



DIGI- JA
VÄESTÖTIETO-
VIRASTO

Varmennuskäytäntö

palvelujen antajien henkilötoimija-varmennetta varten

OID 1.2.246.517.1.10.303.4

OID 1.2.246.517.1.10.353.4

29.9.2022



ISO 9001



ISO/IEC 27001



[Yksikkö] / Kytölä Sanni

29.9.2022

Dokumentinhallinta

Omistaja	
Laatinut	Ville Aarnio
Tarkastanut	
Hyväksynyt	Mikko Pitkänen

Version hallinta

versionro	mitä tehty	pvm/henkilö
Versio 1.0	Versio 1.0	1.6.2021/VA
v 1.1	Päivitetty versio ja linkit varmennepolitiikkasivulle	29.9.2022/SK



Sisällysluettelo

1	Johdanto	9
1.1	Taustaa	9
1.2	Varmennuskäytännön tunnukset	11
2	Osapuolet ja soveltuvuus.....	11
2.1.1	Varmentaja	11
2.1.2	Rekisteröijä.....	12
2.1.3	Varmenteen haltija.....	13
2.1.4	Varmenteeseen luottava osapuoli	13
2.1.5	Muut osapuolet	13
2.2	Varmenteen käyttökohteet.....	14
2.2.1	Sallitut varmenteen käyttötarkoitukset.....	14
2.2.2	Kielletyt varmenteen käyttötarkoitukset.....	14
2.3	Yhteystiedot.....	14
2.3.1	Varmennuskäytännön hallintaorganisaatio	14
2.3.2	Yhteystiedot.....	14
2.3.3	Varmennuskäytäntöjen suhde varmennepolitiikkaan	15
2.3.4	Varmennuskäytäntöjen hyväksymismenettely.....	15
2.4	Määritelmät ja lyhenteet.....	15
3	tietojen Julkaiseminen.....	19
3.1	Julkinen hakemisto	19
3.2	Varmentajan julkaisemat tiedot.....	19
3.3	Julkaisutiheys	20
3.4	Pääsyoikeudet.....	20
4	Tunnistaminen ja todentaminen	20
4.1	Varmenteen haltijan nimeäminen	20
4.1.1	Nimeäminen	20
4.1.2	Nimeämisen merkitys	21
4.1.3	Anonyymit tai salanimet.....	22
4.1.4	Nimikenttien sisältö.....	22
4.1.5	Nimitietueen ainutkertaisuus.....	22
4.1.6	Tuotenimien käyttöoikeus	22
4.2	Henkilöllisyyden todentaminen	22
4.2.1	Menettelytapa yksityisen avaimen omistajuuden todistamiseksi	22
4.2.2	Varmenteen hakijan edustaman organisaation todentaminen.....	22
4.2.3	Henkilön tunnistaminen	22



4.2.4	Varmenteen hakijan tiedot, joita varmentaja ei tarkista	23
4.2.5	Varmenteen myöntämisen edellytykset.....	23
4.2.6	Varmentajien välisen yhteistyön edellytykset ja vaatimukset.....	23
4.3	Tunnistaminen ja todentaminen varmenteen uusimisessa.....	23
4.3.1	Tunnistaminen ja todentaminen varmenteen uusimisessa	23
4.3.2	Tunnistaminen ja todentaminen varmenteen sulkemisen jälkeen.....	23
4.4	Sulkupyynnön tekijän tunnistaminen.....	23
5	VARMENTEEN ELINKAAREN HALLINNAN TOIMINNALLISET VAATIMUKSET	23
5.1	Varmenteen hakeminen.....	24
5.1.1	Kuka voi tehdä varmennehakemuksen	24
5.1.2	Varmenteen myöntämisprosessi ja vastuut.....	24
5.2	Varmennehakemuksen käsittely	24
5.2.1	Tunnistamisen ja todentamisen toteuttaminen	25
5.2.2	Varmennehakemuksen hyväksyminen tai hylkääminen	25
5.2.3	Varmennehakemuksen käsittelyaika.....	25
5.3	Varmenteen myöntäminen.....	25
5.3.1	Varmenteen myöntämiseen liittyvät varmentajan tehtävät	25
5.3.2	Ilmoitus hakijalle varmenteen myöntämisestä	25
5.4	Myönnetyn varmenteen hyväksyminen.....	25
5.4.1	Myönnetyn varmenteen hyväksymismenettely varmenteen hakijan kannalta.....	25
5.4.2	Varmenteen julkaisu varmentajan toimesta.....	25
5.4.3	Ilmoitus muille osapuolille varmenteen myöntämisestä	26
5.5	Varmenteiden ja avainparien käyttö.....	26
5.5.1	Varmenteiden ja avainparien käyttö varmenteen haltijan toimesta	26
5.5.2	Varmenteiden ja julkisten avainten käyttö varmenteisiin luottavan osapuolen toimesta 27	
5.6	Julkisen avaimen uudelleen varmentaminen	27
5.7	Varmenteen uusiminen.....	28
5.7.1	Varmenteen uusimisen syyt.....	28
5.7.2	Varmenteen uusimisen hakeminen.....	28
5.7.3	Varmenteen uusimispyynnön käsittely	28
5.7.4	Ilmoitus varmenteen hakijalle varmennekortin uusimisesta.....	28
5.7.5	Uusitun varmenteen hyväksymismenettely varmenteen haltijan kannalta	28
5.7.6	Uusitun varmenteen julkaisu	28
5.7.7	Ilmoitus uusitun varmenteen myöntämisestä muille osapuolille	28
5.8	Varmenteen muuttaminen	28
5.9	Varmenteen sulkeminen ja määräaikainen sulkeminen	28



5.9.1	Varmenteen sulkemisen edellytykset	29
5.9.2	Kuka voi vaatia varmenteen sulkemista	29
5.9.3	Varmenteen sulkemisprosessi	29
5.9.4	Varmenteen haltijan velvollisuus tehdä sulkupyyntö	30
5.9.5	Varmenteen sulkupyynnön käsittelyaika	30
5.9.6	Varmenteeseen luottavan osapuolen velvollisuus tarkistaa varmenteen voimassaolo	30
5.9.7	Sulkulistan julkaisutiheys	30
5.9.8	Sulkulistan voimassaolon enimmäisaika	30
5.9.9	Reaaliaikainen varmenteen tilan tarkistaminen	30
5.9.10	Vaatimukset varmenteen tilan reaaliaikaiselle tarkistamiselle	31
5.9.11	Muut varmenteen tilan tarkistamisen menettelyt	31
5.9.12	Yksityisen avaimen paljastumisesta johtuva varmenteen sulkeminen	31
5.9.13	Varmenteen sulkeminen määräajaksi	31
5.9.14	Kuka voi vaatia varmenteen sulkemista määräajaksi	31
5.9.15	Menettelytavat varmenteen sulkemiseksi määräajaksi	31
5.9.16	Rajoitukset varmenteen määräajaiselle sulkemiselle	31
5.10	Varmenteen tilan tarkistamismahdollisuus	31
5.11	Varmenteen voimassaolon päättyminen	31
5.12	Vara-avainjärjestelmä ja avainten palautus	31
6	Fyysisen, käyttö- ja henkilöstöturvallisuuden hallinta	31
6.1	Fyysisen turvallisuuden hallinta	32
6.1.1	Tilojen sijoittaminen ja rakenne	32
6.1.2	Fyysinen pääsynvalvonta	32
6.1.3	Sähkö ja ilmastointi	32
6.1.4	Vesivahinko	32
6.1.5	Tulipalo	33
6.1.6	Tietovälineiden säilytys	33
6.1.7	Tietovälineiden hävittäminen	33
6.1.8	Varmuuskopiointi verkon yli	33
6.2	Käyttöturvallisuuden hallinta	33
6.2.1	Työtehtäviin liittyvät roolit	33
6.2.2	Varmennetuotannon työtehtäviin tarvittavien henkilöiden määrä	34
6.2.3	Henkilöiden tunnistaminen ja todentaminen eri rooleihin	34
6.2.4	Tehtävien eriyttämistä vaativat roolit	34
6.3	Henkilöstöturvallisuuden hallinta	34
6.3.1	Tausta-, ansio-, kokemus- ja selvitysvaatimukset	34
6.3.2	Taustojen tarkistamisen menettelytapa	34



6.3.3	Koulutuksen tiheys ja vaatimukset	34
6.3.4	Jatkokoulutuksen tiheys ja vaatimukset	34
6.3.5	Työtehtävien kierrätyksen tiheys ja järjestys	34
6.3.6	Seuraukset luvattomista toimista	35
6.3.7	Alihankkijoiden henkilöstön vaatimukset	35
6.3.8	Asiakirjat, jotka toimitetaan henkilökunnalle	35
6.4	Varmennejärjestelmän turvallisuuden seuranta	35
6.4.1	Arkistoitavat tapahtumat	35
6.4.2	Lokitietojen analysointitiheys	35
6.4.3	Lokitietojen säilytysaika	35
6.4.4	Lokitietojen suojaaminen	36
6.4.5	Lokitietojen varmuuskopiointi	36
6.4.6	Lokitietojen keräysjärjestelmän toteuttaminen (sisäinen/ulkoisen)	36
6.4.7	Lokitapahtumasta ilmoittaminen	36
6.4.8	Haavoittuvuuksien arviointi	36
6.5	Arkistoitavat aineistot	36
6.5.1	Arkistoitavat asiakirjat, tiedostot ja mediat	36
6.5.2	Arkistojen säilytysaika	37
6.5.3	Arkistojen suojaaminen	37
6.5.4	Arkistojen varmuuskopiointimenettely	37
6.5.5	Arkistoitavien tietojen aikaleima	37
6.5.6	Arkistojen keräysjärjestelmä (sisäinen/ulkoisen)	37
6.5.7	Arkistoissa olevien tietojen saatavuus ja eheys	37
6.6	Varmentajan avainparin vaihto	37
6.7	Häiriötilanteisiin varautuminen	37
6.7.1	Suunnitelma toimintahäiriöiden ja toiminnan vaarantumisen varalta	37
6.7.2	Varmennejärjestelmän, ohjelmistojen tai tietojen vahingoittuminen	37
6.7.3	Toiminta varmenteen haltijan yksityisen avaimen paljastuessa	37
6.7.4	Toiminnan jatkuvuus häiriötilanteen jälkeen	38
6.8	Lakkauttaminen	38
6.8.1	Varmentajan toiminnan lakkauttaminen	38
6.8.2	Rekisteröijän toiminnan lakkauttaminen	38
7	Teknisen turvallisuuden hallinta	38
7.1	Avainparien luonti ja toimittaminen varmenteen haltijalle	39
7.1.1	Avainparien luonti	39
7.1.2	Yksityisen avaimen toimittaminen varmenteen haltijalle	39
7.1.3	Varmenteen hakijan julkisen avaimen toimittaminen varmentajalle	39



7.1.4	Varmentajan julkisen avaimen toimittaminen luottaville osapuolille	39
7.1.5	Avainten pituus	39
7.1.6	Julkisen avaimen parametrien luonti ja laatu.....	39
7.1.7	Avainten käyttötarkoitukset	39
7.2	Yksityisen avaimen suojaaminen ja turvalaskentalaitteiston hallinta	40
7.2.1	Käytetyt standardit	40
7.2.2	Yksityinen avain usean henkilön hallinnassa	40
7.2.3	Yksityisten avainten vara-avainjärjestelmä	40
7.2.4	Yksityisen avaimen varmuuskopiointi.....	40
7.2.5	Yksityisten avainten arkistointi	40
7.2.6	Yksityisten avainten käsittely turvalaskentalaitteistossa.....	41
7.2.7	Yksityisten avainten säilyttäminen	41
7.2.8	Yksityisten avainten aktivointi	41
7.2.9	Yksityisten avainten käytön estäminen	41
7.2.10	Yksityisen avaimen tuhoaminen.....	41
7.2.11	Varmennekorttien ja turvalaskentalaitteistojen turvatason luokitus.....	42
7.3	Muita avainparin hallintaan vaikuttavia seikkoja.....	42
7.3.1	Julkisten avainten arkistointi	42
7.3.2	Varmenteiden ja avainten voimassaoloaika	42
7.4	Aktivointitiedot	42
7.4.1	Aktivointitiedon luonti	42
7.4.2	Aktivointitiedon suojaus	42
7.4.3	Muita huomioitavia seikkoja aktivointitiedosta	42
7.5	Tietokonelaitteistojen turvallisuuden hallinta	42
7.5.1	Eritysisvaatimukset.....	43
7.5.2	Laitteistoturvallisuuden luokittelu	43
7.6	Elinkaaren turvallisuuden hallinta	43
7.6.1	Järjestelmien kehittämisen hallinta	43
7.6.2	Turvallisuuden hallinta	43
7.6.3	Elinkaaren turvallisuusluokittelu	43
7.7	Tietoverkon turvallisuuden hallinta.....	43
7.8	Aikaleima.....	44
8	Varmenteen ja sulkulistan profiili	44
8.1	Varmenteen profiili.....	44
8.2	Sulkulistan profiili.....	44
8.3	Reaaliaikainen sulkulistan tarkistus (OCSP)	44
9	Hyväksymistarkastus	44



9.1	Hyväksymistarkastusten suorittaminen	44
9.2	Tarkastaja	45
9.3	Tarkastuksen suorittajan suhde tarkastettavaan osapuoleen	45
9.4	Tarkastuksen kattavuus	45
9.5	Toimenpiteet, joihin ryhdytään poikkeamien esiintyessä	45
9.6	Tarkastuksen tuloksista tiedottaminen	45
10	Yleiset ehdot	45
10.1	Maksut ja muut palkkiot	45
10.1.1	Varmenteen myöntämismaksu	45
10.1.2	Varmenteen käyttömaksu	45
10.1.3	Varmenteen sulkumaksu tai tilan kyselymaksu	46
10.1.4	Maksut muista palveluista kuten Tukipalvelu -maksu	46
10.1.5	Hyvitykset	46
10.2	Taloudelliset velvollisuudet	46
10.3	Luottamuksellisuus ja tietosuojat	46
10.3.1	Yksityiset tiedot	46
10.3.2	Julkiset tiedot	46
10.3.3	Yksityisten tietojen suojaaminen	46
10.4	Yksityisyyden suoja	46
10.4.1	Yksityisten tietojen suojaamissuunnitelma	47
10.4.2	Varmentajan järjestelmissä käsiteltävät yksityiset tiedot	47
10.4.3	Varmentajan järjestelmissä käsiteltävät julkiset tiedot	47
10.4.4	Vastuu yksityisten tietojen suojaamisesta	47
10.4.5	Yksityisten tietojen käyttäminen tai julkistaminen varmenteen haltijan suostumuksella	47
10.4.6	Tietojen luovutus viranomaisille	47
10.4.7	Muut olosuhteet, joissa tiedot voidaan julkistaa	47
10.5	Immateriaalioikeudet	47
10.6	Osapuolten sitoumukset	47
10.6.1	Varmentajan sitoumukset	47
10.6.2	Rekisteröijän sitoumukset	47
10.6.3	Varmenteen haltijan sitoumukset	48
10.6.4	Varmenteisiin luottavien osapuolten sitoumukset	48
10.6.5	Muiden osapuolten sitoumukset	48
10.7	Vastuuvapauslauseke	48
10.8	Vastuunrajoitukset	48
10.9	Vahingonkorvaukset	49



10.10	Voimassaoloaika ja voimassaolon päättymisen	49
10.10.1	Varmennuskäytännön voimassaoloaika	49
10.10.2	Varmennuskäytännön voimassaolon päättymisen	49
10.10.3	Varmennuskäytännön voimassaolon päättymisen vaikutukset	50
10.11	Varmennepalvelun osapuolien keskinäinen viestintä	50
10.12	Varmennuskäytännön muutosten hallinta	50
10.12.1	Varmennuskäytännön muuttaminen	50
10.12.2	Muutoksista tiedottaminen	50
10.12.3	Varmennuskäytännön tunnistetiedon muuttaminen	50
10.13	Erimielisyyksien ratkaiseminen	50
10.14	Sovellettava laki	50
10.15	Lain noudattaminen	50
10.16	Muut järjestelyt	50
10.16.1	Sopimukset	50
10.16.2	Oikeudenluovutus	51
10.16.3	Osapätemättömyyslauseke	51
10.16.4	Täytäntöönpano	51
10.16.5	Ylivoimainen este	51
10.17	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 soveltuvuus-alue 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.

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

Varmenne sitoo yhteen julkisen avaimen ja joukon tietoja, jotka yksilöivät kohteen, kuten henkilön, organisaation, sivuston tai laitteen. Varmennetta käyttävät hyväksyvät varmenteen haltija ja varmenteeseen luottava osapuoli, joka luottaa varmenteen paikansäilyvyyteen 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 muuttui 1.1.2020 Digi- ja väestötietovirastoksi.

1.1 Taustaa

DVV myöntää palvelujen antajien henkilötoimijavarmenteita terveydenhuollon alalla toimivien palvelujen antajien henkilötoimijoille, jotka eivät ole terveydenhuollon ammattihenkilöitä (jäljempänä henkilötoimija). Kyseiseen henkilöstöryhmään kuuluvat muut valtakunnallisia tietojärjestelmiä käyttävät henkilöt ja erityisryhmät, kuten tietosuojavastaavat sekä tietojärjestelmätoimittajat, konsultit jne.

Digi- ja väestötietovirasto tarjoaa tietoturvallisuuden tasoltaan korkealaatuisia sähköisen allekirjoituksen ja tunnistamisen varmenteita ja niihin liittyviä palveluja. Varmenteen avulla varmennetaan varmenteen haltijan henkilöllisyys sekä varmenteeseen sisältyvien tietojen oikeellisuus, eheys ja alkuperäisyys. Allekirjoitusvarmenteella tehty sähköinen allekirjoitus sekä vahvan sähköisten tunnistamisen välineen avulla tehty henkilön vahva sähköinen tunnistaminen antavat kansalaisille mahdollisuuden turvalliseen, ajasta ja paikasta riippumattomaan ja joustavaan verkkoasiointiin. Allekirjoitusvarmenteen ja vahvan sähköisen tunnistuspalvelun tarjoajia valvoo Suomessa Traficom.



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.

Laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) on säädetty varmenteella 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)
- Laki vahvasta sähköisestä tunnistamisesta ja luottamuspalveluista (617/2009)
- 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 (5/2008)
- 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
- Traficomien määräykset Viestintävirasto 7 B/2009 M ja Viestintävirasto 8 C/2010 M
- VAHTI 1/2002: Tietoteknisten laittilojen 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 määritetty.

1.2 Varmennuskäytännön tunnukset

Tämän varmennuskäytännön nimi on Varmennuskäytäntö palvelujen antajien henkilötoimijavarmennetta varten, jonka OID on 1.2.246.517.1.10.303.4 ja 1.2.246.517.1.10.353.4.

Tämä varmennuskäytäntö viittaa Varmennepolitiikkaan Digi- ja väestötietoviraston organisaatiovarmennetta varten, OID 1.2.246.517.1.10.303 ja 1.2.246.517.1.10.353.

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 hyväksytyjä varmenteita ja luontivälineitä kuten Asetuksen 28 ja 29 artiklassa säädetään.

2 Osapuolet ja soveltuvuus

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

2.1.1 Varmentaja

Varmentaja täyttää seuraavat ehdot:

- Varmentaja sitoutuu noudattamaan tämän varmennuskäytännön ehtoja.
- Varmentaja laatii varmennepolitiikan ja varmennuskäytännön sekä muita näitä dokumentteja täydentäviä menettelytapaoheja.
- Varmentaja pitää yllä riittävät taloudelliset valmiudet turvataksaan tässä varmennuskäytännössä määritellyn toiminnan. Varmentaja vastaa varmennetoiminnasta ja siihen liittyvistä



riskeistä ja edellyttää varmennejärjestelmän toimittajien suojautuvan toimintaan liittyviltä riskeiltä asianmukaisin riskienhallintakeinoin.

- Varmentaja pitää yllä rekisteriä hyväksymistään rekisteröijistä.
- Varmentaja päättää ristiinvarmentamisesta yhteistyössä toisten varmentajien kanssa.
- Varmentaja vastaa luomiensa avainparien elinkaaresta (luominen, tallennus, varmuuskopiointi, julkaiseminen ja käytöstä poistaminen).

Varmentaja sitoutuu:

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

Varmentaja voi halutessaan tarjota varmennejärjestelmään liittyviä lisätoimintoja tai -palveluja.

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

Varmentaja tarkastaa ja hyväksyy rekisteröijät sekä niiden henkilökunnan.

2.1.2 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 luotavien 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.

2.1.3 Varmenteen haltija

Palvelujen antajien henkilötoimijavarmenteen haltijana voi olla terveydenhuollon alalla toimiva palvelujen antajan henkilö, joka ei ole terveydenhuollon ammattihenkilö tai terveydenhuollon muuta henkilöstöä.

Palvelujen antajien henkilötoimijavarmenteen hakijan tulee todistaa henkilöllisyytensä varmennehakemusta tehdessään.

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

2.1.4 Varmenteeseen luottava osapuoli

Varmenteeseen luottava osapuoli voi olla sellaisen tietojärjestelmän omistaja, jonka tietojärjestelmän tietoturvamekanismit on rakennettu käyttämään hyväksi palvelujen antajien henkilötoimijavarmenteita.

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

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

2.1.5 Muut osapuolet

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



2.2 Varmenteen käyttökohteet

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

Palvelujen antajien henkilötoimijavarmenteita 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 palvelujen antajien henkilötoimijavarmenteita voidaan käyttää terveydenhuollon ja apteekkilaitoksen muissa tietojärjestelmissä.

2.2.1 Sallitut varmenteen käyttötarkoitukset

Varmente yhdistää henkilön ja hänen käyttöönsä luovutetun julkisen avaimen ja PIN-tunnusluvulla suojatun yksityisen avaimen. Palvelujen antajien henkilötoimijavarmenteita, joita tämän varmennuskäytännön mukaisesti myönnetään, käytetään varmenteen haltijan sähköiseen tunnistamiseen, tiedon salaamiseen sitä viestitettäessä tai tallennettaessa ja sähköiseen allekirjoittamiseen eli digitaalisen dokumentin tai muun tiedon (esimerkiksi potilasasiakirjamerkintä, sähköinen lääkemääräys) aitouden, eheyden ja kiistämättömyyden varmistamiseen.

2.2.2 Kielletyt varmenteen käyttötarkoitukset

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

2.3 Yhteystiedot

2.3.1 Varmennuskäytännön hallintaorganisaatio

Tämän varmennuskäytännön on tuottanut Digi- ja väestötietoviraston Varmennepalvelut. DVV:n Varmennepalvelut on vastuussa tämän dokumentin hallinnasta ja päivityksestä.

2.3.2 Yhteystiedot

Varmentajan yhteystiedot:

Digi- ja väestötietovirasto

PL 123 (Lintulahdenkuja 2)

Puh. +358 295 535 001

00531 Helsinki

Fax. +358 9 876 4369

Y-tunnus: 0245437-2

kirjaamo@dvv.fi





Digi- ja väestötietovirasto (DVV) Varmennepalvelut

PL 123

00531 Helsinki

www.dvv.fi

2.3.3 Varmennuskäytäntöjen suhde varmennepolitiikkaan

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

2.3.4 Varmennuskäytäntöjen hyväksymismenettely

DVV:n Varmennepalvelut määrittelee ja hyväksyy varmennuskäytäntöasiakirjat.

2.4 Määritelmät ja lyhenteet

Ammattioikeus

Ammattioikeudella tarkoitetaan tässä varmennuskäytännössä niitä rekisteröityjä laillistetun, luvan saaneen ja nimesuojatun 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 Sosi-aali- ja terveystietojen 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 salausta- 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.



[Yksikkö] / Kytölä Sanni

29.9.2022

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.

Palvelujen antajien henkilötoimija

Terveystietojärjestelmän alalla toimivan palvelujen antajan henkilö, joka ei ole terveystietojärjestelmän ammattihenkilö tai terveystietojärjestelmän muuta henkilöstöä. Kyseiseen henkilöstöryhmään kuuluvat muut valtakunnallisia tietojärjestelmiä käyttävät henkilöt ja erityisryhmät, kuten tietosuojavastaavat sekä tietojärjestelmätoimittajat, konsultit jne.

Personointiohjelmisto

Rekisteröintipisteissä käytettävä ohjelmisto, jolla hallitaan yhteyksiä KoHa- ja Terhikki-rekistereihin, tehdään varmennekortin pintapainatukset sekä tallennetaan varmenteet kortin sirulle. Personointiohjelmistolla tuotetaan myös PIN-tunnukset ja PUK-avaustunnukset.



[Yksikkö] / Kytölä Sanni

29.9.2022

PIN (<i>Personal identification number</i>)	Varmennekortin avainparin käyttöoikeuden varmistamiseksi käytettävä tunnusluku. Terveydenhuollon varmennekortilla on kaksi tunnuslukua, toinen todentamista ja salausta ja toinen sähköistä allekirjoitusta varten.
Prosessi (<i>Process</i>)	Tapahtumasarja, jolla on tietty suunta, tarkoitus, vaikutus tai tulos, esimerkiksi varmenteen myöntämisprosessi.
PUK (<i>Pin unblocking key</i>)	Avaustunnusluku, joka vapauttaa lukkiutuneen varmennekortin PIN-tunnusluvun tilanteessa, jossa PIN-tunnusluku on syötetty väärin liian monta kertaa peräkkäin.
Rekisteröijä (<i>RA, Registration Authority</i>)	Julkisen avaimen järjestelmässä luotettu taho, joka varmentajan valtuuttamana ja auditoimana toteuttaa rekisteröijän tehtäviä. Rekisteröijä ylläpitää varmentajan lukuun yhtä tai useampaa rekisteröintipistettä.
Rekisteröintipiste (<i>RA-piste</i>)	Palvelupiste, jossa tarkistetaan varmenteen hakijan henkilöllisyys sekä terveydenhuollon ammattihenkilöiden osalta ammattioikeudet ja muiden henkilöiden osalta työnantajatie-dot. Rekisteröintipiste vastaa varmennekorttien, varmenteiden ja PIN-/PUK-tunnuslukujen jakelusta käyttäjille varmennepolitiikan ja varmennuskäytännön mukaisesti.
Sulkulista (<i>CRL, Certificate Revocation List</i>)	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 palvelujen antajien henkilötoimijavarmenteita 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.



[Yksikkö] / Kytölä Sanni

29.9.2022

Terveydenhuollon muu henkilö

Muu terveydenhuollon toimintayksikössä työskentelevä tai sen tehtäviä suorittava henkilö, joka ei ole terveydenhuollon ammattihenkilö.

Terveydenhuollon palvelujen antaja

Terveydenhuollon toimintayksikkö tai itsenäisenä ammatinharjoittajana toimiva 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 salaus-avainten 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 palveluntuottajan julkisesta avaimesta ja tunnistetiedoista muodostettu tietokokonaisuus, jonka varmentaja on muodostanut ja allekirjoittanut yksityisellä avaimellaan. Varmenteen aitous on todennettavissa varmentajan julkisella avaimella (varmentajan varmenteella).



[Yksikkö] / Kytölä Sanni

29.9.2022

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.

3 tietojen Julkaiseminen

3.1 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.

3.2 Varmentajan julkaisemat tiedot

Varmentaja vastaa siitä, että varmennepolitiikat, varmennuskäytännöt, varmennekuvaukset ja varmentajan varmenteet ovat julkisesti saatavilla osoitteesta www.dvv.fi/cps. Hakemistopalvelu on julkinen Internet-palvelu, josta on saatavilla varmentajan myöntämät julkiseen hakemistoon tarkoitetut todentamis- ja salausvarmenteet, varmentajan varmenteet sekä sulkulista. Hakemistopalvelu on saatavissa osoitteesta [ldap://ldap.fineid.fi](https://ldap.fineid.fi). Todentamis- ja salausvarmenteet, varmentajan varmenteet sekä sulkulistat ovat saatavissa julkisesta hakemistosta osoitteesta ldap.fineid.fi kaikkina päivinä, kaikkina vuorokauden aikoina. Allekirjoitusvarmenteita ei julkaista hakemistoon.



3.3 Julkaisutiheys

Varmentaja julkaisee varmennepolitiikan ja varmennuskäytännön. Muutoshallinta on kuvattu luvussa 10.12.

Todentamis- ja salausvarmenteet sekä sulkulistat julkaistaan varmennehakemistoon heti, kun ne on luotu.

3.4 Pääsyoikeudet

Varmentajan julkaisemien tietojen saatavuutta ei rajoiteta pääsyoikeuksin.

4 Tunnistaminen ja todentaminen

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

4.1 Varmenteen haltijan nimeäminen

4.1.1 Nimeäminen

Terveystietoviraston varmenteen haltijan nimeäminen todentamis- ja salausvarmenteessa sekä allekirjoitusvarmenteessa on kuvattu määrityksessä 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 väestötietovirasto CA

C = FI

ja

CN = DVV Gov. Root CA – G3 ECC

OU = Varmennepalvelut

OU = Certification Authority Services

O = Digi- ja väestötietovirasto CA

C = FI



Digi- ja väestötietoviraston organisaatiovarmenteiden varmentaja on:

CN (Common name) = DVV Organisational Certificates - G4R

OU (Organizational unit) = Organisaatiovarmenteet

O (Organization) = Digi- ja väestötietovirasto CA

C (Country) = FI

ja

CN (Common name) = DVV Organisational Certificates - G4E

OU (Organizational unit) = Organisaatiovarmenteet

O (Organization) = Digi- ja väestötietovirasto 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

4.1.2 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.

4.1.3 Anonyymit tai salanimet

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

4.1.4 Nimikenttien sisältö

Nimikenttien sisältö on määritetty luvussa 3.1.1.

4.1.5 Nimitietueen ainutkertaisuus

Luvussa 3.1.1 määritelty nimitietue yksilöi palvelujen antajien henkilötoimijavarmenteen haltijan. Henkilön tunnistetieto on varmenteen haltijan ainutkertaisesti yksilöivä.

4.1.6 Tuotenimien käyttöoikeus

—

4.2 Henkilöllisyyden todentaminen

4.2.1 Menettelytapa yksityisen avaimen omistajuuden todistamiseksi

Palvelujen antajien henkilötoimijan yksityiset avaimet luodaan aina varmennekortin sirulla. Yksityiset avaimet sisältävä varmennekortti luovutetaan palvelujen antajien henkilötoimijalle sen jälkeen, kun hänen henkilöllisyytensä on luotettavasti todettu ja varmenne on rekisteröity ja luotu.

4.2.2 Varmenteen hakijan edustaman organisaation todentaminen

Palvelujen antajien henkilötoimijavarmenteita hakijoiden osalta vaaditaan heidän edustamiensa organisaatioiden todentamista. Varmenteen hakijan edustama organisaatio todennetaan kyseisen organisaation hakijalle luovuttamasta paperimuotoisesta todistuksesta.

4.2.3 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).



4.2.4 Varmenteen hakijan tiedot, joita varmentaja ei tarkista

Kaikki palvelujen antajien henkilötoimijan varmennehakemuksessa tarvittavat henkilötiedot saadaan väestötietojärjestelmästä ja hakijan edustaman organisaation toimitamista työnantajatiedoista.

4.2.5 Varmenteen myöntämisen edellytykset

Vain terveydenhuollon toimintayksikössä työskentelevällä tai sen tehtäviä suorittavalla henkilöllä, joka ei ole terveydenhuollon ammattihenkilö, on oikeus hakea palvelujen antajien henkilötoimijavarmennetta. Palvelussuhteen päättyessä palvelujen antajien henkilötoimijavarmenne on suljettava.

4.2.6 Varmentajien välisen yhteistyön edellytykset ja vaatimukset

Varmentajien välisen yhteistyön edellytykset ja vaatimukset määritellään juurivarmentajan varmennepolitiikassa.

4.3 Tunnistaminen ja todentaminen varmenteen uusimisessa

4.3.1 Tunnistaminen ja todentaminen varmenteen uusimisessa

Varmenteiden uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

4.3.2 Tunnistaminen ja todentaminen varmenteen sulkemisen jälkeen

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

4.4 Sulkupyynnön tekijän tunnistaminen

Varmenteen sulkupyyntö voidaan tehdä puhelimitse tai kirjallisesti varmentajalle.

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

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

5 VARMENTEEN ELINKAAREN HALLINNAN TOIMINNALLISET VAATIMUKSET

Tämä luku kuvaa varmentajan, rekisteröijän ja palvelujen antajien henkilötoimijan toiminnalle asetetut vaatimukset. Luku käsittää myös varmenteiden sulkemisen.



5.1 Varmenteen hakeminen

Palvelujen antajien henkilötoimijavarmennetta haetaan henkilökohtaisesti rekisteröintipisteestä.

Hakemuksen tiedot tallennetaan varmentajan varmenteiden tilaus- ja hallintajärjestelmään (Vartti).

Palvelujen antajien henkilötoimijavarmenteen 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 sisältävät varmennepolitiikka-asia-
kirjoihin.

5.1.1 Kuka voi tehdä varmennehakemuksen

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

5.1.2 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 hallintajärjestelmään käyttävät henkilöt tunnistetaan varmentajan myöntämällä 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-avaustunnusluvut.

Lisäksi rekisteröijä toimittaa varmenteen hakijalle varmennekortin käyttöohjeen.

5.2 Varmennehakemuksen käsittely

Varmennehakemus käsitellään rekisteröintipisteessä ilman aiheetonta viivytystä.

Rekisteröijä tallettaa varmenteen tilaustiedot varmentajan varmenteiden tilaus- ja hallintajärjestelmään.



5.2.1 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.

5.2.2 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 muutוסvaatimuksen varmentajalle.

5.2.3 Varmennehakemuksen käsittelyaika

Varmennehakemus käsitellään ilman aiheetonta viivytystä rekisteröintipisteen aukioloaikana.

5.3 Varmenteen myöntäminen

5.3.1 Varmenteen myöntämiseen liittyvät varmentajan tehtävät

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

Varmenteen myöntämiseen liittyvät tehtävät on kuvattu luvuissa 4.1 ja 4.2.

5.3.2 Ilmoitus hakijalle varmenteen myöntämisestä

Erillistä ilmoitusta palvelujen antajien henkilötoimijavarmenteen myöntämisestä ei tehdä.

5.4 Myönnetyn varmenteen hyväksyminen

5.4.1 Myönnetyn varmenteen hyväksymismenettely varmenteen hakijan kannalta

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

5.4.2 Varmenteen julkaisu varmentajan toimesta

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



5.4.3 Ilmoitus muille osapuolille varmenteen myöntämisestä

Erillistä ilmoitusta palvelujen antajien henkilötoimijavarmenteen myöntämisestä ei tehdä.

5.5 Varmenteiden ja avainparien käyttö

5.5.1 Varmenteiden ja avainparien käyttö varmenteen haltijan toimesta

Palvelujen antajien henkilötoimijavarmenteet ja niihin liittyvät avainparit on tarkoitettu käytettäväksi Suomen sosiaali- ja terveydenhuollon tietojärjestelmissä ja niihin liittyvissä palveluissa.

Palvelujen antajien henkilötoimijan tulee sitoutua toimimaan tämän varmennuskäytännön mukaisesti hakiessaan ja käyttäessään varmennetta.

Palvelujen antajien henkilötoimija vastaa ensisijaisesti vahingosta, jonka hän aiheuttaa:

- voimassaolevan lain, asetuksen tai niiden nojalla annetun määräyksen tai ohjeen vastaisella menettelyllä;
- varmennuskäytännön vastaisella menettelyllä;
- hyväksyntänsä 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.

Palvelujen antajien henkilötoimijan tulee ilmoittaa sulkupalveluun:

- varmennekortin katoaminen tai väärinkäyttöepäily.

Jos varmennekortti rikkoutuu, tulee kortinhaltijan sulkea rikkoutuneen kortin varmenteet ja hakea uusi varmennekortti rekisteröintipisteestä. Kortin uusimisessa noudetaan 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 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. Rekisteröintipisteen virkailija tulostaa uuden tunnuslukukuoren, joka sisältää avaustunnusluvun. Avaustunnuslukua ei ilmoiteta puhelimitse tai kirjeitse tietoturvasyistä.

5.5.2 Varmenteiden ja julkisten avainten käyttö varmenteisiin luottavan osapuolen toimesta

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

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

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

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

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

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

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

5.6 Julkisen avaimen uudelleen varmentaminen

Palvelujen antajien henkilötoimijavarmenteita ei myönnetä aiemmin varmennetuille julkisille avaimille.



5.7 Varmenteen uusiminen

5.7.1 Varmenteen uusimisen syyt

Palvelujen antajien henkilötoimijavarmenne 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.

5.7.2 Varmenteen uusimisen hakeminen

Varmenteen uusimista voi hakea vain varmenteen haltija.

5.7.3 Varmenteen uusimispyynnön käsittely

Varmenteiden uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

5.7.4 Ilmoitus varmenteen hakijalle varmennekortin uusimisesta

Erillistä ilmoitusta palvelujen antajien henkilötoimijavarmenteen uusimisesta ei tehdä.

5.7.5 Uusitun varmenteen hyväksymismenettely varmenteen haltijan kannalta

Uusittu varmenne hyväksytään kappaleessa 4.4.1 kuvatun menetelmän mukaisesti.

5.7.6 Uusitun varmenteen julkaisu

Varmenteet julkaistaan kappaleessa 4.4.2 kuvatun menetelmän mukaisesti.

5.7.7 Ilmoitus uusitun varmenteen myöntämisestä muille osapuolille

Erillistä ilmoitusta palvelujen antajien henkilötoimijavarmenteen uusimisesta ei tehdä.

5.8 Varmenteen muuttaminen

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

5.9 Varmenteen sulkeminen ja määräaikainen sulkeminen

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

Varmentaja ei ilmoita varmenteen haltijalle varmenteen sulkemisesta.



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

5.9.1 Varmenteen sulkemisen edellytykset

Varmente 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 palvelujen antajien henkilötoimijavarmenteen, 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.

5.9.2 Kuka voi vaatia varmenteen sulkemista

Varmenteen sulkemista voivat vaatia:

- palvelujen antajien henkilötoimija tai hänen lakisääteinen edustajansa kyseisen henkilön oman varmenteen osalta;
- varmentaja kohdan 4.9.1 edellytysten täyttyessä.

5.9.3 Varmenteen sulkemisprosessi

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

1. puhelimitse soittamalla maksuttomaan sulkupalveluun +358 800 162 622.
2. kirjallisesti varmentajalle.

Varmenteen sulkupyynnön tekijä tunnistetaan luvussa 3.4 kuvatulla tavalla.

Varmentaja sulkea 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 sulkupyynnön syytä
- sulkupyynnön vastaanottajan henkilötiedot
- mahdolliset muut varmenteen haltijan ilmoittamat lisätiedot
 - varmennekortin katoamisaika, varmenteen haltijan kuolinaika tms.
- varmenteen sulkijan henkilötiedot
- varmenteen sulun ajankohta.

Varmente suljetaan kortinhallintasovelluksella ja varmenteen sulkuihin liittyvät tiedot säilytetään 10 vuotta sulkemisajankohdasta.

5.9.4 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.

5.9.5 Varmenteen sulkupyynnön käsittelyaika

Sulkupalvelu ja rekisteröintipisteet käsittelevät varmenteen sulkupyynnot viipymättä.

5.9.6 Varmenteeseen luottavan osapuolen velvollisuus tarkistaa varmenteen voimassaolo

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

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

5.9.7 Sulkulistan julkaisu tiheys

Päivitetty sulkulista julkaistaan tunnin välein.

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

5.9.8 Sulkulistan voimassaolon enimmäisaika

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

5.9.9 Reaaliaikainen varmenteen tilan tarkistaminen

Reaaliaikainen varmenteen tilan tarkistaminen ei ole käytössä.



5.9.10 Vaatimukset varmenteen tilan reaaliaikaiselle tarkistamiselle

—

5.9.11 Muut varmenteen tilan tarkistamismenettelyt

—

5.9.12 Yksityisen avaimen paljastumisesta johtuva varmenteen sulkeminen

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

5.9.13 Varmenteen sulkeminen määräajaksi

Varmenteita ei suljeta määräajaksi.

5.9.14 Kuka voi vaatia varmenteen sulkemista määräajaksi

—

5.9.15 Menettelytavat varmenteen sulkemiseksi määräajaksi

—

5.9.16 Rajoitukset varmenteen määräajaiselle sulkemiselle

—

5.10 Varmenteen tilan tarkistamismahdollisuus

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

5.11 Varmenteen voimassaolon päättymisen

Varmente on voimassa joko yleisen voimassaoloajan, varmenteen kohtaisen määräajan tai kunnes se sulkemisedellytysten täytyttyä suljetaan.

5.12 Vara-avainjärjestelmä ja avainten palautus

Palvelujen antajien henkilötoimijoiden todentamis- ja salausavaimia ei turvatalleteta. Varmenteita ei siten voida käyttää ilman varmenteen haltijan suostumusta eikä yksityisiä avaimia voida palauttaa kortin hajottua tai hävitessä.

6 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.



6.1 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 varastoituihin tietoihin 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.

6.1.1 Tilojen sijoittaminen ja rakenne

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

6.1.2 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.

6.1.3 Sähkö ja ilmastointi

Rekisteröintipisteiden sähkön saanti ja ilmastoinnin toimivuus tulee erikseen varmistaa.

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

6.1.4 Vesivahinko

Rekisteröintipisteet suojataan vesivahinkoja vastaan.

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



6.1.5 Tulipalo

Rekisteröintipisteet suojataan palovahinkoja vastaan.

Varmennetuotannon järjestelmät sijaitsevat automaattisammutuksella varustetuissa konesalitiloissa.

6.1.6 Tietovälineiden säilytys

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

6.1.7 Tietovälineiden hävittäminen

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

6.1.8 Varmuuskopiointi verkon yli

Varmennetuotantojärjestelmän varmuuskopiointi tapahtuu varmennejärjestelmän sisäisessä tietoliikenneverkossa.

6.2 Käyttöturvallisuuden hallinta

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

6.2.1 Työtehtäviin liittyvät roolit

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

Varmennetoiminnan rooleja ovat:

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

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



6.2.2 Varmennetuotannon työtehtäviin tarvittavien henkilöiden määrä

Varmentajan lukuun toimivat nimetyt organisaatiot ja henkilöt.

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

6.2.3 Henkilöiden tunnistaminen ja todentaminen eri rooleihin

Varmentajan työtehtävissä toimivilla henkilöillä, jotka toimivat 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.

6.2.4 Tehtävien eriyttämistä vaativat roolit

Rekisteröijä ei voi toimia järjestelmän pääkäyttäjän roolissa.

6.3 Henkilöstöturvallisuuden hallinta

6.3.1 Tausta-, ansio-, kokemus- ja selvitysvaatimukset

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

Varmentajan työtehtävissä toimivista henkilöistä tehdään turvallisuusselvitys.

6.3.2 Taustojen tarkistamisen menettelytapa

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

6.3.3 Koulutuksen tiheys ja vaatimukset

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

6.3.4 Jatkokoulutuksen tiheys ja vaatimukset

—

6.3.5 Työtehtävien kierrätyksen tiheys ja järjestys

—



6.3.6 Seuraukset luvattomista toimista

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

6.3.7 Alihankkijoiden henkilöstön vaatimukset

Varmentajan valtuuttamien organisaatioiden henkilöstön tulee täyttää luvun 5.3.1 edellytykset.

6.3.8 Asiakirjat, jotka toimitetaan henkilökunnalle

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

6.4 Varmennejärjestelmän turvallisuuden seuranta

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

6.4.1 Arkistoitavat tapahtumat

Varmentaja säilyttää turvallisuusseurantaa varten seuraavat tiedot:

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

Varmenteiden ja varmennejärjestelmän osalta varmentaja säilyttää:

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

6.4.2 Lokitietojen analysointitiheys

- ♦ Lokitietoja analysoidaan tarvittaessa.

6.4.3 Lokitietojen säilytysaika

- ♦ Lokitiedot säilytetään voimassaolevien arkistosäännösten mukaisesti.



6.4.4 Lokitietojen suojaaminen

- ♦ Lokitietoihin on pääsy vain erikseen oikeutetuilla henkilöillä.
- ♦ Lokitiedot suojataan muuttamiselta, tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä.

6.4.5 Lokitietojen varmuuskopiointi

- ♦ Lokitiedoista otetaan varmuuskopiot päivittäin.

6.4.6 Lokitietojen keräysjärjestelmän toteuttaminen (sisäinen/ulkoinen)

Varmentaja vastaa lokitietojen keräysjärjestelmästä.

6.4.7 Lokitapahtumasta ilmoittaminen

Järjestelmän käyttäjälle ei erikseen ilmoiteta lokitapahtumien syntymisestä.

Lokitietojen valvonnasta vastaaville henkilöille ilmoitetaan erikseen seuraavista tapahtumista:

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

6.4.8 Haavoittuvuuksien arviointi

- ♦ Varmentaja arvioi ja seuraa riskianalyysin avulla varmennejärjestelmän ja tuotanto-ympäristön haavoittuvuutta ja pyrkii minimoimaan niihin liittyviä riskejä.

6.5 Arkistoitavat aineistot

6.5.1 Arkistoitavat asiakirjat, tiedostot ja mediat

- ♦ Varmentaja arkistoi seuraavat tiedot:
 - varmennehakemukset;
 - varmenne- tai muun hakemuksen allekirjoitetut hyväksynnit;
 - varmennepalvelusopimukset;
 - myönnetty varmenteet;
 - ristiinvarmennusasiakirjat mukaanluettuna ristiinvarmennuksen perustelut ja päätökset sekä suoritettut toimet;
 - varmenteen sulkupyynnöt;
 - voimassaolevat ja edelliset varmennepolitiikat ja varmennuskäytännöt;
 - varmentajan ja rekisteröintipisteiden väliset sopimukset; ja
 - varmennejärjestelmän ylläpitoon, käyttöön ja hallintaan liittyvät sopimukset.
 - tarkastusraportit ja pöytäkirjat käsittäen tietoturvatarkastukset ja järjestelmän auditoinnin.



6.5.2 Arkistojen säilytysaika

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

6.5.3 Arkistojen suojaaminen

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

♦ Arkistotiedot suojataan muuttamiselta, tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä.

6.5.4 Arkistojen varmuuskopiointimenettely

♦ Arkistotiedoista ei oteta varmuuskopioita.

6.5.5 Arkistoitavien tietojen aikaleima

Arkistoitavat asiakirjat on päivätty. Aikaleimapalvelu ei ole toistaiseksi käytössä.

6.5.6 Arkistojen keräysjärjestelmä (sisäinen/ulkoinen)

Varmentajalla ei ole keskitettyä arkistojen keräysjärjestelmää.

6.5.7 Arkistoissa olevien tietojen saatavuus ja eheys

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

6.6 Varmentajan avainparin vaihto

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

6.7 Häiriötilanteisiin varautuminen

6.7.1 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.

6.7.2 Varmennejärjestelmän, ohjelmistojen tai tietojen vahingoittuminen

Poikkeustilanteissa varmentaja noudattaa jatkuvuus- ja toipumissuunnitelmaa.

6.7.3 Toiminta varmenteen haltijan yksityisen avaimen paljastuessa

Varmenteen haltijan yksityiset avaimet on suojattu fyysistä tunkeutumista ja avainten paljastumista vastaan. Mikäli varmenteen haltijan yksityinen avain on paljastunut,



suljetaan siihen liittyvä varmenne. Varmenteen haltijalle tuotetaan uusi varmennekortti, jossa on uudet yksityiset avaimet.

6.7.4 Toiminnan jatkuvuus häiriötilanteen jälkeen

Varmentaja pyrkii häiriötilanteen jälkeen saattamaan järjestelmien ydintoiminnot toimintakuntoon viipymättä.

6.8 Lakkauttaminen

6.8.1 Varmentajan toiminnan lakkauttaminen

Varmentajan toiminnan lakkauttaminen on tilanne, jossa varmentaja 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 myönnetty 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.

6.8.2 Rekisteröijän toiminnan lakkauttaminen

Rekisteröijän toiminnan lakkauttaminen on tilanne, jossa varmentajan terveydenhuollon organisaatiolle myöntämä oikeus rekisteröidä palvelujen antajien henkilötoimijavarmenteita suljetaan pysyvästi.

Rekisteröijän toiminnan lakkauttaminen tapahtuu rekisteröijän ja varmentajan välisen sopimuksen mukaisesti.

7 Teknisen turvallisuuden hallinta

Tässä luvussa käsitellään varmentajan, rekisteröijän ja palvelujen antajien henkilötoimijan julkisen ja yksityisen avaimen hallinnan ehdot ja vastaavat tekniset määritykset.

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



7.1 Avainparien luonti ja toimittaminen varmenteen haltijalle

7.1.1 Avainparien luonti

Varmentajan avainpari luodaan ja säilytetään turvalaskentalaitteistossa, joka on Euroopan 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.

7.1.2 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.

7.1.3 Varmenteen hakijan julkisen avaimen toimittaminen varmentajalle

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

7.1.4 Varmentajan julkisen avaimen toimittaminen luottaville osapuolille

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

7.1.5 Avainten pituus

Varmentajan avaimet ovat 4096 bitin pituisia RSA-avaimia tai 384 bittisiä EC avaimia.

Palvelujen antajien henkilötoimijan allekirjoitusavaimet sekä todentamis- ja salausavaimet ovat vähintään 2048 bitin pituisia RSA-avaimia.

7.1.6 Julkisen avaimen parametrien luonti ja laatu

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

7.1.7 Avainten käyttötarkoitukset

Varmentajan avainparin käyttötarkoitukset ovat varmenteen allekirjoitus ja sulkulistan allekirjoitus.

Palvelujen antajien henkilötoimijan avainparien käyttötarkoitukset ovat varmenteen haltijan todentaminen ja tiedon salaaminen sekä kehittynyt sähköinen allekirjoitus.



7.2 Yksityisen avaimen suojaaminen ja turvalaskentalaitteiston hallinta

7.2.1 Käytetyt standardit

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

Varmentaja varmistaa, että palvelujen antajien henkilötoimijan yksityinen avain, joka on talletettu varmennekorttiin, toimitetaan henkilölle tämän varmennuskäytännön menettelytapojen mukaisesti.

◆ Palvelujen antajien henkilötoimijan varmennekortti on kulloinkin voimassaolevien tar-koitukseen soveltuvien standardien mukainen, kuten ISO/IEC 7816, Javacard Platform 2.2.2 ja GlobalPlatform 2.1.1. Varmennekortin sisältö on THPKI T5 -määrittelyn 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.

7.2.2 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.

7.2.3 Yksityisten avainten vara-avainjärjestelmä

Terveydenhuollon varmennekorttien vara-avainjärjestelmä ei ole käytössä.

7.2.4 Yksityisen avaimen varmuuskopiointi

Varmentajan yksityisestä avaimesta on varmuuskopio.

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

Palvelujen antajien henkilötoimijan yksityisistä avaimista ei oteta eikä säilytetä kopioita.

Palvelujen antajien henkilötoimijan yksityinen avain ei missään varmennekortin elinkaaren vaiheessa paljastu ulkopuoliselle henkilölle, eikä palvelujen antajien henkilötoimijan yksityisiä avaimia säilytetä muualla kuin terveydenhuollon varmennekortilla.

7.2.5 Yksityisten avainten arkistointi

Varmentajan yksityiset avaimet tuhoetaan niiden voimassaoloajan päättymisen jälkeen.



Palvelujen antajien henkilötoimijan yksityisiä avaimia ei arkistoida. Varmentajalla ei ole pääsyä varmenteen haltijoiden yksityisiin avaimiin.

7.2.6 Yksityisten avainten käsittely turvalaskentalaitteistossa

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

7.2.7 Yksityisten avainten säilyttäminen

Varmentajan yksityiset avaimet säilytetään turvalaskentalaitteistossa salattuna.

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

7.2.8 Yksityisten avainten aktivointi

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

Varmenteen haltijan yksityiset avaimet on suojattu paljastumiselta ja luvattomalta käytöltä varmennekortin sirulla. Vain sirulla suoritettavilla sisäisillä komendoilla 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.

7.2.9 Yksityisten avainten käytön estäminen

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

Varmennekortin yksityisten avainten käyttö estetään poistamalla varmennekortti kortinlukijasta.

7.2.10 Yksityisen avaimen tuhoaminen

Vain varmentaja voi tuhota varmentajan yksityiset avaimet.

Varmentajan lakkauttamisen yhteydessä varmentajan yksityiset avaimet sekä niiden kopiot tuhoataan.

Mikäli Palvelujen antajien henkilötoimija 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.



7.2.11 Varmennekorttien ja turvalaskentalaitteistojen turvatason luokitus

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

7.3 Muita avainparin hallintaan vaikuttavia seikkoja

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

7.3.1 Julkisten avainten arkistointi

Varmentaja arkistoi varmentamansa julkiset avaimet luvun 5.5 mukaisesti.

7.3.2 Varmenteiden ja avainten voimassaoloaika

Palvelujen antajien henkilötoimijan 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.

7.4 Aktivointitiedot

7.4.1 Aktivointitiedon luonti

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

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

7.4.2 Aktivointitiedon suojaus

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

7.4.3 Muita huomioitavia seikkoja aktivointitiedosta



7.5 Tietokonelaitteistojen turvallisuuden hallinta

Varmentajan järjestelmien turvallisuuden hallintaan kuuluvat muun muassa käyttäjän vahva tunnistus ja varmentajan yksityisiin avaimiin liittyvien toimintojen ja tehtävien



jäljitettävyys henkilötasolle asti sekä lokitietojen keruu. Tietokonelaitteistot sijaitsevat suojatuissa tiloissa.

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

7.5.1 Erityisvaatimukset

Tietokonelaitteistojen turvallisuusvaatimusten osalta noudatetaan VAHTI 5/2004 -ohjetta.

7.5.2 Laitteistoturvallisuuden luokittelu

—

7.6 Elinkaaren turvallisuuden hallinta

7.6.1 Järjestelmien kehittämisen hallinta

Varmentajan järjestelmien kehittäminen tapahtuu tuotantojärjestelmästä 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. Käyttöönottoaihe suunnitellaan siten, että nopea palaaminen vanhaan versioon on mahdollista määrätyn ajan puitteissa.

7.6.2 Turvallisuuden hallinta

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

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

7.6.3 Elinkaaren turvallisuusluokittelu

—

7.7 Tietoverkon turvallisuuden hallinta

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



Tietoliikenneyhteysien turvallisuusvaatimusten osalta noudatetaan VAHTI 5/2004 -ohjetta.

7.8 Aikaleima

Aikaleimapalvelu ei ole toistaiseksi käytössä.

8 Varmenteen ja sulkulistan profiili

8.1 Varmenteen profiili

Palvelujen antajien henkilötoimijan varmenteen profiili on kuvattu määrittämissä Digi- ja väestötietoviraston terveydenhuoltoa koskeva CA-malli = THPKI - T2: Digi- ja väestötietoviraston CA-malli ja varmenteiden tietosisältö terveydenhuollossa.

8.2 Sulkulistan profiili

Palvelujen antajien henkilötoimijan varmenteiden sulkulistan profiili on kuvattu määrittämissä Digi- ja väestötietoviraston terveydenhuoltoa koskeva CA-malli = THPKI - T2: Digi- ja väestötietoviraston CA-malli ja varmenteiden tietosisältö terveydenhuollossa.

8.3 Reaaliaikainen sulkulistan tarkistus (OCSP)

OCSP-protokolla on käytössä.

9 Hyväksymistarkastus

Varmentaja vastaa, että sen varmennetoiminta noudattaa tätä varmennuskäytäntöä sekä varmennepolitiikkaa. Varmentajia valvova Traficom voi tarkastaa varmentajan toiminnan laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista säädettyin 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 Traficomien 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 tietoturvasuhteiden ominaisuuksia ovat luottamuksellisuus, eheys ja käytettävyys.

Tarkastus kattaa Traficomien antamat määräykset tietoturvasuhteesta varmentajalle.

9.1 Hyväksymistarkastusten suorittaminen

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



9.2 Tarkastaja

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

9.3 Tarkastuksen suorittajan suhde tarkastettavaan osapuoleen

Tarkastuksen suorittaja on tarkastettavaan kohteeseen nähden ulkopuolinen ja sitoutunut.

9.4 Tarkastuksen kattavuus

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

Tarkastus koskee myös varmentajan alihankkijoita ja muita toimittajia.

Tarkastuksen tulokset kirjataan lausunnoksi.

9.5 Toimenpiteet, joihin ryhdytään poikkeamien esiintyessä

Varmentaja ryhtyy välittömästi havaittujen poikkeamien vaatimiin toimenpiteisiin tilanteen korjaamiseksi.

9.6 Tarkastuksen tuloksista tiedottaminen

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

10 Yleiset ehdot

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

10.1 Maksut ja muut palkkiot

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

10.1.1 Varmenteen myöntämismaksu

—

10.1.2 Varmenteen käyttömaksu

—



10.1.3 Varmenteen sulkumaksu tai tilan kyselymaksu

—

10.1.4 Maksut muista palveluista kuten Tukipalvelu -maksu

—

10.1.5 Hyvitykset

♦ Hyvitykset määräytyvät varmennejärjestelmän osapuolien kanssa solmittujen sopimusten perusteella.

10.2 Taloudelliset velvollisuudet

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

10.3 Luottamuksellisuus ja tietosuoja

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

10.3.1 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 laki tai asetus tai niiden nojalla annettu määräys sitä edellyttää.

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

10.3.3 Yksityisten tietojen suojaaminen

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

10.4 Yksityisyyden suoja

Yksityisyyden suojan osalta noudatetaan voimassa olevaa Suomen lainsäädäntöä.



10.4.1 Yksityisten tietojen suojaamissuunnitelma

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

10.4.2 Varmentajan järjestelmissä käsiteltävät yksityiset tiedot

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

10.4.3 Varmentajan järjestelmissä käsiteltävät julkiset tiedot

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

10.4.4 Vastuu yksityisten tietojen suojaamisesta

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

10.4.5 Yksityisten tietojen käyttäminen tai julkistaminen varmenteen haltijan suostumuksella

Tietojen luottamuksellisuus ja tietosuojaa on määritelty luvussa 9.3.

10.4.6 Tietojen luovutus viranomaisille

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

10.4.7 Muut olosuhteet, joissa tiedot voidaan julkistaa

Varmentaja ei luovuta tietoja muissa kuin edellä mainituissa olosuhteissa.

10.5 Immateriaalioikeudet

Kaikki varmentajan järjestelmiin liittyvät tekijänoikeudet on määritelty sopimusosapuolten välisissä sopimuksissa.

10.6 Osapuolten sitoumukset

10.6.1 Varmentajan sitoumukset

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

10.6.2 Rekisteröijän sitoumukset

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



10.6.3 Varmenteen haltijan sitoumukset

Varmenteen haltija sitoutuu käyttämään palvelujen antajien henkilötoimijavarmennetta ja varmennekorttia tämän varmennuskäytännön, varmennepolitiikan ja annettujen ohjeiden mukaisesti.

10.6.4 Varmenteisiin luottavien osapuolten sitoumukset

Varmenteisiin luottavat osapuolet sitoutuvat vastaamaan omien terveydenhuollon järjestelmiensä ja palvelujen antajien henkilötoimijavarmenteiden yhteensopivuudesta.

10.6.5 Muiden osapuolten sitoumukset

—

10.7 Vastuuvapauslauseke

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

10.8 Vastuunrajoitukset

Varmennepalveluiden tuottamiseen liittyvä Digi- ja väestötietoviraston vahingonkorvausvastuu määräytyy varmenteen hakijan kanssa tehdyn palvelusopimuksen mukaisesti. Digi- ja väestötietovirastoa koskevat lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista ja sähköisestä asioinnista viranomaistoiminnassa annetun lain mukaiset varmentajan vahingonkorvausvastuut. 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 huoltotoista 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.

10.9 Vahingonkorvaukset

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

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.

10.10 Voimassaoloaika ja voimassaolon päättyminen

10.10.1 Varmennuskäytännön voimassaoloaika

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

10.10.2 Varmennuskäytännön voimassaolon päättyminen

Varmennuskäytännöllä ei ole erikseen määrättyä voimassaoloaikaa.



10.10.3 Varmennuskäytännön voimassaolon päättymisen vaikutukset

—

10.11 Varmennepalvelun osapuolien keskinäinen viestintä

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

10.12 Varmennuskäytännön muutosten hallinta

Varmennuskäytäntöön tehtävistä muutoksista päättää varmentaja.

10.12.1 Varmennuskäytännön muuttaminen

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

10.12.2 Muutoksista tiedottaminen

Varmentaja tiedottaa muista kuin luvussa 10.12.1 mainituista varmennuskäytäntöön liittyvistä muutoksista [www-sivustollaan \(www.dvv.fi/cps\)](http://www.dvv.fi/cps) vähintään 30 päivää ennen muutoksen voimaantumista.

10.12.3 Varmennuskäytännön tunnistetiedon muuttaminen

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

10.13 Erimielisyyksien ratkaiseminen

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

10.14 Sovellettava laki

Terveystietojen varmennepalveluun ja tähän varmennuskäytäntöön sovelletaan Suomen lakia.

10.15 Lain noudattaminen

Terveystietojen varmennepalveluiden järjestämisessä noudatetaan yksinomaan Suomen lakia.

10.16 Muut järjestelyt

10.16.1 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 palvelujen antajien henkilötoimija sitoutuu noudattamaan varmenteen käyttöehtoja. Voimassaolevat käyttöehdot luovutetaan varmenteen haltijalle varmenteen luovutuksen yhteydessä.

Allekirjoituksellaan palvelujen antajien henkilötoimija 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.

10.16.2 Oikeudenluovutus

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

10.16.3 Osapätemättömyyslauseke

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

10.16.4 Täytäntöönpano

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

10.16.5 Ylivoimainen este

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

10.17 Muut ehdot

Terveystietojen varmennepalveluita käsitteleviä dokumentteja ja asiakirjoja, tätä varmennuskäytäntöä sekä varmennejärjestelmän osapuolten ja heidän sopimus-kumppaniensa välisiä sitoumuksia tulkittaessa ja sovellettaessa ratkaisevat ensisijaisesti asiakirjojen suomenkieliset versiot.



[Yksikkö] / Aarnio Ville

palvelujen antajien henkilö-
toi-mi-ja-varmen-netta var-
ten

[Tarkenne]

31.3.2021

[Numero]

[Liite]

52 (52)

