



DIGI- JA
VÄESTÖTIETO-
VIRASTO

Varmennekäytäntö

**sosiaali- ja terveydenhuollon ammatti-
varmennetta varten**

OID: 1.2.246.517.1.10.206.1

22.9.2022



ISO 9001



ISO/IEC 27001



Dokumentinhallinta

Omistaja	
Laatinut	Tuire Saaripuu
Tarkastanut	
Hyväksynyt	Mikko Pitkänen

Version hallinta

versionro	mitä tehty	pvm/henkilö
Versio 1.0	Hyväksytty versio 1.0	3.5.2018
Versio 1.1	Hyväksytty versio 1.1, virastonimimuutokset	1.1.2020
Versio 1.2	Päivitetty versio, saavutettavuusominaisuudet	6.5.2021
Versio 1.3	Päivitetty versio ja linkit varmennepolitiikkasivulle	22.9.2022/SK



Sisällysluettelo

1	[Kirjoita teksti tähän]	9
1.1	[Kirjoita teksti tähän]	9
1.1.1	[Kirjoita teksti tähän]	9
1.1.1.1	[Kirjoita teksti tähän]	9
2	Johdanto	9
2.1	Taustaa	10
2.2	Varmennuskäytännön tunnukset	11
2.3	Osapuolet ja soveltuvuus	12
2.3.1	Varmentaja	12
2.3.2	Rekisteröijä	13
2.3.3	Varmenteen haltija	13
2.3.4	Varmenteeseen luottava osapuoli	14
2.3.5	Muut osapuolet	14
2.4	Varmenteen käyttökohteet	14
2.4.1	Sallitut varmenteen käyttötarkoitukset	14
2.4.2	Kielletyt varmenteen käyttötarkoitukset	15
2.5	Yhteystiedot	15
2.5.1	Varmennuskäytännön hallintaorganisaatio	15
2.5.2	Yhteystiedot	15
2.5.3	Varmennuskäytäntöjen suhde varmennepolitiikkaan	15
2.5.4	Varmennuskäytäntöjen hyväksymismenettely	16
2.6	Määritelmät ja lyhenteet	16
3	tietojen Julkaiseminen	21
3.1	Julkinen hakemisto	21
3.2	Varmentajan julkaisemat tiedot	21
3.3	Julkaisutiheys	21
3.4	Pääsyoikeudet	21
4	Tunnistaminen ja todentaminen	21
4.1	Varmenteen haltijan nimeäminen	21
4.1.1	Nimeäminen	21
4.1.2	Nimeämisen merkitys	22
4.1.3	Anonyymit tai salanimet	23
4.1.4	Nimikenttien sisältö	23



4.1.5	Nimitietueen ainutkertaisuus	23
4.1.6	Tuotenimien käyttöoikeus	23
4.2	Henkilöllisyyden todentaminen	23
4.2.1	Menettelytapa yksityisen avaimen omistajuuden todistamiseksi	23
4.2.2	Varmenteen hakijan edustaman organisaation todentaminen	23
4.2.3	Henkilön tunnistaminen ja voimassaolevan ammattioikeuden todentaminen	23
4.2.4	Varmenteen hakijan tiedot, joita varmentaja ei tarkista	24
4.2.5	Varmenteen myöntämisen edellytykset	24
4.2.6	Varmentajien välisen yhteistyön edellytykset ja vaatimukset	24
4.3	Tunnistaminen ja todentaminen varmenteen uusimisessa	24
4.3.1	Tunnistaminen ja todentaminen varmenteen uusimisessa	24
4.3.2	Tunnistaminen ja todentaminen varmenteen sulkemisen jälkeen	24
4.4	Peruuttamispyynnön tekijän tunnistaminen	24
5	VARMENTEEN ELINKAAREN HALLINNAN TOIMINNALLISET VAATIMUKSET	25
5.1	Varmenteen hakeminen	25
5.1.1	Kuka voi tehdä varmennehakemuksen	25
5.1.2	Varmenteen myöntämisprosessi ja vastuut	25
5.2	Varmennehakemuksen käsittely	26
5.2.1	Tunnistamisen ja todentamisen toteuttaminen	26
5.2.2	Varmennehakemuksen hyväksyminen tai hylkääminen	26
5.2.3	Varmennehakemuksen käsittelyaika	26
5.3	Varmenteen myöntäminen	26
5.3.1	Varmenteen myöntämiseen liittyvät varmentajan tehtävät	26
5.3.2	Ilmoitus hakijalle varmenteen myöntämisestä	27
5.4	Myönnetyn varmenteen hyväksyminen	27
5.4.1	Myönnetyn varmenteen hyväksymismenettely varmenteen hakijan kannalta	27
5.4.2	Varmenteen julkaisu varmentajan toimesta	27
5.4.3	Ilmoitus muille osapuolille varmenteen myöntämisestä	27
5.5	Varmenteiden ja avainparien käyttö	27
5.5.1	Varmenteiden ja avainparien käyttö varmenteen haltijan toimesta	27
5.5.2	Varmenteiden ja julkisten avainten käyttö varmenteisiin luottavan osapuolen toimesta	28
5.6	Julkisen avaimen uudelleen varmentaminen	29
5.7	Varmenteen uusiminen	29
5.7.1	Varmenteen uusimisen syyt	29
5.7.2	Varmenteen uusimisen hakeminen	29



5.7.3	Varmenteen uusimispyynnön käsittely	29
5.7.4	Ilmoitus varmenteen hakijalle ammattikortin uusimisesta	29
5.7.5	Uusitun varmenteen hyväksymismenettely varmenteen haltijan kannalta	29
5.7.6	Uusitun varmenteen julkaisu	29
5.7.7	Ilmoitus uusitun varmenteen myöntämisestä muille osapuolille	29
5.8	Varmenteen muuttaminen	30
5.9	Varmenteen sulkeminen ja määräaikainen sulkeminen	30
5.9.1	Varmenteen sulkemisen edellytykset	30
5.9.2	Kuka voi vaatia varmenteen sulkemista	30
5.9.3	Varmenteen sulkemisprosessi	31
5.9.4	Varmenteen haltijan velvollisuus tehdä sulkupyyntö	31
5.9.5	Varmenteen sulkupyynnön käsittelyaika	31
5.9.6	Varmenteeseen luottavan osapuolen velvollisuus tarkistaa varmenteen voimassaolo	32
5.9.7	Sulkulistan julkaisutiheys	32
5.9.8	Sulkulistan voimassaolon enimmäisaika	32
5.9.9	Reaaliaikainen varmenteen tilan tarkistaminen	32
5.9.10	Vaatimukset varmenteen tilan reaaliaikaiselle tarkistamiselle	32
5.9.11	Muut varmenteen tilan tarkistamismenettelyt	32
5.9.12	Yksityisen avaimen paljastumisesta johtuva varmenteen sulkeminen	32
5.9.13	Varmenteen sulkeminen määräajaksi	32
5.9.14	Kuka voi vaatia varmenteen sulkemista määräajaksi	32
5.9.15	Menettelytavat varmenteen sulkemiseksi määräajaksi	32
5.9.16	Rajoitukset varmenteen määräaikaiselle sulkemiselle	33
5.10	Varmenteen tilan tarkistamismahdollisuus	33
5.11	Varmenteen voimassaolon päättyminen	33
5.12	Vara-avainjärjestelmä ja avainten palautus	33
6	Fyysisen, käyttö- ja henkilöstöturvallisuuden hallinta	33
6.1	Fyysisen turvallisuuden hallinta	33
6.1.1	Tilojen sijoittaminen ja rakenne	33
6.1.2	Fyysinen pääsynvalvonta	33
6.1.3	Sähkö ja ilmastointi	34
6.1.4	Vesivahinko	34
6.1.5	Tulipalo	34
6.1.6	Tietovälineiden säilytys	34
6.1.7	Tietovälineiden hävittäminen	34



6.1.8	Varmuuskopiointi verkon yli	34
6.2	Käyttöturvallisuuden hallinta	34
6.2.1	Työtehtäviin liittyvät roolit	34
6.2.2	Varmennetuotannon työtehtäviin tarvittavien henkilöiden määrä	35
6.2.3	Henkilöiden tunnistaminen ja todentaminen eri rooleihin	35
6.2.4	Tehtävien eriyttämistä vaativat roolit	35
6.3	Henkilöstöturvallisuuden hallinta	35
6.3.1	Tausta-, ansio-, kokemus- ja selvitysvaatimukset	35
6.3.2	Taustojen tarkistamisen menettelytapa	35
6.3.3	Koulutuksen tiheys ja vaatimukset	35
6.3.4	Jatkokoulutuksen tiheys ja vaatimukset	35
6.3.5	Työtehtävien kierrätyksen tiheys ja järjestys	36
6.3.6	Seuraukset luvattomista toimista	36
6.3.7	Alihankkijoiden henkilöstön vaatimukset	36
6.3.8	Asiakirjat, jotka toimitetaan henkilökunnalle	36
6.4	Varmennejärjestelmän turvallisuuden seuranta	36
6.4.1	Arkistoitavat tapahtumat	36
6.4.2	Lokitetöiden analysointitiheys	37
6.4.3	Lokitetöiden säilytysaika	37
6.4.4	Lokitetöiden suojaaminen	37
6.4.5	Lokitetöiden varmuuskopiointi	37
6.4.6	Lokitetöiden keräysjärjestelmän toteuttaminen (sisäinen/ulkoinen)	37
6.4.7	Lokitapahtumasta ilmoittaminen	37
6.4.8	Haavoittuvuuksien arviointi	37
6.5	Arkistoitavat aineistot	37
6.5.1	Arkistoitavat asiakirjat, tiedostot ja mediat	37
6.5.2	Arkistojen säilytysaika	38
6.5.3	Arkistojen suojaaminen	38
6.5.4	Arkistojen varmuuskopiointimenettely	38
6.5.5	Arkistoitavien tietojen aikaleima	38
6.5.6	Arkistojen keräysjärjestelmä (sisäinen/ulkoinen)	38
6.5.7	Arkistoissa olevien tietojen saatavuus ja eheys	38
6.6	Varmentajan avainparin vaihto	38
6.7	Häiriötilanteisiin varautuminen	38
6.7.1	Suunnitelma toimintahäiriöiden ja toiminnan vaarantumisen varalta	38



6.7.2	Varmennejärjestelmän, ohjelmistojen tai tietojen vahingoittuminen	38
6.7.3	Toiminta varmenteen haltijan yksityisen avaimen paljastuessa	39
6.7.4	Toiminnan jatkuvuus häiriötilanteen jälkeen	39
6.8	Lakkauttaminen	39
6.8.1	Varmentajan toiminnan lakkauttaminen	39
6.8.2	Rekisteröijän toiminnan ja siihen liittyvien oikeuksien lakkauttaminen.....	39
7	Teknisen turvallisuuden hallinta	40
7.1	Avainparien luonti ja toimittaminen varmenteen haltijalle	40
7.1.1	Avainparien luonti.....	40
7.1.2	Yksityisen avaimen toimittaminen terveydenhuollon ammattihenkilölle.....	40
7.1.3	Varmenteen hakijan julkisen avaimen toimittaminen varmentajalle	40
7.1.4	Varmentajan julkisen avaimen toimittaminen luottaville osapuolille	40
7.1.5	Avainten pituus	40
7.1.6	Julkisen avaimen parametrien luonti ja laatu	40
7.1.7	Avainten käyttötarkoitukset	41
7.2	Yksityisen avaimen suojaaminen ja turvalaskentalaitteiston hallinta	41
7.2.1	Käytetyt standardit.....	41
7.2.2	Yksityinen avain usean henkilön hallinnassa	41
7.2.3	Yksityisten avainten vara-avainjärjestelmä.....	41
7.2.4	Yksityisen avaimen varmuuskopiointi	41
7.2.5	Yksityisten avainten arkistointi	42
7.2.6	Yksityisten avainten käsittely turvalaskentalaitteistossa.....	42
7.2.7	Yksityisten avainten säilyttäminen	42
7.2.8	Yksityisten avainten aktivointi	42
7.2.9	Yksityisten avainten käytön estäminen	42
7.2.10	Yksityisen avaimen tuhoaminen.....	43
7.2.11	Ammattikorttien ja turvalaskentalaitteistojen turvataso luokitus.....	43
7.3	Muita avainparin hallintaan vaikuttavia seikkoja	43
7.3.1	Julkisten avainten arkistointi.....	43
7.3.2	Varmenteiden ja avainten voimassaoloaika	43
7.4	Aktivointitiedot	43
7.4.1	Aktivointitiedon luonti	43
7.4.2	Aktivointitiedon suojaus	44
7.4.3	Muita huomioitavia seikkoja aktivointitiedosta	44
7.5	Tietokonelaitteistojen turvallisuuden hallinta	44



7.5.1	Erityisvaatimukset	44
7.5.2	Laitteistoturvallisuuden luokittelu	44
7.6	Elinkaaren turvallisuuden hallinta	44
7.6.1	Järjestelmien kehittämisen hallinta	44
7.6.2	Turvallisuuden hallinta	44
7.6.3	Elinkaaren turvallisuusluokittelu	45
7.7	Tietoverkon turvallisuuden hallinta	45
7.8	Aikaleima	45
8	Varmenteen ja sulkulistan profiili	45
8.1	Varmenteen profiili	45
8.2	Sulkulistan profiili	45
8.3	Reaaliaikainen sulkulistan tarkistus (OCSP)	45
9	Hyväksymistarkastus	45
9.1	Hyväksymistarkastusten suorittaminen	45
9.2	Tarkastaja	46
9.3	Tarkastuksen suorittajan suhde tarkastettavaan osapuoleen	46
9.4	Tarkastuksen kattavuus	46
9.5	Toimenpiteet, joihin ryhdytään poikkeamien esiintyessä	46
9.6	Tarkastuksen tuloksista tiedottaminen	46
10	Yleiset ehdot	46
10.1	Maksut ja muut palkkiot	46
10.1.1	Varmenteen myöntämismaksu	46
10.1.2	Varmenteen käyttömaksu	47
10.1.3	Varmenteen sulkumaksu tai tilan kyselymaksu	47
10.1.4	Maksut muista palveluista kuten neuvontapalvelusta	47
10.1.5	Hyvitykset	47
10.2	Taloudelliset velvollisuudet	47
10.3	Luottamuksellisuus ja tietosuojatietosuojat	47
10.3.1	Yksityiset tiedot	47
10.3.2	Julkiset tiedot	47
10.3.3	Yksityisten tietojen suojaaminen	47
10.4	Yksityisyyden suoja	48
10.4.1	Yksityisten tietojen suojaamissuunnitelma	48
10.4.2	Varmentajan järjestelmissä käsiteltävät yksityiset tiedot	48
10.4.3	Varmentajan järjestelmissä käsiteltävät julkiset tiedot	48



10.4.4	Vastuu yksityisten tietojen suojaamisesta	48
10.4.5	Yksityisten tietojen käyttäminen tai julkistaminen varmenteen haltijan suostumuksella	48
10.4.6	Tietojen luovutus viranomaisille	48
10.4.7	Muut olosuhteet, joissa tiedot voidaan julkistaa	48
10.5	Immateriaalioikeudet	48
10.6	Osapuolten sitoumukset	48
10.6.1	Varmentajan sitoumukset	48
10.6.2	Rekisteröijän sitoumukset	49
10.6.3	Varmenteen haltijan sitoumukset	49
10.6.4	Varmenteisiin luottavien osapuolten sitoumukset	49
10.6.5	Muiden osapuolten sitoumukset	49
10.7	Vastuuvapauslauseke	49
10.8	Vastuunrajoitukset	49
10.9	Vahingonkorvaukset	50
10.10	Voimassaoloaika ja voimassaolon päättymisen	50
10.10.1	Varmennuskäytännön voimassaoloaika	50
10.10.2	Varmennuskäytännön voimassaolon päättymisen	50
10.10.3	Varmennuskäytännön voimassaolon päättymisen vaikutukset	50
10.11	Varmennepalvelun osapuolien keskinäinen viestintä	51
10.12	Varmennuskäytännön muutosten hallinta	51
10.12.1	Varmennuskäytännön muuttaminen	51
10.12.2	Muutoksista tiedottaminen	51
10.12.3	Varmennuskäytännön tunnistetiedon muuttaminen	51
10.13	Erimielisyyksien ratkaiseminen	51
10.14	Sovellettava laki	51
10.15	Lain noudattaminen	51
10.16	Muut järjestelyt	52
10.16.1	Sopimukset	52
10.16.2	Oikeudenluovutus	52
10.16.3	Pätemättömyys	52
10.16.4	Täytäntöönpano	52
10.16.5	Ylivoinainen este	52
10.17	Muut ehdot	53



Varmennekäytäntö

[Kirjoita teksti tähän]

1 [Kirjoita teksti tähän]

[Kirjoita teksti tähän]

1.1 [Kirjoita teksti tähän]

[Kirjoita teksti tähän]

1.1.1 [Kirjoita teksti tähän]

[Kirjoita teksti tähän]

1.1.1.1 [Kirjoita teksti tähän]

[Kirjoita teksti tähän]

2 Johdanto

Varmennepolitiikassa määritellään Digi- ja väestötietoviraston – jatkossa varmentaja (Certification Authority) – julkisen avaimen menetelmän (Public Key Infrastructure; PKI) mukaisen 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 Digi- ja väestötietoviraston (jäljempänä DVV) 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 sosiaali- ja 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.

Varmennepalveluita tarjoavan viraston nimenmuutoksesta on säädetty laissa Digi- ja väestötietovirastosta (304/2019). Väestörekisterikeskuksen nimi muuttuu 1.1.2020 Digi- ja väestötietovirastoksi.



2.1 Taustaa

DVV myöntää varmenteita terveydenhuollon ammattihenkilöistä annetussa laissa (559/1994) tarkoitettuille terveydenhuollon ammattihenkilöille. DVV myöntää sosiaalihuollon ammattivarmenteita henkilöille, jotka täyttävät lain (272/2005) sosiaalihuollon ammatillisen henkilöstön kelpoisuusvaatimuksista kuvatut edellytykset laissa luetelluissa tehtävissä toimimiselle.

Digi- ja väestötietovirasto tarjoaa tietoturvallisuuden tasoltaan korkealaatuisia sähköisen allekirjoituksen ja tunnistamisen varmenteita ja niihin liittyviä palveluja. Varmenteen avulla varmennetaan varmenteen haltijan henkilöllisyys sekä varmenteeseen sisältyvien tietojen oikeellisuus, eheys ja alkuperäisyys. Allekirjoitusvarmenteella 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. Allekirjoitusvarmenteen ja vahvan sähköisen tunnistuspalvelun tarjoajia valvoo Suomessa Traficom.

Tässä asiakirjassa määritellään menettelytapavaatimukset, jotka koskevat allekirjoitusvarmenteita myöntäviä varmentajia sekä vahvan sähköisen tunnistamisvälineen tarjoajana olevaa Digi- ja väestötietovirastoa. Menettelytapavaatimuksia asetetaan varmenteita myöntävien varmentajien toiminnalle ja hallintakäytännölle, jotta tilaajat, varmentajan varmentamat allekirjoittajat sekä varmenteeseen luottavat osapuolet voisivat luottaa siihen, että varmenteella voidaan vahvistaa sähköisiä allekirjoituksia.

Digi- ja väestötietoviraston tarjoaman vahvan sähköisen tunnistamisen välineen tarjoamisen tapahtuu samassa tuotantoympäristössä, samanlaisin teknisin ja toiminnallisin ratkaisuin ja siihen sovelletaan samoja menettelytapoja noudattaen kuin Digi- ja väestötietoviraston myöntämän allekirjoitusvarmenteen tarjoamiseen.

Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta annettua asetusta (Asetus) sovelletaan luottamuspalveluiden allekirjoitusvarmenteiden osalta 1.7.2016 alkaen. Tässä asiakirjassa määritellään menettelytapavaatimukset, jotka koskevat Asetun mukaisesti tunnistus- ja allekirjoitusvarmenteita myöntävien varmentajien toimintaa ja hallintokäytäntöjä. Tässä asiakirjassa esitetyissä menettelytapavaatimuksissa kuvataan turvallisen allekirjoituksen luomisvälineen käyttö.

Digi- ja väestötietovirasto toimii 1.12.2010 alkaen terveydenhuollon lakisääteisenä varmentajana sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain, sähköisestä lääkemääräyksestä annetun lain sekä väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain nojalla. Digi- ja väestötietovirasto toimii 1.4.2015 alkaen sosiaalihuollon lakisääteisenä varmentajana sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettuun lakiin tehtyjen muutosten johdosta.

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



- Laki sähköisestä lääkemääräyksestä
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä
- Laki terveydenhuollon ammattihenkilöistä
- Laki sosiaalihuollon ammattillisen henkilöstön kelpoisuusvaatimuksista (272/2005)
- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista
- 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, v 1.4.3: 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
- Traficomin määräys Viestintävirasto M 72/2016 Määräys sähköisistä tunnistus- ja luottamuspalveluista
- Vahti 2/2013 Toimitilojen tietoturvaohje 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 määritetty.

2.2 Varmennuskäytännön tunnukset

Tämän varmennuskäytännön nimi on Varmennuskäytäntö sosiaali- ja terveydenhuollon ammattivarmennetta varten, jonka OID on 1.2.246.517.1.10.206.1.

Tämä varmennuskäytäntö viittaa Varmennepolitiikkaan sosiaali- ja terveydenhuollon ammattivarmennetta varten, OID 1.2.246.517.1.10.206.

Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta annettua asetusta (Asetus) sovelletaan luottamuspalveluiden allekirjoitusvarmenteiden osalta 1.7.2016 alkaen. Tässä



asiakirjassa määritellään menettelytapavaatimukset, jotka koskevat Asetun mukaisesti allekirjoitusvarmenteita myöntävien varmentajien toimintaa ja hallintokäytäntöjä. Tässä asiakirjassa esitetyissä menettelytapavaatimuksissa kuvataan turvallisen allekirjoituksen luomisvälineen käyttö.

Digi- ja väestötietovirasto noudattaa Asetuksen N:o (EU) 910/2014 luottamuspalveluiden mukaista yleisölle myönnettäviä allekirjoitusvarmenteita koskevaa varmennepolitiikkaa. Asiakirjan viitetiedot ovat ETSI EN 319 411-1 [2], QSCD mukaisesti; OID: 0.4.0.194112.1.2. Tämän varmennepolitiikan mukaisesti myönnettäviä tunnistus- ja allekirjoitusvarmenteita voi käyttää sellaisten sähköisten allekirjoitusten vahvistamisessa, jotka vastaavat Asetuksessa kuvattuja sähköisten allekirjoitusten hyväksytyjä varmenteita ja luontivälineitä kuten Asetuksen 28 ja 29 artiklassa säädetään. Tunnistusvarmenteen taso täyttää Asetuksen ja sen nojalla annetun varmuustasoaletuksen mukaisesti vaatimustason ”korkea”.

2.3 Osapuolet ja soveltuvuus

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

2.3.1 Varmentaja

Varmentaja täyttää seuraavat ehdot:

- Varmentaja sitoutuu noudattamaan tämän varmennuskäytännön ehtoja.
- Varmentaja laatii varmennepolitiikan ja varmennuskäytännön sekä muita näitä dokumentteja täydentäviä menettelytapahojeita.
- Varmentaja pitää yllä riittävät taloudelliset valmiudet turvataksaan 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 tunnistamisen menettelyn tämän varmennuskäytännön lukujen 3-4 mukaisesti;
4. myöntämään varmenteita yhdenmukaisesti tämän varmennuskäytännön kanssa;
5. noudattamaan voimassa olevia 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.

2.3.2 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 tunnistamisen tällöin 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.

2.3.3 Varmenteen haltija

Terveystietojen ammattivarmenteen haltijana voi olla terveydenhuollon ammattihenkilöiden keskusrekisteriin (Terhikki) merkitty terveydenhuollon ammattihenkilö. Sosiaalihuollon ammattivarmenteen haltijana voi olla sosiaalihuollon ammattihenkilön kelpoisuuden ehdot täyttävä sosiaalihuollon ammattihenkilö. Sosiaalihuollon ammattioikeudet tarkistetaan Sosiaali- ja terveysalan lupa- ja valvontaviraston (Valvira) ohjeistamalla tavalla¹.

¹ HE 354/2014 vp:ssä ehdotetaan, että laki sosiaalihuollon ammattihenkilöistä tulee korvaamaan lain (272/2005) sosiaalihuollon ammatillisen henkilöstön kelpoisuusvaatimuksista 1.1.2016 alkaen. Hallituksen esityksen mukaan sosiaalihuollon ammattihenkilön ammattioikeudet tarkistetaan Valviran ylläpitämästä sosiaalihuollon ammattihenkilöiden rekisteristä.



Sosiaali- ja terveydenhuollon ammattihenkilön tulee todistaa henkilöllisyytensä varmennehakemusta tehdessään tavalla, joka kohdassa 3.2.3 Henkilön tunnistaminen ja voimassaolevan ammattioikeuden todentaminen on kerrottu.

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

2.3.4 Varmenteeseen luottava osapuoli

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

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

Varmenteeseen luottava osapuoli sitoutuu toteuttamaan järjestelmänsä kaikki varmennepolitiikassa ja varmennuskäytännössä vaadittavat osat (mm. sähköisten allekirjoitusten tarkistus, varmennepolon tarkistus, varmenteen voimassaolon tarkistus (joko sulkulistan tarkistus tai OCSP-palvelun tarkistus) ja muuttamaan järjestelmänsä varmennepolitiikkaan ja varmennuskäytäntöön tehtävien päivitysten mukaiseksi.

2.3.5 Muut osapuolet

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

2.4 Varmenteen käyttökohteet

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

Varmenteiden pääasiallisista käyttökohteista on säädetty laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä ja laissa sähköisestä lääkkeen määräämisestä. Lisäksi varmenteita voidaan käyttää sosiaali- ja terveydenhuollon ja apteekkilaitoksen muissa tietojärjestelmissä.

2.4.1 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 allekirjoitusvarmenteen vaatimukset. Varmenteen hakijan henkilöllisyyden oikeellisuuden takaa Digi- ja väestötietovirasto.

Tämä varmennuskäytäntö kuvaa Asetukseen perustuvan, vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaisen sähköisen allekirjoituksen allekirjoitusvarmenteen myöntämiseen, tuottamiseen ja vastuun jakoon liittyviä yksityiskohtaisia vaatimuksia.



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

2.4.2 Kielletyt varmenteen käyttötarkoitukset

Sosiaali- ja terveysministeriön tekemän päätöksen ”Sähköpostin käytöstä terveydenhuollossa” mukaisesti arkaluonteisen salassa pidettävän potilas- ja hoitotietojenvälittäminen sähköpostitse ei ole suositeltavaa. Lähtökohtaisesti salassa pidettävää luottamuksellista tietoa ei saa välittää sähköpostilla edes potilaan nimenomaisella suostumuksella. Sosiaali- ja terveydenhuollon ammattivarmenteiden hyödyntäminen potilastietoja sisältävien sähköpostien salaamisessa tai allekirjoittamisessa ei siten ole sallittua.

2.5 Yhteystiedot

2.5.1 Varmennuskäytännön hallintaorganisaatio

Tämän sosiaali- ja terveydenhuollon ammattivarmenteen myöntämistä kuvaavan varmennuskäytännön on rekisteröinyt Digi- ja väestötietovirasto.

2.5.2 Yhteystiedot

Varmentajan yhteystiedot:

Digi- ja väestötietovirasto

PL 123 (Lintulahdenkuja 2)

Puh. +358 295 535 001

00531 Helsinki
+358 9 876 4369

Fax.

Y-tunnus: 0245437-2

kirjaamo@dvv.fi

Digi- ja väestötietovirasto (DVV) Varmennepalvelut

PL 123

00531 Helsinki

www.dvv.fi

2.5.3 Varmennuskäytäntöjen suhde varmennepolitiikkaan

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



2.5.4 Varmennuskäytäntöjen hyväksymismenettely

DVV:n Varmennepalvelut määrittelee ja hyväksyy varmennuskäytäntöasiakirjat.

2.6 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 2 §:n nojalla. Ammattioikeus voi olla rajoittamaton, rajoitettu tai kokonaan poistettu. Ammattioikeudet tallennetaan Sosiaali- ja terveysalan lupa- ja valvontaviraston (Valvira) ylläpitämään Terhikki-rekisteriin. Sosiaalihuollon ammattioikeudella tässä varmennuskäytännössä tarkoitetaan sosiaalihuollon ammatillisen henkilöstön kelpisuusvaatimuksista annetun lain (272/2005) mukaisia ammattiryhmien tehtävänimikkeiden haltijoiden ammatillisia oikeuksia.

Avaimen palautus (*Key recovery*)

Key recoveryllä tarkoitetaan tilannetta, jossa yksityinen avain palautetaan ammattikortin hajottua tai hävitessä. Sosiaali- ja 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 jälkepäin todistaa. Kiistämättömyys varmistaa sen, ettei toinen osapuoli voi kieltää toimintaansa, esimerkiksi tekemäänsä sähköistä allekirjoitusta, jälkepäin. 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 henkilötöimija

Sosiaali- ja terveydenhuollon alalla toimivan palvelujen antajan henkilö, joka ei ole sosiaali- ja terveydenhuollon ammattihenkilö tai sosiaali- ja terveydenhuollon muuta henkilöstöä. Kyseiseen henkilöstöryhmään kuuluvat muut valtakunnallisia tietojärjestelmiä käyttävät henkilöt ja erityisryhmät, kuten tietosuojavastavat sekä tietojärjestelmätoimittajat, konsultit jne.

PIN (*Personal identification number*)

Ammattikortin avainparin käyttöoikeuden varmistamiseksi käytettävä tunnusluku. Sosiaali- ja 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 auditoina 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 sosiaali- ja terveydenhuollon ammattioikeudet ja joka vastaa ammattikorttien, varmenteiden ja PIN-/PUK-tunnuslukujen jakelusta käyttäjille varmennepolitiikan ja varmennuskäytännön mukaisesti.

Sosiaali- ja terveystietojen 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 terveydenhuollon laitteiden ja tarvikkeiden vaatimustenmukaisuuden valvonta sekä turvallisen käytön edistäminen.

Sosiaali- ja terveydenhuollon ammattihenkilö

Tässä varmennuskäytännössä sosiaali- ja terveydenhuollon ammattihenkilöllä tarkoitetaan terveydenhuollon ammattihenkilöistä annetun lain (559/1994) mukaista terveydenhuollon ammattihenkilöä tai sosiaalihuollon ammattihenkilöä sekä myös terveydenhuollon ammattihenkilöistä annetun lain 2 §:n 3 momentissa tarkoitettua opiskelijaa ja sosiaalihuollon opiskelijaa.

Sosiaali- ja terveydenhuollon ammattikortti

Sosiaali- ja terveydenhuollon ammattihenkilölle myönnetty ammattivarmenteen sisältävä toimikortti.

Sosiaali- ja terveydenhuollon henkilöstökortti

Sosiaali- ja terveydenhuollon muulle henkilöstölle (muut kuin sosiaali- ja terveydenhuollon ammattihenkilöt) myönnetty varmenteen sisältävä toimikortti.

Sosiaali- ja terveydenhuollon muu henkilö

Muu sosiaali- ja terveydenhuollon toimintayksikössä työskentelevä taikka sen tehtäviä suorittava henkilö, joka ei ole sosiaali- ja terveydenhuollon ammattihenkilö.

Sosiaali- ja terveydenhuollon

Sosiaali- ja terveydenhuollon toimintayksikkö tai itsenäi-



palvelujen antaja

senä ammattinharjoittajana toimiva sosiaali- ja terveydenhuol-
lon ammattihenkilö.

Sosiaali- ja terveydenhuollon toimijakortti

Muulle sosiaali- ja terveydenhuollon toimijalle myönnetty
varmenteen sisältävä toimikortti.

Sulkulista

(CRL, Certificate Revocation List)

Sulkulista on luettelo suljetuista varmenteista. Varmenne sulje-
taan, kun varmenteen haltija pyytää sulkemista, menettää var-
menteeseen merkityn ammattioikeuden, ammattikortti ja
avaustunnusluku ovat kadonneet tai anastettu tai varmenteen
haltija on kuollut.

Sulkupalvelu

Varmentajan palvelu, joka sulkee terveydenhuollon ammattivar-
menteita tehtyjen sulkupyyntöjen perusteella.

Terhikki-rekisteri

Terveydenhuollon ammattihenkilöistä annetun lain (559/1994)
nojalla Valviran ylläpitämä valtakunnallinen rekisteri terveyden-
huollon ammattihenkilöistä ja heidän ammatinharjoittamiso-
keustiedoistaan.

Todentaminen (Authentication)

Järjestelmän käyttäjän (henkilön, organisaation, laitteen tai jär-
jestelmän) tai viestinnässä toisen osapuolen aitouden varmista-
minen. Yleisiä käyttäjän todennuksen menetelmiä ovat: 1) käyt-
tämä tietää ainutkertaisen asian, esimerkiksi salasanan 2) hänellä
on hallussaan jokin ainutkertainen ominaisuus kuten sormenjälki
3) hänellä on hallussaan ainutkertainen väline, esimerkiksi sosi-
aali- ja terveydenhuollon ammattihenkilön ammattikortti.

Tunnistaminen (Identification)

Menettely, jolla yksilöidään esimerkiksi tietojärjestelmän käyt-
tämä. Tyypillisesti tunnistus tapahtuu tarkistamalla, onko esitetty
tunnus tai muu tunniste hyväksyttävien tunnusten joukossa, esi-
merkiksi käyttäjäksi ilmoittautunut henkilö tietojärjestelmän
valtuutettujen käyttäjien luettelossa.

Turvataso

Turvatasolla tarkoitetaan niiden turvatoimien tasoa, joilla varau-
dutaan siihen, että turvallisuutta uhkaavaa välikohtausta yrite-
tään tai se tapahtuu. Tyypillisiä turvataso seuranta kohteita
ovat esimerkiksi tietoturva poikkeamat.

Vara-avainjärjestelmä (Key escrow)

Key escrow on menetelmä, jossa todentamisavainten turvatalle-
tus on pakollista ja turvatalletuksessa oleva avain on tietyissä



tilanteissa käytettävissä ilman varmenteen haltijan suostumusta. Sosiaali- ja terveydenhuollon ammattikorttien yksityisiä avaimia ei turvatalleteta.

Varmenne (*Certificate*)

Julkisen avaimen järjestelmää käyttävän palveluverkon toimijan kuten sosiaali- ja 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, sosiaali- ja 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 Digi- ja väestötietovirasto ja maistraatit. Tietojen rekisteröinti perustuu kansalaisten ja viranomaisten lakisääteisiin ilmoituksiin.



3 tietojen Julkaiseminen

3.1 Julkinen hakemisto

Varmentaja vastaa varmennehakemiston ylläpidosta sekä kohdassa 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.

3.2 Varmentajan julkaisemat tiedot

Varmentaja vastaa siitä, että varmennepolitiikat, varmennuskäytännöt, varmennekuvaukset ja varmentajan varmenteet ovat julkisesti saatavilla osoitteesta www.dvv.fi/cps. 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](http://ldap.fineid.fi).

3.3 Julkaisutiheys

Varmentaja julkaisee varmennepolitiikan ja varmennuskäytännön. Muutoshallinta on kuvattämän varmennuskäytännön kohdassa 9.12 Varmennuskäytännön muutosten hallinta.

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

3.4 Pääsyoikeudet

Varmentajan julkaisemien tietojen saatavuutta ei rajoiteta pääsyoikeuksin.

4 Tunnistaminen ja todentaminen

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

4.1 Varmenteen haltijan nimeäminen

4.1.1 Nimeäminen

Terveydenhuollon ammattihenkilön nimeäminen todentamisvarmenteessa sekä allekirjoitusvarmenteessa on kuvattu määräyksessä THPKI - T2 - Digi- ja väestötietoviraston CA-malli ja varmenteiden tietosisältö terveydenhuollossa.

Nimeämiskäytännöt:

CN (Common name) = VRK Gov. Root CA - G2



OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Vaestorekisterikeskus CA

C (Country) = FI

Digi- ja väestötietoviraston sosiaali- ja terveydenhuollon varmenteiden varmentaja on:

CN (Common name) = VRK CA for Social Welfare and Healthcare Prof. Certs

OU (Organizational unit) = Sosiaali- ja terveydenhuollon ammattivarmennet

O (Organization) = Vaestorekisterikeskus CA

C (Country) = FI

Varmenteen haltijan nimeämiskäytäntö sosiaali- ja terveydenhuollon varmenteissa (pakolliset kentät):

TITLE (Title) = Titteli

O (Organization) = Organisaation nimi

SN (Surname) = Sukunimi

G (Given name) = Etunimi

SERIALNUMBER (Serial Number) = Yksilöllinen tunniste

C (Country) = FI

Valinnaiset kentät

CN (Common Name) = Palvelun nimi

Pseudonym (Pseudonym) = Yksilöllinen tunniste

UPN (User Principal Name) = OID tai arvo

4.1.2 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 sosiaali- ja terveydenhuollon ammattihenkilöiden on toimittava omilla nimillään.

4.1.3 Anonyymit tai salanimet

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

4.1.4 Nimikenttien sisältö

Nimikenttien sisältö on määritetty tämän varmennuskäytännön kohdassa 3.1.1.

4.1.5 Nimitietueen ainutkertaisuus

Kohdassa 3.1.1 määritelty nimitietue yksilöi rekisteröidyn terveydenhuollon ammatihenkilön. Henkilön tunnistetieto on sosiaali- ja terveydenhuollon ammattihenkilön ainutkertaisesti yksilöivä.

4.1.6 Tuotenimien käyttöoikeus

—

4.2 Henkilöllisyyden todentaminen

4.2.1 Menettelytapa yksityisen avaimen omistajuuden todistamiseksi

Sosiaali- ja terveydenhuollon ammattihenkilön yksityiset avaimet luodaan aina ammattikortin sirulla. Yksityiset avaimet sisältävä ammattikortti luovutetaan sosiaali- ja terveydenhuollon ammattihenkilölle sen jälkeen, kun hänen henkilöllisyytensä on luotettavasti todettu kohdassa 3.2.3 Henkilön tunnistaminen ja voimassaolevan ammattioikeuden todentaminen tavalla ja varmenne on rekisteröity ja luotu.

4.2.2 Varmenteen hakijan edustaman organisaation todentaminen

Sosiaali- ja terveydenhuollon ammattihenkilöiden osalta ei vaadita heidän edustamiensa organisaatioiden todentamista. Sosiaali- ja terveydenhuollon ammattihenkilöt voivat työkennellä useassa sosiaali- ja terveydenhuollon toimintayksikössä, joten sosiaali- ja terveydenhuollon ammattivarmenne ja ammattikortti eivät ole organisaatiosidonnaisia.

4.2.3 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). Jos terveydenhuollon varmenteen hakijalla ei ole voimassa olevaa Terhikki-rekisteriin merkittyä ammattioikeutta, varmennetta ei myönnetä. Mikäli terveydenhuollon ammattihenkilön tiedot ei ole rekisteröity Terhikkiin, tulee henkilön ottaa yhteyttä Valviraan ammattioikeutensa rekisteröimiseksi. Sosiaali- ja terveydenhuollon ammattihenkilöiden tietojen tarkistamisessa noudetaan Valviran antamaa ohjeistusta siihen asti, kunnes Valviran ylläpitämä sosiaali- ja terveydenhuollon ammattihenkilöiden valtakunnallinen rekisteri on käytössä. Sosiaali- ja terveydenhuollon ammattivarmenteeseen ja ammattikorttiin sekä sosiaali- ja terveydenhuollon ammattivarmenteeseen ja ammattikorttiin merkitään vain yksi hakijan valitsema ammattioikeus, vaikka hakijalla olisi useita voimassa olevia ammattioikeuksia.

4.2.4 Varmenteen hakijan tiedot, joita varmentaja ei tarkista

Kaikki terveydenhuollon ammattihenkilön varmennehakemuksessa tarvittavat henkilötiedot saadaan Terhikki-rekisteristä.

4.2.5 Varmenteen myöntämisen edellytykset

Vain Valviran rekisteröimällä terveydenhuollon ammattihenkilöllä on oikeus hakea ammattivarmennetta. Sama vaatimus Valviran rekisteröinnistä edellytyksenä oikeudelle hakea ammattivarmennetta koskee myös sosiaali- ja terveydenhuollon ammattihenkilöitä sen jälkeen, kun sosiaali- ja terveydenhuollon ammattihenkilöiden keskusrekisteri on otettu käyttöön. Varmenteen hakijalla on oltava voimassaoleva sosiaali- ja terveydenhuollon ammattioikeus, jotta varmenne voidaan myöntää. Ammattioikeuteen liittyvät mahdolliset rajoitukset eivät estä varmenteen myöntämistä.

4.2.6 Varmentajien välisen yhteistyön edellytykset ja vaatimukset

Varmentajien välisen yhteistyön edellytykset ja vaatimukset määritellään juurivarmentajan varmennepolitiikassa.

4.3 Tunnistaminen ja todentaminen varmenteen uusimisessa

4.3.1 Tunnistaminen ja todentaminen varmenteen uusimisessa

Varmenteiden uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

4.3.2 Tunnistaminen ja todentaminen varmenteen sulkemisen jälkeen

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

4.4 Peruuttamispyynnön tekijän tunnistaminen

Varmenteen sulkupyyntö voidaan tehdä puhelimitse sulkupalveluun tai kirjallisesti varmentajalle.



Kun sulkupyynnöksi 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.

5 VARMENTEEN ELINKAAREN HALLINNAN TOIMINNALLISET VAATIMUKSET

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

5.1 Varmenteen hakeminen

Sosiaali- ja terveydenhuollon ammattivarmennetta haetaan henkilökohtaisesti rekisteröijänä toimivalta organisaatiolta.

Hakemuksen tiedot tallennetaan varmentajan varmennetietojärjestelmään.

Sosiaali- ja terveydenhuollon ammattivarmenteen hakeminen edellyttää, että hakija:

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

Rekisteröijä ilmoittaa hakijalle ammattikortin sekä tunnuslukukuoren toimitustavasta.

5.1.1 Kuka voi tehdä varmennehakemuksen

Varmennehakemuksen voi tehdä Valviran rekisteröimä terveydenhuollon ammattihenkilö. Vaatimus Valviran rekisteröinnistä koskee myös sosiaalihuollon ammattihenkilöitä sen jälkeen, kun Valvira on saanut sosiaalihuollon ammattihenkilöiden keskusrekisterin valmiiksi. Sosiaalihuollon ammattihenkilöiden keskusrekisterin valmistumiseen asti noudatetaan sosiaalihuollon ammattihenkilöiden todetantamisessa Valviralta saatavaa ohjeistusta.

5.1.2 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 myöntämällä 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-kohdassa 1.3.2.

5.2 Varmennehakemuksen käsittely

Varmennehakemus käsitellään rekisteröintipisteessä ilman aiheetonta viivytystä.

Rekisteröijä tallettaa varmenteen tilaustiedot varmentajan varmennetietojärjestelmään.

5.2.1 Tunnistamisen ja todentamisen toteuttaminen

Rekisteröijä tunnistaa varmenteen hakijan luvun 3 mukaisesti ja tarkistaa, että henkilöllä on Terhikki-rekisteriin merkittynä voimassa oleva tieto ammatinharjoittamisoikeudesta. Sosiaalihuollon varmenteen hakijan tieto ammatinharjoittamisoikeudesta tarkistetaan Valviran ohjeistuksen mukaisesti, kunnes Valviran ylläpitämä sosiaalihuollon ammattihenkilöiden keskusrekisteri on käytössä.

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 tunnistamisesta käytetystä tunnistamisasiakirjasta. Sosiaalihuollon osalta noudatetaan Valviralta saatavaa ohjeistusta sosiaalihuollon ammattioikeuden rekisterin käyttöön ottoon asti.

5.2.2 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 muutosesityksen varmentajalle.

5.2.3 Varmennehakemuksen käsittelyaika

Varmennehakemus käsitellään ilman aiheetonta viivytystä rekisteröintipisteen aukioloaikana.

5.3 Varmenteen myöntäminen

5.3.1 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 tämän varmennuskäytännön kohdissa 4.1 ja 4.2.



5.3.2 Ilmoitus hakijalle varmenteen myöntämisestä

Erillistä ilmoitusta terveydenhuollon ammattivarmenteen myöntämisestä ei tehdä.

5.4 Myönnetyn varmenteen hyväksyminen

5.4.1 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.

5.4.2 Varmenteen julkaisu varmentajan toimesta

Varmentaja julkaisee myönnettyt todentamisvarmenteet julkisessa tietoverkossa olevassa varmennehakemistossa kohdassa 2.1 kuvatulla tavalla. Allekirjoitusvarmenteita ei julkaista hakemistossa.

5.4.3 Ilmoitus muille osapuolille varmenteen myöntämisestä

Erillistä ilmoitusta sosiaali- ja terveydenhuollon ammattivarmenteen myöntämisestä ei tehdä.

5.5 Varmenteiden ja avainparien käyttö

5.5.1 Varmenteiden ja avainparien käyttö varmenteen haltijan toimesta

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

Sosiaali- ja terveydenhuollon ammattihenkilön tulee sitoutua toimimaan tämän varmennuskäytännön mukaisesti hakiessaan ja käyttäessään varmennetta.

Sosiaali- ja 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.

Sosiaali- ja 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.

Sosiaali- ja 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.

5.5.2 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 varmenteen voimassaolon tarkistaminen voimassaolevan sulkulistan tai OCSP-palvelun 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.

5.6 Julkisen avaimen uudelleen varmentaminen

Ammattivarmenteita ei myönnetä aiemmin varmennetuille julkisille avaimille.

5.7 Varmenteen uusiminen

5.7.1 Varmenteen uusimisen syyt

Sosiaali- ja terveydenhuollon ammattihenkilön varmenne voidaan uusida edellisen varmenteen voimassaolon päättyessä, mikäli kohdassa 3.2.5 kuvatut varmenteen myöntämisen edellytykset ovat edelleen voimassa.

Varmenne voidaan uusida 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.

5.7.2 Varmenteen uusimisen hakeminen

Varmenteen uusimista voi hakea vain varmenteen haltija.

5.7.3 Varmenteen uusimispyynnön käsittely

Varmenteiden uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

5.7.4 Ilmoitus varmenteen hakijalle ammattikortin uusimisesta

Erillistä ilmoitusta sosiaali- ja terveydenhuollon ammattivarmenteen uusimisesta ei tehdä.

5.7.5 Uusitun varmenteen hyväksymismenettely varmenteen haltijan kannalta

Uusittu varmenne hyväksytään kohdassa 4.4.1 kuvatun menetelmän mukaisesti.

5.7.6 Uusitun varmenteen julkaisu

Varmenteet julkaistaan kohdassa 4.4.2 kuvatun menetelmän mukaisesti.

5.7.7 Ilmoitus uusitun varmenteen myöntämisestä muille osapuolille

Erillistä ilmoitusta sosiaali- ja terveydenhuollon ammattivarmenteen uusimisesta ei tehdä.



5.8 Varmenteen muuttaminen

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

5.9 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. Varmenteen tilatiedon voi saada myös OCSP-palvelun kautta. Varmennetta ei voi sulkea määräajaksi.

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

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

5.9.1 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 sosiaali- ja terveydenhuollon ammattihenkilön varmenteen, mikäli varmennetta on käytetty tämän varmennuskäytännön, sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain tai sähköisestä lääkemääräyksestä 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.

5.9.2 Kuka voi vaatia varmenteen sulkemista

Varmenteen sulkemista voivat vaatia:

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



5.9.3 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 kohdassa 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 sulkupyynnönsä 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 5 vuotta sulkemisajankohdasta.

5.9.4 Varmenteen haltijan velvollisuus tehdä sulkupyyntö

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

5.9.5 Varmenteen sulkupyynnön käsittelyaika

Sulkupalvelu käsittelee varmenteen sulkupyynnot viipymättä.



5.9.6 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 varmenteen voimassaolon tarkistaminen, joko OCSP-palvelun tai voimassaolevan sulkulistan kautta. Varmenteeseen ei tule luottaa, ellei luottava osapuoli ole suorittanut sulkulistan tarkistusta.

5.9.7 Sulkulistan julkaisu tiheys

Päivitetty sulkulista julkaistaan tunnin välein.

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

5.9.8 Sulkulistan voimassaolon enimmäisaika

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

5.9.9 Reaaliaikainen varmenteen tilan tarkistaminen

Reaaliaikainen varmenteen tilan tarkistaminen on käytössä.

5.9.10 Vaatimukset varmenteen tilan reaaliaikaiselle tarkistamiselle

Varmenteen tilatieto voidaan tarkistaa reaaliaikaisesti OCSP-palvelusta tai sulkulistalta.

5.9.11 Muut varmenteen tilan tarkistamismenettelyt

Varmenteen tilatieto voidaan tarkistaa reaaliaikaisesti OCSP-palvelusta tai sulkulistalta.

5.9.12 Yksityisen avaimen paljastumisesta johtuva varmenteen sulkeminen

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

5.9.13 Varmenteen sulkeminen määräajaksi

Varmenteita ei suljeta määräajaksi.

5.9.14 Kuka voi vaatia varmenteen sulkemista määräajaksi

—

5.9.15 Menettelytavat varmenteen sulkemiseksi määräajaksi

—



5.9.16 Rajoitukset varmenteen määräaikaiselle sulkemiselle

—

5.10 Varmenteen tilan tarkistamismahdollisuus

Varmenteen voimassaolotilan tarkistaminen tehdään OCSP-palvelun tai sulkulistan avulla. Varmenteeseen luottavan osapuolen tulee myös tarkistaa, ettei varmenteen voimassaolo-aika ole päättynyt.

5.11 Varmenteen voimassaolon päättyminen

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

5.12 Vara-avainjärjestelmä ja avainten palautus

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

6 Fyysisen, käyttö- ja henkilöstöturvallisuuden hallinta

Digi- ja väestötietoviraston tietoturvallisuutta hallitaan Digi- ja väestötietoviraston tietoturvapolitiikan ja standardin ISO 27001:2005 mukaisesti.

6.1 Fyysisen turvallisuuden hallinta

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

6.1.1 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.

6.1.2 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.



6.1.3 Sähkö ja ilmastointi

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

6.1.4 Vesivahinko

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

6.1.5 Tulipalo

Varmennetuotannon järjestelmät sijaitsevat automaattisammutuksella varustetuissa konesalitiloissa.

6.1.6 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 säädetty.

6.1.7 Tietovälineiden hävittäminen

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

6.1.8 Varmuuskopiointi verkon yli

Varmennetuotantojärjestelmän varmuuskopiointi tapahtuu varmennejärjestelmän sisäisessä tietoliikenneverkossa.

6.2 Käyttöturvallisuuden hallinta

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

6.2.1 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.

6.2.2 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.

6.2.3 Henkilöiden tunnistaminen ja todentaminen eri rooleihin

Varmentajan työtehtävissä toimivilla henkilöillä, jotka toimivat kohdassa 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.

6.2.4 Tehtävien eriyttämistä vaativat roolit

Rekisteröijä ei voi toimia järjestelmän pääkäyttäjän roolissa.

6.3 Henkilöstöturvallisuuden hallinta

6.3.1 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.

6.3.2 Taustojen tarkistamisen menettelytapa

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

6.3.3 Koulutuksen tiheys ja vaatimukset

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

6.3.4 Jatkokoulutuksen tiheys ja vaatimukset

—



6.3.5 Työtehtävien kierrätyksen tiheys ja järjestys

—

6.3.6 Seuraukset luvattomista toimista

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

6.3.7 Alihankkijoiden henkilöstön vaatimukset

Varmentajan valtuuttamien organisaatioiden henkilöstön tulee täyttää kohdan 5.3.1 edellytykset.

6.3.8 Asiakirjat, jotka toimitetaan henkilökunnalle

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

6.4 Varmennejärjestelmän turvallisuuden seuranta

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

6.4.1 Arkistoitavat tapahtumat

Varmentaja säilyttää turvallisuusseurantaan varten seuraavat tiedot:

1. Järjestelmätasojen 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.



6.4.2 Lokitietojen analysointitiheys

Lokitietoja analysoidaan tarvittaessa.

6.4.3 Lokitietojen säilytysaika

Lokitiedot säilytetään voimassaolevien arkistosäännösten mukaisesti.

6.4.4 Lokitietojen suojaaminen

Lokitietoihin on pääsy vain erikseen oikeutetuilla henkilöillä.

Lokitiedot suojataan muuttamiselta, tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä.

6.4.5 Lokitietojen varmuuskopiointi

Lokitiedoista otetaan varmuuskopiot päivittäin.

6.4.6 Lokitietojen keräysjärjestelmän toteuttaminen (sisäinen/ulkoinen)

Varmentaja vastaa lokitietojen keräysjärjestelmästä.

6.4.7 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.

6.4.8 Haavoittuvuuksien arviointi

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

6.5 Arkistoitavat aineistot

6.5.1 Arkistoitavat asiakirjat, tiedostot ja mediat

Varmentaja arkistoi seuraavat tiedot:

- varmennehakemukset;
- varmenne- tai muun hakemuksen allekirjoitetut hyväksynnit;
- varmennepalvelusopimukset;
- myönnetty varmenteet;
- ristiinvarmennusasiakirjat mukaanluettuna ristiinvarmennuksen perustelut ja päätökset sekä suoritettut toimet;
- varmenteen sulkupyynnöt;



- voimassaolevat ja edelliset varmennepolitiikat ja varmennuskäytännöt;
- varmentajan ja rekisteröintipisteiden väliset sopimukset; ja
- varmennejärjestelmän ylläpitoon, käyttöön ja hallintaan liittyvät sopimukset.

6.5.2 Arkistojen säilytysaika

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

6.5.3 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.

6.5.4 Arkistojen varmuuskopiointimenettely

Vain sähköisessä muodossa olevista arkistotiedoista otetaan varmuuskopiot.

6.5.5 Arkistoitavien tietojen aikaleima

Arkistoitavat asiakirjat on päivätty. Aikaleimapalvelu ei ole toistaiseksi käytössä.

6.5.6 Arkistojen keräysjärjestelmä (sisäinen/ulkoinen)

Varmentajalla ei ole keskitettyä arkistojen keräysjärjestelmää.

6.5.7 Arkistoissa olevien tietojen saatavuus ja eheys

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

6.6 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.

6.7 Häiriötilanteisiin varautuminen

6.7.1 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.

6.7.2 Varmennejärjestelmän, ohjelmistojen tai tietojen vahingoittuminen

Poikkeustilanteissa varmentaja noudattaa jatkuvuus- ja toipumissuunnitelmaa.



6.7.3 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.

6.7.4 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.

6.8 Lakkauttaminen

6.8.1 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 myönnettyt 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 kohdassa 5.5.7 mainittu saatavuus varmentajan arkistoihin säilyy varmentajan lakkauttamisen jälkeenkin.
- Sulkulistat ovat saatavilla ilmoitetuilla tavalla niiden voimassaolon ajan.

6.8.2 Rekisteröijän toiminnan ja siihen liittyvien oikeuksien lakkauttaminen

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

Rekisteröijän toiminnan lakkauttaminen tapahtuu rekisteröijän ja varmentajan välisen sopimuksen mukaisesti.



7 Teknisen turvallisuuden hallinta

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

Sosiaali- ja 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.

7.1 Avainparien luonti ja toimittaminen varmenteen haltijalle

7.1.1 Avainparien luonti

Varmentajan avainpari luodaan ja säilytetään turvalaskentalaitteistossa, joka on Euroopan unionin komission vahvistamien ja Euroopan yhteisöjen unionin 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.

7.1.2 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.

7.1.3 Varmenteen hakijan julkisen avaimen toimittaminen varmentajalle

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

7.1.4 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.

7.1.5 Avainten pituus

Varmentajan avaimet ovat 4096 bitin pituisia RSA-avaimia.

Sosiaali- ja terveydenhuollon ammattihenkilön allekirjoitusavaimet sekä todentamisavaimet ovat 2048 bitin pituisia RSA-avaimia.

7.1.6 Julkisen avaimen parametrien luonti ja laatu

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



7.1.7 Avainten käyttötarkoitukset

Varmentajan avainparin käyttötarkoitukset ovat varmenteen allekirjoitus ja sulkulistan allekirjoitus.

Sosiaali- ja terveydenhuollon ammattihenkilön avainparien käyttötarkoitukset ovat varmenteen haltijan todentaminen ja tiedon salaaminen sekä kehittynyt sähköinen allekirjoitus.

7.2 Yksityisen avaimen suojaaminen ja turvalaskentalaitteiston hallinta

7.2.1 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 sosiaali- ja terveydenhuollon ammattihenkilön yksityinen avain, joka on talletettu ammattikorttiin, toimitetaan sosiaali- ja terveydenhuollon ammattihenkilölle tämän varmennuskäytännön menettelytapojen mukaisesti.

Sosiaali- ja terveydenhuollon ammattihenkilön ammattikortti on kulloinkin voimassaolevien tarkoitukseen soveltuvien standardien mukainen, kuten ISO/IEC 7816 ja IAS ECC v 1.01.

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.

7.2.2 Yksityinen avain usean henkilön hallinnassa

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

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

7.2.3 Yksityisten avainten vara-avainjärjestelmä

Sosiaali- ja terveydenhuollon ammattikorttien vara-avainjärjestelmä ei ole käytössä.

7.2.4 Yksityisen avaimen varmuuskopiointi

Varmentajan yksityisestä avaimesta on varmuuskopio.

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

Sosiaali- ja terveydenhuollon ammattihenkilön yksityisistä avaimista ei oteta eikä säilytetä kopioita.



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

7.2.5 Yksityisten avainten arkistointi

Varmentajan yksityiset avaimet tuhotaan niiden voimassaoloajan päättymisen jälkeen.

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

7.2.6 Yksityisten avainten käsittely turvalaskentalaitteistossa

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

7.2.7 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.

7.2.8 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.

7.2.9 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.



7.2.10 Yksityisen avaimen tuhoaminen

Vain varmentaja voi tuhota varmentajan yksityiset avaimet.

Varmentajan lakkautuksen yhteydessä varmentajan yksityiset avaimet sekä niiden kopiot tuhotaan.

Mikäli sosiaali- ja 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.

7.2.11 Ammattikorttien ja turvalaskentalaitteistojen turvatason luokitus

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

7.3 Muita avainparin hallintaan vaikuttavia seikkoja

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

7.3.1 Julkisten avainten arkistointi

Varmentaja arkistoi varmentamansa julkiset avaimet kohdan 5.5 mukaisesti.

7.3.2 Varmenteiden ja avainten voimassaoloaika

Sosiaali- ja 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 luomis päivästä. Avaimia ei käytetä ennen voimassaoloaikaa tai voimassaoloajan päätyttyä mihinkään tarkoitukseen.

7.4 Aktivointitiedot

7.4.1 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.



7.4.2 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.

7.4.3 Muita huomioitavia seikkoja aktivointitiedosta

—

7.5 Tietokonelaitteistojen turvallisuuden hallinta

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

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

7.5.1 Erityisvaatimukset

Tietokonelaitteistojen turvallisuusvaatimusten osalta noudatetaan VAHTI 5/2004 -ohjetta.

7.5.2 Laitteistoturvallisuuden luokittelu

—

7.6 Elinkaaren turvallisuuden hallinta

7.6.1 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. Käyttöönottoaihe suunnitellaan siten, että nopea palaaminen vanhaan versioon on mahdollista määrätyn ajan puitteissa.

7.6.2 Turvallisuuden hallinta

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

- työtehtävien jakoon eri henkilöille kohdan 5.2 mukaisesti;
- turvallisuuden seurantaan;





- säännöllisiin turvallisuuteen kohdistuviin tarkastuksiin;
- tekniisiin turvaratkaisuihin ja -menetelmiin; ja
- sovellusmuutosten valtuutus- ja hyväksymismenettelyyn.

7.6.3 Elinkaaren turvallisuusluokittelu

—

7.7 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.

7.8 Aikaleima

Aikaleimapalvelu ei ole toistaiseksi käytössä.

8 Varmenteen ja sulkulistan profiili

8.1 Varmenteen profiili

Sosiaali- ja terveydenhuollon ammattivarmenteen profiili on kuvattu määrittämissä THPKI - T2: Digi- ja väestötietoviraston CA-malli ja varmenteiden tietosisältö sosiaali- ja terveydenhuollossa.

8.2 Sulkulistan profiili

Sosiaali- ja terveydenhuollon ammattivarmenteiden sulkulistan profiili on kuvattu määrittämissä FINEID S2 - DVV (PRC) CA-model and certificate contents.

8.3 Reaaliaikainen sulkulistan tarkistus (OCSP)

OCSP-protokolla on käytettävissä.

9 Hyväksymistarkastus

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

9.1 Hyväksymistarkastusten suorittaminen

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



9.2 Tarkastaja

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

9.3 Tarkastuksen suorittajan suhde tarkastettavaan osapuoleen

Tarkastuksen suorittaja on tarkastettavaan kohteeseen nähden ulkopuolinen ja sitoutumaton.

9.4 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.

9.5 Toimenpiteet, joihin ryhdytään poikkeamien esiintyessä

Varmentaja ryhtyy välittömästi havaittujen poikkeamien vaatimiin toimenpiteisiin tilanteen korjaamiseksi.

9.6 Tarkastuksen tuloksista tiedottaminen

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

10 Yleiset ehdot

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

10.1 Maksut ja muut palkkiot

Maksut ja muut palkkiot määräytyvät sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain 22§:n nojalla sekä kulloinkin voimassa olevan valtiovarainministeriön asetuksen Digi- ja väestötietoviraston suoritteiden maksuista mukaisesti.

10.1.1 Varmenteen myöntämismaksu

—



10.1.2 Varmenteen käyttömaksu

—

10.1.3 Varmenteen sulkumaksu tai tilan kyselymaksu

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

10.1.4 Maksut muista palveluista kuten neuvontapalvelusta

Neuvontapalvelun käytöstä peritään erillinen maksu voimassaolevan hinnaston mukaisesti.

10.1.5 Hyvitykset

Hyvitykset määräytyvät varmennejärjestelmän osapuolien kanssa solmittujen sopimusten perusteella.

10.2 Taloudelliset velvollisuudet

Varmentaja vastaa lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista mukaisesti, että sillä on riittävät taloudelliset voimavarat varmennetoiminnan asianmukaiseksi järjestämiseksi sekä mahdollisen vahingonkorvausvastuun kattamiseksi.

10.3 Luottamuksellisuus ja tietosuoja

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

10.3.1 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.

10.3.2 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 myönnettyssä varmenteessa, ovat julkisia, ellei sopimuksissa taikka laissa, asetuksessa tai niiden nojalla annetussa määräyksessä toisin määrätä.

10.3.3 Yksityisten tietojen suojaaminen

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



10.4 Yksityisyyden suoja

Yksityisyyden suojan osalta noudatetaan voimassa olevaa lainsäädäntöä.

10.4.1 Yksityisten tietojen suojaamissuunnitelma

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

10.4.2 Varmentajan järjestelmissä käsiteltävät yksityiset tiedot

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

10.4.3 Varmentajan järjestelmissä käsiteltävät julkiset tiedot

Varmentajan järjestelmissä tapahtuvassa julkisten tietojen käsittelyssä noudatetaan lakia viranomaisten toiminnan julkisuudesta.

10.4.4 Vastuu yksityisten tietojen suojaamisesta

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

10.4.5 Yksityisten tietojen käyttäminen tai julkistaminen varmenteen haltijan suostumuksella

Tietojen luottamuksellisuus ja tietosuojaa on määritelty kohdassa 9.3.

10.4.6 Tietojen luovutus viranomaisille

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

10.4.7 Muut olosuhteet, joissa tiedot voidaan julkistaa

Varmentaja ei luovuta tietoja muissa kuin edellä mainituissa olosuhteissa.

10.5 Immateriaalioikeudet

Digi- ja väestötietovirasto omistaa kaikki varmenteisiin ja dokumentaatioon liittyvät tiedot teknisten toimitussopimusten mukaisesti. Digi- ja väestötietovirasto omistaa täydet omistusoikeudet tähän varmennepolitiikkaan.

10.6 Osapuolten sitoumukset

10.6.1 Varmentajan sitoumukset

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



10.6.2 Rekisteröijän sitoumukset

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

10.6.3 Varmenteen haltijan sitoumukset

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

10.6.4 Varmenteisiin luottavien osapuolten sitoumukset

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

10.6.5 Muiden osapuolten sitoumukset

—

10.7 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.

10.8 Vastuunrajoitukset

Varmennepalveluiden tuottamiseen liittyvä Digi- ja väestötietoviraston vahingonkorvausvastuu määräytyy varmenteen hakijan kanssa tehdyn palvelusopimuksen mukaisesti. Digi- ja väestötietovirastoa koskevat lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista ja sähköisestä asioinnista viranomaistoiminnassa annetun lain mukaiset varmentajan vahingonkorvausvastuut. Soveltuvien osin sovelletaan myös vahingonkorvauslakia (412/1974).

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 kustannuksista 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.

10.9 Vahingonkorvaukset

Varmennepalveluiden tuottamiseen liittyvä Digi- ja väestötietoviraston vahingonkorvausvastuu määräytyy varmenteen hakijan kanssa tehdyn palvelusopimuksen mukaisesti. Digi- ja väestötietovirastoa koskevat lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista ja sähköisestä asioinnista viranomaistoiminnassa annetun lain mukaiset varmentajan vahingonkorvausvastuut. Soveltuvien osin sovelletaan myös vahingonkorvauslakia (412/1974).

10.10 Voimassaoloaika ja voimassaolon päättyminen

10.10.1 Varmennuskäytännön voimassaoloaika

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

10.10.2 Varmennuskäytännön voimassaolon päättyminen

Varmennuskäytännöllä ei ole erikseen määrättyä voimassaoloaika.

10.10.3 Varmennuskäytännön voimassaolon päättymisen vaikutukset

—



10.11 Varmennepalvelun osapuolien keskinäinen viestintä

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

10.12 Varmennuskäytännön muutosten hallinta

Varmennuskäytäntöön tehtävistä muutoksista päättää varmentaja.

10.12.1 Varmennuskäytännön muuttaminen

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

10.12.2 Muutoksista tiedottaminen

1. Kaikkia varmennepolitiikan ja varmennuskäytännön kohtia voidaan muuttaa ilmoittamalla tulevista pääasiallisista muutoksista 30 päivää ennen muutosten voimaan astumista.
2. Kohtia, jotka Digi- ja väestötietoviraston mielestä eivät merkittävästi vaikuta varmentaiden haltijoihin ja luottaviin osapuoliin, voidaan muuttaa ilmoittamalla niistä 14 päivää aikaisemmin.

10.12.3 Varmennuskäytännön tunnistetiedon muuttaminen

Varmennuskäytännön tunnistetieto ei muutu, vaikka varmennuskäytännön sisältöä muutetaan.

10.13 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.

10.14 Sovellettava laki

Sosiaali- ja Terveydenhuollon varmennepalveluun ja tähän varmennuskäytäntöön sovelletaan Suomen lakia.

10.15 Lain noudattaminen

Sosiaali- ja terveydenhuollon varmennepalveluiden järjestämisessä noudatetaan yksinomaan Suomen lakia.



10.16 Muut järjestelyt

10.16.1 Sopimukset

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

Allekirjoituksellaan sosiaali- ja 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.

10.16.2 Oikeudenluovutus

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

10.16.3 Pätemättömyys

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

10.16.4 Täytäntöönpano

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

10.16.5 Ylivoimainen este

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



10.17 Muut ehdot

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



[Yksikkö] / Aarnio Ville

**sosiaali- ja terveydenhuol-
lon ammattivarmennetta
varten**

[Tarkenne]

1.4.2021

54 (54)

[Numero]

[Liite]

