DIGI- JA VÄESTÖTIETO-VIRASTO

Varmennuskäytäntö

sosiaali- ja terveydenhuollon muun henkilöstön varmennetta varten

OID 1.2.246.517.1.10.303.3
OID 1.2.246.517.1.10.353.3

1.6.2021

SERTIFIOITU inspecta ORGANISAATIO
ISO 9001

SERTIFIOITU inspecta ORGANISAATIO
ISO/IEC 27001

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

Dokumentinhallinta

Omistaja	
Laatinut	Ville Aarnio
Tarkastanut	
Hyväksynyt	Mikko Pitkänen

Version hallinta

versionro	mitä tehty	pvm/henkilö
Versio 1.0	Version 1.0	1.6.2021/VA

Sisällysluettelo

1 Johdanto 9
1.1 Taustaa 9
1.2 Varmennuskäytännön tunnukset 11
1.3 Osapuolet ja soveltuvuus 11
1.3.1 Varmentaja 11
1.3.2 Rekisteröijä 12
1.3.3 Varmenteen haltija 13
1.3.4 Varmenteeseen luottava osapuoli 13
1.3.5 Muut osapuolet 13
1.4 Varmenteen käyttökohteet 13
1.4.1 Sallitut varmenteen käyttötarkoitukset 14
1.4.2 Kielletyt varmenteen käyttötarkoitukset 14
1.5 Yhteystiedot 14
1.5.1 Varmennuskäytännön hallintaorganisaatio 14
1.5.2 Varmennuskäytäntöjen suhde varmennepolitiikkaan 15
1.5.3 Varmennuskäytäntöjen hyväksymismenettely 15
1.6 Määritelmät ja lyhenteet 15
2 tietojen Julkaiseminen 19
2.1 Julkinen hakemisto 19
2.2 Varmentajan julkaisemat tiedot 19
2.3 Julkaisutiheys 19
2.4 Pääsyoikeudet 20
3 Tunnistaminen ja todentaminen 20
3.1 Varmenteen haltijan nimeäminen 20
3.1.1 Nimeäminen 20
3.1.2 Nimeämisen merkitys 21
3.1.3 Anonyymit tai salanimet 21
3.1.4 Nimikenttien sisältö 21
3.1.5 Nimitietueen ainutkertaisuus 22
3.1.6 Tuotenimien käyttöoikeus 22
3.2 Henkilöllisyyden todentaminen 22
3.2.1 Menettelytapa yksityisen avaimen omistajuuden todistamiseksi 22
3.2.2 Varmenteen hakijan edustaman organisaation todentaminen 22
3.2.3 Henkilön tunnistaminen 22
3.2.4 Varmenteen hakijan tiedot, joita varmentaja ei tarkista 22

3.2.5 Varmenteen myöntämisen edellytykset 22
3.2.6 Varmentajien välisen yhteistyön edellytykset ja vaatimukset 23
3.3 Tunnistaminen ja todentaminen varmenteen uusimisessa 23
3.3.1 Tunnistaminen ja todentaminen varmenteen uusimisessa 23
3.3.2 Tunnistaminen ja todentaminen varmenteen sulkemisen jälkeen 23
3.4 Sulkupyynnön tekijän tunnistaminen 23
4 VARMENTEEN ELINKAAREN HALLINNAN TOIMINNALLISET VAATIMUKSET 23
4.1 Varmenteen hakeminen 23
4.1.1 Kuka voi tehdä varmennehakemuksen 24
4.1.2 Varmenteen myöntämisprosessi ja vastuut 24
4.2 Varmennehakemuksen käsittely 24
4.2.1 Tunnistamisen ja todentamisen toteuttaminen 24
4.2.2 Varmennehakemuksen hyväksyminen tai hylkääminen 25
4.2.3 Varmennehakemuksen käsittelyaika 25
4.3 Varmenteen myöntäminen 25
4.3.1 Varmenteen myöntämiseen liittyvät varmentajan tehtävät 25
4.3.2 Ilmoitus hakijalle varmenteen myöntämisestä 25
4.4 Myönnetyn varmenteen hyväksyminen 25
4.4.1 Myönnetyn varmenteen hyväksymismenettely varmenteen hakijan kannalta 25
4.4.2 Varmenteen julkaisu varmentajan toimesta 25
4.4.3 Ilmoitus muille osapuolille varmenteen myöntämisestä 25
4.5 Varmenteiden ja avainparien käyttö 26
4.5.1 Varmenteiden ja avainparien käyttö varmenteen haltijan toimesta 26
4.5.2 Varmenteiden ja julkisten avainten käyttö varmenteisiin luottavan osapuolen toimesta 27
4.6 Julkisen avaimen uudelleen varmentaminen 27
4.7 Varmenteen uusiminen 27
4.7.1 Varmenteen uusimisen syyt 27
4.7.2 Varmenteen uusimisen hakeminen 28
4.7.3 Varmenteen uusimispyynnön käsittely 28
4.7.4 Ilmoitus varmenteen hakijalle varmennekortin uusimisesta 28
4.7.5 Uusitun varmenteen hyväksymismenettely varmenteen haltijan kannalta 28
4.7.6 Uusitun varmenteen julkaisu 28
4.7.7 Ilmoitus uusitun varmenteen myöntämisestä muille osapuolille 28
4.8 Varmenteen muuttaminen 28
4.9 Varmenteen sulkeminen ja määräaikainen sulkeminen 28
4.9.1 Varmenteen sulkemisen edellytykset 28

4.9.2 Kuka voi vaatia varmenteen sulkemista 29
4.9.3 Varmenteen sulkemisprosessi 29
4.9.4 Varmenteen haltijan velvollisuus tehdä sulkupyyntö 30
4.9.5 Varmenteen sulkupyynnön käsittelyaika 30
4.9.6 Varmenteeseen luottavan osapuolen velvollisuus tarkistaa varmenteen voimassaolo 30
4.9.7 Sulkulistan julkaisutiheys 30
4.9.8 Sulkulistan voimassaolon enimmäisaika 30
4.9.9 Reaaliaikainen varmenteen tilan tarkistaminen 30
4.9.10 Vaatimukset varmenteen tilan reaaliaikaiselle tarkistamiselle 31
4.9.11 Muut varmenteen tilan tarkistamismenettelyt 31
4.9.12 Yksityisen avaimen paljastumisesta johtuva varmenteen sulkeminen 31
4.9.13 Varmenteen sulkeminen määräajaksi 31
4.9.14 Kuka voi vaatia varmenteen sulkemista määräajaksi 31
4.9.15 Menettelytavat varmenteen sulkemiseksi määräajaksi 31
4.9.16 Rajoitukset varmenteen määräaikaiselle sulkemiselle 31
4.10 Varmenteen tilan tarkistamismahdollisuus 31
4.11 Varmenteen voimassaolon päättyminen 31
4.12 Vara-avainjärjestelmä ja avainten palautus 31
5 Fyysisen, käyttö- ja henkilöstöturvallisuuden hallinta 31
5.1 Fyysisen turvallisuuden hallinta 32
5.1.1 Tilojen sijoittaminen ja rakenne 32
5.1.2 Fyysinen pääsynvalvonta 32
5.1.3 Sähkö ja ilmastointi 32
5.1.4 Vesivahinko 32
5.1.5 Tulipalo 33
5.1.6 Tietovälineiden säilytys 33
5.1.7 Tietovälineiden hävittäminen 33
5.1.8 Varmuuskopiointi verkon yli 33
5.2 Käyttöturvallisuuden hallinta 33
5.2.1 Työtehtäviin liittyvät roolit 33
5.2.2 Varmennetuotannon työtehtäviin tarvittavien henkilöiden määrä 34
5.2.3 Henkilöiden tunnistaminen ja todentaminen eri rooleihin 34
5.2.4 Tehtävien eriyttämistä vaativat roolit 34
5.3 Henkilöstöturvallisuuden hallinta 34
5.3.1 Tausta-, ansio-, kokemus- ja selvitysvaatimukset 34
5.3.2 Taustojen tarkistamisen menettelytapa 34
5.3.3 Koulutuksen tiheys ja vaatimukset 34

5.3.4 Jatkokoulutuksen tiheys ja vaatimukset 34
5.3.5 Työtehtävien kierrätyksen tiheys ja järjestys 34
5.3.6 Seuraukset luvattomista toimista 35
5.3.7 Alihankkijoiden henkilöstön vaatimukset 35
5.3.8 Asiakirjat, jotka toimitetaan henkilökunnalle 35
5.4 Varmennejärjestelmän turvallisuuden seuranta 35
5.4.1 Arkistoitavat tapahtumat 35
5.4.2 Lokitietojen analysointitiheys 35
5.4.3 Lokitietojen säilytysaika 35
5.4.4 Lokitietojen suojaaminen 36
5.4.5 Lokitietojen varmuuskopiointi 36
5.4.6 Lokitietojen keräysjärjestelmän toteuttaminen (sisäinen/ulkoinen) 36
5.4.7 Lokitapahtumasta ilmoittaminen 36
5.4.8 Haavoittuvuuksien arviointi 36
5.5 Arkistoitavat aineistot 36
5.5.1 Arkistoitavat asiakirjat, tiedostot ja mediat 36
5.5.2 Arkistojen säilytysaika 37
5.5.3 Arkistojen suojaaminen 37
5.5.4 Arkistojen varmuuskopiointimenettely 37
5.5.5 Arkistoitavien tietojen aikaleima 37
5.5.6 Arkistojen keräysjärjestelmä (sisäinen/ulkoinen) 37
5.5.7 Arkistoissa olevien tietojen saatavuus ja eheys 37
5.6 Varmentajan avainparin vaihto 37
5.7 Häiriötilanteisiin varautuminen 37
5.7.1 Suunnitelma toimintahäiriöiden ja toiminnan vaarantumisen varalta 37
5.7.2 Varmennejärjestelmän, ohjelmistojen tai tietojen vahingoittuminen 37
5.7.3 Toiminta varmenteen haltijan yksityisen avaimen paljastuessa 37
5.7.4 Toiminnan jatkuvuus häiriötilanteen jälkeen 38
5.8 Lakkauttaminen 38
5.8.1 Varmentajan toiminnan lakkauttaminen 38
5.8.2 Rekisteröijän toiminnan lakkauttaminen 38
6 Teknisen turvallisuuden hallinta 38
6.1 Avainparien luonti ja toimittaminen varmenteen haltijalle 38
6.1.1 Avainparien luonti 38
6.1.2 Yksityisen avaimen toimittaminen varmenteen haltijalle 39
6.1.3 Varmenteen hakijan julkisen avaimen toimittaminen varmentajalle 39
6.1.4 Varmentajan julkisen avaimen toimittaminen luottaville osapuolille 39

6.1.5 Avainten pituus 39
6.1.6 Julkisen avaimen parametrien luonti ja laatu 39
6.1.7 Avainten käyttötarkoitukset 39
6.2 Yksityisen avaimen suojaaminen ja turvalaskentalaitteiston hallinta 39
6.2.1 Käytetyt standardit 39
6.2.2 Yksityinen avain usean henkilön hallinnassa 40
6.2.3 Yksityisten avainten vara-avainjärjestelmä 40
6.2.4 Yksityisen avaimen varmuuskopiointi 40
6.2.5 Yksityisten avainten arkistointi 40
6.2.6 Yksityisten avainten käsittely turvalaskentalaitteistossa 40
6.2.7 Yksityisten avainten säilyttäminen 41
6.2.8 Yksityisten avainten aktivointi 41
6.2.9 Yksityisten avainten käytön estäminen 41
6.2.10 Yksityisen avaimen tuhoaminen 41
6.2.11 Varmennekorttien ja turvalaskentalaitteistojen turvatason luokitus 41
6.3 Muita avainparin hallintaan vaikuttavia seikkoja 42
6.3.1 Julkisten avainten arkistointi 42
6.3.2 Varmenteiden ja avainten voimassaoloaika 42
6.4 Aktivointitiedot 42
6.4.1 Aktivointitiedon luonti 42
6.4.2 Aktivointitiedon suojaus 42
6.4.3 Muita huomioitavia seikkoja aktivointitiedosta 42
6.5 Tietokonelaitteistojen turvallisuuden hallinta 42
6.5.1 Erityisvaatimukset 43
6.5.2 Laitteistoturvallisuuden luokittelu 43
6.6 Elinkaaren turvallisuuden hallinta 43
6.6.1 Järjestelmien kehittämisen hallinta 43
6.6.2 Turvallisuuden hallinta 43
6.6.3 Elinkaaren turvallisuusluokittelu 43
6.7 Tietoverkon turvallisuuden hallinta 43
6.8 Aikaleima 44
7 Varmenteen ja sulkulistan profiili 44
7.1 Varmenteen profiili 44
7.2 Sulkulistan profiili 44
7.3 Reaaliaikainen sulkulistan tarkistus (OCSP) 44
8 Hyväksymistarkastus 44

8.1 Hyväksymistarkastusten suorittaminen 44
8.2 Tarkastaja 44
8.3 Tarkastuksen suorittajan suhde tarkastettavaan osapuoleen 45
8.4 Tarkastuksen kattavuus 45
8.5 Toimenpiteet, joihin ryhdytään poikkeamien esiintyessä 45
8.6 Tarkastuksen tuloksista tiedottaminen 45
9 Yleiset ehdot 45
9.1 Maksut ja muut palkkiot 45
9.1.1 Varmenteen myöntämismaksu 45
9.1.2 Varmenteen käyttömaksu 45
9.1.3 Varmenteen sulkumaksu tai tilan kyselymaksu 45
9.1.4 Maksut muista palveluista kuten Tukipalvelu -maksu 46
9.1.5 Hyvitykset 46
9.2 Taloudelliset velvollisuudet 46
9.3 Luottamuksellisuus ja tietosuoja 46
9.3.1 Yksityiset tiedot 46
9.3.2 Julkiset tiedot 46
9.3.3 Yksityisten tietojen suojaaminen 46
9.4 Yksityisyyden suoja 46
9.4.1 Yksityisten tietojen suojaamissuunnitelma 47
9.4.2 Varmentajan järjestelmissä käsiteltävät yksityiset tiedot 47
9.4.3 Varmentajan järjestelmissä käsiteltävät julkiset tiedot 47
9.4.4 Vastuu yksityisten tietojen suojaamisesta 47
9.4.5 Yksityisten tietojen käyttäminen tai julkistaminen varmenteen haltijan suostumuksella 47
9.4.6 Tietojen luovutus viranomaisille 47
9.4.7 Muut olosuhteet, joissa tiedot voidaan julkistaa 47
9.5 Immateriaalioikeudet 47
9.6 Osapuolten sitoumukset 47
9.6.1 Varmentajan sitoumukset 47
9.6.2 Rekisteröijän sitoumukset 47
9.6.3 Varmenteen haltijan sitoumukset 48
9.6.4 Varmenteisiin luottavien osapuolten sitoumukset 48
9.6.5 Muiden osapuolten sitoumukset 48
9.7 Vastuuvapauslauseke 48
9.8 Vastuunrajoitukset 48
9.9 Vahingonkorvaukset 49

9.10 Voimassaoloaika ja voimassaolon päättyminen 49
9.10.1 Varmennuskäytännön voimassaoloaika 49
9.10.2 Varmennuskäytännön voimassaolon päättyminen 49
9.10.3 Varmennuskäytännön voimassaolon päättymisen vaikutukset 50
9.11 Varmennepalvelun osapuolien keskinäinen viestintä 50
9.12 Varmennuskäytännön muutosten hallinta 50
9.12.1 Varmennuskäytännön muuttaminen 50
9.12.2 Muutoksista tiedottaminen 50
9.12.3 Varmennuskäytännön tunnistetiedon muuttaminen 50
9.13 Erimielisyyksien ratkaiseminen 50
9.14 Sovellettava laki 50
9.15 Lain noudattaminen 50
9.16 Muut järjestelyt 50
9.16.1 Sopimukset 50
9.16.2 Oikeudenluovutus 51
9.16.3 Osapätemättömyyslauseke 51
9.16.4 Täytäntöönpano 51
9.16.5 Ylivoimainen este 51
9.17 Muut ehdot 51

1 Johdanto

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

Kaikkien tässä varmennuskäytännössä tarkoitettujen osapuolten tulee noudattaa tämän 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.

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 tarjoaminen tapahtuu samassa tuotantoympäristössä, samanlaisin teknisin ja toiminnallisin ratkaisuin ja siihen sovelletaan samoja menettelytapoja noudattaen kuin Digi- ja väestötietoviraston myöntämän allekirjoitusvarmenteen tarjoamiseen.

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 oikeudelliset 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 varmenteen haltija ja varmenteeseen 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.

1.1 Taustaa

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

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. Laatuvarmenteella tehty sähköinen allekirjoitus sekä vahvan sähköisten tunnistamisen välineen avulla tehty henkilön vahva sähköinen tunnistaminen antavat kansalaisille mahdollisuuden turvalliseen, ajasta ja paikasta riippumattomaan ja joustavaan verkkoasiointiin. Laatuvarmenteen ja vahvan sähköisen tunnistuspalvelun tarjoajia valvoo Suomessa Traficom.

Tämän varmennuskäytännön mukaisesti myönnetyt allekirjoitusvarmenteet täyttävät Asetuksen vaatimukset. Laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) on säädetty laatuvarmenteella tehdyistä sähköisistä allekirjoituksista.

Digi- ja väestötietovirasto toimii 1.12.2010 alkaen terveydenhuollon lakisääteisenä varmentajana sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007), sähköisestä lääkemääräyksestä annetun lain (61/2007) sekä väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2019) nojalla.

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

- Laki sähköisestä lääkemääräyksestä (61/2007)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Laki terveydenhuollon ammattihenkilöistä (559/1994)
- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Laki turvallisuusselvityksistä (177/2002)
- IETF RFC 3647 Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework (11/2003)
- IETF RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (4/2002)
- ETSI TS 101 456, v1.4.3: Policy requirements for certification authorities issuing qualified certificates (5/2007)
- ISO/IEC 17090-3: Health informatics - Digital Certificates in Healthcare - Part 3: Policy management of certification authority
- Viestintävirasto Määräys M 72/2016 Määräys sähköisistä tunnistus- ja luottamuspalveluista
- VAHTI 1/2002: Tietoteknisten laitetilojen turvallisuussuositus
- VAHTI 5/2004: Valtionhallinnon keskeisten tietojärjestelmien turvaaminen

Dokumentin tulkinnassa käytetään seuraavia periaatteita:

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

1.2 Varmennuskäytännön tunnukset

Tämän varmennuskäytännön nimi on Varmennuskäytäntö terveydenhuollon muun henkilöstön varmennetta varten, jonka OID on 1.2.246.517.1.10.303.3 ja 1.2.246.517.1.10.353.3.

Tämä varmennuskäytäntö viittaa Varmennepolitiikkaan organisaatiovarmennetta varten, OID 1.2.246.517.1.10.303 ja 1.2.246.517.1.10.303. sekä ammattivarmenteen sisältämän sähköisen allekirjoituksen laatuvarmenteen politiikka-asiakirjan

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 allekirjoitusvarmenteita voi käyttää sellaisten sähköisten allekirjoitusten vahvistamisessa, jotka vastaavat Asetuksessa kuvattuja sähköisten allekirjoitusten hyväksyttyjä varmenteita ja luontivälineitä kuten Asetuksen 28 ja 29 artiklassa säädetään. Tunnistusvarmenteen taso täyttää Asetuksen ja sen nojalla annetun varmuustasoasetuksen mukaisesti vaatimustason ”korkea”.

1.3 Osapuolet ja soveltuvuus

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

1.3.1 Varmentaja

Varmentaja täyttää seuraavat ehdot:

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

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

Varmentaja sitoutuu:

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

Varmentaja voi halutessaan tarjota varmennejärjestelmään liittyviä lisätoimintoja tai -palveluja.

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

Varmentaja tarkastaa ja hyväksyy rekisteröijät sekä niiden henkilökunnan.

1.3.2 Rekisteröijä

Tämän varmennuskäytännön mukaisesti toimivan rekisteröijän on täytettävä seuraavat ehdot:

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

Tämän varmennuskäytännön mukaisen rekisteröijän tulee sitoutua:

1. noudattamaan voimassa olevaa lainsäädäntöä ja sen nojalla annettuja määräyksiä ja ohjeita;

2. tarjoamaan tämän varmennuskäytännön luvuissa 4-6 vaaditut hallinta- ja seurantatoiminnot;
3. suorittamaan varmenteen hakijan tunnistamismenettelyn tämän varmennuskäytännön lukujen 3-4 ja varmennuskäytännön mukaisesti;
4. täyttämään sovitut toimeksiannot ja tukemaan varmenteiden käyttäjien ja varmenteisiin luottavien osapuolten oikeuksia; ja
5. noudattamaan kaikkia tämän varmennuskäytännön sekä varmennepolitiikan rekisteröintipalveluun liittyviä ehtoja.

Rekisteröijä voi tarjota varmentajan hyväksymiä lisätoimintoja tai -palveluja.

Rekisteröijä kantaa vastuun kaikista antamistaan rekisteröintipalveluista.

1.3.3 Varmenteen haltija

Terveydenhuollon muun henkilöstön varmenteen haltijana voi olla terveydenhuollon palvelujen antajaorganisaatiossa työskentelevä henkilö, joka ei ole terveydenhuollon ammattihenkilö.

Terveydenhuollon muun henkilöstön varmenteen hakijan tulee todistaa henkilöllisyytensä varmennehakemusta tehdessään.

Varmennehakemuksen allekirjoittamalla varmenteen hakija sitoutuu noudattamaan varmenteen käyttöehtoja. Voimassaolevat käyttöehdot luovutetaan hakijalle varmenteen luovutuksen yhteydessä.

1.3.4 Varmenteeseen luottava osapuoli

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

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

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

1.3.5 Muut osapuolet

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

1.4 Varmenteen käyttökohteet

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

Terveydenhuollon muun henkilöstön varmenteita käytetään terveydenhuollon kansallisissa tietojärjestelmissä. Terveydenhuollon kansallisilla tietojärjestelmillä

tarkoitetaan järjestelmiä, joilla toimeenpannaan sähköisestä lääkemääräyksestä (61/2007) ja sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) annetuissa laeissa Kansaneläkelaitokselle osoitetut tehtävät. Lisäksi terveydenhuollon muun henkilöstön varmenteita voidaan käyttää terveydenhuollon ja apteekkilaitoksen muissa tietojärjestelmissä.

1.4.1 Sallitut varmenteen käyttötarkoitukset

Ammattivarmenne koostuu varmenneparista, jolla on kaksi toisistaan poikkeavaa käyttötarkoitusta. Todentamis- ja salausvarmenne täyttää vahvan sähköisen tunnistamisvälineen vaatimukset. Yksinomaan allekirjoituksen toteuttamiseen tarkoitettu allekirjoitusvarmenne täyttää laatuvarmenteen vaatimukset. Varmenteen hakijan henkilöllisyyden oikeellisuuden takaa Digi- ja väestötietovirasto.

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

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

1.4.2 Kielletyt varmenteen käyttötarkoitukset

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

1.5 Yhteystiedot

1.5.1 Varmennuskäytännön hallintaorganisaatio

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

Varmentajan yhteystiedot:

Digi- ja väestötietovirasto
PL 123 (Lintulahdenkuja 2)
00531 Helsinki
4369
Y-tunnus: 0245437-2
Puh. +358 295 535 001
Fax. +358 9 876
kirjaamo@dvv.fi

Digi- ja väestötietovirasto (DVV) Varmennepalvelut
PL 123

00531 Helsinki
www.fineid.fi

1.5.2 Varmennuskäytäntöjen suhde varmennepolitiikkaan

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

1.5.3 Varmennuskäytäntöjen hyväksymismenettely

DVV:n Varmennepalvelut määrittelee ja hyväksyy varmennuskäytäntöasiakirjat.

1.6 Määritelmät ja lyhenteet

Ammattioikeus	Ammattioikeudella tarkoitetaan tässä varmennuskäytännössä niitä rekisteröityjä laillistetun, luvan saaneen ja nimikesuojatun ammattihenkilön sekä terveydenhuollon opiskelijan ammatillisia oikeuksia, jotka henkilö voi saada terveydenhuollon ammattihenkilöistä annetun lain (559/1994) 2 §:n nojalla. Ammattioikeus voi olla rajoittamaton, rajoitettu tai kokonaan poistettu. Ammattioikeudet tallennetaan Sosiaali- ja terveysalan lupa- ja valvontaviraston ylläpitämään Terhikki-rekisteriin.
Avaimen palautus *(Key recovery)*	Key recoveryllä tarkoitetaan tilannetta, jossa yksityinen avain palautetaan varmennekortin hajottua tai hävitessä. Terveydenhuollon varmennekorttien yksityisiä avaimia ei voida palauttaa kortin hajottua tai hävitessä.
Avaintenhallinta (Key management)	Avaintenhallinnalla tarkoitetaan varmentajan avainten sekä varmenteen haltijan todentamis- ja salaus- sekä allekirjoitusavainten hallintamenettelyjä ja -ratkaisuja niiden elinkaaren ajan. Elinkaaren vaiheita ovat avainten tilaaminen, luominen, jakelu, säilyttäminen, käyttö, sulkeminen, uusiminen, arkistointi ja tuhoaminen.
Eheys (*Integrity*)	1) Tietojen tai tietojärjestelmän aitous, väärentämättömyys, sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus 2) ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.

Julkisen avaimen järjestelmä *(PKI, Public Key Infrastructure)*	Julkisen avaimen järjestelmässä nimetty varmentaja tuottaa käyttäjille avainparit, varmentaa ne digitaalisella allekirjoituksellaan, takaa varmenteen haltijan henkilöllisyyden ja jakaa varmenteet käyttäjille, ylläpitää varmennehakemistoa ja sulkulistaa sekä mahdollisesti antaa muita järjestelmän käyttöön liittyviä palveluja. Julkisen avaimen järjestelmässä kullakin käyttäjällä on kaksi toisiinsa liittyvää avainta. Toinen avainparin avaimista on julkinen, toinen on vain avainparin käyttäjän hallussa oleva yksityinen avain. Yksityisellä avaimella sähköisesti allekirjoitettu tiedon aitous voidaan todentaa vain vastaavalla julkisella avaimella, ja vastaavasti tiedon välittämisessä vastaanottajan julkisella avaimella salattu tieto voidaan muuttaa selväkieliseen muotoon vain vastaanottajan yksityisellä avaimella.
Kiistämättömyys (*Non-repudiation*)	Kiistämättömyys tarkoittaa, että osapuolten osallisuus tapahtumaan tai tekoon voidaan jälkeenpäin todistaa. Kiistämättömyys varmistaa sen, ettei toinen osapuoli voi kieltää toimintaansa, esimerkiksi tekemäänsä sähköistä allekirjoitusta, jälkeenpäin. Kiistämättömyyden tavoitteena on juridinen sitovuus.
Kortinhallintasovellus, KoHa	Varmennejärjestelmän erillisenä osana toimiva rekisteröintipalvelua sekä sulkupalvelua tukeva tietokantasovellus, johon on talletettuna mm. korttien ja varmenteiden elinkaari- ja haltijatiedot.
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.
OCSP	Online Certificate Status Protocol, suorakäyttöinen varmenteen tilan palauttava palvelu
Personointiohjelmisto	Rekisteröintipisteissä käytettävä ohjelmisto, jolla hallitaan yhteyksiä KoHa- ja Terhikki-rekistereihin, tehdään varmennekortin pintapainatukset sekä tallennetaan varmenteet kortin sirulle. Personointiohjelmistolla tuotetaan myös PIN- ja PUK-tunnusluvut.
PIN *(Personal identification number)*	Varmennekortin avainparin käyttöoikeuden varmistamiseksi käytettävä tunnusluku. Terveydenhuollon varmennekortilla

	on kaksi tunnuslukua, toinen todentamista ja salausta 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 varmennekortin PIN-tunnusluvun tilanteessa, jossa PIN-tunnusluku on syötetty väärin liian monta kertaa peräkkäin.
Rekisteröijä *(RA, Registration Authority)*	Julkisen avaimen järjestelmässä luotettu taho, joka varmentajan valtuuttamana ja auditoimana toteuttaa rekisteröijän tehtäviä. Rekisteröijä ylläpitää varmentajan lukuun yhtä tai useampaa rekisteröintipistettä.
Rekisteröintipiste *(RA-piste)*	Palvelupiste, jossa tarkistetaan varmenteen hakijan henkilöllisyys sekä terveydenhuollon ammattihenkilöiden osalta ammattioikeudet ja muiden henkilöiden osalta työnantajatiedot. Rekisteröintipiste vastaa varmennekorttien, varmenteiden ja PIN-/PUK-tunnuslukujen jakelusta käyttäjille varmennepolitiikan ja varmennuskäytännön mukaisesti.
Sulkulista *(CRL, Certificate Revocation List)*	Sulkulista on luettelo suljetuista varmenteista. Varmenne suljetaan, kun varmenteen haltija pyytää sulkemista, varmenteeseen merkityt varmenteen haltijan tiedot ovat muuttuneet, varmennekortti ja avaustunnusluku ovat kadonneet tai anastettu tai varmenteen haltija on kuollut.
Sulkupalvelu	Varmentajan palvelu, joka sulkee terveydenhuollon muun henkilöstön varmenteita tehtyjen sulkupyyntöjen perusteella.
Terveydenhuollon ammattihenkilö	Terveydenhuollon ammattihenkilöistä annetun lain (559/1994) 2 §:n 1 momentin mukaan terveydenhuollon ammattihenkilöllä tarkoitetaan henkilöä, joka lain nojalla on saanut ammatinharjoittamisoikeuden (laillistettu ammattihenkilö) tai ammatinharjoittamisluvan (luvan saanut ammattihenkilö) sekä henkilöä, jolla lain nojalla on oikeus käyttää asetuksella säädettyä terveydenhuollon ammattihenkilön ammattinimikettä (nimikesuojattu ammattihenkilö). Tässä varmennuskäytännössä terveydenhuollon ammattihenkilöllä tarkoitetaan myös terveydenhuollon ammattihenkilöistä annetun lain 2 §:n 3 momentissa tarkoitettua opiskelijaa.

Terveydenhuollon muu henkilö	Muu terveydenhuollon toimintayksikössä työskentelevä tai sen tehtäviä suorittava henkilö, joka ei ole terveydenhuollon ammattihenkilö.
Terhikki-rekisteri	Terveydenhuollon ammattihenkilöistä annetun lain (559/1994) nojalla Valviran ylläpitämä valtakunnallinen rekisteri terveydenhuollon ammattihenkilöistä ja heidän ammatinharjoittamisoikeustiedoistaan.
Todentaminen (*Authentication*)	Järjestelmän käyttäjän (henkilön, organisaation, laitteen tai järjestelmän) tai viestinnässä toisen osapuolen aitouden varmistaminen. Yleisiä käyttäjän todennuksen menetelmiä ovat: 1) käyttäjä tietää ainutkertaisen asian, esimerkiksi salasanan 2) hänellä on hallussaan jokin ainutkertainen ominaisuus kuten sormenjälki 3) hänellä on hallussaan ainutkertainen väline, esimerkiksi terveydenhuollon varmennekortti.
Tunnistaminen *(Identification)*	Menettely, jolla yksilöidään esimerkiksi tietojärjestelmän käyttäjä. Tyypillisesti tunnistus tapahtuu tarkistamalla, onko esitetty tunnus tai muu tunniste hyväksyttävien tunnusten joukossa, esimerkiksi käyttäjäksi ilmoittautunut henkilö tietojärjestelmän valtuutettujen käyttäjien luettelossa.
Turvataso	Turvatasolla tarkoitetaan niiden turvatoimien tasoa, joilla varaudutaan siihen, että turvallisuutta uhkaavaa välikohtausta yritetään tai se tapahtuu. Tyypillisiä turvatason seurantakohteita ovat esimerkiksi tietoturvapoikkeamat.
Vara-avainjärjestelmä *(Key escrow)*	Key escrow on menetelmä, jossa todentamis- ja salausavainten turvatalletus on pakollista ja turvatalletuksessa oleva avain on tietyissä tilanteissa käytettävissä ilman varmenteen haltijan suostumusta. Terveydenhuollon varmennekorttien yksityisiä avaimia ei turvatalleteta.
Varmenne *(Certificate)*	Julkisen avaimen järjestelmää käyttävän palveluverkon toimijan kuten terveydenhuollon ammattihenkilön tai palvelun-tuottajan julkisesta avaimesta ja tunnistetiedoista muodostettu tietokokonaisuus, jonka varmentaja on muodostanut ja allekirjoittanut yksityisellä avaimellaan. Varmenteen aitous on todennettavissa varmentajan julkisella avaimella (varmentajan varmenteella).
Varmennehakemisto	Varmennehakemisto on julkinen tietokanta, johon varmentaja tallettaa varmentajan varmenteet, terveydenhuollon todentamis- ja salausvarmenteet 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.
Varmentaja *(CA, Certification Authority)*	Julkisen avaimen järjestelmässä luotettu taho, joka tuottaa järjestelmän käyttäjille avainparit ja tuottaa, allekirjoittaa, jakelee ja tarvittaessa sulkee varmenteet.
Väestötietojärjestelmä, VTJ	Väestörekisteri, joka sisältää perustiedot Suomen kansalaisista ja Suomessa vakinaisesti asuvista ulkomaalaisista. Järjestelmässä on tietoja myös rakennuksista, rakennushankkeista ja huoneistoista sekä kiinteistö- ja toimitilatietoja. Väestötietojärjestelmää ylläpitävät Digi- ja väestötietovirasto ja maistraatit. Sinne ilmoittavat päivitystietoja myös seurakunnat sekä sairaalat. Tietojen rekisteröinti perustuu kansalaisten ja viranomaisten lakisääteisiin ilmoituksiin.

2 tietojen Julkaiseminen

2.1 Julkinen hakemisto

Varmentaja vastaa varmennehakemiston ylläpidosta sekä luvussa 2.2 määritellyn informaation julkaisemisesta. Hakemiston tietosisältö ja rakenne noudattavat THPKI T3 -määritystä.

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

2.2 Varmentajan julkaisemat tiedot

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

2.3 Julkaisutiheys

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

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

2.4 Pääsyoikeudet

Varmentajan julkaisemien tietojen saatavuutta ei rajoiteta pääsyoikeuksin.

3 Tunnistaminen ja todentaminen

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

3.1 Varmenteen haltijan nimeäminen

3.1.1 Nimeäminen

Terveydenhuollon varmenteen haltijan nimeäminen todentamis- ja salausvarmenteessa sekä allekirjoitusvarmenteessa on kuvattu määrityksessä Digi- ja väestötietoviraston terveydenhuoltoa koskeva CA-malli = THPKI - T2: Digi- ja väestötietoviraston CA-malli ja varmenteiden tietosisältö terveydenhuollossa.

Digi- ja väestötietoviraston juurivarmentaja on:
CN = DVV Gov. Root CA – G3 RSA

OU = Varmennepalvelut

OU = Certification Authority Services

O = Digi- ja vaestotietovirasto CA

C = FI

ja

CN = DVV Gov. Root CA – G3 ECC

OU = Varmennepalvelut

OU = Certification Authority Services

O = Digi- ja vaestotietovirasto CA

C = FI

Digi- ja väestötietoviraston organisaatiovarmenteiden varmentaja on:

CN (Common name) = DVV Organisational Certificates - G4R

OU (Organizational unit) = Organisaatiovarmenteet

O (Organization) = Digi- ja vaestotietovirasto CA

C (Country) = FI

ja

CN (Common name) = DVV Organisational Certificates - G4E

OU (Organizational unit) = Organisaatiovarmenteet

O (Organization) = Digi- ja vaestotietovirasto CA

C (Country) = FI

Varmenteen haltijan nimeämiskäytäntö organisaatiovarmenteissa:

2.5.4.5 (Serial Number) = Yksilöivä tunniste

SN (Surname) = Sukunimi

G (Given name) = Etunimi

CN (Common name) = Sukunimi Etunimi Asiointitunnus

C (Country) = FI

Valinnaiset kentät:

O (Organization) = Organisaation nimi

OU (OrganizationalUnit) = Organisaatioyksikkö

T (Title) = Nimike

E (EmailAddress) = Sähköpostiosoite

UPN (Universal Principal Name) = UPN-nimi

3.1.2 Nimeämisen merkitys

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

Attribuuttien joukko, josta muodostuu varmenteeseen kohteen nimitietue, on ainutlaatuinen ja yksilöi asianomaisen varmenteen haltijan. Yksilöivän tunnuksen antaa varmentaja. Kaikkien terveydenhuollon muiden henkilöiden on toimittava omilla nimillään.

3.1.3 Anonyymit tai salanimet

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

3.1.4 Nimikenttien sisältö

Nimikenttien sisältö on määritetty luvussa 3.1.1.

3.1.5 Nimitietueen ainutkertaisuus

Luvussa 3.1.1 määritelty nimitietue yksilöi terveydenhuollon muun henkilöstön varmenteen haltijan. Henkilön tunnistetieto on varmenteen haltijan ainutkertaisesti yksilöivä.

3.1.6 Tuotenimien käyttöoikeus

—

3.2 Henkilöllisyyden todentaminen

3.2.1 Menettelytapa yksityisen avaimen omistajuuden todistamiseksi

Terveydenhuollon muun henkilön yksityiset avaimet luodaan aina varmennekortin sirulla. Yksityiset avaimet sisältävä varmennekortti luovutetaan terveydenhuollon muulle henkilölle sen jälkeen, kun hänen henkilöllisyytensä on luotettavasti todettu ja varmenne on rekisteröity ja luotu.

3.2.2 Varmenteen hakijan edustaman organisaation todentaminen

Terveydenhuollon muun henkilöstön varmenteiden hakijoiden osalta vaaditaan heidän edustamiensa organisaatioiden todentamista.

3.2.3 Henkilön tunnistaminen

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. Henkilön tunnistamiseen liittyvät tiedot tallennetaan varmentajan varmenteiden tilaus- ja hallintajärjestelmään (Vartti).

3.2.4 Varmenteen hakijan tiedot, joita varmentaja ei tarkista

Kaikki terveydenhuollon muun henkilön varmennehakemuksessa tarvittavat henkilötiedot saadaan väestötietojärjestelmästä ja hakijan edustaman organisaation toimittamista työnantajatiedoista.

3.2.5 Varmenteen myöntämisen edellytykset

Vain terveydenhuollon toimintayksikössä työskentelevällä tai sen tehtäviä suorittavalla henkilöllä, joka ei ole terveydenhuollon ammattihenkilö, on oikeus hakea terveydenhuollon muun henkilöstön varmennetta. Palvelussuhteen päättyessä terveydenhuollon muun henkilöstön varmenne on suljettava.

3.2.6 Varmentajien välisen yhteistyön edellytykset ja vaatimukset

Varmentajien välisen yhteistyön edellytykset ja vaatimukset määritellään juurivarmentajan varmennepolitiikassa.

3.3 Tunnistaminen ja todentaminen varmenteen uusimisessa

3.3.1 Tunnistaminen ja todentaminen varmenteen uusimisessa

Varmenteiden uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

3.3.2 Tunnistaminen ja todentaminen varmenteen sulkemisen jälkeen

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

3.4 Sulkupyynnön tekijän tunnistaminen

Varmenteen sulkupyyntö voidaan tehdä puhelimitse, henkilökohtaisesti rekisteröintipisteessä tai kirjallisesti varmentajalle.

Kun sulkupyyntö tehdään puhelimitse tai kirjallisesti, ilmoittajan ja varmenteen haltijan tiedot kirjataan varmenteiden tilaus- ja hallintajärjestelmään (Vartti).

Kun sulkupyyntö tehdään henkilökohtaisesti rekisteröintipisteessä, henkilö tunnistetaan 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.

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

4 VARMENTEEN ELINKAAREN HALLINNAN TOIMINNALLISET VAATIMUKSET

Tämä luku kuvaa varmentajan, rekisteröijän ja terveydenhuollon muun henkilön toiminnalle asetetut vaatimukset. Luku käsittää myös varmenteiden sulkemisen.

4.1 Varmenteen hakeminen

Terveydenhuollon muun henkilöstön varmennetta haetaan henkilökohtaisesti rekisteröintipisteestä.

Hakemuksen tiedot tallennetaan varmentajan varmenteiden tilaus- ja hallintajärjestelmään.

Terveydenhuollon muun henkilöstön varmenteen hakeminen edellyttää, että hakija:

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

Hakijalle ilmoitetaan varmennekortin sekä tunnuslukukuoren toimitustavoista. Hakijalle annetaan varmenteen käyttöehdot, jotka sisältyvät varmennepolitiikka-asiakirjoihin.

4.1.1 Kuka voi tehdä varmennehakemuksen

Varmennehakemuksen voi tehdä terveydenhuollon toimintayksikössä työskentelevä tai sen tehtäviä suorittava henkilö, joka ei ole terveydenhuollon ammattihenkilö.

4.1.2 Varmenteen myöntämisprosessi ja vastuut

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

Varmentajan tietojärjestelmien väliset tietoliikenneyhteydet on suojattu. varmenteiden tilaus- ja hallintajärjestelmää käyttävät henkilöt tunnistetaan varmentajan myöntämillä hallintakorteilla. Varmenteen tietosisältö muodostuu hakemuslomakkeessa ilmoitetuista tiedoista.

Rekisteröijä toimittaa varmennehakemuksen varmentajalle varmenteen myöntämiseksi, kun rekisteröijä ja hakija ovat tarkistaneet ja hyväksyneet allekirjoituksellaan varmennehakemuksen tiedot.

Varmentaja toimittaa hakijalle hakijan tiedoilla yksilöidyn:

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

Lisäksi rekisteröijä toimittaa varmenteen hakijalle varmennekortin käyttöohjeen.

4.2 Varmennehakemuksen käsittely

Varmennehakemus käsitellään rekisteröintipisteessä ilman aiheetonta viivytystä.

Rekisteröijä tallettaa varmenteen tilaustiedot varmentajan varmenteiden tilaus- ja hallintajärjestelmään.

4.2.1 Tunnistamisen ja todentamisen toteuttaminen

Rekisteröijä tunnistaa varmenteen hakijan luvun 3 mukaisesti ja tarkistaa, että henkilö työskentelee terveydenhuollon toimintayksikössä.

Hakijan henkilötiedot saadaan Väestötietojärjestelmästä. Hakemuksessa on mainittu hakijan ilmoittama varmenteeseen talletettava kutsumanimi. Näiden lisäksi rekisteröijä täyttää lomakkeeseen hakijan palvelussuhteeseen liittyviä tietoja, varmenteen tuottamiseen ja toimittamiseen tarvittavia tietoja sekä tiedon hakijan tunnistamisessa käytetystä tunnistamisasiakirjasta.

4.2.2 Varmennehakemuksen hyväksyminen tai hylkääminen

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

4.2.3 Varmennehakemuksen käsittelyaika

Varmennehakemus käsitellään ilman aiheetonta viivytystä rekisteröintipisteen aukioloaikana.

4.3 Varmenteen myöntäminen

4.3.1 Varmenteen myöntämiseen liittyvät varmentajan tehtävät

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

Varmenteen myöntämiseen liittyvät tehtävät on kuvattu luvuissa 4.1 ja 4.2.

4.3.2 Ilmoitus hakijalle varmenteen myöntämisestä

Erillistä ilmoitusta terveydenhuollon muun henkilöstön varmenteen myöntämisestä ei tehdä.

4.4 Myönnetyn varmenteen hyväksyminen

4.4.1 Myönnetyn varmenteen hyväksymismenettely varmenteen hakijan kannalta

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

4.4.2 Varmenteen julkaisu varmentajan toimesta

Varmentaja julkaisee myönnetyt todentamis- ja salausvarmenteet julkisessa tietoverkossa olevassa varmennehakemistossa luvussa 2.1 kuvatulla tavalla. Allekirjoitusvarmenteita ei julkaista hakemistossa.

4.4.3 Ilmoitus muille osapuolille varmenteen myöntämisestä

Erillistä ilmoitusta terveydenhuollon muun henkilöstön varmenteen myöntämisestä ei tehdä.

4.5 Varmenteiden ja avainparien käyttö

4.5.1 Varmenteiden ja avainparien käyttö varmenteen haltijan toimesta

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

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

Terveydenhuollon muu henkilö vastaa ensisijaisesti vahingosta, jonka hän aiheuttaa:

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

Varmenteen haltijan tulee säilyttää ja hallita huolellisesti omia varmenteitaan ja avainparejaan sekä niihin liittyviä tunnuslukuja ja varmennekorttiaan. Varmenteen haltijan tulee estää varmennekortin katoaminen sekä tunnuslukujen paljastuminen tai luvaton käyttö.

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

Terveydenhuollon muun henkilön tulee ilmoittaa sulkupalveluun:

- varmennekortin katoaminen tai väärinkäyttöepäily.

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

PIN-tunnuslukuja, joita käytetään avainten aktivointiin, ei saa säilyttää samassa paikassa varmennekortin 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-avaustunnusluku on kadonnut, tulee kortinhaltijan mennä rekisteröintipisteeseen saadakseen tietoonsa avaustunnusluvun. Avaustunnuslukua kysyttäessä kortinhaltija tunnistetaan 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. Rekisteröintipisteen virkailija tulostaa uuden tunnuslukukuoren, joka sisältää avaustunnusluvun. Avaustunnuslukua ei ilmoiteta puhelimitse tai kirjeitse tietoturvasyistä.

4.5.2 Varmenteiden ja julkisten avainten käyttö varmenteisiin luottavan osapuolen toimesta

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

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

Luottavan osapuolen vastuulla on varmenteen tarkistaminen asianmukaisella tavalla koko varmennepolun läpi IETF RFC 5280 -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 voimassaolotiedon tarkistus (joko OCSP-palvelun tai voimassaolevan sulkulistan tarkistaminen). Varmenteeseen ei tule luottaa, ellei luottava osapuoli suorita suljettujen varmenteiden tarkistusta seuraavalla tavalla:

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

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

4.6 Julkisen avaimen uudelleen varmentaminen

Terveydenhuollon muun henkilöstön varmenteita ei myönnetä aiemmin varmennetuille julkisille avaimille.

4.7 Varmenteen uusiminen

4.7.1 Varmenteen uusimisen syyt

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

Varmenne voidaan uusia myös varmenteen tietosisältöön vaikuttavien varmenteen haltijan tietojen muuttuessa tai varmennekortin rikkoutuessa. Tällöin varmenteen

haltijan tulee ottaa yhteyttä rekisteröintipisteeseen ja hakea uutta varmennekorttia ja varmennetta luvussa 4 kuvatulla tavalla.

4.7.2 Varmenteen uusimisen hakeminen

Varmenteen uusimista voi hakea vain varmenteen haltija.

4.7.3 Varmenteen uusimispyynnön käsittely

Varmenteiden uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

4.7.4 Ilmoitus varmenteen hakijalle varmennekortin uusimisesta

Erillistä ilmoitusta terveydenhuollon muun henkilöstön varmenteen uusimisesta ei tehdä.

4.7.5 Uusitun varmenteen hyväksymismenettely varmenteen haltijan kannalta

Uusittu varmenne hyväksytään kappaleessa 4.4.1 kuvatun menetelmän mukaisesti.

4.7.6 Uusitun varmenteen julkaisu

Varmenteet julkaistaan kappaleessa 4.4.2 kuvatun menetelmän mukaisesti.

4.7.7 Ilmoitus uusitun varmenteen myöntämisestä muille osapuolille

Erillistä ilmoitusta terveydenhuollon muun henkilöstön varmenteen uusimisesta ei tehdä.

4.8 Varmenteen muuttaminen

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

4.9 Varmenteen sulkeminen ja määräaikainen sulkeminen

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

Varmentaja ei ilmoita varmenteen haltijalle varmenteen sulkemisesta.

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

4.9.1 Varmenteen sulkemisen edellytykset

Varmenne suljetaan kun:

- varmenteen haltija pyytää sulkemista

- varmenteen haltija vaihtaa työpaikkaa
- varmennekortti on vahingoittunut, kadonnut tai anastettu
- avaustunnusluku sekä varmennekortti ovat kadonneet tai anastettu
- varmenteen haltija on kuollut.

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

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

4.9.2 Kuka voi vaatia varmenteen sulkemista

Varmenteen sulkemista voivat vaatia:

- terveydenhuollon muu henkilö tai hänen lakisääteinen edustajansa kyseisen henkilön oman varmenteen osalta;
- varmentaja kohdan 4.9.1 edellytysten täyttyessä.

4.9.3 Varmenteen sulkemisprosessi

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

1. puhelimitse soittamalla maksuttomaan sulkupalveluun +358 800 162 622.
2. henkilökohtaisesti rekisteröintipisteessä tai
3. kirjallisesti varmentajalle.

Varmenteen sulkupyynnön tekijä tunnistetaan luvussa 3.4 kuvatulla tavalla.

Varmentaja sulkee viran puolesta varmenteet:

- varmenteen haltijan kuoleman perusteella.

Varmenteen sulkemisesta kirjataan seuraavat tiedot:

- suljettavan varmenteen haltijan käytettävissä olevat henkilötiedot
  - etunimet ja sukunimi
  - yksilöintitunnus/rekisteröintinumero tai henkilötunnus
- sulkupyynnön tekijän henkilötiedot (jos eri kuin varmenteen haltija)
- sulkupyynnön tekijän tunnistamistapa
- sulkupyynnön ajankohta
- sulkupyynnön syy kirjataan, kun sulkupyynnön tekee muu kuin varmenteen haltija; varmenteen haltijan ei tarvitse ilmoittaa sulkupyyntönsä syytä

- sulkupyynnön vastaanottajan henkilötiedot
- mahdolliset muut varmenteen haltijan ilmoittamat lisätiedot
  - varmennekortin katoamisaika, varmenteen haltijan kuolinaika tms.
- varmenteen sulkijan henkilötiedot
- varmenteen sulkemisen ajankohta.

Mikäli varmenteen haltijalle luovutetun varmenteen sulkupyynnön tekijä on eri henkilö kuin varmenteen haltija ja sulkupyyntö ei johdu varmenteen haltijan yhteydenotosta varmentajaan tai rekisteröijään, ilmoitetaan varmenteen sulkutapahtumasta myös kirjeitse varmenteen haltijalle. Varmenne suljetaan kortinhallintasovelluksella ja varmenteen sulkemiseen liittyvät tiedot säilytetään 5 vuotta sulkemisajankohdasta.

4.9.4 Varmenteen haltijan velvollisuus tehdä sulkupyyntö

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

4.9.5 Varmenteen sulkupyynnön käsittelyaika

Sulkupalvelu ja rekisteröintipisteet käsittelevät varmenteen sulkupyynnöt viipymättä.

4.9.6 Varmenteeseen luottavan osapuolen velvollisuus tarkistaa varmenteen voimassaolo

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

Luottavan osapuolen vastuulla on varmenteen voimassaolotiedon. Varmenteeseen ei tule luottaa, ellei luottava osapuoli ole tarkistanut varmenteen voimassaoloa joko voimassaolevalta sulkulistalta tai OCSP-palvelusta.

4.9.7 Sulkulistan julkaisutiheys

Päivitetty sulkulista julkaistaan tunnin välein.

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

4.9.8 Sulkulistan voimassaolon enimmäisaika

Päivitetty sulkulista on voimassa enintään 8 tuntia. Jokaisessa sulkulistassa on mainittu voimassaolon päättymisajankohta.

4.9.9 Reaaliaikainen varmenteen tilan tarkistaminen

Reaaliaikainen varmenteen tilan tarkistaminen ei ole käytössä.

4.9.10 Vaatimukset varmenteen tilan reaaliaikaiselle tarkistamiselle

—

4.9.11 Muut varmenteen tilan tarkistamismenettelyt

—

4.9.12 Yksityisen avaimen paljastumisesta johtuva varmenteen sulkeminen

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

4.9.13 Varmenteen sulkeminen määräajaksi

Varmenteita ei suljeta määräajaksi.

4.9.14 Kuka voi vaatia varmenteen sulkemista määräajaksi

—

4.9.15 Menettelytavat varmenteen sulkemiseksi määräajaksi

—

4.9.16 Rajoitukset varmenteen määräaikaiselle sulkemiselle

—

4.10 Varmenteen tilan tarkistamismahdollisuus

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

4.11 Varmenteen voimassaolon päättyminen

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

4.12 Vara-avainjärjestelmä ja avainten palautus

Terveydenhuollon muiden henkilöiden todentamis- ja salausavaimia ei turvatalleteta. Varmenteita ei siten voida käyttää ilman varmenteen haltijan suostumusta eikä yksityisiä avaimia voida palauttaa kortin hajottua tai hävitessä.

5 Fyysisen, käyttö- ja henkilöstöturvallisuuden hallinta

Tässä luvussa kuvataan varmentajalta, rekisteröijältä ja varmenteen haltijalta edellytettävät fyysisen turvallisuuden sekä käyttö- ja henkilöstöturvallisuuden varmistavat toimenpiteet. Varmentajan ja rekisteröijän turvallisuusvaatimusten osalta noudatetaan VAHTI 5/2004 -ohjetta sekä 1.5.2011 alkaen ISO/IEC 27002 -standardin asettamia vaatimuksia.

5.1 Fyysisen turvallisuuden hallinta

Varmentajan yksityiset avaimet, joilla allekirjoitetaan varmenteet ja sulkulistat, on suojattu fyysistä tunkeutumista vastaan.

Varmentaja, rekisteröintipisteet sekä kortinvalmistaja säilyttävät tuotantovälineitä ja varmuuskopioita siten, että luvattomilla henkilöillä ei ole mahdollisuutta päästä käsiksi varastoituun tietoon ja että tietoja on mahdotonta muuttaa, väärentää tai tuhota. Varmuuskopioita säilytetään sekä tietojen palauttamista että arkistointia varten. Onnettomuuksien varalta varmuuskopiot säilytetään eri tiloissa varmenteiden tuotantojärjestelmien kanssa.

Fyysisen turvallisuuden hallinnan tarkemmat ehdot määritellään varmennuskäytännössä. Varmentaja sopii tarvittaessa erikseen fyysisen turvallisuuden hallinnan yksityiskohdista käyttämiensä toimittajien kanssa.

5.1.1 Tilojen sijoittaminen ja rakenne

Rekisteröintipisteiden toimitilat on sijoitettu VAHTI 1/2002 -ohjeen mukaiseen toimitilaluokkaan 1 (perussuojaus) kuuluviin tiloihin.

Varmenteiden tuottamiseen käytetyt järjestelmät on sijoitettu VAHTI 1/2002 -ohjeen mukaiseen toimitilaluokkaan 3 (erityissuojaus) kuuluvaan konesalitilaan. Konesalitilat on osastoitu ja kahdennetut tietojärjestelmät on sijoitettu eri konesaleihin, jotka voivat toimia toisistaan riippumattomasti.

5.1.2 Fyysinen pääsynvalvonta

Rekisteröintipisteet ovat kulunvalvonnan piirissä siten, että asiattomien pääsy toimitiloihin on estetty lukitsemalla toimitilat riittävän tehokkaasti.

Varmennetuotannon järjestelmät ovat tiloissa, joissa on ympärivuorokautinen miehitetty valvonta, tapahtumat kirjaava sähkölukitus ja nauhoittava kameravalvonta. Tiloihin pääsee vain henkilökohtaisella kulkuavaimella ja kaikki tapahtumat rekisteröidään kulunvalvontajärjestelmään.

5.1.3 Sähkö ja ilmastointi

Rekisteröintipisteiden sähkön saanti ja ilmastoinnin toimivuus tulee erikseen varmistaa.

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

5.1.4 Vesivahinko

Rekisteröintipisteet suojataan vesivahinkoja vastaan.

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

5.1.5 Tulipalo

Rekisteröintipisteet suojataan palovahinkoja vastaan.

Varmennetuotannon järjestelmät sijaitsevat automaattisammutuksella varustetuissa konesalitiloissa.

5.1.6 Tietovälineiden säilytys

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

5.1.7 Tietovälineiden hävittäminen

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

5.1.8 Varmuuskopiointi verkon yli

Varmennetuotantojärjestelmän varmuuskopiointi tapahtuu varmennejärjestelmän sisäisessä tietoliikenneverkossa.

5.2 Käyttöturvallisuuden hallinta

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

5.2.1 Työtehtäviin liittyvät roolit

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

Varmennetoiminnan rooleja ovat:

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

Lisäksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) mukaisesti varmentaja seuraa ja valvoo, että sen antamaan palveluun liittyvä tietosuoja ja tietoturva toteutuvat

5.2.2 Varmennetuotannon työtehtäviin tarvittavien henkilöiden määrä

Varmentajan lukuun toimivat nimetyt organisaatiot ja henkilöt.

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

5.2.3 Henkilöiden tunnistaminen ja todentaminen eri rooleihin

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

5.2.4 Tehtävien eriyttämistä vaativat roolit

Rekisteröijä ei voi toimia järjestelmän pääkäyttäjän roolissa.

5.3 Henkilöstöturvallisuuden hallinta

5.3.1 Tausta-, ansio-, kokemus- ja selvitysvaatimukset

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

Varmentajan työtehtävissä toimivista henkilöistä tehdään turvallisuusselvitys.

5.3.2 Taustojen tarkistamisen menettelytapa

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

5.3.3 Koulutuksen tiheys ja vaatimukset

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

5.3.4 Jatkokoulutuksen tiheys ja vaatimukset

—

5.3.5 Työtehtävien kierrätyksen tiheys ja järjestys

—

5.3.6 Seuraukset luvattomista toimista

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

5.3.7 Alihankkijoiden henkilöstön vaatimukset

Varmentajan valtuuttamien organisaatioiden henkilöstön tulee täyttää luvun 5.3.1 edellytykset.

5.3.8 Asiakirjat, jotka toimitetaan henkilökunnalle

Varmennetoimintaan osallistuvalla henkilökunnalla on käytössään tämän varmennuskäytännön lisäksi heidän toimintaansa määrittelevät toimintaohjeet.

5.4 Varmennejärjestelmän turvallisuuden seuranta

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

5.4.1 Arkistoitavat tapahtumat

Varmentaja säilyttää turvallisuusseurantaa varten seuraavat tiedot:

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

Varmenteiden ja varmennejärjestelmän osalta varmentaja säilyttää:

1. Kaikki tapahtumat, jotka liittyvät varmenteiden, myös varmentajan toiminnassaan käyttämien varmenteiden, luomiseen ja sulkemiseen.
2. Kaikki tapahtumat, jotka liittyvät varmenteiden allekirjoitusavainten hallintaan.
3. Kaikki järjestelmän hallintaan liittymättömät viestit rekisteröintipalvelusta, varmenteiden jakelupalvelusta ja lisäpalveluista.
4. Lokijärjestelmän käynnistykset ja alasajot.
5. Lokijärjestelmän asetusten muutokset.

5.4.2 Lokitietojen analysointitiheys

Lokitietoja analysoidaan tarvittaessa.

5.4.3 Lokitietojen säilytysaika

Lokitiedot säilytetään voimassaolevien arkistosäännösten mukaisesti.

5.4.4 Lokitietojen suojaaminen

Lokitietoihin on pääsy vain erikseen oikeutetuilla henkilöillä.

Lokitiedot suojataan muuttamiselta, tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä.

5.4.5 Lokitietojen varmuuskopiointi

Lokitiedoista otetaan varmuuskopiot päivittäin.

5.4.6 Lokitietojen keräysjärjestelmän toteuttaminen (sisäinen/ulkoinen)

Varmentaja vastaa lokitietojen keräysjärjestelmästä.

5.4.7 Lokitapahtumasta ilmoittaminen

Järjestelmän käyttäjälle ei erikseen ilmoiteta lokitapahtumien syntymisestä.

Lokitietojen valvonnasta vastaaville henkilöille ilmoitetaan erikseen seuraavista tapahtumista:

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

5.4.8 Haavoittuvuuksien arviointi

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

5.5 Arkistoitavat aineistot

5.5.1 Arkistoitavat asiakirjat, tiedostot ja mediat

Varmentaja arkistoi seuraavat tiedot:

- varmennehakemukset;
- varmenne- tai muun hakemuksen allekirjoitetut hyväksynnät;
- varmennepalvelusopimukset;
- myönnetyt varmenteet;
- ristiinvarmennusasiakirjat mukaanluettuna ristiinvarmennuksen perustelut ja päätökset sekä suoritetut toimet;
- varmenteen sulkupyynnöt;
- voimassaolevat ja edelliset varmennepolitiikat ja varmennuskäytännöt;
- varmentajan ja rekisteröintipisteiden väliset sopimukset
- varmennejärjestelmän ylläpitoon, käyttöön ja hallintaan liittyvät sopimukset.
- Tarkastusraportit ja pöytäkirjat käsittäen tietoturvatarkastukset ja järjestelmän auditoinnin

5.5.2 Arkistojen säilytysaika

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

5.5.3 Arkistojen suojaaminen

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

Arkistotiedot suojataan muuttamiselta, tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä.

5.5.4 Arkistojen varmuuskopiointimenettely

Arkistotiedoista ei oteta varmuuskopioita.

5.5.5 Arkistoitavien tietojen aikaleima

Arkistoitavat asiakirjat on päivätty. Aikaleimapalvelu ei ole toistaiseksi käytössä.

5.5.6 Arkistojen keräysjärjestelmä (sisäinen/ulkoinen)

Varmentajalla ei ole keskitettyä arkistojen keräysjärjestelmää.

5.5.7 Arkistoissa olevien tietojen saatavuus ja eheys

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

5.6 Varmentajan avainparin vaihto

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

5.7 Häiriötilanteisiin varautuminen

5.7.1 Suunnitelma toimintahäiriöiden ja toiminnan vaarantumisen varalta

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

5.7.2 Varmennejärjestelmän, ohjelmistojen tai tietojen vahingoittuminen

Poikkeustilanteissa varmentaja noudattaa jatkuvuus- ja toipumissuunnitelmaa.

5.7.3 Toiminta varmenteen haltijan yksityisen avaimen paljastuessa

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

5.7.4 Toiminnan jatkuvuus häiriötilanteen jälkeen

Varmentaja pyrkii häiriötilanteen jälkeen saattamaan järjestelmien ydintoiminnot toimintakuntoon viipymättä.

5.8 Lakkauttaminen

5.8.1 Varmentajan toiminnan lakkauttaminen

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

Ennen varmentajan toiminnan lakkauttamista suoritetaan vähintään seuraavat toimenpiteet:

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

5.8.2 Rekisteröijän toiminnan lakkauttaminen

Rekisteröijän toiminnan lakkauttaminen on tilanne, jossa varmentajan terveydenhuollon organisaatiolle myöntämä oikeus rekisteröidä terveydenhuollon muun henkilöstön varmenteita lakkautetaan pysyvästi.

Rekisteröijän toiminnan lakkauttaminen tapahtuu rekisteröijän ja varmentajan välisen sopimuksen mukaisesti.

6 Teknisen turvallisuuden hallinta

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

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

6.1 Avainparien luonti ja toimittaminen varmenteen haltijalle

6.1.1 Avainparien luonti

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

Varmenteen haltijan avainparit luodaan varmennekortin sirulla.

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

6.1.2 Yksityisen avaimen toimittaminen varmenteen haltijalle

Yksityiset avaimet sisältävä varmennekortti ja sen käytön mahdollistavat tunnusluvut toimitetaan varmenteen haltijalle siten, ettei ulkopuolisten ole mahdollista saada niitä haltuunsa.

6.1.3 Varmenteen hakijan julkisen avaimen toimittaminen varmentajalle

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

6.1.4 Varmentajan julkisen avaimen toimittaminen luottaville osapuolille

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

6.1.5 Avainten pituus

Varmentajan avaimet ovat 4096 bitin pituisia RSA-avaimia ja 384-bittisiä ECC-avaimia.

Terveydenhuollon muun henkilön allekirjoitusavaimet sekä todentamis- ja salausavaimet ovat vähintään 2048 bitin pituisia RSA-avaimia 384-bittisiä ECC-avaimia.

6.1.6 Julkisen avaimen parametrien luonti ja laatu

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

6.1.7 Avainten käyttötarkoitukset

Varmentajan avainparin käyttötarkoitukset ovat varmenteen allekirjoitus ja sulkulistan allekirjoitus.

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

6.2 Yksityisen avaimen suojaaminen ja turvalaskentalaitteiston hallinta

6.2.1 Käytetyt standardit

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

Varmentaja varmistaa, että terveydenhuollon muun henkilön yksityinen avain, joka on talletettu varmennekorttiin, toimitetaan henkilölle tämän varmennuskäytännön menettelytapojen mukaisesti.

Terveydenhuollon muun henkilön varmennekortti on kulloinkin voimassaolevien tarkoitukseen soveltuvien standardien mukainen, kuten ISO/IEC 7816, Javacard Platform 2.2.2 ja GlobalPlat-form 2.1.1. Varmennekortin sisältö on THPKI T5 -määrityksen mukainen.

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

6.2.2 Yksityinen avain usean henkilön hallinnassa

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

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

6.2.3 Yksityisten avainten vara-avainjärjestelmä

Terveydenhuollon varmennekorttien vara-avainjärjestelmä ei ole käytössä.

6.2.4 Yksityisen avaimen varmuuskopiointi

Varmentajan yksityisestä avaimesta on varmuuskopio.

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

Terveydenhuollon muun henkilön yksityisistä avaimista ei oteta eikä säilytetä kopioita.

Terveydenhuollon muun henkilön yksityinen avain ei missään varmennekortin elinkaaren vaiheessa paljastu ulkopuoliselle henkilölle, eikä terveydenhuollon muun henkilön yksityisiä avaimia säilytetä muualla kuin terveydenhuollon varmennekortilla.

6.2.5 Yksityisten avainten arkistointi

Varmentajan yksityiset avaimet tuhotaan niiden voimassaoloajan päättymisen jälkeen.

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

6.2.6 Yksityisten avainten käsittely turvalaskentalaitteistossa

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

6.2.7 Yksityisten avainten säilyttäminen

Varmentajan yksityiset avaimet säilytetään turvalaskentalaitteistossa salattuna.

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

6.2.8 Yksityisten avainten aktivointi

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

Varmenteen haltijan yksityiset avaimet on suojattu paljastumiselta ja luvattomalta käytöltä varmennekortin 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 tunnusluvulla.

Varmennekortin tunnusluku lukittuu viiden epäonnistuneen tunnusluvun syötön jälkeen.

Varmennekortilla on tunnusluvun lukituksen avausmahdollisuus. Lukitun tunnusluvun avaus vaatii oikean avaustunnusluvun syöttämistä.

6.2.9 Yksityisten avainten käytön estäminen

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

Varmennekortin yksityisten avainten käyttö estetään poistamalla varmennekortti kortinlukijasta.

6.2.10 Yksityisen avaimen tuhoaminen

Vain varmentaja voi tuhota varmentajan yksityiset avaimet.

Varmentajan toiminnan lakkauttamisen yhteydessä varmentajan yksityiset avaimet sekä niiden kopiot tuhotaan.

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

6.2.11 Varmennekorttien ja turvalaskentalaitteistojen turvatason luokitus

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

6.3 Muita avainparin hallintaan vaikuttavia seikkoja

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

6.3.1 Julkisten avainten arkistointi

Varmentaja arkistoi varmentamansa julkiset avaimet luvun 5.5 mukaisesti.

6.3.2 Varmenteiden ja avainten voimassaoloaika

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

Varmentajan varmenteen ja avainparin voimassaoloaika on 16 vuotta avainten luomispäivästä. Avaimia ei käytetä ennen voimassaoloaikaa tai voimassaoloajan päätyttyä mihinkään tarkoitukseen.

6.4 Aktivointitiedot

6.4.1 Aktivointitiedon luonti

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

Lukkiutuneen tunnusluvun avaamiseen tarvittava avaustunnusluku on 8 merkkiä pitkä. Avaustunnusluku säilytetään varmentajan tietojärjestelmässä.

6.4.2 Aktivointitiedon suojaus

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

6.4.3 Muita huomioitavia seikkoja aktivointitiedosta

—

6.5 Tietokonelaitteistojen turvallisuuden hallinta

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

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

6.5.1 Erityisvaatimukset

Tietokonelaitteistojen turvallisuusvaatimusten osalta noudatetaan VAHTI 5/2004 -ohjetta.

6.5.2 Laitteistoturvallisuuden luokittelu

—

6.6 Elinkaaren turvallisuuden hallinta

6.6.1 Järjestelmien kehittämisen hallinta

Varmentajan järjestelmien kehittäminen tapahtuu tuotantojärjestelmästä erotetuissa kehitys- ja testiympäristöissä.

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

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

6.6.2 Turvallisuuden hallinta

Tietojärjestelmien turvallisuuden hallinnassa noudatetaan VAHTI 5/2004 -ohjetta sekä ISO/IEC 27002 -standardin asettamia vaatimuksia 1.5.2011 alkaen. Turvallisuuden hallinta perustuu:

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

6.6.3 Elinkaaren turvallisuusluokittelu

—

6.7 Tietoverkon turvallisuuden hallinta

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

Tietoliikenneyhteyksien turvallisuusvaatimusten osalta noudatetaan VAHTI 5/2004 -ohjetta.

6.8 Aikaleima

Aikaleimapalvelu ei ole toistaiseksi käytössä.

7 Varmenteen ja sulkulistan profiili

7.1 Varmenteen profiili

Terveydenhuollon muun henkilöstön varmenteen profiili on kuvattu määrityksessä Digi- ja väestötietoviraston terveydenhuoltoa koskeva CA-malli = THPKI - T2: Digi- ja väestötietoviraston CA-malli ja varmenteiden tietosisältö terveydenhuollossa.

7.2 Sulkulistan profiili

Terveydenhuollon muun henkilöstön varmenteiden sulkulistan profiili on kuvattu määrityksessä Digi- ja väestötietoviraston terveydenhuoltoa koskeva CA-malli = THPKI - T2: Digi- ja väestötietoviraston CA-malli ja varmenteiden tietosisältö terveydenhuollossa.

7.3 Reaaliaikainen sulkulistan tarkistus (OCSP)

OCSP-protokolla on käytössä.

8 Hyväksymistarkastus

Varmentaja vastaa, että sen varmennetoiminta noudattaa tätä varmennuskäytäntöä sekä varmennepolitiikkaa. Laatuvarmentajia valvova Traficom voi tarkastaa varmentajan toiminnan laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista säädetyin edellytyksin.

Varmentaja voi tarkastaa tekniset toimittajansa sen mukaisesti, kuin teknisten toimittajien kanssa tehdyissä teknisissä toimitussopimuksissa tarkastusmenettely on kirjattu. Tarkastus tehdään vähintään kerran vuodessa ja aina, kun uusi sopimuskausi alkaa.
Tarkastuksen avulla selvitetään toimiiko tekninen toimittaja sopimuksen mukaisesti huomioiden tietoturvastandardien vaatimukset. Pääsääntöisesti teknistä toimittajaa arvioidaan ISO 27001 standardin sekä Traficomin määräysten mukaisesti.
Tarkastuksen suorittaa Digi- ja väestötietoviraston tietoturvapäällikkö tai Digi- ja väestötietoviraston hankkima ulkopuolinen tarkastaja, joka on erikoistunut varmennepalveluihin liittyvien teknisten toimittajien auditointiin. Tarkastus suoritetaan huomioiden tietoturvan kahdeksan osa-alueen toteutus. Tarkastettavia tietoturvallisuuden ominaisuuksia ovat luottamuksellisuus, eheys ja käytettävyys.
Tarkastus kattaa Traficomin antamat määräykset tietoturvallisuudesta varmentajalle.

8.1 Hyväksymistarkastusten suorittaminen

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

8.2 Tarkastaja

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

8.3 Tarkastuksen suorittajan suhde tarkastettavaan osapuoleen

Tarkastuksen suorittaja on tarkastettavaan kohteeseen nähden ulkopuolinen ja sitoutumaton.

8.4 Tarkastuksen kattavuus

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

Tarkastus koskee myös varmentajan alihankkijoita ja muita toimittajia.

Tarkastuksen tulokset kirjataan lausunnoksi.

8.5 Toimenpiteet, joihin ryhdytään poikkeamien esiintyessä

Varmentaja ryhtyy välittömästi havaittujen poikkeamien vaatimiin toimenpiteisiin tilanteen korjamiseksi.

8.6 Tarkastuksen tuloksista tiedottaminen

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

9 Yleiset ehdot

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

9.1 Maksut ja muut palkkiot

Maksut ja muut palkkiot määräytyvät sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) annetun lain 22§:n ja sähköisestä lääkemääräyksestä annetun lain (61/2007) 25 §:n, valtion maksuperustelain (150/1992) ja valtiovarainministeriön asetuksen Digi- ja väestötietoviraston suoritteiden maksuista (873/2008) nojalla.

9.1.1 Varmenteen myöntämismaksu

—

9.1.2 Varmenteen käyttömaksu

—

9.1.3 Varmenteen sulkumaksu tai tilan kyselymaksu

—

9.1.4 Maksut muista palveluista kuten Tukipalvelu -maksu

—

9.1.5 Hyvitykset

Hyvitykset määräytyvät varmennejärjestelmän osapuolien kanssa solmittujen sopimusten perusteella.

9.2 Taloudelliset velvollisuudet

Varmentajan tulee vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) 33 §:n mukaisesti huolehtia riittävistä taloudellisista voimavaroista toimintansa järjestämiseksi ja mahdollisen vahingonkorvausvastuun kattamiseksi.

9.3 Luottamuksellisuus ja tietosuoja

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

9.3.1 Yksityiset tiedot

Yksityisiä tietoja voidaan paljastaa vain Suomen lain tai 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 Suomen laki tai asetus tai niiden nojalla annettu määräys sitä edellyttää.

9.3.2 Julkiset tiedot

Todentamis- ja salausvarmenteiden julkiset avaimet ja sulkulista ovat julkista tietoa ja kaikkien saatavilla julkisessa hakemistossa.

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

9.3.3 Yksityisten tietojen suojaaminen

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

9.4 Yksityisyyden suoja

Yksityisyyden suojan osalta noudatetaan voimassa olevaa Suomen lainsäädäntöä.

9.4.1 Yksityisten tietojen suojaamissuunnitelma

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

9.4.2 Varmentajan järjestelmissä käsiteltävät yksityiset tiedot

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

9.4.3 Varmentajan järjestelmissä käsiteltävät julkiset tiedot

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

9.4.4 Vastuu yksityisten tietojen suojaamisesta

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

9.4.5 Yksityisten tietojen käyttäminen tai julkistaminen varmenteen haltijan suostumuksella

Tietojen luottamuksellisuus ja tietosuoja on määritelty luvussa 9.3.

9.4.6 Tietojen luovutus viranomaisille

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

9.4.7 Muut olosuhteet, joissa tiedot voidaan julkistaa

Varmentaja ei luovuta tietoja muissa kuin edellä mainituissa olosuhteissa.

9.5 Immateriaalioikeudet

Kaikki varmentajan järjestelmiin liittyvät tekijänoikeudet on määritelty sopimusosapuolten välisissä sopimuksissa.

9.6 Osapuolten sitoumukset

9.6.1 Varmentajan sitoumukset

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

9.6.2 Rekisteröijän sitoumukset

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

9.6.3 Varmenteen haltijan sitoumukset

Varmenteen haltija sitoutuu käyttämään terveydenhuollon muun henkilöstön varmennetta ja varmennekorttia tämän varmennuskäytännön, varmennepolitiikan ja annettujen ohjeiden mukaisesti.

9.6.4 Varmenteisiin luottavien osapuolten sitoumukset

Varmenteisiin luottavat osapuolet sitoutuvat vastaamaan omien terveydenhuollon järjestelmiensä ja terveydenhuollon muun henkilöstön varmenteiden yhteensopivuudesta.

9.6.5 Muiden osapuolten sitoumukset

—

9.7 Vastuuvapauslauseke

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

9.8 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. Soveltuvin osin sovelletaan myös vahingonkorvauslakia (412/1974).

Digi- ja väestötietovirasto vastaa varmenteen haltijalle ja varmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Digi- ja väestötietoviraston välittömästä toiminnasta, kuitenkin enintään 15 % edeltävän 3 kuukauden varmennelaskutuksen määrä (DVV:lle tuloutettava osuus) ja sähköisestä asioinnista viranomaistoiminnassa annetun lain (13/2003) mukaisia vaatimuksia.

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

Varmentaja ei vastaa varmenteen haltijalle aiheutuneista välillisistä tai seurannaisvahingoista. Varmentaja ei myöskään vastaa varmenteeseen luottavan osapuolen tai varmenteen haltijan muun sopimuskumppanin mahdollisesti kärsimistä välillisistä tai seurannaisvahingoista.
Varmentaja ei vastaa yleisten tietoliikenneyhteyksien eikä tietoverkkojen, esimerkiksi internetin toimivuudesta eikä siitä, jos oikeustoimen suorittaminen estyy varmenteen haltijan käyttämän laitteen tai kortinlukijaohjelmiston toimimattomuudesta eikä siitä, että varmennetta käytetään vastoin sen käyttötarkoitusta.

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

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

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

Varmentaja ei vastaa vahingosta, joka aiheutuu varmenteen haltijan tai varmennejärjestelmää hyödyntävän tahon lain, tämän varmennuskäytännön, varmennepolitiikan tai muiden ohjeiden vastaisesta toiminnasta.

Varmentaja ei milloinkaan vastaa välillisistä vahingoista eikä ylivoimaisen esteen aiheuttamista vahingoista.

Varmentaja voi lisäksi asettaa varmennejärjestelmän toimintaan liittyvissä sopimuksissa sekä varmenteen haltijalle ja varmennejärjestelmää hyödyntävälle taholle asettamissaan vaatimuksissa muita vastuunrajoituksia.

9.9 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. Soveltuvin osin sovelletaan myös vahingonkorvauslakia (412/1974).

Digi- ja väestötietovirasto vastaa varmenteen haltijalle ja varmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Digi- ja väestötietoviraston välittömästä toiminnasta, kuitenkin enintään 15 % edeltävän 3 kuukauden varmennelaskutuksen määrä (DVV:lle tuloutettava osuus) ja sähköisestä asioinnista viranomaistoiminnassa annetun lain (13/2003) mukaisia vaatimuksia.

9.10 Voimassaoloaika ja voimassaolon päättyminen

9.10.1 Varmennuskäytännön voimassaoloaika

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

9.10.2 Varmennuskäytännön voimassaolon päättyminen

Varmennuskäytännöllä ei ole erikseen määrättyä voimassaoloaikaa.

9.10.3 Varmennuskäytännön voimassaolon päättymisen vaikutukset

—

9.11 Varmennepalvelun osapuolien keskinäinen viestintä

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

9.12 Varmennuskäytännön muutosten hallinta

Varmennuskäytäntöön tehtävistä muutoksista päättää varmentaja.

9.12.1 Varmennuskäytännön muuttaminen

Ainoat muutokset, jotka voidaan tehdä hyväksyttyyn varmennuskäytäntöön ilman tiedottamista, ovat ulkoasun tai kirjoitusvirheiden korjaukset tai muutokset yhteystietoihin. Muista muutoksista on ilmoitettava 14 päivää ennen muutoksen voimaantuloa.

9.12.2 Muutoksista tiedottaminen

Varmentaja tiedottaa muista kuin luvussa 9.12.1 mainituista varmennuskäytäntöön liittyvistä muutoksista www-sivustollaan (www.fineid.fi) vähintään 30 päivää ennen muutoksen voimaanastumista.

9.12.3 Varmennuskäytännön tunnistetiedon muuttaminen

Varmennuskäytännön tunnistetieto muuttuu luvun 1.2 mukaisesti, kun varmennuskäytännön sisältöä muutetaan.

9.13 Erimielisyyksien ratkaiseminen

Terveydenhuollon varmennepalveluun ja tähän varmennuskäytäntöön liittyvät mahdolliset riitaisuudet käsitellään Suomessa varmentajan kotipaikan käräjäoikeudessa.

9.14 Sovellettava laki

Terveydenhuollon varmennepalveluun ja tähän varmennuskäytäntöön sovelletaan Suomen lakia.

9.15 Lain noudattaminen

Terveydenhuollon varmennepalveluiden järjestämisessä noudatetaan yksinomaan Suomen lakia.

9.16 Muut järjestelyt

9.16.1 Sopimukset

Varmennehakemus ja yleiset käyttöehdot muodostavat varmenteen hakijan kanssa tehtävän sopimuksen. Käyttöehdot sisältyvät varmennepolitiikka-asiakirjoihin. Varmentajan ja varmenteen haltijan väliset oikeudet, vastuut ja velvollisuudet

määritellään varmennepolitiikassa sekä varmennuskäytännössä. Allekirjoittamalla varmennehakemuksen terveydenhuollon muu henkilö sitoutuu noudattamaan varmenteen käyttöehtoja. Voimassaolevat käyttöehdot luovutetaan varmenteen haltijalle varmenteen luovutuksen yhteydessä.

Allekirjoituksellaan terveydenhuollon muu henkilö sitoutuu välittömästi ilmoittamaan sulkupalveluun varmennekortin katoamisen, epäilemänsä väärinkäytöksen tai sen mahdollisuuden.

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

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

Varmentaja laatii tarvittavat sopimukset varmennepalvelun toimittajan ja osatoimittajien kanssa.

9.16.2 Oikeudenluovutus

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

9.16.3 Osapätemättömyyslauseke

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

9.16.4 Täytäntöönpano

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

9.16.5 Ylivoimainen este

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

9.17 Muut ehdot

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

[Yksikkö] / Aarnio Ville

31.3.2021