ole pääsyä varmenteen haltijoiden yksityisiin avaimiin.

6.2.6. Yksityisten avainten käsittely turvalaskentalaitteistossa

Varmentajalla on oikeus siirtää varmentajan yksityiset avaimet toiseen turvalaskentalaitteistoon alkuperäisen laitteiston huoltoa tai vaihtamista varten.

6.2.7. Yksityisten avainten säilyttäminen

Varmentajan yksityiset avaimet säilytetään turvalaskentalaitteistossa salattuna.

Varmenteen haltijan yksityisiä avaimia säilytetään ammattikortin sirulla siten, että niitä ei voi lukea, muuttaa, kopioida tai siirtää sieltä pois.

6.2.8. Yksityisten avainten aktivointi

Varmentajan yksityisten avainten aktivointi tapahtuu tehtävään oikeutettujen henkilöiden toimesta turvalaskentalaitteiston hallintakorttien avulla.

Varmenteen haltijan yksityiset avaimet on suojattu paljastumiselta ja luvattomalta käytöltä ammattikortin sirulla. Vain sirulla suoritettavilla sisäisillä komennoilla on pääsy sirulla oleviin yksityisiin avaimiin.

Jotta yksityisiin avaimiin liittyvä sirun komento suoritetaan, tulee kyseisen avaimen olla aktivoitu oikealla PIN-tunnusluvulla.

Ammattikortin PIN-tunnusluku lukittuu viiden epäonnistuneen tunnusluvun syötön jälkeen.

Ammattikortilla on PIN-tunnusluvun lukituksen avausmahdollisuus. Lukitun PIN-tunnusluvun avaus vaatii oikean PUK-avaustunnusluvun syöttämistä.

6.2.9. Yksityisten avainten käytön estäminen

Varmentajan yksityisten avainten käyttö estetään tehtävään oikeutettujen henkilöiden toimesta hallintakorttien avulla tai kytkemällä varmentajan yksityiset avaimet sisältävästä turvalaskentalaitteistosta virta pois.

Ammattikortin yksityisten avainten käyttö estetään poistamalla ammattikortti kortinlukijasta.

6.2.10. Yksityisen avaimen tuhoaminen

Vain varmentaja voi tuhota varmentajan yksityiset avaimet.

Varmentajan lakkautuksen yhteydessä varmentajan yksityiset avaimet sekä niiden kopiot tuhotaan.

Mikäli terveydenhuollon ammattihenkilö haluaa tuhota oman yksityisen avaimensa, hänen tulee ilmoittaa sulkupalveluun kyseisen ammattikortin sulkemisesta ja pitää huolta siitä, että ammattikortin sirulla oleva tieto tuhoutuu esimerkiksi leikkaamalla kortti kahtia sirun keskeltä.

6.2.11. Ammattikorttien ja turvalaskentalaitteistojen turvatason luokitus

Ammattikorttien ja turvalaskentalaitteistojen tulee täyttää luvussa 6.2.1 mainitut standardit ja niiden luokat.

6.3. Muita avainparin hallintaan vaikuttavia seikkoja

Jokaisesta yksilöllisestä avainten luontiin liittyvästä prosessista kerätään tietoja. Näihin tietoihin sisältyvät ammattikorttitilauksen tiedot ja valmistettujen ammattikorttien korttinumerot sekä varmenteet.

6.3.1. Julkisten avainten arkistointi

Varmentaja arkistoi varmentamansa julkiset avaimet luvun 5.5 mukaisesti.

6.3.2. Varmenteiden ja avainten voimassaoloaika

Terveydenhuollon ammattihenkilön varmenne ja avainpari ovat voimassa enintään 60 kuukautta. Voimassaoloajan laskeminen alkaa varmenteen myöntämishetkestä. Varmenne voidaan tarvittaessa myöntää myös määräajaksi.

Varmentajan varmenteen ja avainparin voimassaoloaika on 13 vuotta avainten luomispäivästä. Avaimia ei käytetä ennen voimassaoloaikaa tai voimassaoloajan päätyttyä mihinkään tarkoitukseen.

6.4. Aktivointitiedot

6.4.1. Aktivointitiedon luonti

Aktivointitieto eli PIN-tunnusluku sekä avaustunnusluku eli PUK-tunnusluku luodaan ammattikortin yksilöinnin yhteydessä. Tunnusluvut perustuvat satunnaislukuihin. PIN-tunnusluku suojaa ammattikortin yksityisiä avaimia. Varmenteen haltijalla on mahdollisuus muuttaa PIN-tunnusluku haluamakseen vähintään 4 merkkiä pitkäksi luvuksi.

Lukkiutuneen PIN-tunnusluvun avaamiseen tarvittava PUK-avaustunnusluku on 8 merkkiä pitkä. PUK-avaustunnusluku säilytetään varmentajan tietojärjestelmässä.

6.4.2. Aktivointitiedon suojaus

PIN-tunnusluvut toimitetaan varmenteen haltijalle suljetussa tunnuslukukuoressa ja ne ovat vain varmenteen haltijan tiedossa. Varmenteen haltija voi halutessaan vaihtaa ammattikortin PIN-tunnusluvut haluamikseen vähintään 4 merkkiä pitkiksi luvuiksi. PUK-avaustunnuslukua ei voi muuttaa.

6.4.3. Muita huomioitavia seikkoja aktivointitiedosta

—

6.5. Tietokonelaitteistojen turvallisuuden hallinta

Varmentajan järjestelmien turvallisuuden hallintaan kuuluvat muun muassa käyttäjän vahva tunnistus ja varmentajan yksityisiin avaimiin liittyvien toimintojen ja tehtävien jäljitettävyys henkilötasolle asti sekä lokitietojen keruu. Tietokonelaitteistot sijaitsevat suojatuissa tiloissa.

Rekisteröijän tietokonelaitteistojen turvallisuudesta huolehditaan siten, että laitteistojen asiaton käyttö on estetty.

6.5.1. Erityisvaatimukset

Tietokonelaitteistojen turvallisuusvaatimusten osalta noudatetaan VAHTI 5/2004 -ohjetta.

6.5.2. Laitteistoturvallisuuden luokittelu

—

6.6. Elinkaaren turvallisuuden hallinta

6.6.1. Järjestelmien kehittämisen hallinta

Varmentajan järjestelmien kehittäminen tapahtuu tuotantojärjestelmästä erotetussa kehitysympäristössä.

Kaikki varmentajan tietojärjestelmiin tehtävät päivitykset tehdään varmistamalla toimivuus ensin testiympäristössä. Päivitykset suunnitellaan tapauskohtaisesti sekä aikataulutetaan ja tiedotetaan etukäteen. Suunnitelma sisältää testaussuunnitelman ja hyväksymiskriteerit.

Versiovaihdoksissa varmistetaan tietojärjestelmän koko tietojenkäsittelyketjun toimivuus. Käyttöönottovaihe suunnitellaan siten, että nopea palaaminen vanhaan versioon on mahdollista määrätyn ajan puitteissa.

6.6.2. Turvallisuuden hallinta

Tietojärjestelmien turvallisuuden hallinnassa noudatetaan VAHTI 5/2004 -ohjettan. Turvallisuuden hallinta perustuu:

- työtehtävien jakoon eri henkilöille luvun 5.2 mukaisesti;
- turvallisuuden seurantaan;
- säännöllisiin turvallisuuteen kohdistuviin tarkastuksiin;
- teknisiin turvaratkaisuihin ja -menetelmiin; ja
- sovellusmuutosten valtuutus- ja hyväksymismenettelyyn.

6.6.3. Elinkaaren turvallisuusluokittelu

—

6.7. Tietoverkon turvallisuuden hallinta

Varmentajan järjestelmien tietoliikenneyhteydet ja tietoverkot on vahvasti salattu ja suojattu sekä dedikoitu. Tietoverkon valvonnasta vastaa varmentaja.

Tietoliikenneyhteyksien turvallisuusvaatimusten osalta noudatetaan VAHTI 5/2004 -ohjetta.

6.8. Aikaleima

Aikaleimapalvelu ei ole toistaiseksi käytössä.

7. VARMENTEEN JA SULKULISTAN PROFIILI

7.1. Varmenteen profiili

Terveydenhuollon ammattivarmenteen profiili on kuvattu määrityksessä THPKI - T2: Väestörekisterikeskuksen CA-malli ja varmenteiden tietosisältö terveydenhuollossa.

7.2. Sulkulistan profiili

Terveydenhuollon ammattivarmenteiden sulkulistan profiili on kuvattu määrityksessä FINEID S2 - VRK (PRC) CA-model and certificate contents.

7.3. Reaaliaikainen sulkulistan tarkistus (OCSP)

OCSP-protokolla ei ole käytössä.

8. HYVÄKSYMISTARKASTUS

Varmentaja vastaa, että sen varmennetoiminta noudattaa tätä varmennuskäytäntöä sekä varmennepolitiikkaa.

8.1. Hyväksymistarkastusten suorittaminen

Varmentajan toiminta tarkastetaan vähintään kerran vuodessa. Tarkastuksen avulla selvitetään, toimiiko varmentaja varmennepolitiikan ja varmennuskäytännön mukaisesti. Tarkastuksen toimeenpanosta vastaa varmentaja.

8.2. Tarkastaja

Tarkastuksen voi tehdä yleisesti riippumattomaksi ja hyvämaineiseksi tunnustettu tietojärjestelmien tarkastuksiin erikoistunut tarkastuslaitos, joka sijaitsee Suomessa tai muussa Euroopan talousalueeseen kuuluvassa valtiossa.

8.3. Tarkastuksen suorittajan suhde tarkastettavaan osapuoleen

Tarkastuksen suorittaja on tarkastettavaan kohteeseen nähden ulkopuolinen ja sitoutumaton.

8.4. Tarkastuksen kattavuus

Tarkastuksessa verrataan varmennepolitiikkaa ja varmennuskäytäntöä varmentajan koko toimintaan. Tarkastukseen kuuluu myös varmentajan varmentamiseen ja rekisteröimiseen liittyvien tietojärjestelmien tietoturvallisuuden tarkastaminen.

Tarkastus koskee myös varmentajan alihankkijoita ja muita toimittajia.

Tarkastuksen tulokset kirjataan lausunnoksi.

8.5. Toimenpiteet, joihin ryhdytään poikkeamien esiintyessä

Varmentaja ryhtyy välittömästi havaittujen poikkeamien vaatimiin toimenpiteisiin tilanteen korjaamiseksi.

8.6. Tarkastuksen tuloksista tiedottaminen

Tarkastettu dokumenttien ja toiminnan tila kuvataan tarkastuskertomuksen julkisessa lausuntoosassa. Tarkastuskertomus kokonaisuudessaan luovutetaan pyynnöstä sopimuksien mukaan asianosaisille varmentajan yhteistyökumppaneille.

9. YLEISET EHDOT

Tämä luku sisältää varmentajan, rekisteröijän, terveydenhuollon ammattihenkilön ja muiden varmennejärjestelmän toimintaan liittyvien osapuolten velvollisuudet ja vastuut sekä ristiriitojen selvittämiseen liittyvät kysymykset.

9.1. Maksut ja muut palkkiot

Maksut ja muut palkkiot määräytyvät sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) annetun lain 22§:n nojalla sekä kulloinkin voimassa olevan valtiovarainministeriön asetuksen Väestörekisterikeskuksen suoritteiden maksuista mukaisesti.

9.1.1. Varmenteen myöntämismaksu

—

9.1.2. Varmenteen käyttömaksu

—

9.1.3. Varmenteen sulkumaksu tai tilan kyselymaksu

Varmenteen ilmoittaminen sulkulistalle on maksutonta. Myös sulkulistojen noutaminen hakemistosta sekä varmenteen voimassaolon tarkistaminen sulkulistalta on maksutonta.

9.1.4. Maksut muista palveluista kuten neuvontapalvelusta

Neuvontapalvelun käytöstä peritään erillinen maksu voimassaolevan hinnaston mukaisesti.

9.1.5. Hyvitykset

Hyvitykset määräytyvät varmennejärjestelmän osapuolien kanssa solmittujen sopimusten perusteella.

9.2. Taloudelliset velvollisuudet

Varmentaja vastaa lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009) mukaisesti, että sillä on riittävät taloudelliset voimavarat varmennetoiminnan asianmukaiseksi järjestämiseksi sekä mahdollisen vahingonkorvausvastuun kattamiseksi.

9.3. Luottamuksellisuus ja tietosuoja

Luottamuksellisuudessa ja tietosuojassa noudatetaan lakeja, asetuksia sekä hyvää tiedonhallintatapaa ja periaatteita.

9.3.1. Yksityiset tiedot

Yksityisiä tietoja voidaan paljastaa vain lain taikka lakiin perustuvan säännöksen nojalla tai varmenteen haltijan suostumuksella.

Kaikki yksityiset avaimet, joita varmentaja käyttää tai käsittelee tämän varmennuskäytännön alaisessa toiminnassaan, ovat salaisia.

Kerättyjä rekistereitä ja lokitietoja julkaistaan vain, mikäli laki tai asetus taikka niiden nojalla annettu määräys sitä edellyttää.

9.3.2. Julkiset tiedot

Todentamisvarmenteiden julkiset avaimet ja sulkulista ovat julkista tietoa ja kaikkien saatavilla julkisessa hakemistossa.

Yksilöintitiedot tai muut yksityiset tai yritykseen liittyvät tiedot, jotka ovat myönnetyssä varmenteessa, ovat julkisia, ellei sopimuksissa taikka laissa, asetuksessa tai niiden nojalla annetussa määräyksessä toisin määrätä.

9.3.3. Yksityisten tietojen suojaaminen

Kaikkien varmennejärjestelmään liittyvien osapuolten tulee noudattaa yksityisten tietojen suojaamisesta säädettyjä lakeja, asetuksia ja suosituksia.

9.4. Yksityisyyden suoja

Yksityisyyden suojan osalta noudatetaan voimassa olevaa lainsäädäntöä.

9.4.1. Yksityisten tietojen suojaamissuunnitelma

Varmennejärjestelmään liittyvien osapuolten on huolehdittava yksityisten tietojen suojaamissuunnitelman laatimisesta ja toteuttamisesta.

9.4.2. Varmentajan järjestelmissä käsiteltävät yksityiset tiedot

Varmentajan järjestelmissä tapahtuvassa yksityisten tietojen käsittelyssä noudatetaan henkilötietojen käsittelyä ja yksityisyydensuojaa koskevaa lainsäädäntöä.

9.4.3. Varmentajan järjestelmissä käsiteltävät julkiset tiedot

Varmentajan järjestelmissä tapahtuvassa julkisten tietojen käsittelyssä noudatetaan lakia viranomaisten toiminnan julkisuudesta (621/1999).

9.4.4. Vastuu yksityisten tietojen suojaamisesta

Varmentaja vastaa siitä, että varmentajan järjestelmissä käsiteltävät yksityiset tiedot on suojattu asiattomalta käsittelyltä.

9.4.5. Yksityisten tietojen käyttäminen tai julkistaminen varmenteen haltijan suostumuksella

Tietojen luottamuksellisuus ja tietosuoja on määritelty luvussa 9.3.

9.4.6. Tietojen luovutus viranomaisille

Viranomaisille luovutetaan tietoja lakien, asetusten taikka niiden nojalla annettujen määräysten perusteella.

9.4.7. Muut olosuhteet, joissa tiedot voidaan julkistaa

Varmentaja ei luovuta tietoja muissa kuin edellä mainituissa olosuhteissa.

9.5. Immateriaalioikeudet

Väestörekisterikeskus omistaa kaikki varmenteisiin ja dokumentaatioon liittyvät tiedot teknisten toimitussopimusten mukaisesti. Väestörekisterikeskus omistaa täydet omistus- ja käyttöoikeudet tähän varmennepolitiikkaan.

9.6. Osapuolten sitoumukset

9.6.1. Varmentajan sitoumukset

Varmentaja sitoutuu tuottamaan, ylläpitämään ja kehittämään terveydenhuollon varmennepalveluja tämän varmennuskäytännön ja varmennepolitiikan mukaisesti.

9.6.2. Rekisteröijän sitoumukset

Rekisteröijän tulee sitoutua omalta osaltaan tuottamaan, ylläpitämään ja kehittämään terveydenhuollon rekisteröintipalveluja tämän varmennuskäytännön ja varmennepolitiikan mukaisesti.

9.6.3. Varmenteen haltijan sitoumukset

Varmenteen haltija sitoutuu käyttämään terveydenhuollon ammattivarmennetta ja ammattikorttia tämän varmennuskäytännön, varmennepolitiikan ja annettujen ohjeiden mukaisesti.

9.6.4. Varmenteisiin luottavien osapuolten sitoumukset

Varmenteisiin luottavat osapuolet sitoutuvat vastaamaan omien terveydenhuollon järjestelmiensä ja terveydenhuollon ammattivarmenteiden yhteensopivuudesta.

9.6.5. Muiden osapuolten sitoumukset

—

9.7. Vastuuvapauslauseke

Varmentajan ja varmentajan sopimuskumppanin välisten sopimusten sekä varmentajan varmenteen haltijalle ja varmennejärjestelmää hyödyntävälle taholle erikseen asettamien vaatimusten sisältämät vastuuvapauslausekkeet sitovat varmentajan sopimuskumppania, varmenteenhaltijaa ja varmennejärjestelmää hyödyntävää tahoa samalla tavoin kuin tähän varmennuskäytäntöön sisältyvät vastuuvapauslausekkeet ja vastuunrajoitukset.

9.8. Vastuunrajoitukset

Varmennepalveluiden tuottamiseen liittyvä Väestörekisterikeskuksen vahingonkorvausvastuu määräytyy vahingonkorvauslain (412/1974) säännösten mukaisesti. Väestörekisterikeskusta koskevat myös lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista ja sähköisestä asioinnista viranomaistoiminnassa annetun lain mukaiset varmentajan vastuut.

Varmentaja ei vastaa PIN-tunnuslukujen, PUK-avaustunnusluvun ja varmenteen haltijan yksityisten avainten paljastumisen seurauksena syntyvistä vahingoista, ellei paljastuminen välittömästi johdu varmentajan välittömästä toiminnasta.

Varmentaja vastaa varmenteen haltijalle ja varmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu varmentajan välittömästä toiminnasta.

Varmentaja ei vastaa varmenteen haltijalle aiheutuneista välillisistä tai seurannaisvahingoista. Varmentaja ei myöskään vastaa varmenteeseen luottavan osapuolen tai varmenteen haltijan muun sopimuskumppanin mahdollisesti kärsimistä välillisistä tai seurannaisvahingoista.

Varmentaja ei vastaa yleisten tietoliikenneyhteyksien eikä tietoverkkojen, esimerkiksi internetin toimivuudesta eikä siitä, jos oikeustoimen suorittaminen estyy varmenteen haltijan käyttämän laitteen tai kortinlukijaohjelmiston toimimattomuudesta eikä siitä, että varmennetta käytetään vastoin sen käyttötarkoitusta.

Varmentajalla on oikeus keskeyttää palvelu muutos- tai huoltotoimien ajaksi. Sulkulistaa koskevista muutoksista tai huoltotöistä ilmoitetaan etukäteen.

Varmentajalla on oikeus kehittää edelleen varmennepalvelua. Varmenteen haltijan tai varmenteeseen luottavan osapuolen on vastattava tämän vuoksi aiheutuvista omista kustannuksistaan eikä varmentaja ole velvollinen korvaamaan varmenteen haltijalle tai varmenteeseen luottavalle osapuolelle tällaisesta varmentajan kehittämistyöstä aiheutuvista kustannuksista.

Varmentaja ei vastaa varmennetta käytettäessä loppukäyttäjälle tarkoitetun varmenteeseen pohjautuvan verkkopalvelun tai sovelluksen virheistä tai niistä aiheutuvista kustannuksista. Varmenteen haltijan vastuu varmenteen käyttämisestä päättyy, kun hän on ilmoittanut sulkupalveluun tarvittavat tiedot varmenteen sulkemiseksi ja saatuaan puhelun vastaanottaneelta virkailijalta ilmoituksen varmenteen sulkulistalle viemisestä. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

9.9. Vahingonkorvaukset

Varmennepalveluiden tuottamiseen liittyvä Väestörekisterikeskuksen vahingonkorvausvastuu määräytyy vahingonkorvauslain (412/1974) säännösten mukaisesti. Väestörekisterikeskusta koskevat myös lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009) ja sähköisestä asioinnista viranomaistoiminnassa annetun lain (13/2003) mukaiset varmentajan vastuut.

9.10. Voimassaoloaika ja voimassaolon päättyminen

9.10.1. Varmennuskäytännön voimassaoloaika

Varmennuskäytäntö on voimassa siihen asti, kunnes uusi versio kyseisestä varmennepolitiikasta korvaa sen.

9.10.2. Varmennuskäytännön voimassaolon päättyminen

Varmennuskäytännöllä ei ole erikseen määrättyä voimassaoloaikaa.

9.10.3. Varmennuskäytännön voimassaolon päättymisen vaikutukset

—

9.11. Varmennepalvelun osapuolien keskinäinen viestintä

Varmentajan ja varmennetoimintaan liittyvien yhteistyötahojen on tiedotettava kaikissa tapauksissa toimintaansa liittyvistä muutoksista. Tiedottaminen muutoksista tapahtuu kirjallisesti kaikille yhteistyökumppaneille.

9.12. Varmennuskäytännön muutosten hallinta

Varmennuskäytäntöön tehtävistä muutoksista päättää varmentaja.

9.12.1. Varmennuskäytännön muuttaminen

Väestörekisterikeskus hyväksyy sekä ammattivarmennetta koskevan varmennepolitiikan että varmennuskäytännön. Asiakirjoja voidaan muuttaa Väestörekisterikeskuksen sisäisin muutosmenettelyin. Väestörekisterikeskus ilmoittaa muutoksista hyvissä ajoin ennen niiden voimaantuloa sekä Viestintävirastolle että omilla www-sivuillaan. Väestörekisterikeskus pitää asiakirjoista versionhallintaa sekä arkistoi kaikki varmennepolitiikka- ja varmennuskäytäntöasiakirjat. Typografiset korjaukset ja yhteystietojen muutokset ovat mahdollisia välittömästi.

9.12.2. Muutoksista tiedottaminen

1. Kaikkia varmennepolitiikan ja varmennuskäytännön kohtia voidaan muuttaa 1.5.2011 jälkeen ilmoittamalla tulevista pääasiallisista muutoksista 30 päivää ennen muutosten voimaan astumista.

2. Kohtia, jotka Väestörekisterikeskuksen mielestä eivät merkittävästi vaikuta varmenteiden haltijoihin ja luottaviin osapuoliin, voidaan muuttaa 1.5.2011 jälkeen ilmoittamalla niistä 14 päivää aikaisemmin.

9.12.3. Varmennuskäytännön tunnistetiedon muuttaminen

Varmennuskäytännön tunnistetieto ei muutu, vaikka varmennuskäytännön sisältöä muutetaan.

9.13. Erimielisyyksien ratkaiseminen

Terveydenhuollon varmennepalveluun ja tähän varmennuskäytäntöön liittyvät mahdolliset erimielisyydet pyritään ratkaisemaan osapuolten välisissä neuvotteluissa. Mikäli ratkaisuun ei päästä, osapuolten väliset erimielisyydet käsitellään Suomessa varmentajan kotipaikan käräjäoikeudessa.

9.14. Sovellettava laki

Terveydenhuollon varmennepalveluun ja tähän varmennuskäytäntöön sovelletaan Suomen lakia.

9.15. Lain noudattaminen

Terveydenhuollon varmennepalveluiden järjestämisessä noudatetaan yksinomaan Suomen lakia.

9.16. Muut järjestelyt

9.16.1. Sopimukset

Varmentajan ja varmenteen haltijan väliset oikeudet, vastuut ja velvollisuudet määritellään varmennepolitiikassa sekä varmennuskäytännössä. Allekirjoittamalla varmennehakemuksen terveydenhuollon ammattihenkilö sitoutuu noudattamaan varmenteen käyttöehtoja. Voimassaolevat käyttöehdot luovutetaan terveydenhuollon ammattihenkilölle varmenteen luovutuksen yhteydessä.

Allekirjoituksellaan terveydenhuollon ammattihenkilö sitoutuu välittömästi ilmoittamaan sulkupalveluun ammattikortin katoamisen, epäilemänsä väärinkäytöksen tai sen mahdollisuuden.

Varmentaja solmii varmentajan valtuuttamina toimivien rekisteröijien kanssa sopimuksen, josta ilmenevät molempien osapuolten oikeudet, vastuut ja velvollisuudet.

Varmentaja voi laatia sopimuksia luottavien osapuolten tai muiden osapuolten kanssa. Sopimuksista tulee käydä selkeästi ilmi molempien sopimusosapuolten oikeudet, vastuut ja velvollisuudet.

Varmentaja laatii tarvittavat sopimukset varmennepalvelun toimittajan ja osatoimittajien kanssa.

9.16.2. Oikeudenluovutus

Terveydenhuollon varmennepalvelun sopimusosapuolet eivät saa siirtää sopimuksissa määriteltyjä oikeuksiaan muille osapuolille ilman varmentajan etukäteen antamaa hyväksymistä.

9.16.3. Pätemättömyys

Tämän varmennuskäytännön yksittäisen määräyksen mahdollinen mitättömyys, pätemättömyys taikka täytäntöönpanokelvottomuus ei vaikuta varmennuskäytännön pätevyyteen muilta osin.

9.16.4. Täytäntöönpano

Vaikka varmentaja yksittäisessä sopimusrikkomusasiassa luopuisi oikeudestaan vahingonkorvaukseen tai muuhun hyvitykseen, se ei merkitse luopumista oikeudesta vahingonkorvaukseen samasta vahingosta tai muista sopimusrikkomuksista tulevaisuudessa.

9.16.5. Ylivoimainen este

Varmentaja ei vastaa luonnonmullistuksista tai muista vastaavista ylivoimaisista olosuhteista johtuvista vahingoista. Lisää esteitä

9.17. Muut ehdot

Terveydenhuollon varmennepalveluita käsitteleviä dokumentteja ja asiakirjoja, tätä varmennuskäytäntöä sekä varmennejärjestelmän osapuolten ja heidän sopimuskumppaniensa välisiä sitoumuksia tulkittaessa ja sovellettaessa ratkaisevat ensisijaisesti asiakirjojen suomenkieliset versiot.