DIGI- JA VÄESTÖTIETO-VIRASTO

Varmennepolitiikka

sosiaali- ja terveydenhuollon ammattivarmennetta varten

OID: 1.2.246.517.1.10.206

1.10.2021

SERTIFIOITU inspecta ORGANISAATIO
ISO 9001

SERTIFIOITU inspecta ORGANISAATIO
ISO/IEC 27001

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

Dokumentinhallinta

Omistaja	
Laatinut	Tuire Saaripuu
Tarkastanut	
Hyväksynyt	Mikko Pitkänen

Version hallinta

versionro	mitä tehty	pvm/henkilö
v 1.0	Hyväksytty versio 1.0, eIDAS-asetuksen mukainen asiakirja	3.5.2018
v 1.1	Hyväksytty versio 1.1, virastonimimuutos	1.1.2020
v 1.2	Päivitetty versio, saavutettavuusominaisuudet, lain 661/2009 ni-menmuutos	6.5.2021
v 1.3	Lisätty kuvaus lokidatasta	1.10.2021/VA

Sisällysluettelo

1 ESIPUHE

Tämä asiakirja perustuu tekniseen määritykseen, jonka on laatinut sähköisiä allekirjoituksia ja järjestelmiä käsittelevä ETSIn tekninen komitea (ETSI Technical Committee Electronic Signatures and Infrastructures (ESI)).

2 JOHDANTO

Sähköinen asiointi edellyttää sähköisen tiedon lähteen tunnistamista asiakirjoihin käsin tehtyyn allekirjoitukseen verrattavalla tavalla. Tämä voidaan yleensä toteuttaa käyttämällä sähköisiä allekirjoituksia. Varmennepalveluiden tarjoajat, joita yleisesti kutsutaan varmentajiksi, tuottavat sähköisten allekirjoitusten tekemiseen tarkoitettuja varmenteita.
Sähköisten allekirjoitusten käyttäjät voivat luottaa sähköisten allekirjoitusten aitouteen, jos varmentajalla on käytössään asianmukaiset menettelyt ja suojautumiskeinot, joilla minimoidaan julkisiin salausavainten järjestelmiin liittyvät toiminnalliset ja taloudelliset riskit.
Varmennepolitiikka on varmentajan laatima kuvaus menettelytavoista ja toimintaperiaatteista, joita varmenteita myönnettäessä noudatetaan. Varmennuskäytäntö on varmennepolitiikkaa yksityiskohtaisempi kuvaus varmentajan toiminnasta.
Tätä varmennepolitiikkaa sovelletaan Digi- ja väestötietoviraston ammattivarmenteeseen, joka myönnetään väestötietojärjestelmään rekisteröidyille Suomen kansalaisille ja Suomessa pysyvästi asuville ulkomaalaisille.
Ammattivarmenne koostuu varmenneparista, jolla on kaksi eri käyttötarkoitusta: todentamis- ja salausvarmenne ja allekirjoitusvarmenne, joka on vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukainen allekirjoitusvarmenne.

3 Soveltamisala

Tässä asiakirjassa määritellään menettelytapavaatimukset, jotka koskevat allekirjoitusvarmenteita myöntäviä varmentajia. Menettelytapavaatimuksia asetetaan allekirjoitusvarmenteita myöntävien varmentajien toiminnalle ja hallintakäytännölle, jotta tilaajat, varmentajan varmentamat allekirjoittajat sekä varmenteeseen luottavat osapuolet voisivat luottaa siihen, että varmenteella voidaan vahvistaa sähköisiä allekirjoituksia.
Digi- ja väestötietoviraston tarjoaman vahvan sähköisen tunnistamisen välineen tarjoaminen tapahtuu samassa tuotantoympäristössä, samanlaisin teknisin ja toiminnallisin ratkaisuin ja siihen sovelletaan samoja menettelytapoja noudattaen kuin Digi- ja väestötietoviraston myöntämän allekirjoitusvarmenteen tarjoamiseen.

Menettelytapavaatimuksissa:

a) määritellään kaksi yleisölle myönnettäviä allekirjoitusvarmenteita koskevaa, läheisesti toisiinsa liittyvää allekirjoitusvarmennepolitiikkaa, joista toinen edellyttää turvallisen allekirjoituksen luomisvälineen käyttöä

b) esitetään määrittelypuitteet sellaisia allekirjoitusvarmennepolitiikkoja varten, joilla parannetaan edellä mainittuja varmennemenettelytapoja tai jotka koskevat muille kuin yleisöksi katsottaville käyttäjäryhmille myönnettäviä allekirjoitusvarmenteita.

Varmentajaa koskevat menettelytapavaatimukset sisältävät vaatimuksia rekisteröintipalvelujen tarjoamisesta, varmenteiden luomisesta, varmenteiden jakelusta, varmenteiden peruuttamisen hallinnasta, sulkutilasta ja tarvittaessa allekirjoituksen luomisvälineen tarjoamisesta. Muut varmennepalvelujen tarjoajan toiminnot, kuten aikaleimat, attribuuttivarmenteet ja luottamuksellisuutta tukevat palvelut, eivät kuulu tämän asiakirjan soveltamisalaan. Tässä asiakirjassa ei esitetä vaatimuksia varmentajan varmenteille, ei myöskään varmennehierarkioiden tai ristiinvarmentamisen suhteen.
Nämä menettelytapavaatimukset on rajattu koskemaan sähköisten allekirjoitusten yhteydessä käytettävien avainten varmentamista.

Nämä menettelytapavaatimukset on erityisesti kohdistettu yleisölle myönnettäviin varmenteisiin, joita käytetään tukemaan sähköisiä allekirjoituksia

Näiden menettelytapavaatimusten mukaisesti myönnettyjä varmenteita voidaan käyttää henkilön todentamisessa, kun henkilö toimii omasta puolestaan tai edustamansa luonnollisen henkilön, oikeushenkilön tai yhteisön puolesta.
Nämä menettelytapavaatimukset koskevat julkisen avaimen salauksen käyttöä sähköisten allekirjoitusten vahvistamisessa.

Asiantuntevat riippumattomat elimet voivat käyttää tätä asiakirjaa perustana arvioidessaan täyttääkö varmentaja allekirjoitusvarmenteiden myöntämistä koskevat vaatimukset.

Varmenteenhaltijoita ja varmenteeseen luottavia osapuolia suositellaan lukemaan varmentajan varmennuskäytännöstä tarkempia lisätietoja siitä, kuinka kyseinen varmentaja toteuttaa tiettyä varmennepolitiikkaansa.

Tässä asiakirjassa ei kuitenkaan tarkenneta, kuinka riippumattomat osapuolet voivat arvioida tässä yksilöityjä vaatimuksia, esimerkiksi ei määritetä vaatimuksia riippumattomien arvioijien saataville annettavan tiedon tai riippumattomien arvioijien suhteen.

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

4 Viiteluettelo

Tässä asiakirjassa viitataan seuraavissa asiakirjoissa esitettyihin säännöksiin ja määrityksiin, jotka ovat sitovia tässä asiakirjassa kuvattuihin toimintoihin liittyen.

- Käytetyt viittaukset liittyen julkaisupäivään ja laitoksen tai version numeroihin ovat täsmällisiä tai yleisluontoisia.
- Täsmällisten viittausten osalta lähteen myöhempiä tarkistuksia ei sovelleta.
- Yleisluontoisten viittausten osalta sovelletaan lähteen viimeisintä versiota.

Tähän asiakirjaan liittyvää aineistoa on saatavilla muun muassa osoitteessa http://docbox.etsi.org/Reference. ETSI ei takaa linkin toimivuutta pitkällä aikavälillä.

Määräävät viittaukset:

[1] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements

for Trust Service Providers".

[2] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security

requirements for trust service providers issuing certificates; Part 1: General requirements".

[3] Guidelines for The Issuance and Management of Extended Validation Certificates v1.5.5,

CA/Browser Forum.

[4] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5:

QCStatements".

Ohjeelliset viittaukset:

Regulation (EU) N 910/2014 of the European Parliament and of the Council on electronic

identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

***ETSI* 8 Draft ETSI EN 319 411-2 V2.0.6 (2015-06)**

[ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum.

IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider

Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

Terminologiset kuvaukset:

ETSI EN 319 401 [1], ETSI

EN 319 411-1 [2], the Regulation (EU) N° 910/2014 [i.1] and the following apply:

EU Qualified Certificate: qualified certificate as specified in Regulation (EU) No 910/2014 [i.1]

Qualified Electronic Signature/Seal Creation Device: As specified in Regulation (EU) No 910/2014 [i.1].

5 Määritelmät ja lyhenteet

5.1 Määritelmät

Tässä asiakirjassa käytetään seuraavia käsitteitä ja määritelmiä:

Aktivointitieto: Sellainen luottamuksellinen tieto (PIN-tunnus), jota tarvitaan mikrosirulla olevien yksityisten avainten aktivointiin ja niiden käyttöön julkisen avaimen menetelmissä (esim. sähköinen allekirjoitus).

Allekirjoittaja: taho, joka on varmenteessa merkitty varmenteessa annettuun julkiseen avaimeen liittyvän yksityisen avaimen haltijaksi

Allekirjoituksen luomiseen käytettävät tiedot: ainutlaatuinen tietokokonaisuus, esimerkiksi koodit tai yksityiset salausavaimet, joita allekirjoittaja käyttää luodakseen sähköisen allekirjoituksen.
Kun kyseessä ovat julkisen avaimen salaukseen perustuvat allekirjoitusvarmenteet, kuten tämän asiakirjan soveltamisalassa, allekirjoituksen luomiseen käytettävät tiedot sisältävät yksityiset avaimet. Tässä asiakirjassa allekirjoituksen luomiseen käytettävistä tiedoista käytetäänkin käsitettä yksityinen avain.

Allekirjoituksen luomisväline: tarkoituksenmukaisesti määritetty ohjelmisto tai laitteisto, jolla allekirjoituksen luomiseen käytettävät tiedot käsitellään.

Allekirjoituksen todentamiseen käytettävät tiedot: tietokokonaisuus, esimerkiksi koodit tai julkiset salausavaimet, joita käytetään sähköisen allekirjoituksen todentamiseen.

Kun kyseessä ovat julkisen avaimen salaukseen perustuvat allekirjoitusvarmenteet, kuten tämän asiakirjan soveltamisalassa, allekirjoituksen todentamiseen käytettävät tiedot sisältävät julkiset avaimet. Tässä asiakirjassa allekirjoituksen todentamiseen käytettävistä tiedoista käytetäänkin käsitettä julkinen avain.

Ammattioikeus: Ammattioikeudella tarkoitetaan tässä varmennepolitiikassa niitä rekisteröityjä laillistetun, luvan saaneen ja nimikesuojatun ammattihenkilön sekä terveydenhuollon opiskelijan ammatillisia oikeuksia, jotka henkilö voi saada terveydenhuollon ammattihenkilöistä annetun lain (559/1994) 2 §:n nojalla. Ammattioikeus voi olla rajoittamaton, rajoitettu tai kokonaan poistettu. Terveydenhuollon ammattioikeudet tallennetaan Sosiaali- ja terveysalan lupa- ja valvontaviraston ylläpitämään Terhikki-rekisteriin. Ammattioikeudella tarkoitetaan tässä varmennepolitiikassa myös sosiaalihuollon ammattihenkilöitä, jotka täyttävät laissa (272/2005) sosiaalihuollon ammatillisen henkilöstön kelpoisuusvaatimuksista asetetut ehdot sosiaalihuollon ammattilaiselle.
Ammattivarmenne: Digi- ja väestötietoviraston luonnolliselle henkilölle myöntämä tässä asiakirjassa tarkemmin määritelty varmennepari.
Attribuutti: tahoon liitetty tieto, joka määrittelee tahon ominaisuuden, kuten ryhmän jäsenyyden tai roolin, tai muu kyseiseen tahoon liittyvä tieto

Avainpari: Julkisen avaimen menetelmissä käytettävät, toisiinsa liittyvät avaimet, joista toinen on julkinen ja toinen yksityinen. Avainten käyttötarkoitus on määritelty varmenteessa (ks. varmenteen haltijan allekirjoitusvarmenne sekä todentamis- ja salausvarmenne).

Epäsymmetrinen salaus: Epäsymmetrisessä salauksessa käytetään avainparia, joista toinen on julkinen ja toinen yksityinen. Julkisella avaimella salattu viesti voidaan avata vain kyseisen avainparin yksityisellä avaimella.

Julkinen avain: Julkisen avaimen menetelmässä epäsymmetrisessä salauksessa käytettävän avainparin julkinen osa. Varmentaja varmentaa sähköisellä allekirjoituksellaan julkisen avaimen kuulumisen varmenteen haltijalle. Julkinen avain on osa varmenteen tietosisältöä.
Julkisen avaimen järjestelmä: Tietoturvainfrastruktuuri, jossa tietoturvapalveluita tuotetaan julkisen avaimen menetelmillä.
Julkisen avaimen menetelmä: Tietoturvapalvelu, esimerkiksi henkilön sähköinen tunnistaminen, joka tuotetaan käyttämällä julkisia ja yksityisiä avaimia, varmenteita ja epäsymmetristä salausta.
Kehittynyt sähköinen allekirjoitus: sähköinen allekirjoitus, joka täyttää seuraavat vaatimukset: se liittyy yksiselitteisesti

a) sen allekirjoittajaan
b) sillä voidaan yksilöidä allekirjoittaja
c) se on luotu keinoilla, jotka allekirjoittaja voi pitää yksinomaisessa valvonnassaan,
d) se on liitetty sen kohteena olevaan tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita

Kortinlukijaohjelmisto: Kortinlukijaohjelmistoa käytetään työasemassa ns. loppukäyttäjän sovelluksena. Sen avulla käyttäjä voi hyödyntää henkilökorttiaan ja sillä olevia varmenteita erilaisissa käyttö- ja sovellusympäristöissä, esimerkiksi sähköisessä asioinnissa, turvapostissa ja työasemaan kirjautumisessa.

Allekirjoitusvarmenne: varmenne, joka täyttää Asetuksessa säädetyt vaatimukset. Allekirjoitusvarmenteen tietosisältö on määritelty vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa.

Allekirjoitusvarmennepolitiikka: varmennepolitiikka, johon sisältyy Asetuksessa säädetyt vaatimukset

Luottava osapuoli: Taho, joka luottaa varmenteen tietoihin ja käyttää varmennetta erilaisiin tietoturvapalveluihin, kuten varmenteen haltijan sähköiseen tunnistamiseen ja sähköisen allekirjoituksen todentamiseen.

Maksukortti: Pankki-, luotto-, yhdistelmä-, raha- ja maksuaikakortin yleisnimitys.

Mikrosiru: Tekninen alusta, jolla varmenne ja yksityiset avaimet sijaitsevat ja joka on sijoitettu henkilökortille, maksukortille tai mobiilipäätelaitteen kortille.

Mobiilipäätelaite: Matkapuhelin tai muu mobiililaite, jonka avulla voidaan käyttää varmennetta ja mikrosirulla olevia yksityisiä avaimia.

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

PIN-tunnus: Aktivointitieto, jolla mikrosirulla oleva yksityinen avain aktivoidaan käytettäväksi. PIN 1: perustunnusluku todentamista ja salausta varten. PIN 2: allekirjoitustunnusluku sähköistä allekirjoitusta varten.

PUK-koodi: Lukkiutuneen PIN-tunnuksen vapauttamisessa tarvittava koodi.

Rekisteröijä: Rekisteröijä tunnistaa varmenteen hakijan henkilöllisyyden varmennepolitiikan ja varmennuskäytännön mukaisesti varmentajan lukuun ja vastuulla.

Rekisteröintinumero: Rekisteröintinumero on tekninen numerosarja, joka muodostuu kaikille terveydenhuollon ammattihenkilöille, jotka rekisteröityvät tai ovat jo rekisteröityneet terveydenhuollon ammattihenkilöiden keskusrekisteriin, Terhikkiin. Rekisteröintinumeroa käytetään muun muassa ammattihenkilöiden tunnisteena esimerkiksi sähköisissä lääkemääräyksissä.

Rekisteröintipiste: Palvelupiste, jossa tarkistetaan varmenteen hakijan henkilöllisyys ja terveydenhuollon ammattioikeudet ja joka vastaa ammattikorttien, varmenteiden ja PIN-/PUK-tunnuslukujen jakelusta käyttäjille varmennepolitiikan ja varmennuskäytännön mukaisesti.

RSA-algoritmi ja RSA-avain: RSA-algoritmi on eräs yleisesti käytetty julkisen avaimen algoritmi. Ammattivarmenteeseen liittyvät yksityiset ja julkiset avaimet ovat RSA-avaimia.

Sosiaali -ja terveydenhuollon ammattihenkilö: Henkilö, joka terveydenhuollon ammattihenkilöistä annetun lain (559/1994) nojalla on saanut ammatinharjoittamisoikeuden (laillistettu ammattihenkilö) tai ammatinharjoittamisluvan (luvan saanut ammattihenkilö) sekä henkilö, jolla lain nojalla on oikeus käyttää asetuksella säädettyä terveydenhuollon ammattihenkilön ammattinimikettä (nimikesuojattu ammattihenkilö) ja joka on rekisteröity terveydenhuollon ammattihenkilöiden keskusrekisteriin sekä henkilö, joka täyttää vaatimukset, jotka asetetaan sosiaalihuollon henkilöstölle laissa (272/2005) sosiaalihuollon ammatillisen henkilöstön kelpoisuusvaatimuksista.

Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira): Valvira on sosiaali- ja terveydenhuollon lupa- ja valvontaviranomainen. Valvira parantaa ohjauksen ja valvonnan keinoin elinympäristön terveysriskien hallintaa sekä oikeusturvan toteutumista ja palvelujen laatua sosiaali- ja terveydenhuollossa. Valviran tehtäviin kuuluu myös sosiaali- ja terveydenhuollon laitteiden ja tarvikkeiden vaatimustenmukaisuuden valvonta sekä turvallisen käytön edistäminen.

Sulkulista: Varmentajan sähköisesti allekirjoittama ja julkaisema luettelo kesken voimassaoloajan suljetuista varmenteista ja niiden sulkuajankohdista. Sulkulistasta ilmenee sen ja sitä seuraavan sulkulistan julkaisuajankohta. Suljetut varmenteet viedään sulkulistalle.

Sulkupalvelu: Tekninen toimittaja, joka ottaa vastaan ja välittää varmenteiden sulkupyynnöt varmennejärjestelmään varmentajan lukuun.

Sähköinen allekirjoitus: sähköisessä muodossa oleva tieto, joka on liitetty tai loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään kyseisen muun tiedon todentamismenetelmänä.

Sähköinen asiointitunnus: Numeroista ja tarkistusmerkistä muodostettu tunniste, jonka avulla voidaan yksilöidä Suomen kansalaiset ja kotikuntalain mukaisesti Suomessa vakinaisesti asuvat ulkomaalaiset, jotka on merkitty Väestötietojärjestelmään.

Sähköinen allekirjoitus: kehittynyt sähköinen allekirjoitus, joka perustuu allekirjoitusvarmenteeseen ja joka on tehty turvallisella allekirjoituksen luomisvälineellä.
Sosiaali- ja terveydenhuollon ammattikortti: sosiaali- ja terveydenhuollon ammattihenkilölle myönnetty ammattivarmenteen sisältävä toimikortti.
Sosiaali- ja terveydenhuollon henkilöstökortti: sosiaali- ja terveydenhuollon muulle henkilöstölle (muut kuin sosiaali- ja terveydenhuollon ammattihenkilöt) myönnetty varmenteen sisältävä toimikortti.
Sosiaali- ja terveydenhuollon muu henkilö: Muu sosiaali- ja terveydenhuollon toimintayksikössä työskentelevä taikka sen tehtäviä suorittava henkilö, joka ei ole sosiaali- ja terveydenhuollon ammattihenkilö.
Sosiaali- ja terveydenhuollon palvelujen antaja: sosiaali- ja terveydenhuollon toimintayksikkö tai itsenäisenä ammatinharjoittajana toimiva sosiaali- ja terveydenhuollon ammattihenkilö.
Sosiaali- ja terveydenhuollon toimijakortti: Muulle sosiaali- ja terveydenhuollon toimijalle myönnetty varmenteen sisältävä toimikortti.
Terhikki-rekisteri: Terveydenhuollon ammattihenkilöistä annetun lain nojalla Valviran ylläpitämä valtakunnallinen rekisteri terveydenhuollon ammattihenkilöistä ja heidän ammatinharjoittamisoikeustiedoistaan.

Turvallinen allekirjoituksen luomisväline: allekirjoituksen luomisväline, joka täyttää Asetuksessa säädetyt vaatimukset.

Varmenne: sisältää käyttäjän julkisen avaimen sekä muita tietoja, joiden väärentäminen on estetty salakirjoittamalla ne varmenteen myöntäneen varmentajan yksityisellä avaimella. Tarkempi kuvaus perustuu ITU-T:n suositukseen X.509.
Varmenne: Sähköinen todistus, joka liittää allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistaa allekirjoittajan. Varmenne sisältää siihen liittyvän varmennuskäytännön yksilöivän tunnuksen.
Varmennejärjestelmä: Tietotekninen järjestelmä, jonka avulla luodaan varmenteet ja allekirjoitetaan sulkulistat.
Varmennekuvaus: Asiakirja sisältää varmennepolitiikan ja varmennuskäytännön keskeiset kohdat.

Varmennepalvelujen tarjoaja: yhteisö, oikeushenkilö tai luonnollinen henkilö, joka myöntää varmenteita tai tarjoaa muita sähköisiin allekirjoituksiin liittyviä palveluja.
Tässä asiakirjassa käsitellään varmennepalvelujen tarjoajia, jotka myöntävät allekirjoitusvarmenteita. Tässä asiakirjassa ei käsitellä varmennepalvelujen tarjoajan muuntyyppisiä toimintoja, kuten aikaleimausta ja vara-avainjärjestelmiä.

Varmennepolitiikka: nimetty säännöstö, joissa osoitetaan tietyn varmenteen soveltuvuus tietylle yhteisölle ja/tai sovellusluokka, jota koskee yhteiset turvallisuusvaatimukset. Tarkempi kuvaus perustuu ITU-T:n suositukseen X.509.

Lisätietoja varmennepolitiikkojen ja varmennuskäytännön keskinäisestä suhteesta annetaan kohdassa 4.3.
Varmennepolitiikka: Asiakirja, jossa on kuvattu varmenteiden myöntämisessä käytettävät periaatteet sekä varmenteisiin luottavien osapuolten vastuut. Digi- ja väestötietoviraston julkaisemat varmennepolitiikat ovat julkisesti saatavilla. Jokaisella varmennepolitiikalla on yksilöivä tunnuksensa.
Varmennerekisteri: Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukainen rekisteri, jota allekirjoitusvarmenteita yleisölle tarjoavan varmentajan on

velvollisuus pitää. Tiedot on säilytettävä vähintään 5 vuoden ajan varmenteen voimassaolon päättymisestä.
Varmennetietojärjestelmä: Tietotekninen järjestelmä, joka koostuu varmennejärjestelmistä, tietoliikenteestä, varmennehakemistosta ja sulkulistapalvelusta, neuvonta- ja sulkupalvelusta sekä varmenteiden ja korttien hallinnoinnista.
Varmennuskäytännön yksilöivä tunnus on osa varmenteen tietosisältöä.

Varmennuskäytäntö: lausunto toimintatavoista, joita varmentaja noudattaa varmenteiden myöntämisessä, hallinnoimisessa, peruuttamisessa ja uusimisessa sekä varmenteiden avainparin vaihtamisessa. Jokaisella varmennuskäytännöllä on oma yksilöivä tunnuksensa.

Varmentaja: Varmenteita myöntävä organisaatio, joka vastaa varmenteiden tuottamisesta sekä laatii toimintaansa kuvaavan varmennepolitiikan sekä varmennuskäytännön. Varmentajan toimintaan luottaa yksi tai useampi taho. Varmentaja on varmenteita myöntävä varmennepalvelujen tarjoaja. Tarkempi kuvaus perustuu ITU-T:n suositukseen X.509.Varmentajan käsitettä selvennetään lisää kohdassa 4.2.
Varmentajan varmenne: Sisältää varmentajan nimen, sijaintimaan ja julkisen avaimen.
Varmentajan yksityinen avain: Varmentajan myöntämien varmenteiden ja sen julkaisemien sulkulistojen allekirjoittamiseen käyttämä yksityinen avain.
Varmenteen hakija: Henkilö, joka hakee ammattivarmennetta ja joka tunnistetaan hakemisen yhteydessä luotettavasti.
Varmenteen haltija: Henkilö, jonka henkilöllisyys ja julkinen avain on varmennettu varmentajan sähköisellä allekirjoituksella, ja jonka hallussa varmenteeseen liittyvät yksityiset avaimet ovat.
Varmenteenhakija/haltija: taho, joka tilaa varmentajalta palvelun yhden tai useamman allekirjoittajan puolesta. Allekirjoittaja voi olla tilaaja, joka toimii omasta puolestaan.
Varmenteen haltijan allekirjoitusvarmenne: Varmenteella olevalla julkisella avaimella todennetaan sitä vastaavalla yksityisellä avaimella eli allekirjoitusavaimella varmenteen haltijan tekemä sähköinen allekirjoitus. Allekirjoituksen tekemiseen tarvitaan allekirjoitustunnusluku (PIN 2).
Varmenteen haltijan todentamis- ja salausvarmenne: Varmennetta käytetään henkilön sähköiseen tunnistamiseen ja tiedon salaukseen. Varmenteen haltija käyttää yksityistä todentamis- ja salausavaintaan sähköiseen tunnistautumiseen ja salatun tiedon tai viestin salauksen purkuun. Avaimen käyttämiseen tarvitaan perustunnusluku (PIN 1).
Varmenteen käyttö ja käyttötarkoitus: Tässä dokumentissa varmenteen käyttö on nimitys sekä itse varmenteen että siihen liittyvien avainten käytölle. Esimerkiksi varmenteen käytöllä sähköisessä allekirjoituksessa tarkoitetaan sekä yksityisen avaimen käyttöä allekirjoituksessa että julkisen avaimen ja varmenteen käyttöä allekirjoituksen todentamisessa.

Varmenteeseen luottava osapuoli: varmenteen vastaanottaja, joka toimii luottaen kyseiseen varmenteeseen ja/tai digitaalisiin allekirjoituksiin, jotka on todennettu kyseisellä varmenteella. Tarkempi kuvaus perustuu RFC 3647-määritykseen.

Varmenteiden sulkulista: allekirjoitettu varmenneluettelo, jonka sisältämiä varmenteita niiden myöntäjät eivät enää katso voimassa oleviksi. Tarkempi kuvaus perustuu ITU-T:n suositukseen X.509.
Yksityinen avain: Julkisen avaimen menetelmässä epäsymmetrisessä salauksessa käytettävän avainparin yksityinen osa. Varmenteen haltijan yksityiset avaimet on talletettu mikrosirulle niiden suojaamiseksi oikeudettomalta käytöltä.

5.2 3.2 Lyhenteet

ISO 27001 ISO IEC 27001

CA	Certification Authority, varmentaja
CSP	Certification Service Provider: varmennepalvelujen tarjoaja
CP	Certificate Policy, varmennepolitiikka
CPS	Certification Practise Statement, varmennuskäytäntö
CRL	Certificate Revocation List, varmenteiden sulkulista
FINEID	Finnish Electronic Identification
HSM	Hardware Security Module, turvamoduuli
HST	Henkilön sähköinen tunnistaminen
HTTP	Hypertext Transfer Protocol
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol, suorakäyttöinen varmenteen tilan palauttava palvelu
OID	Object Identifier, yksilöivä tunnus
PDS	PKI Disclosure Statement, varmennekuvaus
PIN	Personal Identification Number, PIN-tunnus
PKI	Public Key Infrastructure, julkisen avaimen järjestelmä
PUK	PIN Unblocking Key, PUK-koodi
QCP	Qualified Certificate Policy: allekirjoitusvarmennepolitiikka
RSA	Rivest, Shamir, Adleman, RSA-tunniste, eräs julkisen avaimen algoritmi, epäsymmetrinen algoritmi
SATU	Sähköinen asiointitunnus
SIM	Subscriber Identity Module
SSCD	Secure Signature Creation Device: turvallinen allekirjoituksen luomisväline
DVV	Digi- ja väestötietovirasto

6 Yleiskäsitteet

6.1 Varmentaja

Varmentaja luo ja myöntää varmenteita, jonka toimintaan varmennepalvelujen käyttäjät, eli varmenteen hakijat ja varmenteeseen luottavat osapuolet luottavat. Varmentaja on kokonaisvastuussa kohdassa 4.2 määriteltyjen varmennepalvelujen tarjoamisesta. Varmentaja on yksilöity varmenteessa varmenteen myöntäjäksi. Allekirjoitusvarmenteet allekirjoitetaan sen yksityisellä avaimella.

Varmentaja voi käyttää varmennepalvelussaan muita osapuolia, jotka tarjoavat palvelun osia. Varmentaja vastaa kuitenkin aina koko tuottamansa palvelun osalta ja varmistaa sen, että tässä asiakirjassa määritellyt menettelytapavaatimukset täyttyvät. Varmentaja voi esimerkiksi hankkia alihankintana kaikki osapalvelut, myös varmenteiden luomispalvelun. Varmenteiden allekirjoittamiseen käytettävä avain kuitenkin määritellään kuitenkin varmentajalle kuuluvaksi, ja varmentajalla säilyy kokonaisvastuu tässä asiakirjassa määriteltyjen vaatimusten täyttämisestä sekä vastuu yleisölle myönnettävien varmenteiden myöntämisestä.

Varmentaja on Asetuksen mukainen varmennepalvelujen tarjoaja, joka myöntää varmenteita. 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 (DVV) toimii valtiovarainministeriön hallinnonalalla. DVV on henkilörekisteriä ylläpitävä viranomainen, jonka väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain mukainen tehtävä on tuottaa varmennettuja sähköisen asioinnin palveluita. Digi- ja väestötietovirasto on toiminut myös terveydenhuollon lakisääteisenä varmentajana 1.12.2010 alkaen ja toimii lisäksi sosiaalihuollon lakisääteisenä varmentajana 1.4.2015 alkaen sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä koskevaan lakiin tehtyjen muutosten johdosta. (laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä, laki sähköisestä lääkemääräyksestä sekä laki terveydenhuollon ammattihenkilöistä. Digi- ja väestötietoviraston Varmennepalvelut toiminto vastaa viraston varmennetoiminnasta. DVV on tarjonnut varmennepohjaisia allekirjoitus- ja tunnistusvälineitä vuodesta 1999 lähtien ja toiminut allekirjoitusvarmentajana 31.3.2003 lukien.
Tässä asiakirjassa määritellään menettelytapavaatimukset, jotka koskevat allekirjoitusvarmenteita myöntäviä varmentajia sekä vahvan sähköisen tunnistamisvälineen tarjoajana olevaa Digi- ja väestötietovirastoa. Menettelytapavaatimuksia asetetaan varmenteita myöntävien varmentajien toiminnalle ja hallintakäytännölle, jotta tilaajat, varmentajan varmentamat allekirjoittajat sekä varmenteeseen luottavat osapuolet voisivat luottaa siihen, että varmenteella voidaan vahvistaa sähköisiä allekirjoituksia.
Digi- ja väestötietoviraston tarjoaman vahvan sähköisen tunnistamisen välineen tarjoaminen tapahtuu samassa tuotantoympäristössä, samanlaisin teknisin ja toiminnallisin ratkaisuin ja siihen sovelletaan samoja menettelytapoja noudattaen kuin Digi- ja väestötietoviraston myöntämän allekirjoitusvarmenteen tarjoamiseen.
DVV:n varmennetietojärjestelmä ja varmennepalvelut perustuvat julkisen avaimen järjestelmään (Public Key Infrastructure eli PKI). DVV:n varmenneinfrastruktuuri muodostuu varmennejärjestelmästä, kortteihin sisältyvien varmennetietojen toimittajasta, sulkulistasta, neuvontapalvelusta ja hakemistopalvelusta. DVV:n toimintoja varmentajana ovat varmenne- hakemisto- ja sulkupalveluiden tuottaminen, rekisteröinti sekä varmenteen sisältävän kortin valmistus ja yksilöinti. DVV vastaa

koko varmennejärjestelmän toimivuudesta, myös käyttämiensä rekisteröijien ja teknisten toimittajien osalta. DVV:n Varmennepalvelut-toiminto ylläpitää varmenteitaan koskevia varmennepolitiikka-, varmennuskäytäntö- ja varmennekuvausasiakirjoja, jotka ovat saatavilla sähköisesti osoitteessa www.fineid.fi.
Henkilökortista on säädetty henkilökorttilaissa (829/1999) ja Digi- ja väestötietoviraston myöntämistä varmenteista on säädetty väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa.
DVV tuottaa 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.
Tämän ammattivarmenteen myöntämistä kuvaavan varmennepolitiikan on rekisteröinyt Digi- ja väestötietovirasto.
Tämä varmennepolitiikka kuvaa Asetukseen perustuvan ja vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaisen sähköisen allekirjoituksen allekirjoitusvarmenteen myöntämiseen, tuottamiseen ja vastuun jakoon liittyviä yksityiskohtaisia vaatimuksia.
Tämä asiakirja kuvaa myös ammattivarmenteeseen sisältyvän, vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaisen vahvan sähköisen tunnistamisen välineenä tarjottavan tunnistusvarmenteen myöntämiseen, tuottamiseen ja tietojen tallentamiseen liittyviä ratkaisuja ja menettelytapoja allekirjoitusvarmenteen tuotantoympäristön vaatimuksia noudattaen.
Ammattivarmenne koostuu varmenneparista, jolla on kaksi toisistaan poikkeavaa käyttötarkoitusta. Todentamis- ja salausvarmenne täyttää vahvan sähköisen tunnistamisvälineen vaatimukset. Yksinomaan allekirjoituksen toteuttamiseen tarkoitettu allekirjoitusvarmenne täyttää allekirjoitusvarmenteen vaatimukset. Varmenteen hakijan henkilöllisyyden oikeellisuuden takaa Digi- ja väestötietovirasto.
Varmenteiden myöntämiseen sekä peruuttamiseen liittyvää lokidataa säilytetään vähintään seitsemän (7) vuotta varmenteen voimassaoloajan jälkeen.

6.2 Varmennepalvelut

Varmenne on sähköinen todistus, joka liittää allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistaa varmenteen haltijan henkilöllisyyden. Varmenteen tiedot on sähköisesti allekirjoitettu varmentajan yksityisellä avaimella. Tämän varmennepolitiikan mukainen varmenne perustuu julkisen avaimen järjestelmään ja menetelmiin. Tämän varmennepolitiikan mukaisten varmenteiden tietosisältö on määritelty väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa.
Tämän varmennepolitiikan mukainen ammattivarmenne voidaan myöntää Suomen kansalaiselle tai kotikuntalain (201/1994) mukaisesti Suomessa vakinaisesti asuvalle ulkomaalaiselle, jonka henkilötiedot on talletettu väestötietojärjestelmään.
Varmentajana toimiva Digi- ja väestötietovirasto yksilöi varmenteen haltijan sähköisen asiointitunnuksen (SATU) avulla, joka on myös osa varmenteen tietosisältöä. Sähköinen asiointitunnus on sähköistä asiointia varten erikseen luotu väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa määritelty tekninen tunnistetieto, joka ei sisällä henkilöön liittyviä tunnistetietoja.
Ammattivarmenne voidaan myöntää ja tallettaa erilaisille teknisille alustoille eli mikrosiruille kuten henkilökortille. Tämä varmennepolitiikka on yhteinen kuvaus näillä eri teknisillä alustoilla oleville ammattivarmenteille.

Digi- ja väestötietoviraston varmennepolitiikalla ja varmennuskäytännöllä on molemmilla yksilöivä tunnuksensa (OID).
Digi- ja väestötietoviraston allekirjoitusvarmenteiden myöntäminen on tässä asiakirjassa jaoteltu vaatimusten luokittelusyistä seuraaviin osapalveluihin:

- **Rekisteröintipalvelu:** Rekisteröintipalvelussa todennetaan allekirjoittajan henkilöllisyys ja mahdolliset häneen liittyvät erityiset attribuutit, jotka välitetään varmenteiden luomispalveluun. Rekisteröintipalvelu sisältää toimintana myös asiakkaan itsensä tai jonkin muun kuin varmentajan generoiman avaimen toimittamisen. Digi- ja väestötietoviraston rekisteröintipalvelussa ei käsitellä muita kuin sen itsensä tuottamat avainparit. Ammattivarmenteen rekisteröinti tapahtuu noudattaen lain väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista mukaista menettelytapaa. Tarkempi menettelytapa kuvataan kyseessä olevaa teknistä alustaa kuvaavassa varmennuskäytännössä.

- **Varmenteiden luomispalvelu:** Varmenteiden luomispalvelussa luodaan ja allekirjoitetaan varmenteet, jotka perustuvat rekisteröintipalvelussa todennettuun henkilöllisyyteen ja muihin attribuutteihin.

- **Jakelupalvelu:** Jakelupalvelun kautta varmenteet jaetaan allekirjoittajille sekä asetetaan varmenteeseen luottavien osapuolten saataville, jos allekirjoittajalta saadaan siihen lupa. Lisäksi palvelussa asetetaan varmentajan käyttöehdot sekä kaikki julkaistut varmennepolitiikkoja ja varmennuskäytäntöä koskevat tiedot tilaajien ja varmenteeseen luottavien osapuolten saataville. Digi- ja väestötietovirasto toimittaa todentamisvarmenteen tiedot julkiseen hakemistoon. Hakemistopalvelu on julkinen Internet-palvelu, josta on saatavilla kaikki varmentajan myöntämät todentamisen ammattivarmenteet sekä varmentajan varmenteet sekä sulkulista. Hakemistopalvelu on saatavissa osoitteesta ldap://ldap.fineid.fi.

- **Peruutustenhallintapalvelu:** Peruutustenhallintapalvelu sulkee varmenteet, jotka varmenteen haltija haluaa suljettavaksi ennen varmenteen voimassaoloajan päättymistä. Peruutusten hallintapalvelussa käsitellään peruuttamispyynnöt ja -ilmoitukset, ja määritetään tarvittavat toimet käsittelyn perusteella. Palvelun tulokset jaetaan sulkulistan välityksellä. Varmenteen voimassaolotieto on saatavilla myös OCSP-palvelun kautta.

- **Sulkutilasta tiedottava palvelu:** Sulkutilasta tiedottavan palvelun kautta annetaan varmenteiden sulkutilatietoja varmenteeseen luottaville osapuolille. Palvelussa voidaan käyttää varmenteiden sulkulistoja tai reaaliaikaista yksittäisten tilatietojen välittämistä. Digi- ja väestötietovirasto ilmoittaa tiedot sulkupalveluun varmenteeseen luottavien osapuolten saataville. Tilatietoja päivitetään tietyin väliajoin, joka on yksityiskohtaisesti kuvattu varmennuskäytäntöasiakirjassa.

- **Allekirjoituksen luomisvälineen tarjoaminen allekirjoittajalle:** Allekirjoituksen luomisväline valmistetaan ja toimitetaan allekirjoittajille. Toimikortin tai mikrosirun valmistaja ja yksilöijä toimii varmenteen, siihen liittyvien avainparien ja aktivointitietojen osalta varmentajan toimeksiannosta ja vastuulla ja yhteistyösopimuksen mukaisesti. Toimikortit ja mikrosirut yksilöidään rekisteröijän toimittamien tietojen mukaisesti.

Käytetyn palvelujaottelun ainoa tarkoitus on selventää menettelytapavaatimuksia. Tässä kuvauksessa ei rajoiteta varmentajan palvelutoteutuksen jaottelua.

Varmenteeseen luottava osapuoli: Varmenteeseen luottava osapuoli on henkilö tai organisaatio, joka luottaa varmenteen tietoihin ja joka käyttää varmennetta todentamiseen, tiedon salaukseen ja sähköiseen allekirjoitukseen. Varmenteeseen luottavan osapuolen on tarkastettava, että käytettävä varmenne on voimassa. Tämä voidaan tehdä tarkistamalla varmenteen tilatieto joko OCSP-palvelusta tai että varmenne ei ole sulkulistalla.

6.3 Varmennepolitiikka ja varmennuskäytäntö

Tässä kohdassa kuvataan varmennepolitiikan ja varmennuskäytännön välistä suhdetta. Varmennepolitiikan muotoa tai varmennuskäytännön erittelyjä koskevia rajoituksia ei sovelleta tässä luvussa.

6.3.1 Tarkoitus

Varmennepolitiikka, jonka tunnus ilmoitetaan varmenteessa, kertoo yleisellä tasolla varmennustoiminnan pääperiaatteet. Varmennuskäytännössä kerrotaan varmennetoiminnan, erityisesti luomisen ja ylläpitämisen osalta vaadittavat yksityiskohtaiset toteuttamiseen liittyvät käytännöt ja menetelmät sen osalta, kuinka varmennepolitiikassa esitetyt vaatimukset täytetään.
Tässä asiakirjassa määritetään varmennepolitiikka, joilla täytetään Asetuksen ja kansallisen lain mukaiset vaatimukset. Varmentajana toimiva Digi- ja väestötietovirasto määrittää varmennuskäytännöissään, kuinka nämä vaatimukset täytetään.
Digi- ja väestötietovirasto noudattaa tätä varmennepolitiikkaa myöntäessään ammattivarmenteen. Varmenteen haltijoiden ja varmenteeseen luottavien osapuolien tulee toimia tämän varmennepolitiikan mukaisesti.
Tämän varmennepolitiikan mukaista ammattivarmennetta voidaan käyttää henkilön vahvaan sähköiseen tunnistamiseen, tiedon salaukseen ja sähköiseen allekirjoitukseen. Ammattivarmennetta voidaan käyttää käyttötarkoituksensa mukaisesti rajoituksitta sekä hallinnollisissa että yksityisten organisaatioiden tarjoamissa sovelluksissa ja palveluissa.
Varmennepolitiikka ja varmennuskäytäntö sisältävät vaatimuksia, jotka koskevat varmentajan, rekisteröijän, varmenteen haltijan ja varmenteeseen luottavan osapuolen velvoitteita sekä lainsäädäntöön ja mahdollisten erimielisyyksien ratkaisuun liittyviä kysymyksiä.
Varmentajana toimiva Digi- ja väestötietovirasto vaihtaa varmennepolitiikkaa koskevan yksilöivän tunnuksen, jos se muuttaa varmennepolitiikkaansa sovellettavuuden osalta.

6.3.2 Yksityiskohtaisuus

Varmennepolitiikka kuvaa varmentajan toiminnan yleiset vaatimukset. Varmennuskäytännössä kuvataan varmennepolitiikkaa yksityiskohtaisemmin menettelytavat, joita varmentaja toteuttaa varmenteiden myöntämisessä ja muussa hallinnoinnissa. Varmennuskäytännössä määritellään, kuinka varmentaja täyttää varmennepolitiikassa määritetyt tekniset sekä organisaatioon ja menettelyihin liittyvät vaatimukset.
Varmentajana toimiva Digi- ja väestötietovirasto on laatinut sisäisten toimintojensa sekä ulkoistettujen toimintojensa ohjaamista varten asiakirjoja, jotka eivät ole julkisia.
Tämän varmennepolitiikan on rekisteröinyt Digi- ja väestötietovirasto. Digi- ja väestötietovirasto on julkista luottamusta nauttivaa valtakunnallista henkilörekisteriä ylläpitävä viranomainen, jonka väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain mukainen tehtävä on tuottaa varmennettuja sähköisen asioinnin palveluita.

6.3.3 Lähestymistapa

Varmennepolitiikka- ja varmennuskäytäntöasiakirjat on laadittu erilaisia käyttötarkoituksia varten. Varmennepolitiikka on yleiskuvaus varmentajan toiminnasta. Varmennuskäytäntö kuvaa varmentajan toiminnan yksityiskohdat organisaatiorakenteen, toimintatapojen, toimitilojen ja tietoteknisen ympäristön mukaisesti.

6.3.4 Muut varmentajan julkaisemat asiakirjat

Varmennepolitiikan ja varmennuskäytännön lisäksi varmentaja voi julkaista muita varmennetoimintaa ohjaavia asiakirjoja. Tällaisia asiakirjoja ovat muun muassa käyttöohjeet ja varmennetoiminnan yleisesitykset kuluttajia, asiakasorganisaatioita ja palvelunrakentajien tarpeita varten.

Ammattivarmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa ja ennen ammattivarmennehakemuksen allekirjoittamista annettavissa yleisissä käyttöohjeissa, jotka muodostavat ammattivarmenteen hakijan kanssa tehtävän sopimuksen. Ammattivarmenteen hakijana oleva organisaatio hakee ammattivarmennetta omille jäsenilleen, jotka tunnistetaan henkilökohtaisella tavalla varmennetta haettaessa. Hakemusasiakirjassa on tiedot kummankin osapuolen oikeuksista ja velvollisuuksista. Kun ammattivarmenteen hakija hakee varmennetta, hän hyväksyy samalla yleiset käyttöehdot.
Hakemusasiakirjassa ja käyttöohjeissa mainitaan selkeästi, että ammattivarmenteen hakija vahvistaa allekirjoituksellaan annettujen tietojen oikeellisuuden sekä hyväksyy varmenteen luomisen ja julkaisunsopimuksen mukaisesti. Samalla hakija hyväksyy ammattivarmenteen käyttöön liittyvät säännöt ja ehdot sekä huolehtii ammattivarmenteen ja PIN-tunnusten säilyttämisestä sekä mahdollisen väärinkäytön tai varmenteiden/mikrosirun katoamisen ilmoittamisesta.

Varmennekuvaus on varmentajan käyttöehtojen osa, joka liittyy julkisen avaimen järjestelmän toimintaan. Varmentajana toimiva Digi- ja väestötietovirasto julkaisee varmennekuvauksen sekä varmenteen hakijan että varmenteeseen luottavien osapuolien saataville.

6.4 Varmenteen hakija

Varmenteen hakija voi hakea varmennetta omissa nimissään tapahtuvaa käyttöä varten tai mahdollisesti yhteisön jäsenenä allekirjoittaessaan asiakirjoja yhteisön nimissä. Tämä ero on kuvattu tässä asiakirjassa silloin, kun sen erotteleminen on välttämätöntä. Varmennetta haettaessa kuitenkin tunnistetaan aina yksityinen henkilö henkilökohtaisella tavalla.

Hakijaorganisaatio hakee ammattivarmennetta jäsenilleen, jotka ovat henkilökohtaisella tavalla tunnistettuja luonnollisia henkilöitä.

7 Johdanto allekirjoitusvarmennepolitiikkoihin

7.1 Yleistä

Varmennepolitiikalla tarkoitetaan periaatteita, jotka osoittavat tietyn varmenteen soveltuvuuden tietylle yhteisölle. Varmennepolitiikassa on kuvattu myös yhteisesti sovellettavat turvallisuusvaatimukset.

Tässä asiakirjassa menettelytapavaatimukset määritellään varmennepolitiikkojen mukaan. Nämä varmennepolitiikat koskevat Asetuksen mukaisia allekirjoitusvarmenteita, minkä vuoksi näitä asiakirjoja kutsutaan allekirjoitusvarmennepolitiikoiksi.

Tämän asiakirjan mukaisesti myönnetyt varmenteet sisältävät varmennepolitiikan OID-yksilöintitunnuksen, jonka avulla varmenteeseen luottavat osapuolet voivat määrittää varmenteen käyttökelpoisuuden ja luotettavuuden tiettyyn käyttötarkoitukseen. Tässä asiakirjassa määritetään kaksi allekirjoitusvarmennepolitiikkaa:

1) yleisölle myönnettäviä allekirjoitusvarmenteita koskeva allekirjoitusvarmennepolitiikka, jossa edellytetään turvallisten allekirjoituksen luomisvälineiden käyttöä

Tässä asiakirjassa yleisökäsitteen tulkinta määräytyy tilanteeseen sovellettavan kansallisen lainsäädännön mukaan. Varmentaja voidaan katsoa yleisölle varmenteita myöntäväksi, jos kyseisten varmenteiden käyttöä ei ole rajoitettu osanottajien välisin vapaaehtoisin yksityisoikeudellisin sopimuksin.

2) yleisölle myönnettäviä allekirjoitusvarmenteita koskeva allekirjoitusvarmennepolitiikka.

Kohdassa 8 esitetään määrittelyn edellytykset muille allekirjoitusvarmennepolitiikoille,

a) joilla tehostetaan tai rajoitetaan edellä mainittuja politiikkoja ja/tai

b) jotka mahdollisesti koskevat muille kuin yleisölle myönnettäviä allekirjoitusvarmenteita.

Tässä asiakirjassa käytettävät periaatteet on määritelty julkaisuissa RFC 3647 ja ANSI X9.79. Tässä asiakirjassa pyritään mahdollisimman suureen yhdenmukaisuuteen edellä mainittujen asiakirjojen periaatteiden ja vaatimusten kanssa.
Digi- ja väestötietovirasto laatii erillisen varmennepolitiikan jokaiselle myöntämälleen varmennetyypille sekä varmennuskäytännön jokaista eri teknistä alustaa koskien. Varmennepolitiikka kuvaa varmennetyypeittäin käytettävät menettelytavat, käyttöehdot, vastuiden jaon ja muut varmenteen käyttöön liittyvät näkökulmat yleisellä tasolla. Varmennuskäytäntö kuvaa noudatettavat menettelytavat yksityiskohtaisella tasolla.

Tämän varmennepolitiikan nimi on Varmennepolitiikka sosiaali- ja terveydenhuollon ammattivarmennetta varten, jonka OID on 1.2.246.517.1.10.206.

. Tämä varmennepolitiikka viittaa varmentajan varmennepolitiikkaan, jonka OID on 1.2.246.517.1.10.201.
Digi- ja väestötietovirasto noudattaa Asetuksen N:o (EU) 910/2014 luottamuspalveluiden mukaista yleisölle myönnettäviä allekirjoitusvarmenteita koskevaa varmennepolitiikkaa. Asiakirjan viitetiedot

ovat ETSI EN 319 411-1 [2] QSCD mukaisesti; OID: 0.4.0.194112.1.2. Tämän varmennepolitiikan mukaisesti myönnettäviä allekirjoitusvarmenteita voi käyttää sellaisten sähköisten allekirjoitusten vahvistamisessa, jotka vastaavat Asetuksessa kuvattuja sähköisten allekirjoitusten hyväksyttyjä varmenteita ja luontivälineitä kuten Asetuksen 28 ja 29 artiklassa säädetään. Tunnistusvarmenteen taso täyttää Asetuksen ja sen nojalla annetun varmuustasoasetuksen mukaisesti vaatimustason ”korkea”.

Sekä varmennepolitiikka että varmennuskäytäntö ovat saatavilla osoitteesta www.fineid.fi.
Tämän varmennepolitiikan on rekisteröinyt Digi- ja väestötietovirasto. Se on henkilörekisteriä ylläpitävä viranomainen, jonka väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain mukainen tehtävä on tuottaa muiden tehtäviensä lisäksi varmennettuja sähköisen asioinnin palveluita. Digi- ja väestötietovirasto vastaa tämän varmennepolitiikan hallinnoinnista ja päivityksistä.
Tätä varmennepolitiikkaa koskevat kysymykset lähetetään seuraavaan osoitteeseen:

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

Varmennepolitiikkaan liittyviin kysymyksiin sekä näistä asiakirjoista vastaa Digi- ja väestötietoviraston varmennehallinto-vastuualue.

Digi- ja väestötietovirasto (DVV) Varmennepalvelut
PL 123
00531 Helsinki
www.fineid.fi

Digi- ja väestötietovirasto omistaa kaikki ammattivarmenteisiin ja dokumentaatioon liittyvät tiedot teknisten toimitussopimusten mukaisesti. Digi- ja väestötietovirasto omistaa täydet omistus- ja käyttöoikeudet tähän varmennepolitiikkaan.

7.2 Yksilöintitunnukset

Tässä asiakirjassa määriteltyjen allekirjoitusvarmennepolitiikkojen OID-yksilöintitunnukset ovat seuraavat:
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.
Tämän varmennepolitiikan mukaisesti myönnetty allekirjoitusvarmenne täyttää Asetuksen hyväksytylle allekirjoitusvarmenteelle asettamat vaatimukset. Tunnistusvarmenteen taso täyttää Asetuksen ja sen nojalla annetun varmuustasoasetuksen mukaisesti vaatimustason ”korkea”.
Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa on säädetty allekirjoitusvarmenteella tehdyistä sähköisistä luottamuspalveluista. Sähköisestä henkilökortista on säädetty henkilökorttilaissa ja Digi- ja väestötietoviraston myöntämistä varmenteista on säädetty väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa.
Tämä varmennepolitiikka astuu voimaan 1.10.2021.

Varmentaja sisällyttää noudattamiensa allekirjoitusvarmennepolitiikkojen OID-yksilöintitunnukset myös varmenteen hakijoiden ja varmenteeseen luottavien osapuolten saataville asetettaviin käyttöehtoihin ja tällä tavoin ilmaisee noudattavansa kyseistä allekirjoitusvarmennepolitiikkaa.

7.3 Käyttäjäyhteisö ja sovellettavuus

7.3.1 QCP n + QSCD -allekirjoitusvarmennepolitiikka

Tämä varmennepolitiikka koskee varmenteita,

a) jotka täyttävät Asetuksessa säädetyt vaatimukset
b) jotka myöntävä varmentaja täyttää Asetuksessa säädetyt vaatimukset
c) joita myönnetään yleisölle.

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

7.4 Vaatimustenmukaisuus

7.4.1 Yleistä

Varmentajalla on oikeus käyttää varmennepolitiikan yksilöintitunnusta vain,

a) jos varmentaja ilmaisee noudattavansa yksilöityä allekirjoitusvarmennepolitiikkaa ja asettaa pyynnöstä tilaajan ja varmenteeseen luottavien osapuolten saataville todisteita vaatimustenmukaisuudesta tai

b) jos pätevä ja riippumaton osapuoli on hiljattain arvioinut yksilöidyn allekirjoitusvarmennepolitiikan vaatimusten noudattamisen nykytilaa varmentajalla. Vaatimustenmukaisuuden osoittamiseen vaadittavat keinot voivat vaihdella varmentajan sijoittautumisvaltion lainsäädännön mukaan. Varmentajan vaatimustenmukaisuus tarkistetaan säännöllisesti sekä aina, kun varmentajan toimintaa muutetaan merkittävästi.

7.4.2 QCPn + QSCD -allekirjoitusvarmennepolitiikka

Vaatimusten mukaisen varmentajan on osoitettava, että

a) se täyttää sille määritellyt vaatimukset
b) se on ottanut käyttöön hallintakeinot, jotka täyttävät vaatimukset.

8 Velvollisuudet ja vastuu sekä vastuunrajoitukset

Tämän kohdan vaatimuksia sovelletaan varmennepolitiikkaan eli QCP n + QSCD, ellei muuta mainita.

8.1 Varmentajan velvollisuudet

Varmentaja varmistaa, että kaikki varmentajalle valittua allekirjoitusvarmennepolitiikkaa koskevat vaatimukset toteutetaan.

Varmentaja on vastuussa allekirjoitusvarmennepolitiikassa määrättyjen menettelyjen noudattamisesta, vaikka varmentajan toimintaa toteutettaisiin toimeksiantosopimuksin.

Varmentaja tarjoaa kaikki varmennepalvelu osa-alueet varmennuskäytännössään mainitun mukaisesti.

Digi- ja väestötietovirasto voi myöntää varmenteen myös omiin tarkoituksiinsa. Tällöin se noudattaa samoja vaatimuksia kuin muut organisaatiot.

8.1.1 Varmentajan velvollisuudet

Digi- ja väestötietovirastolla on lakiin perustuva tehtävä toimia varmentajana.
Varmentaja noudattaa toiminnassaan voimassaolevaa lainsäädäntöä.
Varmentaja toimii huolellisesti, luotettavasti ja asianmukaisesti.
Varmentajalla on riittävät tekniset taidot ja taloudelliset voimavarat varmennetoiminnan asianmukaiseksi järjestämiseksi sekä mahdollisen vahingonkorvausvastuun kattamiseksi.
Varmentaja vastaa kaikista varmennetoiminnan osa-alueista, myös varmentajan apunaan käyttämien teknisten toimittajien tai henkilöiden, kuten rekisteröijien ja kortinvalmistajien tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta.

Varmentaja laatii ja ylläpitää varmennepolitiikkaa, joka kuvaa ammattivarmenteen myöntämisessä, ylläpidossa ja hallinnoinnissa käytettävät menettelytavat, käyttöehdot, vastuiden jaot ja muut ammattivarmenteen käyttöön liittyvät näkökulmat yleisellä tasolla.
Varmentaja laatii ja ylläpitää varmennuskäytäntöjä, jotka kuvaavat, miten varmentaja soveltaa varmennepolitiikkaa.
Varmentaja noudattaa varmennepolitiikkaa ja varmennuskäytäntöä.
Varmentaja julkaisee varmennepolitiikan ja varmennuskäytännön yleisesti saataville.
Varmentaja pitää palveluksessaan riittävästi henkilökuntaa, jolla on varmennepalvelujen tuottamisen edellyttämä asiantuntemus, kokemus ja pätevyys.
Varmentaja käyttää luotettavia järjestelmiä ja tuotteita, jotka on suojattu oikeudettomalta käytöltä.
Varmentaja pitää yleisesti saatavilla ammattivarmennetta ja varmennetoimintaa koskevat tiedot, joiden perusteella varmentajan toiminta ja luotettavuus voidaan arvioida.
Varmentaja turvaa allekirjoituksen luomistietojen luottamuksellisuuden.
Varmentaja ei tallenna tai jäljennä allekirjoittajalle luovutettuja allekirjoituksen luomistietoja.

8.1.2 Rekisteröijää koskevat velvollisuudet

Rekisteröijä toimii varmentajan vastuulla ja lukuun sekä noudattaa varmentajan kanssa sovittuja rekisteröintiin liittyviä menettelytapoja.
Rekisteröijä noudattaa rekisteröinnin yhteydessä varmennepolitiikkaa ja varmennuskäytäntöä.
Rekisteröijä tunnistaa varmenteen hakijan henkilökohtaisesti ja luotettavasti varmennuskäytännössä kuvatulla tavalla siten, että hakijan henkilöllisyys ja muut varmenteen myöntämisessä tarpeelliset hakijan henkilöön liittyvät tiedot tulevat huolellisesti tarkastetuiksi.
Rekisteröijä huolehtii henkilötietojen huolellisesta käsittelystä ja luottamuksellisuudesta.
Rekisteröijä antaa varmenteen hakijalle tiedot varmenteen käyttöehdoista.

8.2 Varmenteen hakijan velvollisuudet

Varmentaja velvoittaa sopimuksella (katso kohdan 7.3.1 alakohta i) varmenteenhakijaa noudattamaan kaikkia seuraavassa mainittavia velvollisuuksia. Jos allekirjoittaja ja varmenteen hakija ovat eri tahoja, tilaajan on saatettava allekirjoittajan tietoon kaikki allekirjoittajaan sovellettavat velvollisuudet seuraavan luettelon mukaisesti:

a) Varmentajalle on annettava oikeat ja täydelliset tiedot allekirjoitusvarmennepolitiikan vaatimusten mukaisesti, etenkin rekisteröinnin yhteydessä.

b) Avainparia saa käyttää vain sähköisiin allekirjoituksiin ja mahdollisten muiden tilaajalle ilmoitettujen rajoitusten mukaisesti (katso kohta 7.3.4).

c) Varmenteen haltijan on toiminnassaan noudatettava erityistä huolellisuutta, jotta allekirjoittajan yksityistä avainta ei käytetä luvattomasti.

d) Jos varmenteenhakija luo allekirjoittajan avaimet:
   i. allekirjoittajan avaimet on luotava käyttämällä algoritmia, jonka on todettu soveltuvan sähköisiin allekirjoituksiin
   ii. avainpituutena ja algoritmina on käytettävä yhdistelmää, jonka on todettu soveltuvan sähköisiin allekirjoituksiin varmenteen voimassaolon ajan

      Algoritmeja ja niiden parametreja koskevat määritykset ja ohjeet on julkaistu asiakirjassa TS 102 176-1.

   iii. allekirjoittajan yksityinen avain voidaan pitää yksinomaan allekirjoittajan valvonnassa.

e) Jos varmennepolitiikassa edellytetään turvallisen allekirjoituksen luomisvälineen

käyttöä (eli käytössä on QCP public + SSCD -allekirjoitusvarmennepolitiikka), varmennetta saa käyttää vain tällaisella välineellä luotujen sähköisten allekirjoitusten yhteydessä.

Edellä kuvattu vaatimus ei koske QCP public -allekirjoitusvarmennepolitiikkaa.

f) Jos varmentaja on myöntänyt varmenteen QCP public + SSCD -allekirjoitusvarmennepolitiikan mukaisesti ja allekirjoittajan avaimet luodaan tilaajan tai allekirjoittajan valvonnassa, allekirjoittajan avaimet on luotava allekirjoittamiseen käytettävällä turvallisella allekirjoituksen luomisvälineellä.

Edellä oleva vaatimus ei koske QCP public -allekirjoitusvarmennepolitiikkaa.

g) Varmentajalle on ilmoitettava ilman aiheetonta viivästystä, mikäli ennen varmenteessa ilmoitetun voimassaolon päättymistä tapahtuu jokin seuraavista:

i. allekirjoittajan yksityinen avain on kadonnut tai sen käyttö on mahdotonta (esimerkiksi siksi, että avaimen käyttöön tarvittava PIN-koodi on unohtunut), yksityinen avain on varastettu, se on mahdollisesti joutunut vääriin käsiin tai

ii. allekirjoittajan yksityisen avaimen käyttö ei ole enää hallittavissa, koska aktivointitiedot (esimerkiksi PIN-koodi) ovat joutuneet vääriin käsiin tai muista syistä, ja/tai

iii. varmenteen sisältö on tilaajalle tai allekirjoittajalle ilmoitettuun nähden virheellinen tai sitä on muutettu.

h) Jos allekirjoittajan yksityinen avain on joutunut vääriin käsiin, se peruutetaan välittömästi ja lopullisesti.

Jos allekirjoittajan varmenteen myöntäneen varmentajan toiminta on vaarantunut, on varmistettava, että allekirjoittaja ei käytä varmennetta.
Digi- ja väestötietoviraston myöntämän ammattivarmenteen käyttötarkoitus on määritelty kunkin varmennetyypin varmennepolitiikassa, varmennuskäytännössä sekä varmenteen haltijan käyttöohjeissa. Varmennetta saa käyttää vain sen käyttötarkoituksen mukaisesti sähköiseen allekirjoitukseen, todentamiseen tai tiedon salaamiseen
Ammattivarmenteen haltija vastaa siitä, että ammattivarmennetta haettaessa ilmoitetut tiedot ovat oikeita.
Ammattivarmenteen haltija on vastuussa ammattivarmenteen käytöstä, ammattivarmenteella tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista. Allekirjoitusvarmenteen osalta noudatetaan, mitä Asetuksessa ja laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista on määrätty.
Ammattivarmenteen haltija säilyttää mikrosirulla olevat yksityiset avaimensa ja niiden käyttämiseen tarvittavat tunnusluvut erillään sekä pyrkii estämään yksityisten avaintensa katoamisen, joutumisen ulkopuolisten käsiin, muuttamisen tai luvattoman käytön. Mikrosirun luovuttaminen tai PIN-tunnuksen paljastaminen toiselle henkilölle esim. lainaamalla vapauttaa varmentajan ja ammattivarmenteeseen luottavan osapuolen ammattivarmenteen käyttämisestä mahdollisesti aiheutuvista vastuista.
Ammattivarmennetta käsitellään ja suojataan noudattaen samaa huolellisuutta kuin muita vastaavia mikrosiruja, kortteja tai asiakirjoja, kuten esimerkiksi luottokortteja, ajokorttia ja passia. Henkilökohtaiset PIN-tunnukset on säilytettävä fyysisesti eri paikassa kuin ammattivarmenteen ja yksityiset avaimet sisältävä mikrosiru.

Mikrosirun ja kortin häviämisestä tai väärinkäytön mahdollisuudesta on ilmoitettava viipymättä varmentajalle soittamalla maksuttomaan sulkupalveluun +358 800 162 622.

8.3 Tiedottaminen varmenteeseen luottaville osapuolille

Varmenteeseen luottavien osapuolten saataville asetetuissa ohjeissa (katso kohta 7.3.4) on ilmoitettava, että varmenteeseen luottaminen perustellulla tavalla edellyttää, että osapuoli

a) todentaa varmenteeseen luottavalle osapuolelle osoitetun ajantasaisen sulkutilatiedon (katso kohta 7.3.4) avulla, onko varmenne voimassa tai onko se asetettu keskeytystilaan tai peruutettu. Varmentajan käytännöistä ja sulkutilatietojen jakelutavasta riippuen sulkutilatietojen jakelussa voi esiintyä viivettä, joka on enintään yksi (1) päivä.

b) ottaa huomioon mahdolliset varmenteen käytön rajoitukset, jotka tiedotetaan varmenteeseen luottavalle osapuolelle varmenteessa tai kohdan 7.3.4 mukaisesti toimitetuissa ehdoissa

c) noudattaa sopimuksissa tai muualla määrättyjä ehtoja

Asetukseen perustuvaa, yleisölle allekirjoitusvarmenteita myöntävän varmentajan vastuuta sovelletaan osapuoliin, jotka "perustellulla tavalla tukeutuvat" varmenteeseen.
Ammattivarmenteet (todentaminen) julkaistaan yleisesti saatavilla olevassa julkisessa hakemistossa ja suljetut ammattivarmenteet sulkulistalla, josta varmenteeseen luottavan osapuolen on tarkistettava sen voimassaolotieto.
Varmenteeseen luottavan osapuolen velvollisuus on varmistaa, että varmennetta käytetään sen käyttötarkoituksen mukaisesti. Allekirjoitusvarmenteen käyttötarkoitus on sähköinen allekirjoitus. Todentamis- ja salausvarmenteen käyttötarkoitus on henkilön todentaminen ja tiedon salaus.
Varmenteeseen luottavan osapuolen on noudatettava varmennepolitiikkaa ja varmennuskäytäntöä.
Ammattivarmenteeseen luottava osapuoli voi vilpittömässä mielessä luottaa ammattivarmenteeseen, kun hän on tarkistanut, että **ammattivarmenne on voimassa ja että se ei ole sulkulistalla**.
Ammattivarmenteeseen luottavalla osapuolella on velvollisuus tarkistaa varmenteet sulkulistalta tai OCSP-palvelusta. Ammattivarmenteen voimassaolon luotettavuuden varmistamiseksi ammattivarmenteeseen luottavan osapuolen on noudatettava varmenteen tilatiedon tarkistustoimia.
Jos ammattivarmenteeseen luottava osapuoli kopioi sulkulistan hakemistosta, sen on varmistettava sulkulistan aitous tarkistamalla sulkulistan varmentajan sähköinen allekirjoitus. Lisäksi on tarkistettava sulkulistan voimassaoloaika.
Mikäli uusinta sulkulistaa ei voida saada hakemistosta laitteiston tai hakemistopalvelun toimintahäiriön vuoksi, ammattivarmennetta ei pidä hyväksyä, mikäli viimeisen saadun sulkulistan voimassaoloaika on päättynyt. Kaikki ammattivarmenteen hyväksymiset tämän voimassaoloajan jälkeen tapahtuvat ammattivarmenteeseen luottavan osapuolen omalla riskillä.

8.4 Vastuu

Yleisölle allekirjoitusvarmenteita myöntäviä varmentajia koskee Asetuksessa ja laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista säädetyn mukainen vastuu. Vahvan sähköisen tunnistamisvälineen tai –palvelun tarjoavia palveluntarjoajia koskee laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista säädetyn mukainen vastuu.

8.4.1 Varmentajan vastuut

Digi- ja väestötietovirasto vastaa varmentajana koko varmennejärjestelmän turvallisuudesta. Varmentaja vastaa toimeksiantona hankkimistaan palveluista samoin kuin olisi itse tuottanut palvelun.

Digi- ja väestötietovirasto vastaa siitä, että ammattivarmenne on luotu noudattaen väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa, laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista, laissa sähköisestä asioinnista viranomaistoiminnassa ja varmennepolitiikassa sekä varmennuskäytännössä esitettyjä menettelyjä ja varmenteen hakijan antamien tietojen mukaisesti. Digi- ja väestötietovirasto vastaa ainoastaan niistä tiedoista, jotka se on tallettanut ammattivarmenteeseen.
Digi- ja väestötietovirasto vastaa siitä, että kun ammattivarmennetta käytetään asianmukaisesti, se on käytettävissä luovutushetkestä koko sen voimassaoloajan, ellei sitä ole asetettu sulkulistalle.
Ammattivarmenne on luovutettu henkilölle, joka on tunnistettu ammattivarmenteelta edellytettävällä tavalla. Varmenteen haltijalle on luovutettu ennen sopimuksen allekirjoitusta ammattivarmenteen käyttöön liittyvät käyttöohjeet ennen sopimuksen allekirjoittamista.

Allekirjoittaessaan ammattivarmenteen yksityisellä avaimellaan varmentaja vakuuttaa tarkistaneensa ammattivarmenteessa olevat henkilötiedot varmennepolitiikassa ja varmennuskäytännössä esitettyjen menettelyjen mukaisesti.

Varmentaja vastaa siitä, että sulkulistalle viedään oikean henkilön ammattivarmenne ja että ne ilmestyvät tässä varmennepolitiikassa mainitussa ajassa sulkulistalle.

8.4.2 Rekisteröijän vastuut

Ammattivarmenteen rekisteröijänä toimii rekisteröintipiste, joka rekisteröi varmenteen hakijan varmentajana toimivan Digi- ja väestötietoviraston lukuun ja vastuulla. Rekisteröinnin osalta noudatetaan väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain ja vahvasta sähköisestä tunnistamisesta ja sähköisen allekirjoituslain vaatimuksia sekä henkilökorttilain vaatimuksia silloin, kun ammattivarmenne on henkilökortilla.

8.4.3 Ammattivarmenteen haltijan vastuut

Ammattivarmenne on haltijansa sähköinen henkilöllisyys eikä sitä tämän vuoksi saa luovuttaa toisen henkilön käytettäväksi
Ammattivarmenteen haltija on vastuussa sen käytöstä, sillä tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista.
Mikrosirun sisältävän kortin jättäminen lukijalaitteeseen saattaa mahdollistaa ammattivarmenteen väärinkäytön. Lopettaessaan pääteistunnon tai jättäessään päätelaitteen valvomatta ammattivarmenteen haltijan vastuulla on poistaa ammattivarmenteen sisältävä mikrosiru lukijalaitteesta ja sulkea käytetyt sovellukset asianmukaisesti tai muuten katkaistava ammattivarmenteen käyttämiseksi tarvittava tekninen yhteys.
Ammattivarmenteen haltijan vastuu sen käyttämisestä päättyy, kun hän on ilmoittanut sulkupalveluun tarvittavat tiedot sen sulkemiseksi ja saatuaan puhelun vastaanottaneelta virkailijalta sulkemista koskevan ilmoituksen. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

8.4.4 Ammattivarmenteeseen luottavan osapuolen vastuut

Ammattivarmenteeseen luottava osapuoli ei voi luottaa siihen ja sähköisen allekirjoituksen oikeellisuuteen vilpittömässä mielessä, mikäli ammattivarmenteen voimassaoloa ei ole tarkastettua. Ammattivarmenteen hyväksyminen mainitussa tapauksessa vapauttaa Digi- ja väestötietoviraston vastuusta. Ammattivarmenteeseen luottavan osapuolen on tarkistettava, että myönnetty varmenne vastaa käyttötarkoitustaan siinä oikeustoimessa, jossa sitä on käytetty.

8.4.5 Vastuiden rajoitukset

Digi- ja väestötietovirasto ei vastaa PIN-tunnusten, PUK-koodin ja ammattivarmenteen haltijan yksityisten avainten paljastumisen seurauksena syntyvistä vahingoista, ellei paljastuminen välittömästi johdu Digi- ja väestötietoviraston välittömästä toiminnasta.

Digi- ja väestötietovirasto vastaa ammattivarmenteen haltijalle ja ammattivarmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Digi- ja väestötietoviraston välittömästä toiminnasta.
Digi- ja väestötietovirasto ei vastaa ammattivarmenteen haltijalle aiheutuneista välillisistä tai seurannaisvahingoista. Digi- ja väestötietovirasto ei myöskään vastaa ammattivarmenteeseen luottavan osapuolen tai ammattivarmenteen haltijan muun sopimuskumppanin mahdollisesti kärsimistä välillisistä tai seurannaisvahingoista.
Digi- ja väestötietovirasto ei vastaa yleisten tietoliikenneyhteyksien eikä tietoverkkojen, esimerkiksi Internetin toimivuudesta eikä siitä, jos oikeustoimen suorittaminen estyy ammattivarmenteen haltijan käyttämän laitteen tai ohjelmiston toimimattomuudesta eikä siitä, että ammattivarmennetta käytetään vastoin sen käyttötarkoitusta.

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

Varmentajalla on oikeus kehittää edelleen varmennepalvelua. Ammattivarmenteen haltijan tai ammattivarmenteeseen luottavan osapuolen on vastattava tämän vuoksi aiheutuvista omista kustannuksistaan eikä varmentaja ole velvollinen korvaamaan ammattivarmenteen haltijalle tai ammattivarmenteeseen luottavalle osapuolelle tällaisesta varmentajan kehittämistyöstä aiheutuvista kustannuksista.
Varmentaja ei vastaa varmennetta käytettäessä kansalaiselle ja organisaatiolle tarkoitetun varmenteeseen pohjautuvan verkkopalvelun tai sovelluksen virheistä tai niistä aiheutuvista kustannuksista.

8.4.6 Muut osapuolet

Ammattivarmenteeseen luottava osapuoli voi luottaa ammattivarmenteen ja sähköisen allekirjoituksen oikeellisuuteen, jos hän on tarkastanut joko voimassaolotiedon OCSP-palvelusta tai ettei ammattivarmennetta ole asetettu sulkulistalle eikä varmenteen voimassaoloaika ole päättynyt eikä hänellä ole muita syitä perustellusti epäillä varmenteen käytön oikeellisuutta.
Varmentaja vastaa ammattivarmenteesta sen mukaisesti kuin varmentaja on sitoutunut tässä varmennepolitiikassa ja ammattivarmennetta koskevassa varmennuskäytännössä.
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 ammattivarmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Digi- ja väestötietoviraston toiminnasta.

9 Varmentajan toimintaa koskevat vaatimukset

Tätä kohtaa sovelletaan kumpaankin kohdassa 5 yksilöityyn allekirjoitusvarmennepolitiikkaan eli QCP public- ja QCP public + SSCD -allekirjoitusvarmennepolitiikkaan, ellei muuta mainita.
Varmentajan toteuttaa seuraavat vaatimukset täyttävät hallintakeinot.
Tämä asiakirja koskee allekirjoitusvarmenteita myöntävänä varmentajana toimivaa Digi- ja väestötietovirastoa. Tässä asiakirjassa kuvatun palvelun toteuttamiseen sisältyy rekisteröintipalvelujen tarjoaminen, varmenteiden luominen, varmenteiden jakelu, varmenteiden peruuttamisen hallinta ja sulkutilasta tiedottaminen (kohta 4.2). Jos vaatimus liittyy varmentajan tiettyyn palvelualueeseen, se kuvataan vastaavien alaotsikoiden alla. Mikäli seuraavassa ei yksilöidä palvelualuetta tai jos mainitaan "varmentaja yleisesti", vaatimus koskee varmentajan yleistä toimintaa.
Näiden menettelytapavaatimusten tarkoituksena ei ole rajoittaa varmentajan palveluista veloittamista.

Esitettävät vaatimukset koskevat turvallisuustavoitteita sekä niiden saavuttamiseen käytettäviä hallintakeinoja, joiden osalta esitetään yksityiskohtaisia vaatimuksia, mikäli se on katsottu tavoitteiden täyttymisen kannalta tarpeelliseksi.

9.1 Varmennuskäytäntö

Varmentaja varmistaa, että se osoittaa varmennepalvelujen tarjoamisen edellyttämän luotettavuuden.

Tässä asiakirjassa kuvattuihin toimenpiteisiin liittyvä yksityiskohtainen menettely on kuvattu jokaista varmennetyyppiä ja tallennusalustaa koskevassa varmennuskäytännössä.

9.2 Julkisen avaimen järjestelmässä käytettävien avainten elinkaaren hallinta

9.2.1 Varmentajan avaimen luominen

Varmentaja luo tarkoituksenmukaisen ajan ennen varmentajan allekirjoitusavaimen voimassaolon päättymistä uuden avainparin varmenteen allekirjoittamiseen ja tekee kaikki tarpeelliset toimet, ettei kyseiseen varmentajan avaimeen mahdollisesti luottavien yhteisöjen toimintaan aiheutuisi häiriöitä. Uusi varmentajan avain luodaan ja sen jakelu toteutetaan näiden menettelytapojen mukaisesti. Nämä toimet tehdään riittävän ajoissa, jotta kaikki varmentajaan jossakin suhteessa toimivat osapuolet (allekirjoittajat, varmenteen hakijat, varmenteeseen luottavat osapuolet, ylemmällä tasolla toimivat varmentajat) saavat ajoissa tiedon varmentajan avainparin vaihtamisesta ja jotta ne voivat toteuttaa toiminnan häiriöttömän jatkumisen kannalta tarvittavat toimet. Tämä ei koske varmentajaa, joka lopettaa toimintansa ennen sen oman varmentajan varmenteen viimeistä voimassaolopäivää.

9.2.2 Varmentajan avaimen tallennus, varmuuskopiointi, ja palauttaminen

Avainten tallentaminen

Varmentaja varmistaa, että varmentajan yksityisten avainten luottamuksellisuus ja eheys säilyvät Asetuksen mukaisesti.
Digi- ja väestötietovirasto luo yksityiset allekirjoitusavaimensa ja yksityisiä allekirjoitusavaimiaan vastaavat julkiset avaimet.
Varmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa, jotka täyttävät turvallisuusstandardin vaatimukset.

Varmentaja huolehtii siitä, että varmentajan yksityiset avaimet on suojattu paljastumiselta ja luvattomalta käytöltä.
Yksityisen avaimen luontiin ja käyttöön liittyvään ympäristöön vaaditaan vähintään kahden henkilön samanaikainen läsnäolo tai toiminnan aktivoiminen.
Digi- ja väestötietoviraston ammattivarmenteessa olevista yksityisistä avaimista ei luoda kopiota.

9.2.3 Varmentajan julkisen avaimen jakelu

Varmenteiden jakelu

Varmentaja varmistaa, että allekirjoituksen todentamiseen käytettävän varmentajan (julkisen) avaimen sekä siihen liittyvien parametrien eheys ja aitous säilyvät varmenteeseen luottaville osapuolille jakelun aikana Asetuksen mukaisesti.
Varmentajan varmenne sisältää varmentajan julkisen avaimen. Varmentajan varmenne talletetaan julkiseen hakemistoon. Varmentajan varmenne on saatavilla varmentajan julkisesta hakemistosta sekä varmentajan www-sivuilta.
Varmentaja arkistoi kaikki varmentamansa julkiset avaimet.

9.2.4 Vara-avainjärjestelmä

Allekirjoittajan yksityisiä allekirjoitusavaimia ei säilytetä tavalla, joka mahdollistaa salauksen purun ja varmuuskopioinnin, jolloin valtuutetut tahot voisivat tietyissä tilanteissa purkaa salauksen hyödyntämällä yhden tai useamman osapuolen antamia tietoja.
Digi- ja väestötietoviraston ammattivarmenteessa olevista yksityisistä avaimista ei luoda kopiota.

9.2.5 Varmentajan avaimen käyttö

Varmentajan vastaa siitä, että varmentajan yksityisiä allekirjoitusavaimia käytetään ainoastaan käyttötarkoituksensa mukaisesti.

Varmentajan varmenne:
Käyttötarkoitus: Varmenteiden ja sulkulistojen allekirjoitus. Tekninen kuvaus on FINEID S2 -määrityksissä.

9.2.6 Varmentajan avaimen elinkaaren päättyminen

Varmentajan varmistaa, ettei varmentajan yksityisiä allekirjoitusavaimia käytetä niiden elinkaaren päättymisen jälkeen.

Digi- ja väestötietovirasto ei luo yksityisistä allekirjoitusavaimista kopioita.

9.2.7 Varmenteiden allekirjoittamisessa käytettävän salauslaitteiston elinkaaren hallinta

Varmentaja varmistaa salauslaitteiston turvallisuuden koko sen elinkaaren ajan.

9.2.8 Varmentajan tarjoamat allekirjoittajan avaimen hallintapalvelut

Varmentaja varmistaa, että kaikki sen luomat allekirjoittajan avaimet luodaan turvallisesti ja että allekirjoittajan yksityisen avaimen luottamuksellisuus on turvattu.

Varmenteiden luominen
Ammattivarmenteen allekirjoittamiseen käytetty varmentajan yksityinen avain sekä sitä vastaava julkinen avain ovat 4096-bittisiä RSA-avaimia.
Ammattivarmenteen haltijan yksityiset ja julkiset avaimet ovat 2048-bittisiä RSA-avaimia.

Varmenteen tietosisällössä käyttötarkoituksen määräävä kenttä määrittelee varmenteisiin liittyvän avaimen käyttötarkoituksen. Avaimen käyttö rajataan käytettäväksi vain ilmoitettuun käyttötarkoitukseensa.

Varmentajan varmenne:
Käyttötarkoitus: Varmenteiden ja sulkulistojen allekirjoitus. Tekninen kuvaus on FINEID S2 -määrityksissä.

Varmenteen haltijan todentamis- ja salausvarmenne:
Käyttötarkoitus: Sähköisen henkilöllisyyden todentaminen tai tiedon salaus.

Varmenteen haltijan allekirjoitusvarmenne:
Käyttötarkoitus: Sähköinen allekirjoitus

9.2.9 Turvallisen allekirjoituksen luomisvälineen valmistaminen

Erillisyys voidaan saada aikaan varmistamalla, että aktivointitietojen jakelu ja turvallisen allekirjoituksen luomisvälineen toimittaminen tapahtuvat eri aikoina tai eri reittejä.
Turvallisen allekirjoituksen luomisvälineen valmistamista koskevat edellä luetellut vaatimukset voidaan täyttää esimerkiksi käyttämällä soveltuvaa suojausprofiilia, joka on määritelty ISO/IEC 15408 -standardin mukaisesti tai vastaavasti.

9.3 Julkisen avaimen järjestelmässä käytettävien varmenteiden elinkaaren hallinta

9.3.1 Allekirjoittajan rekisteröinti

Varmentaja varmistaa, että allekirjoittajat tunnistetaan ja todennetaan asianmukaisesti ja että allekirjoittajan varmennepyynnöt ovat virheettömiä, paikkansapitäviä ja jotka perustuvat asianmukaiseen valtuutukseen.

Kun varmentaja myöntää ammattivarmenteen, se samalla hyväksyy varmennehakemuksen. Varmentaja vastaa myöntäessään ammattivarmenteen, että sen tietosisältö on oikea sen luovuttamishetkellä.

Ammattivarmenteella olevat tiedot määrittelevät ammattivarmenteen haltijan yksikäsitteisesti. Varmentaja selvittää tarvittaessa varmenteen hakijan virallisen henkilöllisyyden.

Ammattivarmenteeseen liittyvät, mikrosirulla tai muussa turvallisessa ympäristössä luodut yksityiset avaimet toimitetaan ammattivarmenteen hakijalle luovutuksen yhteydessä.

Ammattivarmenteen hakijalle korostetaan varmenteen luovutushetkellä, että yksityisistä avaimista ei ole eikä niistä voi myöhemminkään valmistaa kopiota.

Ammattivarmenne voidaan noutaa henkilökohtaisesti rekisteritoimipisteestä.

Ammattivarmenteen haltijan vastuulla on estää hänelle kuuluvien yksityisten avaintensa ja niihin liittyvien PIN-tunnusten käyttäminen käyttöehtojen vastaisella tavalla huolehtimalla niistä käyttöehdoissa mainitulla tavalla.

Ammattivarmenteen haltijan avainpari luodaan turvatiloissa. Julkista avainta käytetään varmenteen luomiseen ja yksityinen avain säilytetään luku- ja kirjoitussuojattuna mikrosirulla.

Kortinvalmistaja luo avainten käytön mahdollistavat aktivointitiedot eli PIN-tunnukset. PIN-tunnukset on suojattu niin, ettei niitä voi lukea tai kopioida kortilta. Varmenteen haltijan vastuulla on suojata avaintensa käyttö huolehtimalla mikrosirustaan tai kortistaan ja tunnusluvuistaan käyttöehdoissa mainitulla tavalla.

Ammattivarmenteen käyttämiseksi tarvittavia PIN-tunnuksia ja PUK-koodeja käsitellään turvallisuuden takaamiseksi siten, etteivät ne ole yhtä aikaa samassa paikassa ennen toimitusta ja toimituksessa varmenteen hakijalle.

Ammattivarmenteen haltija voi ladata Digi- ja väestötietoviraston www-sivuilta kortinlukijaohjelmiston, jolla ammattivarmennetta voidaan käyttää sähköisissä asiointipalveluissa. Ammattivarmenteen haltijalle selvitetään, että hänellä on mahdollisuus vaihtaa alkuperäiset PIN-tunnukset uusiksi tunnuksiksi. PIN-tunnusten vaihto-ohjelma on maksutta kortinhaltijan saatavissa osoitteessa www.fineid.fi.

Varmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa ja yleisissä käyttöehdoissa, jotka muodostavat varmenteen hakijan kanssa tehtävän sopimuksen. Hakemusasiakirjassa ja käyttöehdoissa mainitaan selkeästi, että ammattivarmenteen hakija vahvistaa allekirjoituksellaan annettujen tietojen oikeellisuuden sekä hyväksyy varmenteen luomisen ja julkaisun asiakasorganisaation kanssa tehdyn sopimuksen mukaisesti tai julkisessa hakemistossa. Samalla hakija hyväksyy ammattivarmenteen käyttöön liittyvät säännöt ja ehdot sekä huolehtii ammattivarmenteen ja PIN-tunnusten säilyttämisestä sekä mahdollisen väärinkäytön tai kortin katoamisen ilmoittamisesta.

Ammattivarmenteen hakija vastaa siitä, että kaikki ammattivarmenteen kannalta olennaiset tiedot, jotka ammattivarmenteen hakija on antanut varmentajalle tai rekisteröijälle, ovat oikeita. Ammattivarmenteen haltijan on käytettävä ammattivarmennettaan vain sen käyttötarkoitusten mukaisesti.

Ammattivarmenteen haltijan vastuulla on estää hänelle kuuluvien yksityisten avaintensa ja niihin liittyvien PIN-tunnusten käyttäminen käyttöehtojen vastaisella tavalla huolehtimalla niistä käyttöehdoissa mainitulla tavalla.

Varmenteen haltijan on ilmoitettava välittömästi ammattivarmenteensa sulkupalveluun, mikäli hän epäilee, että sopimusehtojen vastainen käyttö on tullut mahdolliseksi.

Varmenteen haltijaa koskevat tiedot määrittelevät varmenteen haltijan yksikäsitteisesti. Varmentaja selvittää tarvittaessa varmenteen haltijan virallisen henkilöllisyyden.

Ammattivarmenteeseen liittyvät, mikrosirulla tai muussa turvallisessa ympäristössä luodut yksityiset avaimet toimitetaan varmenteen haltijalle luovutuksen yhteydessä. Mikrosirulla luoduista yksityisistä allekirjoitusavaimista ei ole eikä niistä voi myöhemminkään valmistaa kopiota.

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

Sosiaali- ja terveydenhuollon ammattihenkilön nimeäminen todentamisvarmenteessa sekä allekirjoitusvarmenteessa on kuvattu määrityksessä THPKI - T2 - Digi- ja väestötietoviraston CA-malli ja varmenteiden tietosisältö sosiaali- ja terveydenhuollossa.

Terveydenhuollon varmenteen haltijan nimeämisessä käytetään luonnollisen henkilön Terhikki-

rekisteriin kirjattuja etu- ja sukunimiä.

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

Varmentaja ei myönnä anonyymejä varmenteita.

Määritelty nimitietue yksilöi rekisteröidyn sosiaali- ja terveydenhuollon ammattihenkilön. Henkilön tunnistetieto on sosiaali- ja terveydenhuollon ammattihenkilön ainutkertaisesti yksilöivä.

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

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

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.

Sosiaalihuollon ammattihenkilön ammattioikeus tarkistetaan Valviran voimassa olevan ohjeistuksen mukaisesti. Kun sosiaalihuollon ammattihenkilöiden keskusrekisteri on valtakunnallisesti käytössä, tarkistetaan sosiaalihuollon ammattioikeuden voimassaolo tästä rekisteristä.

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

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

Kaikki terveydenhuollon ammattihenkilön varmennehakemuksessa tarvittavat henkilötiedot perustuvat Terhikki-rekisteriin.

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

Varmentajien välisen yhteistyön edellytykset ja vaatimukset määritellään juurivarmentajan varmennepolitiikassa.

Varmenteiden uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

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

Sosiaali- ja terveydenhuollon ammattivarmennetta haetaan henkilökohtaisesti rekisteröijänä toimivalta organisaatiolta.

Hakemuksen tiedot tallennetaan varmentajan varmennetietojärjestelmään.
Sosiaali- ja terveydenhuollon ammattivarmenteen hakeminen edellyttää, että hakija:

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

Rekisteröijä ilmoittaa hakijalle ammattikortin sekä tunnuslukukuoren toimitustavasta.

Varmennehakemuksen voi tehdä Valviran rekisteröimä terveydenhuollon ammattihenkilö. Sosiaalihuollon ammattihenkilö voi tehdä hakemuksen Valviran kulloinkin voimassa olevan ohjeistuksen mukaisesti siihen asti, kunnes sosiaalihuollon ammattihenkilöiden keskusrekisteri on valmis ja käytössä.

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

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

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

Varmentaja toimittaa hakijalle hakijan tiedoilla yksilöidyn:

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

Lisäksi rekisteröijä toimittaa varmenteen hakijalle ammattikortin käyttöohjeen.
Varmenteen myöntämiseen liittyvät rekisteröijän vastuut on kuvattu luvussa 1.3.2.

Varmennehakemus käsitellään rekisteröintipisteessä ilman aiheetonta viivytystä.

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

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

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

Varmennehakemus käsitellään ilman aiheetonta viivytystä rekisteröintipisteen aukioloaikana. Sosiaali- ja terveydenhuollon ammattivarmenteen myöntämisestä ei tehdä erillistä ilmoitusta.

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

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.

Varmentaja julkaisee myönnetyt todentamisvarmenteet julkisessa tietoverkossa olevassa varmennehakemistossa. Allekirjoitusvarmenteita ei julkaista hakemistossa.

9.3.2 7.3.2 Varmenteen uusiminen, sen avainparin vaihtaminen ja varmenteen päivittäminen

Varmentaja varmistaa, että jo aikaisemmin rekisteröityneelle allekirjoittajalle myönnettäviä varmenteita koskevat pyynnöt ovat täydelliset, paikkansapitävät ja asianmukaisesti valtuutetut. Näihin sisältyvät varmenteen uusiminen, peruuttamisen jälkeen tai ennen voimassaolon päättymistä tehtävä avainparin vaihtaminen, sekä allekirjoittajan attribuuttien muuttumisesta johtuva päivittäminen. Sosiaali- ja terveydenhuollon ammattihenkilön varmenne voidaan uusia edellisen varmenteen voimassaolon päättyessä, mikäli varmenteen myöntämisen edellytykset ovat edelleen voimassa.

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

Varmenteen uusimista voi hakea vain varmenteen haltija.

Varmenteiden uusimisessa, hyväksymismenettelyssä sekä varmenteen julkaisussa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.
Erillistä ilmoitusta sosiaali- ja terveydenhuollon ammattivarmenteen uusimisesta ei tehdä.

9.3.3 Varmenteiden luominen

Varmentaja varmistaa, että se myöntää varmenteita turvallisesti niiden aitouden.
Ammattivarmenteen haltijoiden yksityiset avaimet luodaan turvallisesti allekirjoitusvarmenteen vaatimukset täyttävällä tavalla. Varmenteen haltijan itsensä luomia avainpareja ei hyväksytä.

Yksityisistä avaimista ei tehdä kopioita niiden luontivaiheessa, eivätkä ne ole siirrettävissä tai kopioitavissa mikrosirulta. Varmentajalla ja kortinvalmistajalla ei ole pääsyä varmenteen haltijoiden yksityisiin avaimiin.
Avainten luontivaiheessa avaimia ei ole vielä kohdistettu kenellekään henkilölle.
Varmentajan yksityiset avaimet ja niiden varmuuskopiot säilytetään vahvasti salattuina kriittisen tietoturvallisuuden vaatimukset täyttävissä laitteissa.
Varmenteen haltijan yksityisistä avaimista ei ole kopioita.
Varmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa.
Varmentajan yksityiset allekirjoitusavaimet suojataan korkean luotettavuuden fyysisillä ja loogisilla turvatoimilla. Niitä käytetään vain turvalliseen ympäristöön sijoitetussa järjestelmässä.

9.3.4 Käyttöehtojen jakelu

Varmentaja varmistaa, että käyttöehdot ja ohjeet asetetaan tilaajien ja varmenteeseen luottavien osapuolten saataville.

Tämän varmennepolitiikan mukaisesti myönnetty allekirjoitusvarmenne täyttää Asetuksen mukaiset vaatimukset.
Tiedot voidaan toimittaa varmenteenhakijan tai varmenteeseen luottavan osapuolen sopimuksen osana. Käyttöehdot voidaan sisällyttää varmennuskäytäntöön niin, että lukijan on ne helppo havaita ja tunnistaa.
Yleisölle myönnettäviä varmenteita koskevien sopimusehtojen osalta otetaan huomioon kuluttajalainsäädännön vaatimukset, myös kuluttajasopimusten kohtuuttomista ehdoista annettu direktiivi 93/13/ETY
Ammattivarmenteen haltija voi ladata Digi- ja väestötietoviraston www-sivuilta kortinlukijaohjelmiston, jolla ammattivarmennetta voidaan käyttää sähköisissä asiointipalveluissa.
Ammattivarmennetta haetaan sen mukaisesti kuin varmennuskäytännössä on kuvattu.
Muilla mikrosiruilla olevat varmenteet on hinnoiteltu voimassaolevan Digi- ja väestötietoviraston liiketaloudellisia suoritteita koskevan hinnaston mukaisesti.
Varmentaja ei erikseen veloita ammattivarmenteen haltijaa ammattivarmenteiden, sulkupalvelun tai julkisen hakemiston käytöstä. Yksittäiset verkkopalveluntarjoajat saattavat veloittaa oman palvelunsa käytöstä. Ammattivarmenteiden käyttö ei edellytä erillistä ilmoitusta tai lupaa varmentajalta.
Ammattivarmenteen ilmoittaminen sulkulistalle on maksutonta. Myös sulkulistojen noutaminen hakemistosta sekä ammattivarmenteen voimassaolon tarkistaminen sulkulistalta on maksutonta.
Neuvontapalvelun käytöstä peritään erillinen maksu voimassaolevan hinnaston mukaisesti.
Jos palveluntarjoaja haluaa järjestää tietohuoltopalvelun ammattivarmenteiden yksilöivän tunnisteen ja oman taustajärjestelmänsä tunnistetietojen tai muiden päivitystietojen välillä, palveluntarjoaja voi hakea tietopalveluun tietojenluovutuslupaa Digi- ja väestötietovirastolta. Tämä palvelu hinnoitellaan voimassa olevan maksuperustelain ja valtiovarainministeriön asetuksen rekisterihallinnon suoritteista mukaisesti.
Ammattivarmenteen käyttöön liittyvät ohjeet ja käyttöehdot annetaan varmenteen hakijoiden tutkittaviksi ennen varmennetta koskevan sopimuksen ja myöntämispäätöksen tekemistä sekä rekisteröintipisteessä että Digi- ja väestötietoviraston verkkosivuilla.

9.3.5 Varmenteiden jakelu

Varmentaja varmistaa, että varmenteet asetetaan tarvittavalla tavalla tilaajien, allekirjoittajien ja varmenteeseen luottavien osapuolten saataville.
Juurivarmenteen, varmentajan varmenteiden ja varmenteen haltijan varmenteiden tietosisällöt on kuvattu dokumentissa FINEID S2. Dokumentti on saatavilla varmentajan www-sivuilla, www.fineid.fi.
Varmentaja julkaisee ammattivarmenteet ja sulkulistat maksuttomassa, yleisesti saatavilla olevassa julkisessa hakemistossa. Allekirjoitusvarmenteita ei julkaista julkisessa hakemistossa.

Varmentaja julkaisee varmennepolitiikan, varmennuskäytännöt, varmennekuvauksen (PDS) sekä muut julkiset varmennepalvelujen tuottamiseen liittyvät dokumentit www-sivuillaan.
Ammattivarmenne toimitetaan sopimuksen mukaisesti tai julkaistaan julkisessa hakemistossa heti, kun se on luotu, ja se on hakemistossa koko voimassaolonsa ajan. Varmentaja julkaisee sulkulistan, joka on voimassa kaksi tuntia julkaisemisestaan. Tämä sulkulista päivitetään kerran tunnissa uudella sulkulistalla.
Hakemisto- ja sulkulistatiedot ovat yleisesti saatavilla. Varmentajan julkaisemat julkiset FINEID-määritykset ovat saatavilla varmentajan www-sivuilla. Varmennepolitiikat ja varmennuskäytännöt ovat niin ikään saatavilla varmentajan www-sivuilla.
7.3.6 Varmenteen peruuttaminen ja asettaminen keskeytystilaan
Varmentaja varmistaa, että varmenteet peruutetaan oikea-aikaisesti valtuutettujen ja vahvistettujen varmenteiden peruutuspyyntöjen perusteella.

Varmentaja voi sulkea sosiaali- ja terveydenhuollon ammattihenkilön varmenteen, mikäli varmennetta on käytetty tämän varmennepolitiikan, 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.

Varmenteen sulkemista voivat vaatia:
- sosiaali- ja terveydenhuollon ammattihenkilö tai hänen lakisääteinen edustajansa ammattihenkilön oman varmenteen osalta
- varmentaja kohdan 4.9.1 edellytysten täyttyessä

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

1) puhelimitse
2) kirjallisesti varmentajalle.

Varmentaja sulkee viran puolesta varmenteet:

- ammattioikeuden menettämisen perusteella tai
- varmenteen haltijan kuoleman perusteella.

Varmenteen sulkemisesta kirjataan seuraavat tiedot:
- suljettavan varmenteen haltijan käytettävissä olevat henkilötiedot
- etunimet ja sukunimi
- rekisteröintinumero, henkilötunnus
- sulkupyynnön tekijän henkilötiedot (jos eri kuin varmenteen haltija)
- sulkupyynnön tekijän tunnistamistapa
- sulkupyynnön ajankohta
- sulkupyynnön vastaanottajan henkilötiedot
- mahdolliset muut varmenteen haltijan ilmoittamat lisätiedot
- ammattikortin katoamisaika, varmenteenhaltijan kuolinaika tms.
- varmenteen sulkijan henkilötiedot
- varmenteen sulkemisen ajankohta

Digi- ja väestötietovirasto ei tarjoa varmenteen keskeytystilan palvelua.

Varmenteen sulkupyyntö voidaan tehdä puhelimitse sulkupalveluun tai kirjallisesti varmentajalle.

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

Jos sulkupyynnön tekijää ei saada tunnistettua riittävän luotettavasti ja on olemassa riski varmenteen väärinkäyttämisestä, varmentaja asettaa varmenteen sulkemisen etusijalle.
Sulkupyynnön syy kirjataan, kun sulkupyynnön tekee muu kuin varmenteen haltija; varmenteen haltijan ei tarvitse ilmoittaa sulkupyyntönsä syytä.

Varmentaja ei lähetä varmenteen haltijalle erillistä vahvistusta varmenteen sulkemisesta muutoin kuin siinä tapauksessa, että varmenteen sulkeminen johtuu ammattioikeuden menettämisestä.
Varmenne suljetaan varmennejärjestelmän kautta ja varmenteen sulkemiseen liittyvät tiedot säilytetään 5 vuotta sulkemisajankohdasta.

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

Sulkupalvelu käsittelee varmenteen sulkupyynnöt viipymättä.

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

Luottavan osapuolen vastuulla on varmenteen voimassaolon tarkistaminen. Varmenteeseen ei tule luottaa, ellei luottava osapuoli ole suorittanut sulkulistan tarkistusta tai voimassaolotiedon tarkistusta OCSP-palvelusta.
Päivitetty sulkulista julkaistaan tunnin välein.

Sulkulistasta ilmenee seuraavan sulkulistan suunnitelman mukainen julkaisuajankohta. Uusi sulkulista voidaan julkaista myös ennen suunnitelman mukaista julkaisuajankohtaa.
Päivitetty sulkulista on voimassa enintään 72 tuntia. Jokaisessa sulkulistassa on mainittu voimassaolon päättymisajankohta.
Yksityisen avaimen paljastumisesta johtuva varmenteen sulkeminen ei poikkea muilla perusteilla tapahtuvasta varmenteen sulkemisesta.
Varmenteita ei suljeta määräajaksi.
Reaaliaikainen varmenteen tilan tarkistaminen on käytössä.
Varmenteen tilan tarkistaminen tehdään sulkulistan tai OCSP-palvelun avulla. Varmenteeseen luottavan osapuolen on myös tarkistettava, ettei varmenteen voimassaoloaika ole päättynyt.
Varmenne on voimassa joko yleisen voimassaoloajan, varmennekohtaisen määräajan tai kunnes se sulkemisedellytysten täytyttyä suljetaan.
Varmentaja ei talleta ammattihenkilöiden salausavaimia kortin ulkopuolella. Varmenteita ei siten voida käyttää ilman varmenteen haltijan suostumusta eikä yksityisiä avaimia voida palauttaa kortin hajottua tai sen häviämisen yhteydessä.
Ammattivarmenteen sulkupyynnön tekee ensisijaisesti sen haltija. Mikäli soittaja on eri henkilö kuin suljettavan varmenteen haltija, tunnistetaan haltijan lisäksi myös soittaja.
Sulkupyynnön voi tehdä myös varmentaja, kortinvalmistaja tai rekisteröijä. Varmenteen sulkemista pyytäneen henkilön todentamiseen käytetty menetelmä kirjataan.

Varmenteen sulkemisen perusteet, ajankohta ja suorittajan tiedot talletetaan.
Sulkulistan julkaisutiheys
Tieto varmenteen viennistä sulkulistalle on julkisesti saatavilla viimeistään tunnin kuluttua siitä, kun sulkupyyntö on todettu päteväksi ja hyväksytty. Sulkulista on voimassa kaksi tuntia.
Sulkulista sisältää seuraavan sulkulistan julkaisuajankohdan.
Uusi sulkulista julkaistaan viimeistään voimassaolevan sulkulistan voimassaolon päättymisajankohtaan mennessä.
Järjestelmäpäivityksissä ja muissa poikkeavissa tilanteissa DVV voi julkaista sulkulistoja eri julkaisutiheyksillä ja pidennetyillä voimassaoloajoilla.
Varmentaja tarjoaa suorakäyttöisen varmenteen tilan tarkistuspalvelun eli OCSP-palvelun. Varmentaja julkaisee suljetuista varmenteista sulkulistan.

Varmenteiden sulkeminen Digi- ja väestötietoviraston pyynnöstä
Digi- ja väestötietovirasto sulkee varmenteet aina silloin, kun se on saanut tiedon varmenteen haltijan kuolemasta. Digi- ja väestötietovirasto tekee sulkemista koskevan ilmoituksen kuolleen varmenteen haltijan oikeudenomistajille.
Digi- ja väestötietovirasto sulkee myöntämänsä varmenteet, mikäli varmenteiden tietosisällössä havaitaan virhe.
Digi- ja väestötietovirasto voi sulkea käyttämällään yksityisellä avaimellaan allekirjoitetut varmenteet, mikäli on syytä epäillä Digi- ja väestötietoviraston yksityisten avainten paljastuneen tai joutuneen vääriin käsiin.
Kaikki paljastuneella avaimella myönnetyt ja voimassa olevat varmenteet on suljettava yhdellä tai useammalla sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeisen suljetun varmenteen voimassaoloaika on päättynyt.
Mikäli Digi- ja väestötietoviraston varmenteiden luonnissa käyttämä yksityinen avain tai muu tekninen menetelmä on paljastunut tai tullut muutoin käyttökelvottomaksi, Digi- ja väestötietoviraston on ilmoitettava tapahtuneesta kaikille kortinhaltijoille ja Traficomille asianmukaisella tavalla.
Digi- ja väestötietovirasto voi sulkea varmenteen erityisestä syystä.
Varmenteen sulkeminen toteutetaan välittömästi sulkupyynnön yhteydessä.
Avainparin uusiminen varmenteen sulkulistalle asettamisen jälkeen
Ammattivarmenteella olevia julkisia avaimia ja sirulla olevia yksityisiä avaimia ei voi uusia. Suljettuja ammattivarmenteita ei voi palauttaa käyttöön.
Uusien avainparien muodostaminen edellyttää uuden ammattivarmenteen hakemista.
Ammattivarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.
Ammattivarmenteiden voimassaoloa ei voi keskeyttää tilapäisesti, ellei Väestörekisteri-keskuksen ja asiakasorganisaation kanssa tästä menettelystä ole erikseen sovittu.
Varmentajan julkaisemien sulkulistojen tietosisällöt on kuvattu dokumentissa FINEID S2. Dokumentti on saatavilla varmentajan www-sivuilla, www.fineid.fi.
Varmenteen haltijan vastuulla on suojata yksityisten avaintensa käyttö huolehtimalla mikrosirustaan tai kortistaan ja tunnusluvuistaan käyttöehdoissa mainitulla tavalla. Varmenteen haltijan on ilmoitettava varmenteet välittömästi sulkulistalle, mikäli hän epäilee, että sopimusehtojen vastainen käyttö on tullut mahdolliseksi.

9.4 Varmentajan johtamis- ja toimintakäytännöt

9.4.1 Turvallisuuden hallinta

Varmentaja varmistaa, että se noudattaa asianmukaisia ja tunnustettujen standardien mukaisia hallinnollisia ja liikkeenjohdollisia menettelytapoja.

Kyseisissä asiakirjoissa (järjestelmän tietoturvakuvauksissa) yksilöidään kaikki tarjottaviin palveluihin liittyvät asiaankuuluvat kohteet ja mahdolliset uhat sekä suojauskeinot, joilla pyritään välttämään kyseisten uhkien toteutuminen tai rajoittamaan toteutumisen vaikutuksia. Asiakirjoissa kuvataan ne säännöt, ohjeet ja menettelyt, joilla yksilöidyt palvelut ja niiden turvataso toteutetaan, sekä määritellä menettelytavat tietoturvaloukkausten ja hätätilanteiden yhteydessä.
Varmistaja varmistaa tietoturvallisuuden säilymisen, mikäli varmentaja hankkii palveluita toiselta organisaatiolta tai yhteisöltä.
7.4.2 Varantojen luokittelu ja hallinta
Varmentaja varmistaa, että sen tietovarantojen ja tietojen suojaustaso on tarkoituksenmukainen.
Digi- ja väestötietoviraston julkaisemat tiedot ovat saatavilla varmentajan www-sivuilla. Varmennejärjestelmän luottamukselliset tiedot on talletettu varmentajan omaan, luottamukselliseen tietovarastoon. Varmentajan tiedot arkistoidaan voimassaolevien arkistosäännösten mukaisesti. Henkilötietojen käsittelyyn kiinnitetään erityistä huolellisuutta ja Digi- ja väestötietovirasto on julkaissut varmennepalveluiden tuottamisesta erityiset henkilötietolain mukaiset käytännesäännöt. Varmentaja on valmistellut myös varmennejärjestelmän henkilötietolain mukaisen rekisteriselosteen henkilötietojen käsittelyn osalta.
Varmennejärjestelmän tiedot ovat salaisia, elleivät ne perustu henkilötietolain, viranomaisten julkisuudesta annetun lain, väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain tai vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain säännöksiin tietojen luovuttamisesta tai varmennepolitiikassa tai varmennuskäytännössä määriteltyihin tarkoituksiin.
Julkisen hakemiston ja sulkulistan tiedot ovat julkisia, samoin varmennuskäytännöt ja varmennepolitiikassa määritellyt tiedot sekä julkaistut FINEID-määritykset.
Ammattivarmenteen voimassaoloaika on merkitty ammattivarmenteeseen. Kesken voimassaoloajan suljetut ammattivarmenteet julkaistaan yleisesti saatavilla olevalla sulkulistalla.
Viranomaisille luovutettavat tiedot määritellään voimassaolevan lainsäädännön mukaisesti.
Varmennejärjestelmän tietoja ei luovuteta kuin edellä tässä asiakirjassa mainittuihin tarkoituksiin.
Varmenteen haltijalla on oikeus saada häntä koskevia tietoja, esimerkiksi henkilötietoja, voimassaolevan lainsäädännön mukaisesti.
Varmentajan luotettavuuden vuoksi on olennaista, että Digi- ja väestötietovirasto huolehtii kaikin keinoin sille varmennetoiminnan yhteydessä tulevan luottamuksellisen aineiston salassa pitämisestä ja hyvästä tietojenhallintatavasta, ellei viranomaisten oikeudesta saada tietoa varmennejärjestelmän toiminnasta muuta johdu.
Digi- ja väestötietovirasto noudattaa henkilötietojen käsittelyssä henkilötietolakia sekä erityislainsäädäntöä. Digi- ja väestötietovirasto on valmistellut käytännesäännöt sekä tietojen luovuttamisesta että varmennetoiminnan yhteydessä tapahtuvasta henkilötietojen käsittelystä. Henkilötietojen käsittelyssä noudatetaan erityistä huolellisuutta.
Digi- ja väestötietoviraston tuottamat varmennepalvelut ovat sellaisen taloushallinnollisen järjestelmän ja valvonnan piirissä kuin on erikseen säädetty. Varmentajan taloushallinnon toteuttaminen on kuvattu yksityiskohtaisesti varmennuskäytännössä.
Yksityiskohtaiset vaatimukset on kuvattu ISO/IEC 17799 -standardissa.

9.4.2 Henkilöstö ja tietoturva

Varmentaja varmistaa, että henkilöstö ja rekrytointikäytännöt edistävät ja tukevat varmentajan toiminnan luotettavuutta.
Digi- ja väestötietovirasto toimii varmentajana, joka vastaa varmennetoiminnasta. Teknisten palveluiden toimittajien valinta perustuu julkisiin hankintoihin liittyvään kilpailutusmenettelyyn ja ne toimivat Digi- ja väestötietoviraston vastuulla ja lukuun.
Digi- ja väestötietovirasto kiinnittää erityistä huomioita sekä oman henkilökuntansa että teknisten palveluiden toimittajien ja rekisteröijien luotettavuuteen ja tehtävien suorittamiseen tarvittaviin taitoihin.

Digi- ja väestötietovirasto teettää omasta henkilöstöstään sekä teknisten toimittajien varmennetietojärjestelmän kanssa työskentelevistä henkilöistä perusmuotoisen turvallisuusselvityksen.
Henkilökunnan työkokemus kartoitetaan työhönottovaiheessa. Henkilöön kohdistetaan turvallisuusselvitys antamiensa tietojen perusteella määrämuotoisella lomakkeella.
Digi- ja väestötietoviraston henkilökunnan koulutus suunnitellaan ja toteutetaan siten, että tehtävän hoitaminen parhaalla mahdollisella tavalla on mahdollista. Digi- ja väestötietovirastossa on koulutussuunnitelma, jonka toteuttamisesta vastaa Digi- ja väestötietoviraston hallinto ja johdon tuki -yksikkö.
Kun varmentajan tehtävissä suunnitellaan tehtäväkiertoa, tehtävät organisoidaan siten, että henkilö voi huolehtia uusista tehtävistään parhaalla mahdollisella tavalla. Tehtäväkierron toteuttamisessa on otettava huomioon hyvän tietojenhallintatavan säilyminen ja riittävän tehtäväkohtaisen osaamistason ylläpitäminen.
Myös tehtäväkierrossa noudatetaan Digi- ja väestötietoviraston tietoturvapolitiikkaa ja tietoturvasuunnitelmaa sekä Digi- ja väestötietoviraston muita yleisiä ohjeita.
Digi- ja väestötietoviraston henkilökunta toimii tehtävissään virkavastuulla ja Digi- ja väestötietoviraston sisäisten ohjeiden mukaisesti. Virkamiehen asemasta on säännelty valtion virkamieslaissa (750/1994).
Henkilökuntaa rekrytoitaessa on huolehdittava siitä, että henkilökunta vastaa taidoiltaan tehtävän edellyttämiä vaatimuksia ja että henkilön taustaselvityksestä ei ilmene mitään sellaista, että henkilön tehtävät ovat ristiriidassa varmennepalveluiden tuottamisen kanssa.
Henkilökunnalla on aina käytössään Digi- ja väestötietoviraston laatu- ja turvallisuusasiakirjat.

9.4.3 Fyysinen ja ympäristön turvallisuus

Varmentajan on varmistettava, että fyysistä pääsyä kriittisiin palveluihin valvotaan ja että varantoja koskevat fyysiset riskit minimoidaan.
Digi- ja väestötietovirastolle on myönnetty tietoturvasertifikaatti, joka varmentaa, että DVV:n tietoturvallisuus täyttää standardin ISO/IEC 27001 vaatimukset. Digi- ja väestötietovirasto käyttää teknisiä palvelutoimittajia varmennepalvelun tietoteknisten tehtävien hoitamiseen. DVV vastaa varmentajana varmennetuotannon turvallisuudesta ja toiminnasta asianmukaisella tavalla sen kaikilla osa-alueilla.
Varmentajan järjestelmät sijaitsevat korkean turvatason konesalitiloissa ja täyttävät tietokonekeskuksille annetut turvallisuutta koskevat ohjeet ja määräykset.
Toimitilaturvallisuus on toteutettu siten, että asiattomien pääsy toimitiloihin on estetty.
Toimitiloihin, joissa tehdään varmennejärjestelmän tuotannollisia tehtäviä, on valvottu pääsy. Kulunvalvontajärjestelmä havaitsee sekä luvallisen että luvattoman sisäänmenon. Konesalitiloihin vaaditaan henkilön tunnistautuminen, jolloin henkilö tunnistetaan ja pääsyoikeudet tarkistetaan sekä tapahtumat rekisteröidään. Konesalitiloja vartioidaan vuorokauden ympäri.
Laitteistoratkaisut on toteutettu hyvän tiedonhallintatavan mukaisesti siten, että järjestelmän pettäessä voidaan siirtyä käyttämään varajärjestelmää vaarantamatta järjestelmään sisältyvien tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä.
Toiminnan kannalta kriittisten laitteiden varaosien saanti ja huolto on varmistettu.
Varmentajan yksityisen avaimen luominen, aktivointi, varmuuskopiointi ja palauttaminen suoritetaan valvotusti kahden järjestelmän ylläpitotehtäviin oikeutetun henkilön läsnä ollessa.
Varmentajan yksityisen avaimen peruuttaminen on mahdollista vain kahden oikeutetun henkilön valvonnassa.
Varmentajan yksityisen avaimen turvamoduulin alustuksessa on läsnä vähintään kaksi järjestelmän ylläpitotehtäviin oikeutettua henkilöä.
Järjestelmän käyttämiseen vaaditaan yhden tehtävään oikeutetun henkilön läsnäolo.
Ammattivarmenteen rekisteröiminen ja hakijan tunnistaminen vaatii yhden henkilön läsnäolon.

Ammattivarmenteen rekisteröijän, varmennejärjestelmän ylläpitäjän ja varmennejärjestelmän käyttäjän tunnistaminen ja tehtäväkuvaus on kuvattu yksityiskohtaisesti varmennuskäytännössä.

9.4.4 Toiminnan hallinta

Varmentajan on varmistettava, että varmentajan järjestelmät ovat turvalliset ja että niitä käytetään asianmukaisesti toimintahäiriöriskit.

Digi- ja väestötietovirasto käyttää varmennetuotannon rekisteröinti- ja tietoteknisiin tehtäviin teknisiä palvelutoimittajia. Digi- ja väestötietovirasto toimii varmentajana, joka vastaa varmennetoiminnasta.
Varmentajan tehtävät on jaettu tehtävänmukaisiin vastuualueisiin, jotka on kuvattu yksityiskohtaisesti varmennuskäytännössä.
Varmentajan turvallisuudesta vastaava taho johtaa näitä vastuualueita, mutta käytännön toiminnassa käyttöhenkilökunta toteuttaa niitä valvonnan alaisena turvallisuutta koskevan asianmukaisen menettelytapaohjeen sekä roolit ja vastuualueet määrittävien asiakirjojen mukaisesti.
Digi- ja väestötietovirasto tarkastaa teknisten toimittajiensa toimitilat, laitteet ja toiminnan tarkoituksenmukaisella tavalla.
Digi- ja väestötietoviraston tietoturvatarkastuksen tekee Digi- ja väestötietoviraston tietoturvapäällikkö tai ulkopuolinen tarkastaja, joka on erikoistunut varmennepalveluihin liittyvien teknisten toimittajien auditointiin.
Digi- ja väestötietovirastolle on myönnetty tietoturvasertifikaatti, joka varmentaa, että DVV:n tietoturvallisuus täyttää standardin ISO/IEC 27001 vaatimukset.
Tarkastuksen kohteet määräytyvät laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista tai Digi- ja väestötietoviraston suorittaessa tarkastusta tietoturvastandardin ISO/IEC 27001, Digi- ja väestötietoviraston tietoturvapolitiikan tai teknisten toimitussopimusten mukaisesti.
Tarkastus tehdään ottaen huomioon tietoturvan kahdeksan osa-alueen toteutus. Tarkastettavia tietoturvallisuuden ominaisuuksia ovat luottamuksellisuus, eheys ja käytettävyys.
Tarkastuksessa verrataan politiikkaa, varmennuskäytäntöä ja soveltamisohjeita koko varmenneorganisaation ja -järjestelmän toimintaan. Digi- ja väestötietoviraston valvoo, että soveltamisohjeet ovat yhdenmukaiset varmennepolitiikan kanssa.
Tarkastuksissa otetaan huomioon hallinnollisen tietoturvallisuuden lisäksi palveluntoimittajat.
Havaitut poikkeamat kirjataan tarkastusraporttiin ja niihin reagoidaan lain, tietoturvastandardin ISO/IEC 27001 ja voimassaolevien toimitussopimusten mukaisesti.
Tarkastuksen tuloksesta tiedotetaan lain, tietoturvastandardin ISO/IEC 27001, Digi- ja väestötietoviraston tietoturvapolitiikan ja voimassa olevien toimitussopimusten mukaisesti. Sisäiseen käyttöön tarkoitettu yksityiskohtainen määrämuotoinen tarkastustulos on luottamuksellinen eikä siitä anneta tietoja julkisuuteen. Määrämuotoiset raportit laaditaan erikseen organisaation ulkopuoliseen käyttöön.
Digi- ja väestötietovirasto tiedottaa tarkastuksen tuloksista Traficomille vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain sekä Traficomin määräysten ja suositusten mukaisesti.
Allekirjoitusvarmentajia valvova Traficom voi tarkastaa varmentajan toiminnan laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista säädetyin edellytyksin.
Tarkastus kattaa Traficomin antamat määräykset varmentajan toiminnan tietoturvallisuudesta.

9.4.5 Järjestelmiin pääsyn hallinta

Varmentaja varmistaa, että vain asianmukaisesti valtuutetuilla henkilöillä on pääsy varmentajan järjestelmään.

Digi- ja väestötietovirasto pitää yllä tärkeysluokitusta varmennepalveluiden kohteista ja järjestelmistä, niiden varmistamisesta, priorisoinnista ja minimiylläpitotasosta.
Varmennejärjestelmän laitteistoina käytetään vain käyttötarkoitukseensa sopivia laitteistoja.
Järjestelmän kehitys ja testaus tapahtuu erillisessä testiympäristössä. Ainoastaan testatut, toimivat ja hyväksytyt ratkaisut siirretään tuotantojärjestelmään.
Digi- ja väestötietoviraston tietoturvallisuutta hallitaan Digi- ja väestötietoviraston tietoturvapolitiikan ja standardin ISO/IEC 27001 mukaisesti.
Tietoliikenneturvallisuus on toteutettu siten, että varmennejärjestelmän tietoverkko on yhtenäinen kokonaisuus, joka on eriytetty muista tietoverkoista ja jonka kriittiset osat on kahdennettu.

9.4.6 Luotettavien järjestelmien käyttöönotto ja ylläpito

Varmentaja käyttää luotettavia järjestelmiä ja tuotteita, jotka on suojattu muutostöiltä.
Varmentaja ilmoittaa jokaisessa varmennuskäytännössä ne toimenpiteet, joihin varmenteen haltijoiden, varmenteeseen luottavan osapuolen ja rekisteröijien ja varmentajan työntekijöiden on ryhdyttävä, mikäli varmentajan yksityinen avain on paljastunut tai tullut muutoin käyttökelvottomaksi.
Digi- ja väestötietovirastolla on poikkeusoloja koskeva jatkuvuus- ja valmiussuunnitelma, joka mahdollistaa Digi- ja väestötietoviraston toiminnan jatkuvuuden.
Digi- ja väestötietoviraston turvapolitiikassa on otettu huomioon ulkoisen turvallisuuden vaarantumisen aiheuttamat toimenpiteet. Digi- ja väestötietovirasto on saanut ISO 27001 -tietoturvasertifikaatin, joka asettaa vaatimukset Digi- ja väestötietoviraston toiminnalle myös mahdollisen katastrofin tapahduttua.

9.4.7 Varmentajan toiminnan lakkauttaminen

Varmentaja varmistaa, että sen varmennepolitiikan alaisten palvelujen lakkauttamisesta tilaajille ja varmenteeseen luottaville osapuolille aiheutuvat mahdolliset häiriöt minimoidaan ja että sellaisia tietoja ylläpidetään jatkuvasti, joilla varmentamista koskevia todisteita voidaan esittää oikeudellisissa menettelyissä.

9.4.8 Lainsäädäntöön perustuvien vaatimusten noudattaminen

Varmentajan on varmistettava, että lainsäädäntöön perustuvia vaatimuksia noudatetaan.
Yleisölle myönnettäviä varmenteita koskevien sopimusehtojen osalta otetaan huomioon kuluttajalainsäädännön vaatimukset, myös kuluttajasopimusten kohtuuttomista ehdoista annettu direktiivi 93/13/ETY
Tämän varmennepolitiikan mukaisesti myönnetty allekirjoitusvarmenne täyttää Asetuksen mukaiset vaatimukset.
Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009) on säädetty allekirjoitusvarmenteella tehdyistä sähköisistä allekirjoituksista ja vahvan sähköisen tunnistamisen välineestä. Digi- ja väestötietoviraston myöntämistä varmenteista on säädetty väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa (661/2019).
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 vahingonkorvauslakia (412/1974) ja sähköisestä asioinnista viranomaistoiminnassa annettua lakia (13/2003).
Sähköisestä asioinnista viranomaistoiminnassa annetun lain mukaan allekirjoitusvarmenteella voidaan aina asioida viranomaishallinnossa tarjottavissa sähköisissä palveluissa.
Digi- ja väestötietovirasto noudattaa henkilötietolain (523/1999) mukaista henkilötietojen hyvää tietojenkäsittelytapaa ja viranomaisten toiminnan julkisuudesta annetun lain (621/1999) mukaista

hyvää tiedonhallintatapaa. Digi- ja väestötietovirastossa tietoturvallisuus turvataan mm. jatkuvalla koulutuksella. Digi- ja väestötietovirasto on myös valmistellut käytännesäännöt sekä tietopalveluille että varmennepalveluille.
Digi- ja väestötietovirasto hankkii rekisteröintiin ja henkilön tunnistamiseen liittyvät tehtävät erillisellä rekisteröintitoimia koskevalla yksityisoikeudellisella sopimuksella. Digi- ja väestötietovirasto voi hankkia palvelun esimerkiksi noudattamalla julkisen hallinnon yhteispalvelusta annetussa laissa (2007/223) noudatettuja säännöksiä.
Digi- ja väestötietoviraston asemasta on säädetty laissa Digi- ja väestötietovirastosta (304/2019).
Allekirjoitusvarmentajia valvoo Suomessa Traficom.
Valitusten ja riitojen ratkaisussa sekä hallinnollisessa valvonnassa ja lainkäytössä noudatetaan voimassaolevaa lainsäädäntöä. Sosiaali- ja terveydenhuollon ammattivarmenteen liikkeellelaskemisessa huomioon on otettava erityisesti laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista ja siinä kuvattu valvonta- ja muutoksenhallintamenettely.
Digi- ja väestötietovirasto vastaa varmenteita myöntäessään siitä, että sosiaali- ja terveydenhuollon ammattivarmenne täyttää tässä varmennepolitiikassa esitetyt vaatimukset. Mahdolliset erimielisyydet ratkaistaan Suomen oikeusjärjestyksen mukaisesti Helsingin käräjäoikeudessa.

9.4.9 Allekirjoitusvarmenteita koskevan tiedon säilyttäminen

Varmentaja varmistaa, että kaikki allekirjoitusvarmennetta koskevat tiedot tallennetaan tarkoituksenmukaiseksi ajaksi, erityisesti jotta se voi esittää varmentamista koskevia todisteita oikeudellisissa menettelyissä.
Ammattivarmenteen arkistoinnissa sovelletaan yleislakina arkistolain (831/1994) säännöksiä. Oikeus tietojensaantiin määräytyy viranomaisen toiminnan julkisuudesta annetun lain (621/ 1999) mukaisesti. Varmenteiden arkistoinnissa osalta sovelletaan lisäksi, mitä sähköisen asioinnin lainsäädännössä on arkistoinnista määrätty. Varmennerekisterin tiedot säilytetään 5 vuoden ajan varmenteiden voimassaolon päättymisestä.
Varmentajan arkistoimat tiedot on kuvattu yksityiskohtaisesti varmennuskäytännössä.
Arkistotiedot säilytetään varmentajana toimivaa viranomaista koskevien säännösten mukaisesti.
Arkistoitava tieto säilytetään korkean turvatason tiloissa, joissa on pääsynvalvonta.
Varmuuskopiot varastoidaan fyysisesti erilliseen tilaan alkuperäisistä tiedoista.
Varmentaja varmistaa arkistojen tavoitettavuuden ja lukukelpoisuuden siinäkin tapauksessa, että varmentajan toiminta keskeytyy tai päättyy.

9.4.10 Organisaatioon liittyvät vaatimukset

Varmentajan on varmistettava, että sen organisaatio on luotettava.
Digi- ja väestötietovirasto on tämän varmennepolitiikan mukainen varmenteen myöntäjä. Digi- ja väestötietoviraston asemasta on säädetty rekisterihallintolaissa (166/1996) ja asetuksessa (248/1996).
Tämän varmennepolitiikan mukaisesti myönnetty allekirjoitusvarmenne täyttää Asetuksen mukaiset vaatimukset.
Digi- ja väestötietovirasto noudattaa henkilötietolain (523/1999) mukaista henkilötietojen hyvää tietojenkäsittelytapaa ja viranomaisten toiminnan julkisuudesta annetun lain mukaista hyvää tiedonhallintatapaa. Digi- ja väestötietovirastossa tietoturvallisuus turvataan mm. jatkuvalla koulutuksella. Digi- ja väestötietovirasto on myös valmistellut käytännesäännöt sekä tietopalveluille että varmennepalveluille.
Digi- ja väestötietovirasto hankkii rekisteröintiin ja henkilön tunnistamiseen liittyvät tehtävät erillisellä rekisteröintitoimia koskevalla yksityisoikeudellisella sopimuksella. Digi- ja väestötietovirasto

voi hankkia palvelun esimerkiksi noudattamalla julkisen hallinnon yhteispalvelusta annetussa laissa (2007/223) noudatettuja säännöksiä.
Digi- ja väestötietovirasto vastaa siitä, että ammattivarmenteet on luotu noudattaen väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa, laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista, laissa sähköisestä asioinnista viranomaistoiminnassa ja varmennepolitiikassa esitettyjä menettelyjä ja varmenteen hakijan antamien tietojen mukaisesti.
Henkilötietojen käsittely osalta Digi- ja väestötietovirasto noudattaa henkilötietolakia. Digi- ja väestötietovirasto on jatkuvassa yhteistyössä henkilötietojen käsittelyn osalta tietosuojavaltuutetun kanssa.
Valitusten ja riitojen ratkaisussa sekä hallinnollisessa valvonnassa ja lainkäytössä noudatetaan voimassaolevaa lainsäädäntöä. Ammattivarmenteen tuotannossa huomioon on otettava erityisesti laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista ja siinä kuvattu valvonta- ja muutoksenhallintamenettely.
Digi- ja väestötietovirasto vastaa ammattivarmenteita myöntäessään siitä, että ammattivarmenne täyttää tässä ammattivarmennetta koskevassa varmennepolitiikassa esitetyt vaatimukset. Mahdolliset erimielisyydet ratkaistaan Suomen oikeusjärjestyksen mukaisesti.
Ammattivarmenteet on hinnoiteltu voimassaolevan Digi- ja väestötietoviraston liiketaloudellisia suoritteita koskevan hinnaston mukaisesti.

10 Määrittelypuitteet muita allekirjoitusvarmennepolitiikkoja varten

Määritysasiakirjojen hallinta
Tässä kohdassa määritellään allekirjoitusvarmenteita myöntävien varmentajien muita varmennepolitiikkoja koskevat yleiset puitteet.
Digi- ja väestötietoviraston ammattivarmenteet ovat allekirjoitusvarmenteita, minkä vuoksi tätä kohtaa ei sovelleta tämän ammattivarmenteen tarjoamiseen liittyen.

10.1 Allekirjoitusvarmennepolitiikan hallinta

Varmentaja varmistaa, että sen varmennepolitiikka on ajantasainen.
Digi- ja väestötietovirasto voi muuttaa määrityksiä lainsäädännöllisten tai toiminnallisten vaatimusten vuoksi. Määritysten muutokset kirjataan varmennepolitiikka- ja varmennuskäytäntöasiakirjoihin tässä kohdassa kuvatulla tavalla.
Digi- ja väestötietovirasto julkaisee varmennepolitiikan ja varmennuskäytännön, jotka ovat saatavilla Internet-sivuilla ja www.fineid.fi.
Digi- ja väestötietoviraston julkiset varmenteiden tuotantoon liittyvät määritykset ovat saatavilla samoilla Internet-sivuilla.
Tietoteknisten toimittajien kanssa tehdyt varmenteiden toimittamista koskevat sopimukset sekä tuotantojärjestelmien kuvaukset ja tuotteisiin liittyvät määritykset ovat luottamuksellisia.
Digi- ja väestötietovirasto hyväksyy sekä ammattivarmennetta koskevan varmennepolitiikan että varmennuskäytännöt. Asiakirjoja voidaan muuttaa Digi- ja väestötietoviraston sisäisin muutosmenettelyin.
Digi- ja väestötietovirasto ilmoittaa muutoksista hyvissä ajoin ennen niiden voimaantuloa sekä Traficomille että omilla www-sivuillaan.
Digi- ja väestötietovirasto pitää asiakirjoista versionhallintaa sekä arkistoi kaikki varmennepolitiikka- ja varmennuskäytäntöasiakirjat. Typografiset korjaukset ja yhteystietojen muutokset ovat mahdollisia välittömästi.

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

10.2 Poikkeukset allekirjoitusvarmennepolitiikkoihin, jotka koskevat muille kuin yleisölle myönnettäviä allekirjoitusvarmenteita

Mikäli varmenteita myönnetään muille kuin yleisölle, kyseistä toimintaa koskevan allekirjoitusvarmennepolitiikan ei tarvitse noudattaa seuraavia allekirjoitusvarmenteita koskevia menettelytapavaatimuksia:
Digi- ja väestötietoviraston ammattivarmenteet sisältävät yleisölle tarjottavan allekirjoitusvarmenteen ja vahvan sähköisen tunnistamisen välineen. Tämän vuoksi tätä kohtaa ei sovelleta tämän ammattivarmenteen tarjoamiseen liittyen.

10.3 Lisävaatimukset

Tilaajille ja varmenteeseen luottaville osapuolille on ilmoitettava
a) mikäli varmennepolitiikka ei koske yleistä käyttöä
b) mikäli varmennepolitiikka sisältää vaatimuksia turvallisen allekirjoituksen luomisvälineen käytöstä
c) millä tavoin kyseinen politiikka lisää tai tiukentaa tässä asiakirjassa määritellyn allekirjoitusvarmennepolitiikan vaatimuksia.

10.4 Vaatimustenmukaisuus

Varmentaja saa ilmaista toimivansa tämän asiakirjan ja sovellettavan allekirjoitusvarmennepolitiikan mukaisesti vain,
a) jos varmentaja ilmaisee noudattavansa yksilöityä allekirjoitusvarmennepolitiikkaa ja asettaa pyynnöstä tilaajan ja varmenteeseen luottavien osapuolten saataville selvityksen vaatimustenmukaisuudesta tai
Selvityksenä voi olla esimerkiksi auditoijan kertomus, jossa vahvistetaan varmentajan noudattavan yksilöidyn allekirjoitusvarmennepolitiikan vaatimuksia. Kyseessä voi olla varmentajan organisaation sisäinen auditoija, mutta auditoija ei saa olla hierarkkisessa suhteessa varmentajan toimintaa toteuttavaan osastoon.
b) jos pätevä ja riippumaton osapuoli on hiljattain arvioinut yksilöidyn allekirjoitusvarmennepolitiikan vaatimusten noudattamisen nykytilaa varmentajalla. Arviointitulokset on asetettava pyynnöstä tilaajien ja varmenteeseen luottavien osapuolten saataville

[Yksikkö] / Aarnio Ville

6.5.2021