DIGI- JA VÄESTÖTIETO-VIRASTO

VARMENNEKUVAUS SOTE-AMMATTI-VARMENNE

sosiaali- ja terveydenhuollon ammattivarmennetta varten

13.9.2025

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

13.9.2025

Dokumentinhallinta

Omistaja	
Laatinut	Ville Aarnio, Anniina Tamminen
Tarkastanut	
Hyväksynyt	Mikko Pitkänen

Version hallinta

versionro	mitä tehty	pvm/henkilö
v 1.0	Versio 1.0	1.6.2021/VA
v 1.1	Lisätty kuvaus lokidatasta	1.10.2021/VA
v 1.2	Päivitetty versio ja linkit varmennepolitiikkasivulle	30.9.2022/SK
v 1.3	Päivitetty versionumero. Poistettu maininnat PUK-koodista sekä ajokortista hyväksyttynä tunnistusasiakirjana.	15.9.2023/AT
v 1.4	Päivitetty versio ja päiväys. Yhdistetty G3- ja G2-juurivarmentaja-hierarkioiden politiikat samaan asiakirjaan. Lisätty kohtaan 2.6 yli-voimainen este.	13.9.2024/JH
v 1.5	Päivitetty versio ja päiväys.	13.9.2025/JH

13.9.2025

Sisällysluettelo

1 Johdanto 3

2 Varmennekuvaus 3

2.1 Varmentajan yhteystiedot 3

2.2 Varmenteen tyyppi, tarkistusmenettelyt ja käyttötarkoitukset 4

2.3 Varmenteeseen luottaminen 4

2.4 Varmenteen haltijan velvollisuudet 5

2.5 Varmenteeseen luottavan osapuolen velvollisuus tarkistaa varmenteen voimassaolo 5

2.6 Vastuuvapauslauseke ja vastuunrajoitukset 6

2.7 Sopimukset, varmennuskäytäntö ja varmennepolitiikka 7

2.8 Yksityisyyden suoja 8

2.9 Vahingonkorvaukset 8

2.10 Sovellettava laki 8

2.11 Varmentajan toiminnan hyväksymistarkastus 9

1 Johdanto

Tämä varmennekuvaus on yhteenveto Digi- ja väestötietoviraston (jäljempänä DVV) Varmenne-politiikasta sosiaali- ja terveydenhuollon ammattivarmennetta varten. Varmennepolitiikassa määritellään Digi- ja väestötietoviraston julkisen avaimen menetelmän mukaisten varmentamistoimintojen edellytykset, soveltuvuusalue sekä rajaukset. Varmennepolitiikan sisältämät periaatteet määritellään käytännön tasolla varmennuskäytännössä ja muissa varmennepolitiikkaa täydentävissä menettelytapaohjeissa.

Tämä varmennekuvaus viittaa seuraaviin asiakirjoihin:

Varmennepolitiikka sosiaali- ja terveydenhuollon ammattivarmennetta varten, OID: 1.2.246.517.1.10.206, 1.2.246.517.1.10.306 ja 1.2.246.517.1.10.356

Varmennuskäytäntö sosiaali- ja terveydenhuollon ammattivarmennetta varten, OID: 1.2.246.517.1.10.206.1, 1.2.246.517.1.10.306.1 ja 1.2.246.517.1.10.356.1

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

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

2 Varmennekuvaus

2.1 Varmentajan yhteystiedot

Digi- ja väestötietovirasto

PL 123 (Lintulahdenkuja 2)

00531 Helsinki

Y-tunnus: 0245437-2

Puh. +358 295 535 001

kirjaamo@dvv.fi

Digi- ja väestötietovirasto (DVV) Varmennepalvelut

PL 123

00531 Helsinki

www.dvv.fi

2.2 Varmenteen tyyppi, tarkistusmenettelyt ja käyttötarkoitukset

DVV myöntää todentamisvarmenteita sekä allekirjoitusvarmenteita terveydenhuollon ammattihenkilöistä annetussa laissa (559/1994) tarkoitetuille terveydenhuollon ammattihenkilöille sekä sosiaalihuollon ammattihenkilöille, jotka täyttävät laissa (272/2005) sosiaalihuollon ammatillisen henkilöstön kelpoisuusvaatimuksista asetetut kelpoisuusvaatimukset sosiaalihuollon ammattitehtävissä toimimiselle.

Varmennetta haettaessa henkilöllisyys tarkistetaan voimassa olevasta, poliisin myöntämästä henkilöllisyyden osoittavasta asiakirjasta, joita ovat henkilökortti ja passi. Hyväksyttäviä tunnistamisasiakirjoja ovat myös Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä voimassa oleva passi tai henkilökortti ja muun valtion viranomaisen myöntämä voimassa oleva passi. Jos hakijalla ei ole em. asiakirjoja, poliisi tunnistaa hakijan henkilöllisyyden muilla tavoin. Sosiaali- ja terveydenhuollon ammattihenkilön ammattioikeuden voimassaolo tarkistetaan Valviran ylläpitämästä terveydenhuollon ammattihenkilöiden keskusrekisteristä (Terhikki) tai sosiaalihuollon ammattihenkilöiden keskusrekisteristä (Suosikki). Varmennetta voidaan käyttää henkilön todentamiseen ja tiedon salaukseen sekä sähköiseen allekirjoittamiseen. Varmennetta voidaan käyttää käyttötarkoituksensa mukaisesti rajoituksitta hallinnollisissa sekä yksityisen organisaation tarjoamissa sovelluksissa ja palveluissa.

Sosiaali- ja terveydenhuollon ammattivarmenteita käytetään varmenteen haltijan sähköiseen tunnistamiseen ja sähköiseen allekirjoittamiseen eli digitaalisen dokumentin tai muun tiedon (esimerkiksi potilasasiakirjamerkintä, sähköinen lääkemääräys) aitouden, eheyden ja kiistämättömyyden varmistamiseen.

Varmenteiden myöntämiseen sekä peruuttamiseen liittyvää lokidataa säilytetään vähintään seitsemän (7) vuotta varmenteen voimassaoloajan jälkeen.

2.3 Varmenteeseen luottaminen

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

Varmenteen käyttötarkoitus on määritelty varmenteen varmennepolitiikassa ja varmennuskäytännössä. Varmennetta saa käyttää vain sen käyttötarkoituksen mukaisesti.

Varmenteeseen luottavan osapuolen on tarkastettava, että käytettävän varmenteen voimassaoloaika ei ole päättynyt joko OCSP-palvelusta tai että varmenne ei ole sulkulistalla. Varmenteeseen luottava osapuoli ei voi vilpittömässä mielessä luottaa

varmenteeseen, mikäli varmenteen voimassaoloa ei ole tarkistettu sulkulistalta tai OCSP-palvelusta. Varmenteeseen luottavalla osapuolella on velvollisuus tarkistaa varmenteet sulkulistalta tai OCSP-palvelusta ennen hyväksymistä mitätöinnin varalta.

Varmenteeseen luottavan osapuolen vastuulla on omien tietojärjestelmiensä osalta varmistaa, että varmennetta käytetään varmennepolitiikassa määriteltyyn tarkoitukseen. Varmenteen oikean käyttötarkoituksen varmistamisessa luottava osapuoli voi tukeutua varmenteen sisältämään viittaukseen varmennepolitiikkaan.

Luottavan osapuolen tulee varmistaa, että käytettävät sovellukset täyttävät varmennepolitiikan vaatimukset.

2.4 Varmenteen haltijan velvollisuudet

Sosiaali- ja Terveydenhuollon ammattihenkilön tulee sitoutua toimimaan varmennepolitiikan mukaisesti hakiessaan ja käyttäessään sosiaali- ja terveydenhuollon ammattivarmennetta. Varmenteen haltija vastaa siitä, että varmennetta haettaessa ilmoitetut tiedot ovat oikeita.

Varmenteen haltija on vastuussa toimikortin käytöstä, kortilla tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista.

Sosiaali- ja terveydenhuollon ammattihenkilön 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.

Sosiaali- ja terveydenhuollon ammattihenkilön tulee ilmoittaa sulkupalveluun:

- varmennekortin katoaminen tai väärinkäyttöepäily

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

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

Kortinhaltija pystyy vaihtamaan PIN-tunnusluvut sekä vapauttamaan lukkiutuneet PIN-tunnusluvut hallussaan olevalla aktivointitunnusluvulla. Mikäli aktivointitunnusluku on kadonnut, kortinhaltija voi tehdä uudelleentilauksen rekisteröintipisteessä.

2.5 Varmenteeseen luottavan osapuolen velvollisuus tarkistaa varmenteen voimassaolo

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

Luottavan osapuolen vastuulla on varmenteen tilatiedon tarkistaminen OCSP-palvelusta tai voimassa olevan sulkulistan tarkistaminen. Varmenteeseen ei tule luottaa, ellei luottava osapuoli suorita peruutettujen 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 luottavan osapuolen järjestelmään, mutta varmenteen voimassaolo tulee tarkistaa ennen varmenteen hyväksymistä.

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

2.6 Vastuuvapauslauseke ja vastuunrajoitukset

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

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

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

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

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

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

Varmentaja ei vastaa vahingosta, joka aiheutuu ylivoimaisesta esteestä. Tällainen vastuusta vapauttava este voi olla esimerkiksi: lakko, tulipalo, sota, kapina,

takavarikko, valuuttarajoitukset, viranomaisen toimenpide, lainsäännökset ja viranomaismääräykset, häiriöt yleisessä tietoliikenteessä, tai muu vaikutuksiltaan yhtä merkittävä ja epätavallinen varmentajasta riippumaton syy.Varmentajalla on oikeus keskeyttää palvelu muutos- tai huoltotoimien ajaksi. Sulkulistaa koskevista muutoksista tai huoltotöistä ilmoitetaan etukäteen.

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

Varmentaja ei vastaa varmennetta käytettäessä loppukäyttäjälle tarkoitetun varmenteeseen pohjautuvan verkkopalvelun tai sovelluksen virheistä tai niistä aiheutuvista kustannuksista.

Varmenteen haltijan vastuu varmenteen käyttämisestä päättyy, kun hän tai varmenteen haltijan organisaation edustaja 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.

2.7 Sopimukset, varmennuskäytäntö ja varmennepolitiikka

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

Allekirjoituksellaan sosiaali- ja terveydenhuollon ammattihenkilö sitoutuu välittömästi ilmoittamaan sulkupalveluun 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.

Varmennehakemus ja yleiset käyttöehdot muodostavat varmenteen hakijan kanssa tehtävän sopimuksen. Käyttöehdot sisältyvät varmennepolitiikka-asiakirjoihin.

Hakemusasiakirjassa ja käyttöohjeissa mainitaan selkeästi, että varmenteen hakija hyväksyy allekirjoituksellaan annettujen tietojen oikeellisuuden sekä varmenteen luomisen ja julkaisun.

Digi- ja väestötietovirasto laatii erillisen varmennuskäytännön jokaiselle myöntämälleen varmennetyypille. Varmennuskäytäntö viittaa varmennepolitiikkaan, joka on varmennetyyppiä kuvaava yleisempi säännöstö ja ohjeisto ja joka on yhteinen kaikille

varmenteille siitä riippumatta, mille tekniselle välineelle varmenne on sijoitettu. Varmennuskäytäntö kuvaa tarkemmin, miten varmennepolitiikkaa sovelletaan eri teknisillä alustoilla.

Sekä varmennepolitiikka että varmennuskäytäntö ovat saatavilla osoitteesta www.dvv.fi/cps.

2.8 Yksityisyyden suoja

Varmentajan järjestelmissä tapahtuvassa yksityisten tietojen käsittelyssä noudatetaan henkilötietojen käsittelyä ja yksityisyydensuojaa koskevaa lainsäädäntöä. Varmentajan järjestelmissä tapahtuvassa julkisten tietojen käsittelyssä noudatetaan lakia viranomaisten toiminnan julkisuudesta (621/1999). Varmentaja vastaa siitä, että varmentajan järjestelmissä käsiteltävät yksityiset tiedot on suojattu asiattomalta käsittelyltä. Viranomaisille luovutetaan tietoja lakien, asetusten taikka niiden nojalla annettujen määräysten perusteella.

Varmentaja on julkaissut varmennepalveluiden osalta erityiset henkilötietolain mukaiset käytännesäännöt.

2.9 Vahingonkorvaukset

Varmennepalveluiden tuottamiseen liittyvä Digi- ja väestötietoviraston vahingonkorvausvastuu määräytyy varmenteen hakijan kanssa tehdyn palvelusopimuksen mukaisesti. Digi- ja väestötietovirastoa koskevat lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista ja sähköisestä asioinnista viranomaistoiminnassa annetun lain mukaiset varmentajan vahingonkorvausvastuut. Soveltuvin osin sovelletaan myös vahingonkorvauslakia (412/1974) ja sähköisestä asioinnista viranomaistoiminnassa annettua lakia (13/2003).

2.10 Sovellettava laki

Sosiaali- ja terveydenhuollon varmennepalveluun sovelletaan Suomen lakia. Sosiaali- ja terveydenhuollon varmennepalveluun liittyvät mahdolliset erimielisyydet pyritään ratkaisemaan osapuolten välisissä neuvotteluissa. Mikäli ratkaisuun ei päästä, osapuolten väliset erimielisyydet käsitellään Suomessa varmentajan kotipaikan käräjäoikeudessa.

Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa on säädetty vahvan sähköisen tunnistamisen välineellä tehdystä tunnistamisesta sekä allekirjoitusvarmenteella tehdyistä sähköisistä allekirjoituksista. Digi- ja väestötietoviraston myöntämistä varmenteista on säädetty sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa, sähköisestä lääkemääräyksestä annetussa laissa ja väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa (304/2019).

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).

2.11 Varmentajan toiminnan hyväksymistarkastus

Allekirjoitusvarmentajia valvova Traficom voi tarkastaa varmentajan toiminnan laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista säädetyin edellytyksin.

Varmentaja voi tarkastaa tekniset toimittajansa sen mukaisesti, kuin teknisten toimittajien kanssa tehdyissä teknisissä toimitussopimuksissa tarkastusmenettely on kirjattu. Tarkastus tehdään vähintään kerran vuodessa ja aina, kun uusi sopimuskausi alkaa.

Tarkastuksen avulla selvitetään toimiiko tekninen toimittaja sopimuksen mukaisesti huomioiden tietoturvastandardien vaatimukset. Pääsääntöisesti teknistä toimittajaa arvioidaan ISO 27001 -standardin sekä Traficomin määräysten mukaisesti.

Tarkastuksen suorittaa Digi- ja väestötietoviraston tietoturvapäällikkö tai Digi- ja väestötietoviraston hankkima ulkopuolinen tarkastaja, joka on erikoistunut varmennepalveluihin liittyvien teknisten toimittajien auditointiin. Tarkastus suoritetaan huomioiden tietoturvan kahdeksan osa-alueen toteutus. Tarkastettavia tietoturvallisuuden ominaisuuksia ovat luottamuksellisuus, eheys ja käytettävyys.

Tarkastus kattaa Traficomin antamat määräykset tietoturvallisuudesta varmentajalle.