Väestörekisterikeskus
Befolkningsregistercentralen

Varmennepolitiikka Tilapäisvarmennetta varten

OID: 1.2.246.517.1.10.6

ISO 9001

ISO/IEC 27001

Sisällysluettelo

Määritelmät ja lyhenteet

Määritelmät

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

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

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

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

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

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

Mobiilipäätelaite: matkapuhelin tai muu mobiilipäätelaite, jonka avulla voidaan käyttää varmennetta ja mikrosirulla olevia yksityisiä avaimia

Organisaatiovarmenne: Väestörekisterikeskuksen luonnolliselle henkilölle myöntämä laatuvarmenne, jonka tietosisältö on määritelty vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa.

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

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

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

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

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.

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 sekä myös terveydenhuollon ammattihenkilöistä annetun lain 2 §:n 3 momentissa tarkoitettua opiskelijaa ja sosiaalihuollon opiskelijaa.

Sosiaali- ja terveydenhuollon ammattikortti (ammattikortti) VRK: sosiaali- ja terveydenhuollon ammattihenkilölle myöntämä ammattivarmenteen sisältävä toimikortti.

Sosiaali- ja terveydenhuollon henkilöstö: terveydenhuollon ammattihenkilöistä annetussa laissa tarkoitettu terveydenhuollon palvelujen antajien henkilöstö, jotka eivät ole terveydenhuollon ammattihenkilöitä ja henkilöstö, joka ei myöskään ole sosiaalihuollon ammattihenkilöstöä. Kyseiseen henkilöstöryhmään kuuluu esimerkiksi sosiaali- ja terveydenhuollon toimintayksikön tuki-, toimisto- ja tietopalveluhenkilöstö. Sosiaali- ja terveydenhuollon palvelujen antajaorganisaatiossa työskentelevä henkilö, joka ei ole sosiaali- ja terveydenhuollon ammattihenkilö.

Sosiaali- ja terveydenhuollon henkilöstökortti (henkilöstökortti): VRK:n terveydenhuollon muulle henkilöstölle (muut kuin terveydenhuollon ammattihenkilöt) myöntämä varmenteen sisältävä toimikortti.

Sosiaali- ja terveydenhuollon opiskelija: Laillistetun ammattihenkilön tehtävissä voi valtioneuvoston asetuksella säädetyin edellytyksin toimia tilapäisesti myös kyseiseen ammattiin opiskeleva kyseistä ammattia itsenäisesti harjoittamaan oikeutetun laillistetun ammattihenkilön johdon ja valvonnan alaisena. Opiskelijaan sovelletaan tällöin soveltuvin osin, mitä säädetään terveydenhuollon ammattihenkilöstä. Lääketieteen, hammaslääketieteen ja farmasian opiskelijat saavat terveydenhuollon ammattikortin. Muuhun sosiaali- ja terveydenhuollon ammattiin opiskeleva, asetuksella säädetyt työskentelyn edellytykset täyttävä opiskelija saa organisaatiokohtaisen sosiaali- ja terveydenhuollon henkilöstökortin.

Sosiaali- ja terveydenhuollon toimijat: Sosiaali- ja terveydenhuollon alalla toimivien palvelujen antajien työntekijät, joka ei ole sosiaali- ja terveydenhuollon ammattihenkilöitä tai sosiaali- ja terveydenhuollon henkilöstöä. Kyseiseen henkilöstöryhmään kuuluvat muut valtakunnallisia tietojärjestelmiä käyttävät henkilöt ja erityisryhmät, kuten tietosuojavastaavat sekä tietojärjestelmätoimittajat, konsultit jne.

Sosiaali- ja terveydenhuollon toimijakortti (toimijakortti): VRK:n muulle sosiaali- ja terveydenhuollon toimijalle myöntämä varmenteen sisältävä toimikortti.

Tilapäisvarmenne: Väestörekisterikeskuksen luonnolliselle henkilölle myöntämä varmenne, jota voidaan käyttää todentamiseen ja salaukseen tai todentamiseen ja salaukseen sekä sähköiseen allekirjoittamiseen.

Varakortti: Organisaation toimikortin varakortti, jonka tekniseen osaan, mikrosiruun on talletettu kortinhaltijan tilapäisvarmenne. Erityisestä syystä varakortti voidaan myöntää myös henkilölle, jolla ei ole organisaation toimikorttia.

Varmenne: Sähköinen todistus, jonka avulla henkilö voidaan todentaa ja tietoja salata ja 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.

Varmennepolitiikka: Asiakirja, jossa on kuvattu varmenteiden myöntämisessä käytettävät periaatteet sekä varmenteisiin luottavien osapuolten vastuut. Väestörekisterikeskuksen julkaisemat varmennepolitiikat ovat julkisesti saatavilla. Jokaisella varmennepolitiikalla on yksilöivä tunnuksensa.

Varmennerekisteri: Rekisteri, jota varmenteita yleisölle tarjoava varmentaja ylläpitää. Tiedot säilytetään vähintään 10 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: Kuvaus miten varmentaja toteuttaa varmennepolitiikkaa. Jokaisella varmennuskäytännöllä on yksilöivä tunnuksensa.

Varmentaja: Varmenteita myöntävä organisaatio, joka vastaa varmenteiden tuottamisesta sekä laatii toimintaansa kuvaavan varmennepolitiikan sekä varmennuskäytännön.

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 tilapäisvarmennetta 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.

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.

Yksityinen avain: Julkisen avaimen menetelmässä epäsymmetrisessä salauksessa käytettävän avainparin yksityinen osa. Varmenteen haltijan yksityiset avaimet on talletettu mikrosirulle niiden suojaamiseksi oikeudettomalta käytöltä.

Lyhenneluettelo

CA	Certification Authority, varmentaja
CP	Certificate Policy, varmennepolitiikka
CPS	Certification Practise Statement, varmennuskäytäntö
CRL	Certificate Revocation List, sulkulista
FINEID	Finnish Electronic Identification
HSM	Hardware Security Module, turvamoduuli
HST	Henkilön sähköinen tunnistaminen
HTTP	Hypertext Transport Protocol
ISO 27001	ISO/IEC 27001
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
RSA	Rivest, Shamir, Adleman, eräs julkisen avaimen algoritmi, epä symmetrinen algoritmi
VRK	Väestörekisterikeskus

1. Johdanto

Varmennepolitiikka on varmentajan laatima kuvaus menettelytavoista ja toimintaperiaatteista, joita varmenteita myönnettäessä noudatetaan. Varmennuskäytäntö on varmennepolitiikkaa yksityiskohtaisempi kuvaus varmentajan toiminnasta.

Tätä varmennepolitiikkaa sovelletaan Väestörekisterikeskuksen tilapäisvarmenteeseen. Varmenteen tiedot välitetään varmenteeseen luottavan osapuolen käytettäväksi julkiseen hakemistoon tai muulla tavoin asiakasorganisaation kanssa tehtävän sopimuksen mukaisesti.

Tilapäisvarmenne on varmenne, joka tukee Väestörekisterikeskuksen myöntämän organisaatiovarmenteen, OID: 1.2.246.517.1.10.3, käyttöä.

1.1. Yleistä

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 mukaisen varmenteen tietosisältö on määritelty laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista.

Tilapäisvarmenne on todentamis- ja salausvarmenne tai todentamis- ja salausvarmenne sekä allekirjoitusvarmenne. Henkilöllisyyden oikeellisuuden takaa Väestörekisterikeskus.

Tämän politiikan mukainen tilapäisvarmenne voidaan myöntää organisaatioasiakkaalle. Jos organisaatioasiakas rekisteröi tilapäisvarmenteita sosiaali- ja terveydenhuollon henkilöstölle tai sosiaali- ja terveydenhuollon toimijoille tulee kaikkien tässä varmennepolitikassa tarkoitettujen osapuolten noudattaa tämän varmennepolitiikan lisäksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007) ja laissa sähköisestä lääkemääräyksestä (61/2007) sekä niiden nojalla annetuissa säädöksissä ja niiden nojalla asetettuja vaatimuksia.

Varmentajana toimiva Väestörekisterikeskus yksilöi varmenteen haltijan yksilöivän tunnuksen avulla, joka on myös osa varmenteen tietosisältöä. Tunnus on sähköistä asiointia varten erikseen luotu tekninen tunnistetieto, joka ei sisällä henkilöön liittyviä tunnistetietoja. Tilapäisvarmenne voidaan tallentaa erilaisille toimikorteille.

Väestörekisterikeskuksen varmennepolitiikalla ja varmennuskäytännöllä on molemmilla yksilöivä tunnuksensa (OID).

Varmentajan toimintoja ovat varmenne-, hakemisto- ja sulkupalveluiden tuottaminen, rekisteröinti sekä toimikortin valmistus ja yksilöinti. Nämä toiminnot on kuvattu tarkemmin kohdassa 1.3.

Väestörekisterikeskus 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.

Lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009) mukaan Väestörekisterikeskus toimii tunnistuspalvelun tarjoajana tarjotessaan yleisölle varmennepohjaisia tunnistusvälineitä. Tunnistuspalvelun tarjoajia valvoo Suomessa Viestintävirasto.

Väestörekisterikeskus toimii myös 1.12.2010 alkaen terveydenhuollon lakisääteisenä varmentajana sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain, sähköisestä lääkemääräyksestä annetun lain sekä väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain (661/2009) nojalla.

1.2. Tunnistetiedot

Tämän varmennepolitiikan nimi on Varmennepolitiikka Väestörekisterikeskuksen tilapäisvarmennetta varten, jonka OID on 1.2.246.517.1.10.6.

Tämä varmennepolitiikka viittaa juurivarmentajan varmennepolitiikkaan, jonka OID on 1.2.246.517.1.10.1

Sekä varmennepolitiikka että varmennuskäytäntö ovat saatavilla osoitteesta www.fineid.fi.

1.3. Varmentaja ja varmenteiden sovellusalueet

Varmentaja tuottaa varmennepalvelut tässä varmennepolitiikassa mainituin ehdoin ja vastaa niiden toimivuudesta varmenteen haltijalle varmentajan vastuita kuvaavan kohdan 2.2.1 mukaisesti. Varmentaja vastaa koko varmennejärjestelmän toimivuudesta, myös käyttämiensä rekisteröijien ja teknisten toimittajien osalta. Tämän varmennepolitiikan on rekisteröinyt Väestörekisterikeskus. Se on henkilörekisteriä ylläpitävä viranomainen, jonka lain väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista ja sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa ja laissa sähköisestä lääkemääräyksestä mukainen tehtävä on tuottaa varmennettuja sähköisen asioinnin palveluita. Väestörekisterikeskuksen varmennepalvelu jakaantuu toiminnallisesti seuraaviin osa-alueisiin.

1.3.1. Varmentaja

Varmentajan tehtävänä on:

- tarjota varmennepolitiikan ja varmennuskäytännön mukaisia varmenne- ja hakemistopalveluita sekä sulkulistapalveluita
- tunnistaa varmenteen hakija henkilökohtaisesti
- huolehtia varmenteiden tietosisällön virheettömyydestä
- huolehtia varmenteiden sulkemisesta ja varmenteiden sulkulistojen julkaisemisesta
- noudattaa varmenteen haltijoiden henkilötietojen käsittelyssä hyvää tietosuojan tasoa sekä hyvää tietojenkäsittelytapaa.
- luo henkilön yksilöintiä varten asiointitunnuksen
- tarjoaa rekisteröintiä ja sulkemista varten korttien tilaus- ja hallintajärjestelmän.

1.3.2. Rekisteröijä

Tilapäisvarmenteen rekisteröinti tapahtuu noudattaen vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain mukaista ja varmennuskäytäntöasiakirjassa kuvattua menettelytapaa. Organisaation varakortilla olevien tilapäisvarmenteiden rekisteröijänä toimii Väestörekisterikeskuksen kanssa rekisteröintisopimuksen tehnyt yhteistyökumppani. Tarkempi menettelytapa kuvataan kyseessä olevaa teknistä alustaa kuvaavassa varmennuskäytännössä.

- Rekisteröijä toimii varmentajan toimeksiannosta ja vastuulla.

- Rekisteröijä noudattaa varmentajan varmennepolitiikkaa ja varmennuskäytäntöä.
- Rekisteröijä tunnistaa varmenteen hakijan varmennuskäytännön mukaisella tavalla.
- Rekisteröintipiste toimittaa varmenteen hakemiseen liittyvät henkilön tunnistamiseen liittyvät tiedot, joiden perusteella varmenne luodaan.
- Rekisteröijä noudattaa tehtävissään henkilötietojen hyvän käsittelyn periaatteita.
- Väestörekisterikeskus valvoo, että asiakasorganisaatio noudattaa rekisteröintiä koskevia sopimuksessa mainittuja ehtoja ja vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain rekisteröintiä koskevia säännöksiä.
- Rekisteröijä käyttää rekisteröintiin, varakorttien tilaamiseen ja tilapäisvarmenteen sulkemiseen varmentajan tarjoamaa tilaus- ja hallintajärjestelmää.

1.3.3. Varakortin tai mikrosirun valmistaja ja yksilöijä

- Valmistaja ja yksilöijä toimivat varmenteen, siihen liittyvän avainparin ja aktivointitietojen osalta varmentajan toimeksiannosta ja vastuulla ja yhteistyösopimuksen mukaisesti.
- Valmistaja ja yksilöijä noudattavat varmentajan varmennepolitiikkaa ja varmennuskäytäntöä.
- Varakortit ja mikrosirut yksilöidään rekisteröijän toimittamien tietojen mukaisesti.

1.3.4. Sulkupalvelu

Varakorttien osalta ei ole käytössä saman tyyppista varmenteiden sulkupalvelua kuin muilla korteilla, vaan sulkeminen tehdään varmenteen haltijan organisaation rekisteröijän toimesta korttien tilaus- ja hallinnointijärjestelmässä. Suljettavia varmenteita ovat varmenteet, jotka varmenteen haltija haluaa suljettavaksi ennen varmenteen voimassaoloajan päättymistä. Suljetut varmenteet toimitetaan sulkulistalle.

1.3.5. Tilapäisvarmenteen tietojen julkaiseminen

Hakemistopalvelu on julkinen Internet-palvelu, josta on saatavilla varmentajan varmenteet sekä sulkulista. Luotuja tilapäisvarmenteita ei julkaista hakemistossa. Hakemistopalvelu on saatavissa osoitteesta ldap://ldap.fineid.fi.

1.3.6. Varmenteen haltija

Tämän varmennepolitiikan mukaisia tilapäisvarmenteita voidaan myöntää vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain mukaisesti tunnistetuille henkilöille tai terveydenhuollon henkilöstön tai terveydenhuollon toimijoiden ollessa kyseessä tilapäisvarmenteita voidaan sen lisäksi luovuttaa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa lain ja lain sähköisestä lääkemääräyksestä sekä niiden nojalla annetuissa säädöksien ja niiden nojalla asetettujen vaatimuksien mukaisesti. Terveydenhuollon henkilöstön ja terveydenhuollon toimijoiden tilapäisvarmenteen haltijana voi olla ainoastaan terveydenhuollon henkilöstö tai terveydenhuollon toimija.

Varmenteen haltijan tulee noudattaa varmentajan varmennepolitiikkaa ja varmennuskäytäntöä.

1.3.7. Varmenteeseen luottava osapuoli

Varmenteeseen luottava osapuoli on henkilö tai organisaatio, joka luottaa varmenteen tietoihin ja joka käyttää varmennetta todentamiseen ja tiedon salaukseen tai todentamiseen, tiedon salaukseen ja sähköiseen allekirjoittamiseen. Varmenteeseen luottavan osapuolen on tarkastettava, että käytettävä varmenne on voimassa ja varmenne ei ole sulkulistalla.

1.3.8. Varmenteen käyttäminen

Väestörekisterikeskus noudattaa tätä varmennepolitiikkaa myöntäessään tilapäisvarmenteita. Varmenteen haltijoiden ja varmenteeseen luottavien osapuolien tulee toimia tämän varmennepolitiikan mukaisesti.

Tämän varmennepolitiikan mukaista tilapäisvarmennetta voidaan käyttää henkilön todentamiseen ja tiedon salaukseen tai sähköiseen allekirjoittamiseen. Varmennetta voidaan käyttää käyttötarkoituksensa mukaisesti rajoituksitta hallinnollisissa sekä yksityisen organisaation 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.

1.4. Yhteystiedot

1.4.1. Varmennepolitiikkaa hallinnoiva organisaatio

Tämän varmennepolitiikan on rekisteröinyt Väestörekisterikeskus. Se on henkilörekisteriä ylläpitävä viranomainen, jonka väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain ~~(661/2009)~~ mukainen tehtävä on tuottaa muiden tehtäviensä lisäksi varmennettuja sähköisen asioinnin palveluita. Väestörekisterikeskus vastaa tämän varmennepolitiikan hallinnoinnista ja päivityksistä.

Tämän varmennepolitiikan mukaiset tekijänoikeudet kuuluvat Väestörekisterikeskukselle.

1.4.2. Yhteyshenkilö

Tätä varmennepolitiikkaa koskevat kysymykset lähetetään seuraavaan osoitteeseen:

Väestörekisterikeskus (VRK)	vaestorekisterikeskus@vrk.fi
PL 123 (Lintulahdenkuja 4)	Puh. 0295 535 001
00531 Helsinki	Fax. 09 876 4369
Y-tunnus: 0245437-2	

Varmennepolitiikkaan liittyviin kysymyksiin vastaa Väestörekisterikeskuksen Varmennepalvelut-yksikkö.

2. Yleiset ehdot

Tämä varmennepolitiikka astuu voimaan 1.4.2015. Varmennepolitiikan muutosmenettely ja julkaiseminen on kuvattu tämän asiakirjan luvussa 8.

2.1. Velvollisuudet

2.1.1. Varmentajan velvollisuudet

- Väestörekisterikeskuksella on lakisääteinen tehtävä toimia varmentajana.
- Asiakasorganisaatio vastaa omalta osaltaan varmenteiden sulkemisesta VRK:n ja asiakasorganisaation välisen sopimuksen mukaisesti.
- Asiakasorganisaation on tarkastettava loppukäyttäjiä koskevien tietojen oikeellisuus VRK:n ja asiakasorganisaation välisen sopimuksen mukaisesti.
- Varmentaja noudattaa toiminnassaan voimassaolevaa lainsäädäntöä.
- Varmentaja toimii huolellisesti, luotettavasti ja asianmukaisesti.
- Varmentajalla on riittävät tekniset taidot, ja taloudelliset voimavarat sekä mahdollisuus 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 tilapäisvarmenteiden myöntämisessä, ylläpidossa ja hallinnoinnissa käytettävät menettelytavat, käyttöehdot, vastuiden jaot ja muut tilapäisvarmenteen 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 varmennetta ja varmennetoimintaa koskevat tiedot, joiden perusteella varmentajan toiminta ja luotettavuus voidaan arvioida.

2.1.2. Rekisteröijää koskevat velvollisuudet

- 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.
- Rekisteröijä noudattaa varmentajan kanssa sovittuja rekisteröintiin liittyviä menettelytapoja.

2.1.3. Varmenteen haltijaa koskevat velvollisuudet

- Varmenteen käyttötarkoitus on määritelty kunkin varmennetyypin varmennepolitiikassa, varmennuskäytännössä sekä varmenteen haltijan käyttöohjeissa. Varmenteita saa käyttää vain sen käyttötarkoituksen mukaisesti todentamiseen tai tiedon salaamiseen tai sähköiseen allekirjoittamiseen.
- Tilapäisvarmenteen haltija vastaa siitä, että tilapäisvarmenteita haettaessa ilmoitetut tiedot ovat oikeita.
- Tilapäisvarmenteen haltija on vastuussa tilapäisvarmenteen käytöstä, tilapäisvarmenteella tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista.
- Tilapäisvarmenteen haltija säilyttää mikrosirulla olevat yksityisen avaimensa ja sen käyttämiseen tarvittavan tunnusluvun erillään sekä pyrkii estämään yksityisen avaimensa katoamisen, joutumisen ulkopuolisten käsiin, muuttamisen tai luvattoman käytön. Mikrosirun luovuttaminen tai PIN-tunnuksen paljastaminen toiselle henkilölle esim. lainaamalla vapauttaa varmentajan ja tilapäisvarmenteeseen luottavan osapuolen mikrosirun käyttämisestä mahdollisesti aiheutuvista vastuista.
- Tilapäisvarmennetta käsitellään ja suojataan samalla huolellisuudella kuin muita vastaavia mikrosiruja, kortteja tai asiakirjoja, kuten esimerkiksi luottokortteja, ajokorttia ja passia. Henkilökohtaiset PIN-tunnukset on säilytettävä fyysisesti eri paikassa kuin tilapäisvarmenteen ja yksityisen avaimen sisältävä mikrosiru.
- Mikrosirun ja kortin häviämisestä tai väärinkäytön mahdollisuudesta tulee ilmoittaa viipymättä varmenteen haltijan organisaation rekisteröijälle, joka sulkee varmenteen korttien tilaus- ja hallinnointijärjestelmässä.

2.1.4. Tilapäisvarmenteeseen luottavaa osapuolta koskevat velvollisuudet

Varmenteeseen luottavan osapuolen velvollisuus on varmistaa, että varmennetta käytetään sen käyttötarkoituksen mukaisesti. Todentamis- ja salausvarmenteen käyttötarkoitus on henkilön todentaminen ja tiedon salaus. Allekirjoitusvarmenteen käyttötarkoitus on sähköinen allekirjoitus.

Varmenteeseen luottavan osapuolen on noudatettava varmennepolitiikkaa ja varmennuskäytäntöä.

Tilapäisvarmenteeseen luottava osapuoli voi vilpittömässä mielessä luottaa tilapäisvarmenteeseen, kun hän on tarkistanut, että varmenneketju on ehjä, tilapäisvarmenne on voimassa ja että se ei ole sulkulistalla. Tilapäisvarmenteeseen luottavalla osapuolella on velvollisuus tarkistaa varmenteet sulkulistalta. Tilapäisvarmenteen voimassaolon luotettavuuden varmistamiseksi tilapäisvarmenteeseen luottavan osapuolen on noudatettava alla esitettyjä sulkulistan tarkistustoimia.

Jos tilapäisvarmenteeseen 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, tilapäisvarmennetta ei pidä hyväksyä, mikäli viimeisen saadun sulkulistan voimassaoloaika on päättynyt. Kaikki tilapäisvarmenteen hyväksymiset tämän voimassaoloajan jälkeen tapahtuvat tilapäisvarmenteeseen luottavan osapuolen omalla riskillä.

2.1.5. Tilapäisvarmenteen julkaisemiseen liittyvät velvollisuudet

Suljetut tilapäisvarmenteet julkaistaan sulkulistalla, josta varmenteeseen luottavan osapuolen on tarkistettava sen voimassaolotieto. Luotuja tilapäisvarmenteita ei julkaista hakemistossa.

2.2. Vastuut

2.2.1. Varmentajan vastuut

Väestörekisterikeskus vastaa varmentajana koko varmennejärjestelmän turvallisuudesta. Varmentaja vastaa toimeksiantona hankkimistaan palveluista samoin kuin olisi itse tuottanut palvelun.

Väestörekisterikeskus vastaa siitä, että tilapäisvarmenne on luotu noudattaen laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista, varmennepolitiikassa sekä varmennuskäytännössä esitettyjä menettelyjä ja varmenteen hakijan antamien tietojen mukaisesti ja että se täyttää laeissa määritellyt varmentajan vahingonkorvausvastuut tai jos kyseessä on terveydenhuollon henkilöstölle tai terveydenhuollon toimijoille luotava tilapäisvarmenne, niin edellisten lisäksi noudatetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa ja laissa sähköisestä lääkemääräyksestä sekä niiden nojalla annettuja säädöksiä ja niiden nojalla asetettuja vaatimuksia. Väestörekisterikeskus vastaa ainoastaan niistä tiedoista, jotka se on tallettanut varmenteeseen.

Väestörekisterikeskus vastaa siitä, että kun tilapäisvarmennetta käytetään asianmukaisesti, se on käytettävissä luovutushetkestä koko sen voimassaoloajan, ellei sitä ole asetettu sulkulistalle. Tilapäisvarmenne on luovutettu henkilölle, joka on tunnistettu tilapäisvarmenteelta edellytettävällä tavalla. Varmenteen haltijalle on luovutettu ennen sopimuksen allekirjoitusta tilapäisvarmenteen käyttöön liittyvät käyttöohjeet.

Allekirjoittaessaan tilapäisvarmenteen yksityisellä avaimellaan varmentaja vakuuttaa tarkistaneensa tilapäisvarmenteessa olevat henkilötiedot varmennepolitiikassa ja varmennuskäytännössä esitettyjen menettelyjen mukaisesti.

Varmentaja vastaa siitä, että varmenteen haltijan organisaation rekisteröijän sulkemat varmenteet ilmestyvät tässä varmennepolitiikassa mainitussa ajassa sulkulistalle.

2.2.2. Rekisteröijän vastuut

Tilapäisvarmenteen rekisteröijänä toimii rekisteröintipiste, joka rekisteröi varmenteen hakijan varmentajana toimivan Väestörekisterikeskuksen lukuun erikseen tätä toimintaa varten solmitun sopimuksen perusteella. Rekisteröijä vastaa suorittamastaan rekisteröinnistä ja varmenteen sulkemisesta. Rekisteröinnin osalta noudatetaan laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista ja varmennuskäytännössä kuvattuja vaatimuksia tai jos kyseessä on terveydenhuollon henkilöstölle tai terveydenhuollon toimijoille luotava tilapäisvarmenne, niin edellisten lisäksi noudatetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa ja laissa sähköisestä lääkemääräyksestä sekä niiden nojalla annettuja säädöksiä ja niiden nojalla asetettuja vaatimuksia.

2.2.3. Varmenteen haltijan vastuut

Varmenteen haltija on vastuussa tilapäisvarmenteen käytöstä, sillä tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista.

Mikrosirun sisältävän kortin jättäminen lukijalaitteeseen saattaa mahdollistaa tilapäisvarmenteen väärinkäytön. Lopettaessaan pääteistunnon varmenteen haltijan vastuulla on poistaa tilapäisvarmenteen sisältävä mikrosiru lukijalaitteesta ja sulkea käytetyt sovellukset asianmukaisesti tai muuten katkaistava varmenteen käyttämiseksi tarvittava tekninen yhteys.

Varmenteen haltijan vastuu varmenteen käyttämisestä päättyy, kun hän on ilmoittanut varmenteen haltijan organisaation rekisteröijälle tarpeesta sulkea varmenne ja saatuaan ilmoituksen varmenteen sulkupyynnön vastaanottamisesta. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

2.2.4. Tilapäisvarmenteeseen luottavan osapuolen vastuut

Varmenteeseen luottava osapuoli ei voi luottaa tilapäisvarmenteen oikeellisuuteen vilpittömässä mielessä, mikäli tilapäisvarmenteen voimassaoloa ei ole tarkastettu sulkulistalta. Tilapäisvarmenteen hyväksyminen mainitussa tapauksessa vapauttaa Väestörekisterikeskuksen vastuusta. Tilapäisvarmenteeseen luottavan osapuolen on tarkistettava, että myönnetty varmenne vastaa käyttötarkoitustaan siinä oikeustoimessa, jossa sitä on käytetty.

2.2.5. Vastuiden rajoitukset

Varmennepalveluiden tuottamiseen liittyvä Väestörekisterikeskuksen vahingonkorvausvastuu määräytyy vahingonkorvauslain (412/1974) ja soveltuvien sopimusten säännösten mukaisesti.

Väestörekisterikeskus ei vastaa PIN-tunnuksen, varmenteen haltijan yksityisen avainten paljastumisen seurauksena syntyvistä vahingoista, ellei paljastuminen välittömästi johdu Väestörekisterikeskuksen välittömästä toiminnasta.

Väestörekisterikeskus vastaa varmenteen haltijalle ja varmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Väestörekisterikeskuksen välittömästä toiminnasta, kuitenkin enintään 15 % kyseessä olevan asiakasorganisaation edeltävän 3 kuukauden varmennelaskutuksen määrästä (VRK:lle tuloutettava osuus).

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

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

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

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

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

2.3. Taloudellinen vastuu

2.3.1. Varmentaja

Varmennepalveluiden tuottamiseen liittyvä Väestörekisterikeskuksen vahingonkorvausvastuu määräytyy vahingonkorvauslain ja soveltuvien sopimusten säännösten mukaisesti.

Väestörekisterikeskus vastaa varmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista kohdan vastuiden rajoitukset mukaisesti

2.3.2. Muut osapuolet

Tilapäisvarmenteeseen luottava osapuoli voi luottaa tilapäisvarmenteen oikeellisuuteen, jos hän on tarkastanut, että varmenneketju on ehjä, tilapäisvarmennetta ei ole asetettu sulkulistalle, varmenteen voimassaoloaika ei ole päättynyt eikä hänellä ole muita syitä perustellusti epäillä varmenteen käytön oikeellisuutta.

Varmentaja vastaa tilapäisvarmenteesta sen mukaisesti kuin varmentaja on sitoutunut tässä varmennepolitiikassa ja tilapäisvarmennetta koskevassa varmennuskäytännössä.

2.3.3. Varmentajan taloushallinto

Väestörekisterikeskuksen tuottamat varmennepalvelut ovat sellaisen taloushallinnollisen järjestelmän ja valvonnan piirissä kuin on erikseen säädetty.

Varmentajan taloushallinto on kuvattu yksityiskohtaisesti varmennuskäytännössä.

2.4. Tulkinta ja täytäntöönpano

2.4.1. Sovellettava lainsäädäntö

Varmennepalveluiden tuottamiseen liittyvä Väestörekisterikeskuksen vahingonkorvausvastuu määräytyy vahingonkorvauslain ja soveltuvien sopimusten säännösten mukaisesti. Väestörekisterikeskusta koskevat myös lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista mukaiset vaatimukset tai jos kyseessä on sosiaali- ja terveydenhuollon henkilöstölle tai sosiaali- ja terveydenhuollon toimijoille luotava tilapäisvarmenne, niin edellisten lisäksi noudatetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa ja laissa sähköisestä lääkemääräyksestä sekä niiden nojalla annettuja säädöksiä ja niiden nojalla asetettuja vaatimuksia.

Väestörekisterikeskus noudattaa henkilötietolain (523/1999) mukaista henkilötietojen hyvän käsittelyn periaatteita ja viranomaisten toiminnan julkisuudesta annetun lain (621/1999) mukaista hyvää tiedonhallintatapaa. Väestörekisterikeskuksessa tietoturvallisuus turvataan mm. jatkuvalla koulutuksella. Väestörekisterikeskus on myös valmistellut käytännesäännöt sekä tietopalveluille että varmennepalveluille.

Väestörekisterikeskus hankkii rekisteröintiin ja henkilön tunnistamiseen liittyvät tehtävät erillisellä rekisteröintitoimia koskevalla yksityisoikeudellisella sopimuksella. Väestörekisterikeskus voi hankkia palvelun esimerkiksi noudattamalla julkisen hallinnon yhteispalvelusta annetussa laissa (223/2007) noudatettuja säännöksiä.

Väestörekisterikeskuksen asemasta on säädetty rekisterihallintolaissa (166/1996) ja -asetuksessa (248/1996).

Väestörekisterikeskus vastaa siitä, että tilapäisvarmenteet on luotu noudattaen laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista, varmennepolitiikassa ja varmennuskäytännössä esitettyjä menettelyjä noudattaen ja varmenteen hakijan antamien tietojen mukaisesti tai jos kyseessä on terveydenhuollon henkilöstö tai terveydenhuollon toimijoille luotava tilapäisvarmenne, niin edellisten lisäksi noudatetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa ja laissa sähköisestä lääkemääräyksestä sekä niiden nojalla annettuja säädöksiä ja niiden nojalla asetettuja vaatimuksia.

Väestörekisterikeskuksen toimintaa valvoo vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain mukainen valvontaelin Viestintävirasto, joka antaa tarvittavat toimintaa koskevat määräykset ja suositukset.

Henkilötietojen käsittelyn osalta Väestörekisterikeskus noudattaa henkilötietolakia. Väestörekisterikeskus on jatkuvassa yhteistyössä henkilötietojen käsittelyn osalta Tietosuojavaltuutetun kanssa.

Valitusten ja riitojen ratkaisussa sekä hallinnollisessa valvonnassa ja lainkäytössä noudatetaan voimassaolevaa lainsäädäntöä.

2.4.2. Erimielisyyksien ratkaiseminen

Väestörekisterikeskus vastaa varmenteita myöntäessään siitä, että tilapäisvarmenne täyttää tässä tilapäisvarmennetta koskevassa varmennepolitiikassa esitetyt vaatimukset. Mahdolliset erimielisyydet ratkaistaan Suomen oikeusjärjestyksen mukaisesti.

2.5. Maksut

Tässä kappaleessa on määritelty tilapäisvarmenteen käyttöön liittyvät maksut.

2.5.1. Tilapäisvarmenteen myöntäminen ja uusiminen

Tilapäisvarmennetta haetaan sen mukaisesti kuin varmennuskäytännössä on kuvattu.

Varakortin hankintahinta määräytyy kulloinkin voimassa olevan valtiovarainministeriön asetuksen Väestörekisterikeskuksen suoritteiden maksuista mukaisesti.

Tilapäisvarmenteet on hinnoiteltu voimassaolevan Väestörekisterikeskuksen liiketaloudellisia suoritteita koskevan hinnaston mukaisesti.

2.5.2. Tilapäisvarmenteen käyttöön liittyvät maksut

Varmentaja ei erikseen veloita varmenteen haltijaa varmenteiden, sulkupalvelun tai julkisen hakemiston käytöstä. Yksittäiset verkkopalveluntarjoajat saattavat veloittaa oman palvelunsa käytöstä. Varmenteen käyttö ei edellytä erillistä ilmoitusta tai lupaa varmentajalta.

2.5.3. Tilapäisvarmenteen sulkulistamerkintään liittyvät maksut

Tilapäisvarmenteen ilmoittaminen sulkulistalle on maksutonta. Myös sulkulistojen noutaminen hakemistosta sekä tilapäisvarmenteen voimassaolon tarkistaminen sulkulistalta on maksutonta.

2.5.4. Muut maksut

Neuvontapalvelun käytöstä peritään erillinen maksu voimassaolevan hinnaston mukaisesti.

Jos palveluntarjoaja haluaa järjestää tietohuoltopalvelun tilapäisvarmenteiden yksilöivän tunnisteen ja oman taustajärjestelmänsä tunnistetietojen tai muiden päivitystietojen välillä, palveluntarjoaja voi hakea tietopalveluun tietojenluovutuslupaa Väestörekisterikeskukselta. Tämä palvelu hinnoitellaan voimassa olevan maksuperustelain ja valtiovarainministeriön asetuksen Väestörekisterikeskuksen suoritteiden maksuista mukaisesti.

Tilapäisvarmenteen käyttöehdot luovutetaan tilapäisvarmennetta vastaanotettaessa tilapäisvarmenteen haltijalle.

2.6. Tietojen julkaiseminen ja saatavuus

Varmentajan tietojen julkaiseminen

Varmentaja julkaisee varmentajan varmenteet ja sulkulistat maksuttomassa, yleisesti saatavilla olevassa julkisessa hakemistossa. Luotuja tilapäisvarmenteita ei julkaista. Varmentaja julkaisee varmennepolitiikan, varmennuskäytännöt, varmennekuvauksen (PDS) sekä muut julkiset varmennepalvelujen tuottamiseen liittyvät dokumentit www-sivuillaan.

2.6.1 Julkaisutiheys

Varmentaja julkaisee sulkulistan, joka on voimassa kahdeksan tuntia julkaisemisestaan. Tämä sulkulista päivitetään kerran tunnissa uudella sulkulistalla.

2.6.2 Tietojen saatavuus

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.

2.6.3 Tietovarastot

Varmentajan julkaisemat tiedot ovat saatavilla varmentajan www-sivuilla ja tämän varmennepolitiikan mukaisesti julkisessa hakemistossa Varmennejärjestelmän luottamukselliset tiedot on talletettu varmentajan omaan, luottamukselliseen tietovarastoon. Varmentajan tiedot arkistoidaan voimassaolevien arkistosäännösten mukaisesti. Henkilötietojen käsittelyyn kiinnitetään erityistä huolellisuutta. Väestörekisterikeskus on julkaissut varmennepalveluiden tuottamisesta erityiset henkilötietolain mukaiset käytännesäännöt. Varmentaja on valmistellut myös varmennejärjestelmän henkilötietolain mukaisen rekisteriselosteen henkilötietojen käsittelyn osalta.

2.7. Tietoturvatarkastus

Tunnistuspalvelun tarjoajia valvova Viestintävirasto voi tarkastaa tunnistuspalvelun tarjoajan toiminnan laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista säädetyin edellytyksin.

2.7.1. Tarkastusten tiheys

Väestörekisterikeskus tarkastaa teknisten toimittajiensa toimitilat, laitteet ja toiminnan tarkoituksenmukaisella tavalla.

Yksityiskohtainen tarkastusmenettely on kuvattu varmennuskäytännössä.

2.7.2. Tarkastaja

Väestörekisterikeskuksen tietoturvatarkastuksen tekee Väestörekisterikeskuksen tietoturvapäällikkö tai ulkopuolinen tarkastaja, joka on erikoistunut varmennepalveluihin liittyvien teknisten toimittajien auditointiin.

2.7.3. Tarkastuksen kohteet ja kattavuus

Tarkastuksen kohteet määräytyvät laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista tai Väestörekisterikeskuksen suorittaessa tarkastusta tietoturvastandardin ISO/IEC 27001, Väestörekisterikeskuksen tietoturvapolitiikan tai teknisten toimitussopimusten mukaisesti.

Tarkastus tehdään ottaen huomioon tietoturvan kahdeksan osa-alueen toteutus. Tarkastettavia tietoturvallisuuden ominaisuuksia ovat mm. luottamuksellisuus, eheys ja käytettävyys.

Tarkastuksessa verrataan politiikkaa, varmennuskäytäntöä ja soveltamisohjeita koko varmenneorganisaation ja -järjestelmän toimintaan. Väestörekisterikeskus valvoo, että soveltamisohjeet ovat yhdenmukaiset varmennepolitiikan kanssa.

Tarkastuksissa otetaan huomioon hallinnollisen tietoturvallisuuden lisäksi palveluntoimittajat.

Poikkeamista johtuvat toimenpiteet

Havaitut poikkeamat kirjataan tarkastusraporttiin ja niihin reagoidaan lain, tietoturvastandardin ISO/IEC 27001 ja voimassaolevien toimitussopimusten mukaisesti.

2.7.4. Tarkastuksen tuloksesta tiedottaminen

Tarkastuksen tuloksesta tiedotetaan lain, tietoturvastandardin ISO/IEC 27001, Väestörekisterikeskuksen 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.

Väestörekisterikeskus tiedottaa tarkastuksen tuloksista muun muassa Viestintävirastolle.

2.8. Tietojen julkaiseminen

2.8.1. Varmentajan julkaisemat tiedot

Varmennejärjestelmän tiedot ovat luottamuksellisia, elleivät ne perustu henkilötietolain, viranomaisten julkisuudesta annetun lain tai lain väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista tai vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain säännöksiin tietojen luovuttamisesta tai varmennepolitiikassa tai varmennuskäytännössä määriteltyihin tarkoituksiin.

2.8.2. Julkiset tiedot

Julkisen hakemiston ja sulkulistan tiedot ovat julkisia, samoin varmennuskäytännöt ja varmennepolitiikassa määritellyt tiedot sekä julkaistut FINEID-määritykset.

Tilapäisvarmenteen voimassaolon päättymiseen tai keskeyttämiseen liittyvät tiedot

Tilapäisvarmenteen voimassaolon alkamis- ja päätymisajankohta on merkitty tilapäisvarmenteeseen. Kesken voimassaoloajan suljetut varmenteet julkaistaan kaikkien saatavilla olevalla sulkulistalla.

2.8.3. Viranomaisille luovutettavat tiedot

Viranomaisille luovutettavat tiedot määritellään voimassaolevan lainsäädännön mukaisesti.

2.8.4. Muut tiedot

Varmennejärjestelmän tietoja ei luovuteta kuin edellä tässä kappaleessa mainittuihin tarkoituksiin.

2.8.5. Varmenteen haltijan pyynnöstä tapahtuva tiedon luovuttaminen

Varmenteen haltijalla on oikeus saada häntä koskevia tietoja, esimerkiksi henkilötietoja, voimassaolevan lainsäädännön mukaisesti.

2.8.6. Muut tiedon luovuttamiseen liittyvät periaatteet

Varmentajan luotettavuuden vuoksi on olennaista, että Väestörekisterikeskus huolehtii kaikin keinoin sille varmennetoiminnan yhteydessä tulevan luottamuksellisen aineiston salassa pitämisestä ja hyvästä tietojenhallintatavasta, ellei viranomaisten oikeudesta saada tietoa varmennejärjestelmän toiminnasta muuta johdu.

Väestörekisterikeskus noudattaa henkilötietojen käsittelyssä henkilötietolakia sekä erityislainsäädäntöä. Väestörekisterikeskus on valmistellut käytännesäännöt sekä tietojen luovuttamisen että varmennetoiminnan yhteydessä tapahtuvasta henkilötietojen käsittelystä. Henkilötietojen käsittelyssä noudatetaan erityistä huolellisuutta.

2.9. Immateriaalioikeudet

Väestörekisterikeskus omistaa kaikki varmenteisiin ja dokumentaatioon liittyvät tiedot teknisten toimitussopimusten mukaisesti. Väestörekisterikeskus omistaa täydet omistus- ja käyttöoikeudet tähän tilapäisvarmennepolitiikkaan.

3. Varmenteen hakijan tunnistaminen

3.1. Rekisteröinti

Luvussa 4 kohdissa 4.1 - 4.3 esitetään ne käytännöt ja toimintaprosessit, joita noudatetaan varmenteen haltijoiden tunnistamisessa ja todentamisessa.

Hakemusasiakirjassa mainitaan selkeästi, että tilapäisvarmenteiden hakija vahvistaa allekirjoituksellaan annettujen tietojen oikeellisuuden sekä hyväksyy tilapäisvarmenteiden luomisen. Samalla hakija hyväksyy tilapäisvarmenteiden käyttöön liittyvät säännöt ja ehdot sekä huolehtii tilapäisvarmenteiden ja PIN-tunnuksien säilyttämisestä sekä mahdollisen väärinkäytön tai kortin katoamisen ilmoittamisesta.

Varmentajan, rekisteröijän, kortinvalmistajan sekä muiden varmennepalveluiden osa-alueita tuottavien toimittajien kesken on tehty sopimukset, jotka ilmaisevat kiistattomasti kaikkien osapuolten oikeudet, vastuut ja velvoitteet. Tilapäisvarmenteiden hakija vastaa siitä, että kaikki tilapäisvarmenteiden kannalta olennaiset tiedot, jotka tilapäisvarmenteiden hakija on antanut varmentajalle tai rekisteröijälle, ovat oikeita. Tilapäisvarmenteiden haltijan on käytettävä tilapäisvarmenteitaan vain sen käyttötarkoitusten mukaisesti.

Kun varmentaja myöntää tilapäisvarmenteen, se samalla hyväksyy varmennehakemuksen.

Tilapäisvarmenteiden haltijan vastuulla on estää hänelle kuuluvien yksityisten avaimiensa ja siihen liittyvän PIN-tunnuksien käyttäminen käyttöehtojen vastaisella tavalla huolehtimalla niistä käyttöehdoissa mainitulla tavalla.

Varmenteen haltijan on ilmoitettava välittömästi tarpeesta sulkea tilapäisvarmenne varmenteen haltijan organisaation rekisteröijälle, mikäli hän epäilee, että sopimusehtojen vastainen käyttö on tullut mahdolliseksi.

3.1.1. Nimeämiskäytännöt

Nimeämiskäytännöt on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Varmentajan julkinen avain on osa varmentajan varmennetta. Varmentajan varmenne on saatavilla julkisessa hakemistossa. Jos tilapäisvarmenne sijaitsee varakortilla, varmentajan varmenne sijoitetaan myös varakortin mikrosirulle.

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

3.1.2. Yksityisten avainten toimittaminen varmenteen haltijalle

Tilapäisvarmenteeseen liittyvä, mikrosirulla tai muussa turvallisessa ympäristössä luotu yksityinen avain toimitetaan varmenteen haltijalle luovutuksen yhteydessä.

Yksityiskohtainen kuvaus yksityisen avaimen toimittamisesta on kuvattu varmennuskäytännössä.

3.2. Avainparin uusiminen

Tilapäisvarmenteilla olevia julkisia avaimia ja sirulla olevia yksityisiä avaimia ei voida uusia. Uuden avainparin muodostaminen edellyttää uutta tilapäisvarmennetta.

Tilapäisvarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

3.3. Avainparin uusiminen varmenteen sulkulistalle asettamisen jälkeen

Tilapäisvarmenteilla olevia julkisia avaimia ja sirulla olevia yksityisiä avaimia ei voida uusia. Uuden avainparin muodostaminen edellyttää uutta tilapäisvarmennetta.

Tilapäisvarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

3.4. Sulkupyynnön tekijän tunnistaminen

Tilapäisvarmenteen haltija voi halutessaan saada varmenteen suljettavaksi ennen tilapäisvarmenteen voimassaoloajan päättymistä.

Varmenteen sulkemisen tekee varmenteen haltijan organisaation rekisteröijä huomatessaan varmenteen kadonneen tai jos sen väärinkäyttö on tullut mahdolliseksi.

Varmenteen sulkeminen on tehtävä välittömästi, kun on syytä epäillä varmenteen väärinkäyttöä esimerkiksi katoamisen tai anastamisen vuoksi.

Kaikki sulkemiseen liittyvät sähköiset toimenpiteet arkistoidaan.

Varmenteen sulkeminen on kuvattu yksityiskohtaisesti varmennuskäytännössä.

4. Toiminnalliset vaatimukset

4.1. Varmenteen hakeminen

Varmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa ja yleisissä käyttöohjeissa, jotka muodostavat varmenteen hakijan kanssa tehtävän sopimuksen. Hakemusasiakirjassa on tiedot kummankin osapuolen oikeuksista ja velvollisuuksista. Kun tilapäisvarmenteen hakija hakee varmennetta, hän hyväksyy samalla yleiset käyttöehdot.

Hakemusasiakirjassa ja käyttöohjeissa mainitaan selkeästi, että tilapäisvarmenteen hakija hyväksyy nimikirjoituksellaan annettujen tietojen oikeellisuuden sekä varmenteen luomisen. Samalla hakija hyväksyy tilapäisvarmenteen käyttöön liittyvät säännöt ja ehdot sekä huolehtii tilapäisvarmenteiden ja PIN-tunnuksien säilyttämisestä sekä mahdollisen väärinkäytön tai varmenteiden / mikrosirun katoamisen ilmoittamisesta.

4.2. Varmenteen myöntäminen

Varmentaja myöntää tilapäisvarmenteen hyväksyessään varmennehakemuksen. Varmentaja vastaa myöntäessään tilapäisvarmenteen, että sen tietosisältö on oikea varmenteen luovuttamishetkellä.

4.3. Varmenteen vastaanottaminen

Tilapäisvarmenteet noudetaan henkilökohtaisesti rekisteröintipisteestä.

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

4.4. Varmenteen voimassaolon päättyminen ja keskeyttäminen

4.4.1. Varmenteen sulkemisen edellytykset

Tilapäisvarmenne on asetettava sulkulistalle, kun on syytä epäillä väärinkäyttöä esimerkiksi sen katoamisen tai anastamisen vuoksi.

4.4.2. Sulkupyynnön tekijä

Varmenteen sulkemisen tekee varmenteen haltijan organisaation rekisteröijä.

4.4.3. Sulkutapahtuma

Varmenteen sulkeminen voidaan tehdä Väestörekisterikeskuksen tarjoaman korttien tilaus- ja hallinnointijärjestelmän kautta.

Tieto varmenteen viennistä sulkulistalle on julkisesti saatavilla viimeistään tunnin kuluttua siitä, kun sulkupyyntö on todettu päteväksi ja hyväksytty. Sulkulista on voimassa kahdeksan tuntia.

Varmenteen sulkeminen ja sen vaikutukset on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Varmenteiden sulkeminen Väestörekisterikeskuksen pyynnöstä

Väestörekisterikeskus ei suorita varmenteiden sulkemista muissa kuin seuraavissa tapauksissa:

- Väestörekisterikeskus voi sulkea yksityisellä avaimellaan allekirjoitetut varmenteet, mikäli on syytä epäillä Väestörekisterikeskuksen 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 Väestörekisterikeskuksen varmenteiden luonnissa käyttämä yksityinen avain tai muu tekninen menetelmä on paljastunut tai tullut muutoin käyttökelvottomaksi, Väestörekisterikeskuksen on ilmoitettava tapahtuneesta kaikille kortinhaltijoille.
- Väestörekisterikeskus voi sulkea varmenteen myös muusta erityisestä syystä.

4.4.4. Sulkutapahtuman ajoitus

Varmenteen sulkeminen toteutetaan välittömästi sulkupyynnön yhteydessä. Suljettuja tilapäisvarmenteita ei voi palauttaa käyttöön.

4.4.5. Varmenteen voimassaolon keskeyttämiseen liittyvät vaatimukset

Tilapäisvarmenteiden voimassaoloa ei voi keskeyttää tilapäisesti.

4.4.6. Keskeyttämispyynnön tekijä

Tilapäisvarmenteiden voimassaoloa ei voi keskeyttää tilapäisesti.

4.4.7. Keskeyttämispyynnön tekeminen

Tilapäisvarmenteiden voimassaoloa ei voi keskeyttää tilapäisesti.

4.4.8. Keskeyttämisajan rajoitukset

Tilapäisvarmenteiden voimassaoloa ei voi keskeyttää tilapäisesti.

4.4.9. Sulkulistan julkaisutiheys

Tieto varmenteen viennistä sulkulistalle on julkisesti saatavilla viimeistään tunnin kuluttua siitä, kun sulkupyyntö on todettu päteväksi ja hyväksytty. Sulkulista on voimassa kahdeksan tuntia.

Sulkulista sisältää seuraavan sulkulistan julkaisuajankohdan.

Uusi sulkulista julkaistaan viimeistään voimassaolevan sulkulistan voimassaolon päättymisajankohtaan mennessä.

Järjestelmäpäivityksissä ym. poikkeavissa tilanteissa varmentaja voi julkaista sulkulistoja eri julkaisutiheyksillä ja pidennetyillä voimassaoloajoilla.

4.4.10. Sulkulistatarkistukseen liittyvät vaatimukset

Varmenteeseen luottavan osapuolen velvollisuudet on kuvattu kohdassa 2.1.4

4.4.11. Suorakäyttöinen varmenteen tilan tarkistaminen

Varmentaja ei toistaiseksi tarjoa suorakäyttöistä varmenteen tilan tarkistuspalvelua eli OCSP-palvelua. Varmentaja julkaisee suljetuista varmenteista sulkulistan.

4.4.12. Suorakäyttöiseen varmenteen tilan tarkistamiseen liittyvät vaatimukset

Varmentaja ei toistaiseksi tarjoa suorakäyttöistä varmenteen tilan tarkistuspalvelua.

4.4.13. Varmenteen haltijan yksityisen avaimen paljastumista koskevat erityisvaatimukset

Varmenteen haltijan vastuulla on suojata yksityisen avaimensa käyttö huolehtimalla mikrosirustaan tai kortistaan ja tunnusluvustaan käyttöehdoissa mainitulla tavalla. Varmenteen haltijan on ilmoitettava välittömästi tarpeesta sulkea tilapäisvarmenne varmenteen haltijan organisaation rekisteröijälle, mikäli hän epäilee, että sopimusehtojen vastainen käyttö on tullut mahdolliseksi.

4.5. Järjestelmän valvonta

Järjestelmän valvonta on kuvattu varmennuskäytännössä.

4.6. Varmenteisiin liittyvien tietojen arkistointi

4.6.1. Talletettava aineisto

Arkistoinnissa sovelletaan yleislakina arkistolain (831/1994) säännöksiä. Oikeus tietojensaantiin määräytyy viranomaisen toiminnan julkisuudesta annetun lain mukaisesti. Varmenteiden arkistoinnissa osalta sovelletaan lisäksi, mitä sähköisen asioinnin lainsäädännössä on arkistoinnista määrätty. Varmennerekisterin tiedot säilytetään vähintään 10 vuoden ajan varmenteiden voimassaolon päättymisestä tai jos kyseessä on sosiaali- ja terveydenhuollon henkilöstölle tai sosiaali- ja terveydenhuollon toimijoille luotava tilapäisvarmenne, niin edellisten lisäksi noudatetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa ja laissa sähköisestä lääkemääräyksestä sekä niiden nojalla annettuja säädöksiä ja niiden nojalla asetettuja vaatimuksia.

Varmentajan arkistoimat tiedot on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Arkistotiedot säilytetään viranomaista koskevien säännösten mukaisesti.

4.6.2. Arkistojen suojaus

Arkistoitava tieto säilytetään korkean turvatason tiloissa, joissa on pääsynvalvonta.

4.6.3. Arkistotietojen varmistusmenettelyt

Varmuuskopiot varastoidaan fyysisesti erilliseen tilaan alkuperäisistä tiedoista.

4.6.4. Arkistotietojen hankinta- ja varmistusmenetelmät

Varmentaja varmistaa arkistojen tavoitettavuuden ja lukukelpoisuuden siinäkin tapauksessa, että varmentajan toiminta keskeytyy tai päättyy.

4.7. Toiminnan jatkumisen hallinta ja poikkeustapausten käsittely

Väestörekisterikeskuksella on jatkuvuus- ja valmiussuunnitelma, joka mahdollistaa Väestörekisterikeskuksen toiminnan jatkuvuuden.

Poikkeustapauksiin varautuminen on kuvattu varmennuskäytännössä.

4.7.1. Varmentajan yksityinen avain on paljastunut tai varmentajan varmenne on suljettu

Varmentaja ilmoittaa jokaisessa varmennuskäytännössä ne toimenpiteet, joihin varmenteen haltijoiden, varmenteeseen luottavan osapuolen ja rekisteröijien ja varmentajan henkilöiden on ryhdyttävä, mikäli varmentajan yksityinen avain on paljastunut tai tullut muutoin käyttökelvottomaksi.

4.7.2. Turvallisuuden vaarantuminen luonnonmullistuksen tai muun katastrofin seurauksena

Väestörekisterikeskuksen turvapolitiikassa on otettu huomioon ulkoisen turvallisuuden vaarantumisen aiheuttamat toimenpiteet. Väestörekisterikeskus on saanut ISO/IEC 27001 -tietoturvasertifikaatin, joka asettaa vaatimukset Väestörekisterikeskuksen toiminnalle myös mahdollisen katastrofin tapahduttua.

4.8. Varmentajan toiminnan lakkauttaminen

Varmentajan lakkauttamisena pidetään tilannetta, jossa kaikki varmentajan varmenteen myöntämiseen liittyvät palvelut lakkautetaan pysyvästi. Varmentajan lakkauttamisella ei tarkoiteta tilannetta, jossa varmennuspalvelu siirretään organisaatiolta toiselle.

Varmentaja ilmoittaa varmennepalveluiden lakkauttamisesta kohdan 4.7.1 -kohdassa mainituille tahoille mahdollisimman pian, kuitenkin vähintään yhtä kuukautta ennen lakkauttamisen ajankohtaa.

Ennen varmentajan lakkauttamista suoritetaan vähintäänkin seuraavat toimenpiteet:

- Kaikki myönnetyt ja voimassa olevat varmenteet suljetaan yhdellä tai useammalla sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeisten suljetun varmenteen voimassaoloaika on päättynyt.
- Varmentaja lakkauttaa kaikki sopimuskumppaniensa valtuudet suorittaa varmenteiden myöntämisprosessiin liittyviä tehtäviä varmentajan puolesta.
- Varmentaja varmistaa, että kohdassa 4.6 mainittu saatavuus varmentajan arkistoihin säilyy varmentajan lakkauttamisen jälkeenkin.
- Varmentaja huolehtii lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista mukaisten tietojen arkistoinnista sekä noudattaa muutoinkin arkistolain säännöksiä tietojen arkistoinnin osalta tai jos kyseessä on terveydenhuollon henkilöstölle tai terveydenhuollon toimijoille luotava tilapäisvarmenne, niin edellisten lisäksi noudatetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa ~~(159/2007)~~ ja laissa sähköisestä lääkemääräyksestä ~~(61/2007)~~ sekä niiden nojalla annettuja säädöksiä ja niiden nojalla asetettuja vaatimuksia.

5. Fyysiset, toiminnalliset ja henkilöstöturvallisuuteen liittyvät vaatimukset

Väestörekisterikeskukselle on myönnetty tietoturvasertifikaatti, joka varmentaa, että VRK:n tietoturvallisuus täyttää standardin ISO/IEC 27001 vaatimukset.

5.1. Fyysiseen turvallisuuteen liittyvät järjestelyt

Väestörekisterikeskukselle on myönnetty tietoturvasertifikaatti, joka varmentaa, että VRK:n tietoturvallisuus täyttää standardin ISO/IEC 27001 vaatimukset. Väestörekisterikeskus käyttää teknisiä toimittajia varmennepalvelun tietoteknisten tehtävien hoitamiseen. VRK vastaa varmentajana varmennetuotannon turvallisuudesta ja toiminnasta asianmukaisella tavalla sen kaikilla osa-alueilla.

Yksityiskohtainen kuvaus turvallisuuteen liittyvistä järjestelyistä on kuvattu varmennuskäytännössä.

5.1.1. Sijainti ja rakennusten ominaisuudet

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.

5.1.2. Fyysinen pääsy toimitilaan

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.

5.1.3. Varajärjestelyt

Laitteistoratkaisut on toteutettu hyvän tiedonhallintatavan mukaisesti siten, että järjestelmän pettäessä voidaan siirtyä käyttämään varajärjestelmää vaarantamatta järjestelmään sisältyvien tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä.

Tärkeiden laitteiden varaosien saanti ja huolto on varmistettu.

5.2. Toiminnalliset vaatimukset

5.2.1. Vastuunjako

Väestörekisterikeskus käyttää varmennetuotannon rekisteröinti- ja tietoteknisiin tehtäviin teknisiä toimittajia. Väestörekisterikeskus toimii varmentajana, joka vastaa varmennetoiminnasta.

Varmentajan tehtävät on jaettu tehtävänmukaisiin vastuualueisiin, jotka on kuvattu yksityiskohtaisesti varmennuskäytännössä.

5.2.2. Tehtäviin vaadittavien henkilöiden lukumäärä

Varmentajan yksityisen avaimen luominen, aktivointi, varmuuskopiointi ja palauttaminen suoritetaan valvotusti kahden järjestelmän ylläpitotehtäviin oikeutetun henkilön läsnäollessa.

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.

Tilapäisvarmenteen rekisteröiminen ja tunnistaminen vaatii yhden henkilön läsnäolon.

5.2.3. Tehtäväkohtainen tunnistaminen

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

5.3. Henkilöturvallisuus

Väestörekisterikeskus toimii varmentajana, joka vastaa varmennetoiminnasta. Tekniset toimittajat on hankittu kilpailuttamalla ja ne toimivat Väestörekisterikeskuksen vastuulla ja lukuun.

Väestörekisterikeskus kiinnittää erityistä huomioita sekä oman henkilökuntansa että teknisten toimittajien ja rekisteröijien luotettavuuteen ja tehtävien suorittamiseen tarvittaviin taitoihin.

5.3.1. Henkilökuntaa koskevan taustaselvityksen tekeminen

Väestörekisterikeskus teettää omasta henkilöstöstään sekä teknisten toimittajien varmennetietojärjestelmän parissa työskentelevistä henkilöistä perusmuotoisen turvallisuusselvityksen.

5.3.2. Taustaselvityksen tekemisessä noudatettava menettely

Henkilökunnan työkokemus kartoitetaan työhönottovaiheessa. Henkilöön kohdistetaan turvallisuusselvitys antamiensa tietojen perusteella määrämuotoisella lomakkeella.

Turvallisuusselvitysmenettely on kuvattu yksityiskohtaisesti varmennuskäytännössä.

5.3.3. Koulutukseen liittyvät vaatimukset

Väestörekisterikeskuksen henkilökunnan on oltava koulutettu siten, että tehtävän hoitaminen parhaalla mahdollisella tavalla on mahdollista. Väestörekisterikeskuksessa on koulutussuunnitelma, jonka toteuttamisesta vastaa Väestörekisterikeskuksen hallintoyksikkö.

5.3.4. Asiantuntemuksen ja osaamisen ylläpito

Henkilökunnan koulutusta suunnitellaan ja ylläpidetään siten, että tehtävän hoitamiseen liittyvä asiantuntemus on aina tehtävän edellyttämällä tavalla parhaalla mahdollisella tasolla.

5.3.5. Tehtäväkiertoon liittyvät vaatimukset

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 Väestörekisterikeskuksen tietoturvapolitiikkaa ja tietoturvasuunnitelmaa sekä Väestörekisterikeskuksen muita yleisiä ohjeita.

5.3.6. Poikkeamista johtuvat toimenpiteet

Väestörekisterikeskuksen henkilökunta toimii tehtävissään virkavastuulla ja Väestörekisterikeskuksen sisäisten ohjeiden mukaisesti. Virkamiehen asemasta on säännelty valtion virkamieslaissa (750/1994).

5.3.7. Organisaatiota edustava henkilökunta

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.

5.3.8. Henkilökunnan käyttöön annettavat asiakirjat

Henkilökunnalla on aina käytössään Väestörekisterikeskuksen laatu- ja turvallisuusasiakirjat.

6. Tekniset turvajärjestelyt

6.1. Avainparin luominen ja tallettaminen

6.1.1. Avainparin luominen

Varmentaja:

Varmentaja luo yksityiset allekirjoitusavaimensa ja yksityisiä allekirjoitusavaimiaan vastaavat julkiset avaimet. Varmentajan yksityistä avainta säilytetään turvamoduulissa.

Varmenteen haltija:

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

6.1.2. Yksityisen avaimen luovuttaminen varmenteen haltijalle

Varmenteen käyttämiseksi tarvittavia PIN- tunnusluku annetaan varmenteen haltijalle rekisteröinnin yhteydessä.

Varakortin luovuttamisen yhteydessä varmenteen hakija saa haltuunsa sirulle talletetun yksityisen avaimensa.

6.1.3. Varmenteen haltijan julkisen avaimen toimittaminen varmentajalle

Mikrosirun julkisia avaimia käyttäen suoritetaan varmenteen luontipyyntö, jossa varmenteen hakijan rekisteröintitiedot yhdistetään kyseessä olevaan julkiseen avaimeen. Näin syntyy varmenteen haltijan tilapäisvarmenne.

Tilapäisvarmenne sisältää varmenteen haltijan julkisen avaimen.

6.1.4. Varmentajan julkisen avaimen jakelu varmenteen haltijalle

Varmentajan varmenne sisältää varmentajan julkisen avaimen. Varmentajan varmenne talletetaan julkiseen hakemistoon. Varmentajan varmenne on myös saatavilla varmentajan julkisesta hakemistosta sekä varmentajan www-sivuilta.

6.1.5. Avainten pituudet

Tilapäisvarmenteen allekirjoittamiseen käytetty Varmentajan yksityinen avain sekä yksityistä avainta vastaava julkinen avain ovat 2048 -bittisiä RSA-avaimia.

Varmenteen haltijan yksityinen ja julkinen avain ovat 1024 -bittisiä RSA-avaimia.

6.1.6. Avainten käyttötarkoitukset

Varmenteen tietosisällössä käyttötarkoituksen määräävä kenttä määrittelee varmenteisiin liittyvän avaimen käyttötarkoituksen (esimerkiksi todentaminen ja tiedon salaaminen). Avaimen käyttö rajataan vain käyttötarkoitukseensa, todentamiseen ja tiedon salaukseen tarkoitettua avainta tulee siis käyttää vain tähän tarkoitukseen ja allekirjoittamiseen tarkoitettua avainta vain sähköiseen allekirjoittamiseen.

Varmentajan varmenne:

Käyttötarkoitus: Varmenteiden ja sulkulistojen allekirjoitus. Tekninen kuvaus on FI-NEID S2 määrityksissä.

Varmenteen haltijan todentamis- ja salausvarmenne:

Käyttötarkoitus: Sähköisen henkilöllisyyden todentaminen tai tiedon salaus.

Varmenteen haltijan allekirjoitusvarmenne

Käyttötarkoitus: Sähköinen allekirjoitus.

6.2. Yksityisen avaimen suojaus

6.2.1. Turvamoduulia koskevat standardit

Varmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa, jotka täyttävät tarvittavan turvallisuusstandardin vaatimukset.

Varmentaja huolehtii siitä, että varmentajan yksityiset avaimet on suojattu paljastumiselta ja luvattomalta käytöltä. Varmentajan yksityisistä avaimista otetaan varmuuskopio kriittisen tietoturvallisuuden edellyttämällä tavalla.

6.2.2. Varmentajan yksityisen avaimen käsittelyyn osallistuva henkilökunta

Yksityisen avaimen luontiin ja käyttöön liittyvään ympäristöön vaaditaan vähintään kahden henkilön samanaikainen läsnäolo tai toiminnan aktivoiminen.

6.2.3. Yksityisen avaimen luovutus luotetun osapuolen huostaan

Varmenteen haltijoiden yksityinen avain luodaan varmenteelta edellytettävällä tavalla turvallisesti. Varmenteen haltijan itsensä luomia avainpareja ei hyväksytä. Yksityinen avain ei ole siirrettävissä tai kopioitavissa varakortilta. Varmentajalla ja kortinvalmistajalla ei ole pääsyä varmentamiensa henkilöiden yksityisiin avaimiin.

Avainten luontivaiheessa avaimia ei ole vielä kohdistettu kenellekään henkilölle.

6.2.4. Yksityisen avaimen varmuuskopio

Varmentajan yksityiset avaimet ja niiden varmuuskopiot säilytetään vahvasti salattuina kriittisen tietoturvallisuuden vaatimukset täyttävissä laitteissa.

6.2.5. Yksityisen avaimen arkistointi

Varmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa.

6.2.6. Yksityisen avaimen hallinnointi turvamoduuleissa

Varmentajan yksityiset allekirjoitusavaimet suojataan korkean luotettavuuden fyysisillä ja loogisilla turvatoimilla. Niitä käytetään vain turvalliseen ympäristöön sijoitetussa järjestelmässä.

Yksityisen avaimen hallinnointi on kuvattu yksityiskohtaisesti varmennuskäytännössä.

6.3. Muut avaintenhallintaan liittyvät seikat

6.3.1. Julkisen avaimen arkistointi

Varmentaja arkistoi kaikki varmentamansa julkiset avaimet.

6.3.2. Julkisten ja yksityisten avainten käyttöaika

Tilapäisvarmenteen käyttöaika on sopimuksen mukainen, enintään kuitenkin kolme (3) kuukautta. Varmenne voidaan sulkea voimassaoloaikansa kuluessa.

6.4. Aktivointitieto

6.4.1. Aktivointitiedon luominen ja käyttöönotto

Kortinvalmistaja luo avainten käytön mahdollistavan aktivointitiedon eli PIN-tunnuksen.

Yksityiskohtainen menettely on kuvattu varmennuskäytännössä.

6.4.2. Aktivointitiedon suojaus

PIN-tunnus on suojattu niin, ettei sitä voi lukea tai kopioida kortilta. Varmenteen haltijan vastuulla on suojata avaintensa käyttö huolehtimalla mikrosirustaan tai kortistaan ja tunnusluvustaan käyttöehdoissa mainitulla tavalla.

6.4.3. Muut aktivointitietoon liittyvät seikat

Tilapäisvarmenteen haltijalle selvitetään, että hänellä on mahdollisuus vaihtaa alkuperäinen PIN-tunnus uudeksi tunnukseksi. PIN-tunnusluvun vaihto-ohjelma on maksutta kortinhaltijan käytettävissä osoitteessa www.fineid.fi.

Yksityiskohtainen menettely on kuvattu varmennuskäytännössä.

6.5. Tietokoneiden käyttöön ja niihin pääsyyn liittyvät turvallisuusvaatimukset

6.5.1. Laitteistoturvallisuus

Varmennejärjestelmän laitteistoina käytetään vain käyttötarkoitukseensa sopivia laitteistoja.

Yksityiskohtainen menettely on kuvattu varmennuskäytännössä.

6.6. Varmennejärjestelmän elinkaaren hallinta

Väestörekisterikeskus pitää yllä tärkeysluokitusta varmennepalveluiden kohteista ja järjestelmistä, niiden varmistamisesta, priorisoinnista ja minimiylläpitotasosta.

6.6.1. Järjestelmän kehittämiseen liittyvä valvonta

Järjestelmän kehitys ja testaus tapahtuu erillisessä testiympäristössä. Ainoastaan testatut, toimivat ja hyväksytyt ratkaisut siirretään tuotantojärjestelmään.

6.6.2. Turvallisuuden hallinta

Väestörekisterikeskuksen tietoturvallisuutta hallitaan Väestörekisterikeskuksen tietoturvapolitiikan ja standardin ISO/IEC 27001 mukaisesti.

6.7. Tietoverkon turvallisuus

Tietoliikenneturvallisuus on toteutettu siten, että varmennejärjestelmän tietoverkko on yhtenäinen kokonaisuus, joka on eriytetty muista tietoverkoista ja jonka kriittiset osat on kahdennettu.

Tarkempi kuvaus tietoverkon turvallisuudesta on kuvattu varmennuskäytännössä.

6.8. Turvamoduulin käytön valvonta

Varmentaja huolehtii siitä, että varmentajan yksityiset avaimet on suojattu paljastumista ja luvatonta käyttöä vastaan. Varmentajan yksityisistä avaimista otetaan varmuuskopio kriittisen tietoturvallisuuden edellyttämällä tavalla.

Yksityiskohtainen menettely on kuvattu varmennuskäytännössä.

7. Varmenne- ja sulkulistaprofiilit

7.1. Varmenteiden tekniset tiedot

Juurivarmenteen, varmentajan varmenteiden ja varmenteen haltijan varmenteiden tietosisällöt on kuvattu dokumentissa FINEID S2. Dokumentti on saatavilla varmentajan www-sivuilla, www.fineid.fi.

7.2. Sulkulistaprofiili

Varmentajan julkaisemien sulkulistojen tietosisällöt on kuvattu dokumentissa FINEID S2. Dokumentti on saatavilla varmentajan www-sivuilla, www.fineid.fi.

8. Määritysasiakirjojen hallinta

8.1. Määritysten muuttaminen

Varmentaja voi muuttaa määrityksiä lainsäädännöllisten tai toiminnallisten vaatimusten vuoksi. Määritysten muutokset on kirjattava varmennepolitiikka- ja varmennuskäytäntö-asiakirjoihin seuraavassa kuvatulla tavalla.

8.2. Julkaiseminen ja tiedottaminen

Varmentaja julkaisee varmennepolitiikan ja varmennuskäytännön, jotka ovat saatavilla internet-sivuilla www.vaestorekisterikeskus.fi ja www.fineid.fi.

Varmentajan 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.

8.3. Varmennepolitiikan muutos- ja hyväksymismenettely

Väestörekisterikeskus hyväksyy sekä tilapäisvarmennetta koskevan varmennepolitiikan että varmennuskäytännön. Asiakirjoja voidaan muuttaa Väestörekisterikeskuksen sisäisin muutosmenettelyin.

Väestörekisterikeskus ilmoittaa muutoksista hyvissä ajoin ennen niiden voimaantuloa omilla www-sivuillaan.

Väestörekisterikeskus 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 1.4.2015 jälkeen ilmoittamalla tulevista pääasiallisista muutoksista 30 päivää ennen muutosten voimaan astumista.
2. Kohtia, jotka Väestörekisterikeskuksen mielestä eivät merkittävästi vaikuta varmenteiden haltijoihin ja luottaviin osapuoliin, voidaan muuttaa 1.4.2015 jälkeen ilmoittamalla niistä 14 päivää aikaisemmin.

8.4. Versionhallinta

Varmennepolitiikka Väestörekisterikeskuksen tilapäisvarmennetta varten, v. 1.4.

Versio	Päivämäärä	Kuvaus/muutokset
v 1.0	24.10.2008	Hyväksytty versio 1.0.
v 1.01	1.11.2008	Toimitukselliset muutokset
v 1.02	4.7.2009	Toimitukselliset muutokset
v 1.1	1.3.2010	Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009) tulee voimaan 1.3.2010. Väestötietolaki (507/1993) on kumottu. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009), laki on tullut voimaan 1.9.2009. Laki sähköisistä allekirjoituksista (14/2003) on kumottu. Valtiovarainministeriön asetus Väestörekisterikeskuksen suoritteiden maksuista (873/2008), asetus on tullut voimaan 1.1.2009. Toimitukselliset muutokset.
v1.2	1.12.2010	Terveydenhuollon varmentamista koskevat muutokset (Väestörekisterikeskus toimii terveydenhuol-

		lon varmentajana) lakiin sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007), lakiin sähköisestä lääkemääräyksestä (61/2007) ja lakiin väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009) tulevat voimaan 1.12.2010.
v1.2.1	1.12.2010	Toimitukselliset muutokset
v1.3	1.3.2013	Yhteystietojen muutos
v.1.4	1.4.2015	Lainsäädännön muutoksen johdosta Väestörekisterikeskus toimii 1.4.2015 alkaen sosiaalihuollon lakisääteisenä varmentajana. Sosiaalihuollon varmentamisesta johtuvat muutokset päivitetty varmennepolitiikkaan. Lisäksi tehty toimituksellisia muutoksia.