DIGI- JA VÄESTÖTIETO-VIRASTO

VARMENNUSKÄYTÄNTÖ VÄESTÖREKISTERIKESKUKSEN ORGANISAATIOVARMENNE SOPIMUSJAKELU

organisaatiovarmennetta varten, sopimuksen mukainen varmenteen jakelu

OID: 1.2.246.517.1.10.303.2
OID: 1.2.246.517.1.10.303.2

1.6.2021

CERTIFIED SFS ORGANIZATION
ISO 9001

SERTIFIOITU inspecta ORGANISAATIO
ISO/IEC 27001

Dokumentinhallinta

Omistaja	
Laatinut	Ville Aarnio
Tarkastanut	
Hyväksynyt	Mikko Pitkänen

Version hallinta

versionro	mitä tehty	pvm/henkilö
v.1.0	Versio 1.0	1.6.2021/VA

Sisällysluettelo

Määritelmät ja lyhenteet

Määritelmät

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

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.

Allekirjoitusvarmenne: Varmenne, jonka sisältö vastaa laissa allekirjoitusvarmenteelle määriteltyä sisältöä ja jonka lain vaatimukset täyttävä allekirjoitusvarmenteita tarjoava varmentaja on myöntänyt. Allekirjoitusvarmenteen tietosisältö on määritelty vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa.

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

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

Organisaatiovarmenne: Digi- ja väestötietoviraston luonnolliselle henkilölle myöntämä allekirjoitusvarmenne, jonka tietosisältö on määritelty vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa.

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.

RSA-algoritmi ja RSA-avain: RSA-algoritmi on eräs yleisesti käytetty julkisen avaimen algoritmi. Organisaatiovarmenteeseen 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.

Toimikortti: Organisaation toimikortti, jonka tekniseen osaan, mikrosiruun on tallennettu kortinhaltijan organisaatiovarmenne.

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.

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.

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 organisaatiovarmennetta 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 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.

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
ECC	Elliptic Curve Cryptography
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 tilatiedon tarkastuspalvelu
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, epäsymmetrinen algoritmi
DVV	Digi- ja väestötietovirasto

Johdanto

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

Tätä varmennuskäytäntöä sovelletaan toimikortilla olevaan Digi- ja väestötietoviraston organisaatiovarmenteeseen, kun varmenteen tiedot toimitetaan varmenteeseen luottavan osapuolen käytettäväksi asiakasorganisaation kanssa tehtävän sopimuksen mukaisesti. Organisaatiovarmenne on allekirjoitusvarmenne, josta on säädetty laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista.

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

1 Yleistä

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

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 luottamuspalveluista.

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.

Varmentajana toimiva Digi- ja väestötietovirasto 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.

Organisaatiovarmennetta voidaan käyttää erilaisilla toimikorteilla.

Digi- ja väestötietoviraston 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 luvussa 1.3.

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.

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.

Lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista mukaan Digi- ja väestötietovirasto toimii myös tunnistuspalvelun tarjoajana tarjotessaan yleisölle varmennepohjaisia tunnistusvälineitä.

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

Tämän organisaatiovarmenteen myöntämistä kuvaavan varmennuskäytännön on rekisteröinyt Digi- ja väestötietovirasto.

Organisaatiovarmenne 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

Tämä varmennuskäytäntö 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 organisaatiovarmenteeseen 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.

1.1 Tunnistetiedot

Varmentaja laatii varmennepolitiikan jokaiselle myöntämälleen varmennetyypille ja varmennuskäytännön jokaiselle eri tekniselle alustalle, jolla varmennetta voidaan käyttää.

Tämän varmennuskäytännön nimi on Varmennuskäytäntö Digi- ja väestötietoviraston organisaatiovarmennetta varten, sopimuksen mukainen varmenteen jakelu, jonka OID on 1.2.246.517.1.10.303.2 ja 1.2.246.517.1.10.353.2.

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

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

Digi- ja väestötietovirasto noudattaa Asetuksen N:o (EU) 910/2014 luottamuspalveluiden mukaista yleisölle myönnettäviä allekirjoitusvarmenteita koskevaa varmennepolitiikkaa. Asiakirjan viitetiedot ovat ETSI EN 319 411-1 [2] QSCD mukaisesti; OID: 0.4.0.194112.1.2. Tämän varmennepolitiikan mukaisesti myönnettäviä allekirjoitusvarmenteita voi käyttää sellaisten sähköisten allekirjoitusten vahvistamisessa, jotka vastaavat Asetuksessa kuvattuja sähköisten allekirjoitusten 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.

1.2 Varmentaja ja varmenteiden sovellusalueet

Varmentaja tuottaa varmennepalvelut tässä varmennuskäytännössä mainituin ehdoin ja vastaa niiden toimivuudesta varmenteen haltijalle varmentajan vastuita kuvaavan luvun 2.2.1 mukaisesti. Varmentaja vastaa koko varmennejärjestelmän toimivuudesta, myös käyttämiensä rekisteröijien ja teknisten toimittajien osalta. Tämän varmennuskäytännön on rekisteröinyt Digi- ja väestötietovirasto. Digi- ja väestötietovirasto on henkilörekisteriä ylläpitävä viranomainen, jonka väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lainmukainen tehtävä on tuottaa muiden tehtäviensä lisäksi varmennettuja sähköisen asioinnin palveluita. Digi- ja väestötietoviraston varmennepalvelu jakaantuu toiminnallisesti seuraaviin osa-alueisiin:

1.3 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.

1.4 Rekisteröijä

Organisaatiovarmenteen rekisteröinti tapahtuu noudattaen vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaista menettelytapaa. Organisaation toimikortilla olevien organisaatiovarmenteiden rekisteröijänä Digi- ja väestötietoviraston kanssa rekisteröintisopimuksen kanssa tehnyt yhteistyökumppani.

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 periaatteista.

Digi- ja väestötietovirasto valvoo, että asiakasorganisaatio noudattaa rekisteröintiä koskevia sopimuksessa mainittuja ehtoja ja vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain rekisteröintiä koskevia säännöksiä.

1.5 Toimikortin tai mikrosirun valmistaja ja yksilöijä

Valmistaja toimii varmenteen, siihen liittyvien avainparien ja aktivointitietojen osalta varmentajan toimeksiannosta ja vastuulla ja yhteistyösopimuksen mukaisesti.

Varmenteessa henkilön yksilöintiin käytetään organisaation sisäistä tunnusta, jonka käytöstä on sovittu Digi- ja väestötietoviraston kanssa.

Valmistaja noudattaa varmentajan varmennepolitiikkaa ja varmennuskäytäntöä.

Toimikortit ja mikrosirut yksilöidään rekisteröijän toimittamien tietojen mukaisesti.

1.6 Sulkupalvelu

Varmenteiden sulkupalvelu sulkee varmenteet, jotka varmenteen haltija haluaa suljettavaksi ennen varmenteen voimassaoloajan päättymistä. Suljetut varmenteet toimitetaan sulkulistalle.

1.7 Organisaatiovarmenteen tietojen jakaminen varmenteeseen luottavalle osapuolelle

Hakemistopalvelu on julkinen Internet-palvelu, josta on saatavilla varmentajan myöntämät julkiseen hakemistoon tarkoitetut organisaatiovarmenteet ja varmentajan varmenteet sekä sulkulista. Hakemistopalvelu on saatavissa osoitteesta ldap://ldap.fineid.fi.

Varmenteen tiedot välitetään varmenteeseen luottavan osapuolen käytettäväksi asiakasorganisaation kanssa tehtävän sopimuksen mukaisesti.

1.8 Varmenteen haltija

Tämän varmennepolitiikan mukainen organisaatiovarmenne voidaan myöntää vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaisesti tunnistetuille henkilöille.

Varmenteen haltijan tulee noudattaa varmentajan varmennepolitiikkaa ja varmennuskäytäntöä.

1.9 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 ja varmenne ei ole sulkulistalla. Varmenteen voimassaolo voidaan tarkistaa suorakäyttöisestä varmenteen tilatiedon tarkistuspalvelusta eli OCSP-palvelusta.

1.10 Varmenteen käyttäminen

Digi- ja väestötietovirasto noudattaa tätä varmennuskäytäntöä myöntäessään organisaatiovarmennetta. Varmenteen haltijoiden ja varmenteeseen luottavien osapuolien tulee toimia tämän varmennuskäytännön mukaisesti.

Tämän varmennuskäytännön mukaista organisaatiovarmennetta voidaan käyttää henkilön todentamiseen, tiedon salaukseen ja sähköiseen allekirjoitukseen. 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.

1.11 Yhteystiedot

1.12 Varmennuskäytäntöä hallinnoiva organisaatio

Tämän varmennuskäytännön on rekisteröinyt Digi- ja väestötietovirasto (DVV). DVV vastaa tämän varmennuskäytännön hallinnoinnista ja päivityksistä.

Tämän varmennuskäytännön mukaiset tekijänoikeudet kuuluvat Digi- ja väestötietovirastolle.

1.13 Yhteyshenkilö

Tätä varmennuskäytäntöä koskevat kysymykset lähetetään seuraavaan osoitteeseen:

Digi- ja väestötietovirasto

PL 123 (Lintulahdenkuja 2) Puh. +358 295 535 001

00531 Helsinki Fax. +358 9 876 4369

Y-tunnus: 0245437-2 kirjaamo@dvv.fi

Varmennepolitiikkaan liittyviin kysymyksiin vastaa Digi- ja väestötietoviraston kirjaamo, sähköpostiosoite kirjaamo@dvv.fi.

Digi- ja väestötietovirasto (DVV) Varmennepalvelut

PL 123

00531 Helsinki

www.fineid.fi

2 Yleiset ehdot

Tämä varmennuskäytäntö astuu voimaan 1.6.2021.

2.1 Velvollisuudet

2.1.1 Varmentajaa koskevat velvollisuudet

- Digi- ja väestötietovirastolla on lakisääteinen tehtävä toimia varmentajana.
- Asiakasorganisaatio vastaa omalta osaltaan varmenteiden mitätöinnistä DVV:n ja asiakasorganisaation välisen sopimuksen mukaisesti.
- Asiakasorganisaation on tarkastettava loppukäyttäjiä koskevien tietojen oikeellisuus DVV: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 organisaatiovarmenteen myöntämisessä, ylläpidossa ja hallinnoinnissa käytettävät menettelytavat, käyttöehdot, vastuiden jaot ja muut organisaatiovarmenteen 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 laatii ja ylläpitää varmennuskäytäntöjä (CPS), jotka kuvaavat, miten Varmentaja soveltaa varmennepolitiikkaa.
- 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.
- Varmentaja turvaa allekirjoituksen luomistietojen luottamuksellisuuden.
- Varmentaja ei tallenna tai jäljennä allekirjoittajalle luovutettuja allekirjoituksen luomistietoja.

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. Varmennetta saa käyttää vain sen käyttötarkoituksen mukaisesti sähköiseen allekirjoitukseen, todentamiseen tai tiedon salaamiseen.
- Organisaatiovarmenteen haltija vastaa siitä, että organisaatiovarmennetta haettaessa ilmoitetut tiedot ovat oikeita.
- Organisaatiovarmenteen haltija on vastuussa organisaatiovarmenteen käytöstä, organisaatiovarmenteella tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista. Allekirjoitusvarmenteen osalta noudatetaan, mitä Asetuksessa ja laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista on määrätty.
- Organisaatiovarmenteen 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 organisaatiovarmenteeseen luottavan osapuolen mikrosirun käyttämisestä mahdollisesti aiheutuvista vastuista.
- Organisaatiovarmennetta 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 organisaatiovarmenteen ja yksityiset avaimet sisältävä mikrosiru.
- Mikrosirun ja kortin häviämisestä tai väärinkäytön mahdollisuudesta tulee ilmoittaa viipymättä Varmentajalle soittamalla maksuttomaan sulkupalveluun +358 800 162 622. Vastaavasti kuuroille ja kuulovammaisille on oma tekstipuhelinpalvelunumero +358 100 2288.

2.1.4 Varmenteeseen luottavaa osapuolta koskevat velvollisuudet

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.

Organisaatiovarmenteeseen luottava osapuoli voi vilpittömässä mielessä luottaa organisaatiovarmenteeseen, kun hän on tarkistanut, että ***organisaatiovarmenne on voimassa ja että se ei ole sulkulistalla***. Organisaatiovarmenteeseen luottavalla osapuolella on velvollisuus tarkistaa varmenteet sulkulistalta. Varmenteen voimassaolo voidaan tarkistaa suorakäyttöisestä varmenteen tilatiedon tarkistuspalvelusta eli OCSP-palvelusta. Organisaatiovarmenteen voimassaolon luotettavuuden varmistamiseksi Organisaatiovarmenteeseen luottavan osapuolen on noudatettava alla esitettyjä sulkulistan tarkistustoimia.

Jos organisaatiovarmenteeseen 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, organisaatiovarmennetta ei pidä hyväksyä, mikäli viimeisen saadun sulkulistan voimassaoloaika on päättynyt. Kaikki organisaatiovarmenteen hyväksymiset tämän voimassaoloajan jälkeen tapahtuvat organisaatiovarmenteeseen luottavan osapuolen omalla riskillä.

2.1.5 Varmenteen julkaisemiseen liittyvät velvollisuudet

Organisaatiovarmenteet julkaistaan asiakasorganisaation kanssa tehtävän sopimuksen mukaisesti. Suljetut organisaatiovarmenteet julkaistaan sulkulistalla, josta varmenteeseen luottavan osapuolen on tarkistettava sen voimassaolotieto. Varmenteen voimassaolo voidaan tarkistaa suorakäyttöisestä varmenteen tilatiedon tarkistuspalvelusta eli OCSP-palvelusta.

2.2 Vastuut

2.2.1 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 organisaatiovarmenne on luotu noudattaen laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista, laissa sähköisestä asioinnista hallinnossa ja varmennepolitiikassa sekä varmennuskäytännössä esitettyjä menettelyjä ja varmenteen hakijan antamien tietojen mukaisesti ja että se täyttää laeissa määritellyt varmentajan vahingonkorvausvastuut. Digi- ja väestötietovirasto vastaa ainoastaan niistä tiedoista, jotka se on tallettanut varmenteeseen.

Digi- ja väestötietovirasto vastaa siitä, että kun organisaatiovarmennetta käytetään asianmukaisesti, se on käytettävissä luovutushetkestä koko sen voimassaoloajan, ellei sitä ole asetettu sulkulistalle. Organisaatiovarmenne on luovutettu henkilölle, joka on tunnistettu organisaatiovarmenteelta edellytettävällä tavalla. Varmenteen haltijalle on luovutettu ennen sopimuksen allekirjoitusta organisaatiovarmenteen käyttöön liittyvät käyttöohjeet.

Allekirjoittaessaan organisaatiovarmenteen yksityisellä avaimellaan varmentaja vakuuttaa tarkistaneensa organisaatiovarmenteessa olevat henkilötiedot varmennepolitiikassa ja varmennuskäytännössä esitettyjen menettelyjen mukaisesti.

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

2.2.2 Rekisteröijän vastuut

Organisaatiovarmenteen rekisteröijänä toimii rekisteröintipiste, joka rekisteröi varmenteen hakijan varmentajana toimivan Digi- ja väestötietoviraston lukuun erikseen tätä toimintaa varten solmitun sopimuksen perusteella. Rekisteröinnin osalta noudatetaan sähköisen allekirjoituslain vaatimuksia.

2.2.3 Varmenteen haltijan vastuut

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

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

Varmenteen haltijan vastuu organisaatiovarmenteen käyttämisestä päättyy, kun organisaatio tai varmenteen haltija on ilmoittanut sulkupalveluun tarvittavat tiedot organisaatiovarmenteen sulkemiseksi ja saatuaan puhelun vastaanottaneelta virkailijalta sulkemista koskevan ilmoituksen. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

2.2.4 Varmenteeseen luottavan osapuolen vastuut

Varmenteeseen luottava osapuoli ei voi luottaa organisaatiovarmenteen ja sähköisen allekirjoituksen oikeellisuuteen vilpittömässä mielessä, mikäli organisaatiovarmenteen voimassaoloa ei ole tarkastettu sulkulistalta. Varmenteen voimassaolo voidaan tarkistaa suorakäyttöisestä varmenteen tilatiedon tarkistuspalvelusta eli OCSP-palvelusta. Organisaatiovarmenteen hyväksyminen mainitussa tapauksessa vapauttaa Digi- ja väestötietoviraston vastuusta. Organisaatiovarmenteeseen luottavan osapuolen on tarkistettava, että myönnetty varmenne vastaa käyttötarkoitustaan siinä oikeustoimessa, jossa sitä on käytetty.

2.2.5 Vastuiden rajoitukset

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

Digi- ja väestötietovirasto vastaa varmenteen haltijalle ja varmenteeseen luottavalle osapuolelle vain välittömistä vahingoista vahingon euromääräiseen summaan saakka, mikäli vahinko johtuu Digi- ja väestötietoviraston välittömästä toiminnasta kuitenkin enintään 15 % edeltävän 3 kuukauden varmennelaskutuksen määrä (DVV:lle tuloutettava osuus).

Digi- ja väestötietovirasto ei vastaa varmenteen haltijalle aiheutuneista välillisistä tai seurannaisvahingoista. Digi- ja väestötietovirasto ei myöskään vastaa organisaatiovarmenteeseen luottavan osapuolen tai varmenteen 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 varmenteen haltijan käyttämän laitteen tai ohjelmiston 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 luotavan 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 Digi- ja väestötietoviraston vahingonkorvausvastuu määräytyy varmenteen hakijan kanssa tehdyn palvelusopimuksen mukaisesti. Digi- ja väestötietovirastoa koskevat lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista ja sähköisestä asioinnista viranomaistoiminnassa annetun lain mukaiset varmentajan vahingonkorvausvastuut. Soveltuvin osin sovelletaan myös vahingonkorvauslakia (412/1974).

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

2.3.2 Muut osapuolet

Organisaatiovarmenteeseen luottava osapuoli voi luottaa organisaatiovarmenteen ja sähköisen allekirjoituksen oikeellisuuteen, jos hän on tarkastanut, ettei organisaatiovarmennetta ole asetettu sulkulistalle eikä varmenteen voimassaoloaika ole päättynyt eikä hänellä ole muita syitä perustellusti epäillä varmenteen käytön oikeellisuutta.

Varmentaja vastaa organisaatiovarmenteesta sen mukaisesti kuin varmentaja on sitoutunut tässä varmennepolitiikassa ja organisaatiovarmennetta koskevassa varmennuskäytännössä.

2.3.3 Varmentajan taloushallinto

Digi- ja väestötietoviraston tuottamat varmennepalvelut ovat sellaisen taloushallinnollisen järjestelmän ja valvonnan piirissä kuin on erikseen säädetty. Digi- ja väestötietovirasto on valtiovarainministeriön alaisuudessa toimiva virasto. Digi- ja väestötietoviraston taloushallinnon hoito perustuu valtion taloutta ohjaaviin lakeihin ja asetuksiin sekä valtiovarainministeriön ja Valtiokonttorin määräyksiin. Valtiontalouden tarkastusvirasto hoitaa talouden valvonnan. Lisäksi toiminnan tuloksellisuutta kuvataan vaikuttavuuden, taloudellisuuden ja tuottavuuden näkökulmasta.

2.4 Tulkinta ja täytäntöönpano

2.4.1 Sovellettava lainsäädäntö

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 vahvasta sähköisestä tunnistamisesta.

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

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

Sähköisestä asioinnista viranomaistoiminnassa annetun lain mukaan allekirjoitusvarmenteella voidaan aina asioida viranomaishallinnossa.

Digi- ja väestötietovirasto noudattaa henkilötietolain (523/1999) mukaista henkilötietojen hyvän käsittelyn periaatteita 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 asiakaspalvelun järjestämisestä yhteisessä palveluyksikössä annetussa laissa (802/1993) noudatettuja säännöksiä.

Digi- ja väestötietoviraston asemasta on säädetty laissa Digi- ja väestötietovirastosta (304/2019).

Allekirjoitusvarmentajia valvoo Suomessa Traficom.

Digi- ja väestötietovirasto vastaa siitä, että organisaatiovarmenteet on luotu noudattaen laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista, laissa sähköisestä asioinnista viranomaistoiminnassa ja varmennepolitiikassa esitettyjä menettelyjä ja varmenteen hakijan antamien tietojen mukaisesti.

Digi- ja väestötietoviraston varmennepalveluita valvoo vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukainen valvontaelin Traficom, joka antaa määräykset ja suositukset allekirjoitusvarmennetoiminnasta. Digi- ja väestötietovirasto ei tämän vuoksi osallistu vapaaehtoisiin akkreditointijärjestelmiin. 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. Allekirjoitusvarmenteen tuotannossa huomioon on otettava erityisesti laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista ja siinä kuvattu valvonta- ja muutoksenhallintamenettely.

2.4.2 Erimielisyyksien ratkaiseminen

Digi- ja väestötietovirasto vastaa allekirjoitusvarmenteita myöntäessään siitä, että varmenteet täyttävät tässä varmennuskäytännössä sekä organisaatiovarmennetta koskevassa varmennepolitiikassa esitetyt vaatimukset. Mahdolliset erimielisyydet ratkaistaan Suomen oikeusjärjestyksen mukaisesti.

2.4.3 Maksut

Tässä kappaleessa on määritelty organisaatiovarmenteen käyttöön liittyvät maksut.

2.4.4 Organisaatiovarmenteen myöntäminen ja uusiminen

Organisaatiovarmennetta haetaan sen mukaisesti kuin varmennuskäytännössä on kuvattu.

Toimikortin hankintahinta määräytyy kulloinkin voimassa olevan valtiovarainministeriön asetuksen Digi- ja väestötietoviraston suoritteiden maksuista mukaisesti.

Muilla mikrosiruilla olevat organisaatiovarmenteet on hinnoiteltu voimassaolevan Digi- ja väestötietoviraston liiketaloudellisia suoritteita koskevan hinnaston mukaisesti.

2.4.5 Organisaatiovarmenteen 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.

2.4.6 Organisaatiovarmenteen sulkulistamerkintään liittyvät maksut

Organisaatiovarmenteen ilmoittaminen sulkulistalle on maksutonta. Myös sulkulistojen noutaminen hakemistosta sekä organisaatiovarmenteen voimassaolon tarkistaminen sulkulistalta on maksutonta.

2.4.7 Muut maksut

Neuvontapalvelun käytöstä peritään erillinen maksu voimassaolevan hinnaston mukaisesti.

Jos palveluntarjoaja haluaa järjestää tietohuoltopalvelun organisaatiovarmenteiden 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 Digi- ja väestötietoviraston suoritteiden maksuista mukaisesti.

Organisaatiovarmenteen käyttöehdot luovutetaan organisaatiovarmennetta vastaanotettaessa organisaatiovarmenteen haltijalle.

2.5 Tietojen julkaiseminen ja saatavuus

2.5.1 Varmentajan tietojen julkaiseminen

Varmentaja julkaisee varmentajan varmenteet ja sulkulistat maksuttomassa, yleisesti saatavilla olevassa julkisessa hakemistossa. Varmentaja julkaisee varmennepolitiikan, varmennuskäytännöt, varmennekuvauksen (PDS) sekä muut julkiset varmennepalvelujen tuottamiseen liittyvät dokumentit www-sivuillaan. Varmenteen tiedot julkaistaan asiakasorganisaation kanssa tehdyn sopimuksen mukaisesti.

2.5.2 Julkaisutiheys

Varmenteen tiedot julkaistaan asiakasorganisaation kanssa tehdyn sopimuksen mukaisesti.

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

2.5.3 Tietojen saatavuus

Hakemisto- ja sulkulistatietoja ei julkaista julkiseen hakemistoon, vaan ne jaetaan sopimuksen mukaisesti. Varmentajan julkaisemat julkiset FINEID-määritykset ovat saatavilla varmentajan www-sivuilla. Varmennepolitiikat ja varmennuskäytännöt ovat niin ikään saatavilla varmentajan www-sivuilla.

2.5.4 Tietovarastot

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

2.5.5 Tietoturvatarkastus

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

2.5.6 Tarkastusten tiheys

Digi- ja väestötietovirasto tarkastaa teknisten toimittajiensa toimitilat ja laitteet ja toiminnan tarkoituksenmukaisella tavalla. Tarkastus tehdään vähintään kerran vuodessa ja aina, kun uusi sopimuskausi alkaa. Tarkastusmenettelyssä Digi- ja väestötietovirasto noudattaa ISO/IEC 27001 tietoturvastandardin mukaisia menettelytapoja.

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

2.5.7 Tarkastaja

Digi- ja väestötietoviraston tietoturvatarkastuksen tekee Digi- ja väestötietoviraston tietoturvapäällikkö tai ulkopuolinen tarkastaja, joka on erikoistunut varmennepalveluihin liittyvien teknisten toimittajien auditointiin.

2.5.8 Tarkastuksen kohteet ja kattavuus

Tarkastuksen kohteet määräytyvät laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista tai Digi- ja väestötietoviraston suorittaessa tarkastusta tietoturvastandardin ISO/IEC 27001 tai teknisten toimitussopimusten mukaisesti.

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

Tarkastus kattaa Traficomin antamat määräykset tietoturvallisuudesta varmentajalle.

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 eri palveluntoimittajia mm. seuraavan jaottelun mukaisesti:

Sulkupalvelu:

- Tietoliikenneturvallisuus
- Henkilöstöturvallisuus
- Fyysinen turvallisuus

Varmennetuotanto:

- työnjaot ja kunkin tehtävät – henkilöstöturvallisuus
- fyysinen turvallisuus
- CA avaimeen liittyvä turvallisuus
- CA tuotantojärjestelmä ja varajärjestelmä
- Tietoliikenneturvallisuus

Korttituotanto:

- tuotantolinja kokonaisuutena päästä päähän
- laadunvalvonta korttien tuotannossa
- tietoliikenneturvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus

Hakemistopalvelu:

- käytetyt komponentit
- hallintayhteydet
- hakemiston ylläpito ja toiminta vikatilanteissa
- henkilöstöturvallisuus
- tietoliikenneturvallisuus
- fyysinen turvallisuus

HelpDesk -toiminta:

- tietoliikenneturvallisuus
- henkilöstön ammattitaito ja koulutus
- menettelyprosessi erilaisissa aputoiminnoissa

2.5.9 Poikkeamista johtuvat toimenpiteet

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

2.5.10 Tarkastuksen tuloksesta tiedottaminen

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.

2.6 Tietojen julkaiseminen

2.6.1 Varmentajan julkaisemat tiedot

Varmennejärjestelmän tiedot ovat luottamuksellisia, 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.

2.6.2 Julkiset tiedot

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

2.6.3 Organisaatiovarmenteen voimassaolon päättymiseen tai keskeyttämiseen liittyvät tiedot

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

2.6.4 Viranomaisille luovutettavat tiedot

Viranomaisille luovutettavat tiedot määritellään voimassaolevan lainsäädännön mukaisesti.

2.6.5 Muut tiedot

Varmennejärjestelmän tietoja ei luovuteta kuin edellä tässä kappaleessa mainittuihin tarkoituksiin.

2.6.6 Varmenteen haltijan pyynnöstä tapahtuva tiedon luovuttaminen

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

2.6.7 Muut tiedon luovuttamiseen liittyvät periaatteet

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 luovuttamisen että varmennetoiminnan yhteydessä tapahtuvasta henkilötietojen käsittelystä. Henkilötietojen käsittelyssä noudatetaan erityistä huolellisuutta.

2.6.8 Immateriaalioikeudet

Digi- ja väestötietovirasto omistaa kaikki varmenteisiin ja dokumentaatioon liittyvät tiedot teknisten toimitussopimusten mukaisesti. Digi- ja väestötietovirasto omistaa täydet omistus- ja käyttöoikeudet tähän varmennuskäytäntöön ja organisaatiovarmennepolitiikkaan.

3 Varmenteen hakijan tunnistaminen

3.1 Rekisteröinti

Luvuissa 4.1 – 4.3 esitetään ne käytännöt ja toimintaprosessit, joita noudatetaan varmenteen haltijoiden tunnistamisessa ja todentamisessa.

Varmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa ja yleisissä käyttöehdoissa, jotka muodostavat varmenteen hakijan kanssa tehtävän sopimuksen.

Hakemusasiakirjassa ja käyttöehdoissa mainitaan selkeästi, että organisaatiovarmenteen hakija vahvistaa allekirjoituksellaan annettujen tietojen oikeellisuuden sekä hyväksyy organisaatiovarmenteen luomisen ja julkaisun asiakasorganisaation kanssa tehdyn sopimuksen mukaisesti. Samalla hakija hyväksyy organisaatiovarmenteen käyttöön liittyvät säännöt ja ehdot sekä huolehtii organisaatiovarmenteen ja PIN-tunnusten säilyttämisestä sekä mahdollisen väärinkäytön tai kortin katoamisen ilmoittamisesta.

Varmentajan ja rekisteröijän, kortinvalmistajan sekä muiden varmennepalveluiden osa-alueita tuottavien toimittajien kesken on tehty sopimukset, jotka ilmaisevat kiistattomasti kaikkien osapuolten oikeudet, vastuut ja velvoitteet.

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

Kun Varmentaja myöntää organisaatiovarmenteen, se samalla hyväksyy varmennehakemuksen.

Organisaatiovarmenteen 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 organisaatiovarmenteensa sulkupalveluun, mikäli hän epäilee, että sopimusehtojen vastainen käyttö on tullut mahdolliseksi.

3.2 Nimeämiskäytännöt

Digi- ja väestötietoviraston juurivarmentaja on:

CN = DVV Gov. Root CA – G3 RSA

OU = Varmennepalvelut

OU = Certification Authority Services

O = Digi- ja vaestotietovirasto CA

C = FI

ja

CN = DVV Gov. Root CA – G3 ECC

OU = Varmennepalvelut

OU = Certification Authority Services

O = Digi- ja vaestotietovirasto CA

C = FI

Digi- ja väestötietoviraston organisaatiovarmenteiden varmentaja on:

CN (Common name) = DVV Organisational Certificates - G4R

OU (Organizational unit) = Organisaatiovarmenteet

O (Organization) = Digi- ja vaestotietovirasto CA

C (Country) = FI

ja

CN (Common name) = DVV Organisational Certificates - G4E

OU (Organizational unit) = Organisaatiovarmenteet

O (Organization) = Digi- ja vaestotietovirasto CA

C (Country) = FI

Varmenteen haltijan nimeämiskäytäntö organisaatiovarmenteissa:

2.5.4.5 (Serial Number) = Yksilöivä tunniste

SN (Surname) = Sukunimi

G (Given name) = Etunimi

CN (Common name) = Sukunimi Etunimi Yksilöivä tunniste

C (Country) = FI

Valinnaiset kentät:

O (Organization) = Organisaation nimi

OU (OrganizationalUnit) = Organisaatioyksikkö

T (Title) = Nimike

E (EmailAddress) = Sähköpostiosoite

UPN (Universal Principle Name) = UPN nimi

Varmentajan julkinen avain on osa varmentajan varmennetta. Varmentajan varmenne on saatavilla julkisessa hakemistossa. Jos organisaatiovarmenne sijaitsee toimikortilla, varmentajan varmenne sijoitetaan myös toimikortin mikrosirulle.

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

3.3 Yksityisten avainten toimittaminen varmenteen haltijalle

Organisaatiovarmenteeseen 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. Todentamis- ja salausvarmenteesta on Digi- ja väestötietoviraston ja varmennepalveluita tilaavan organisaation välillä solmitun sopimuksen mukaisesti mahdollisuus toteuttaa key escrow-toiminto.

Organisaatiovarmenteen sisältävä toimikortti luovutetaan varmenteen haltijalle vain henkilökohtaisesti tämän käydessä varmentajaa edustavan rekisteröijän luona. Organisaatiovarmenteen haltijan on osoitettava henkilöllisyytensä tavalla, joka vastaa hakemusvaiheessa noudatettua menettelyä. Tunnistustapa merkitään

vastaanottokuittiin, jonka asiakkaan lisäksi allekirjoittaa myös toimikortin luovuttava rekisteröijävirkailija.

Kortinvalmistaja postittaa kortin käytön kannalta välttämättömät perus- ja allekirjoitustunnukset hakemuksessa mainitulle henkilölle hakemuksessa mainittuun osoitteeseen.

3.4 Avainparin uusiminen

Organisaatiovarmenteella olevia julkisia avaimia ja sirulla olevia yksityisiä avaimia ei voi uusia. Uusien avainparien muodostaminen edellyttää uutta organisaatiovarmennetta.

Organisaatiovarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

3.5 Avainparin uusiminen varmenteen sulkulistalle asettamisen jälkeen

Organisaatiovarmenteella olevia julkisia avaimia ja sirulla olevia yksityisiä avaimia ei voi uusia. Uusien avainparien muodostaminen edellyttää uutta organisaatiovarmennetta.

Organisaatiovarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

3.6 Sulkupyynnön tekijän tunnistaminen

Organisaatiovarmenteen haltija voi halutessaan saada varmenteen suljettavaksi ennen organisaatiovarmenteen voimassaoloajan päättymistä.

Sulkupyyntömenettely

Varmenteen sulkupyynnön tekee ensisijaisesti organisaation edustaja huomatessaan varmenteen kadonneen tai jos sen väärinkäyttö on tullut mahdolliseksi. Sulkupyynnön voi kuitenkin tehdä esimerkiksi kortinvalmistaja tai rekisteröijä.

Sulkupyyntö on tehtävä välittömästi, kun on syytä epäillä varmenteen väärinkäyttöä esimerkiksi katoamisen tai anastamisen vuoksi. Organisaatiovarmenne voidaan sulkea soittamalla maksuttomaan yleiseen sulkupalvelunumeroon +358 800 162 622 Kaikki sulkupyynnöt, sulkemisen perusteet, sulkupyynnön tekijän tunnistustapa ja pyyntöä seuranneet varmentajan toimenpiteet arkistoidaan.

3.7 Organisaatiovarmenteen sulkupyynnön tekijän tunnistaminen

Sulkupyynnön tekijän tunnistaminen tapahtuu tarkistamalla soittajan tiedot. Mikäli soittaja on eri henkilö kuin suljettavan varmenteen haltija, tunnistetaan soittajan lisäksi myös varmenteen haltija.

Varmenteen haltijan tunnistetietojen perusteella saadaan selville sulkupyynnön mahdollistava varmenteen yksilöivä tieto.

Mikäli sulkupyynnön tekee rekisteröijä tai kortinvalmistaja, suoritetaan tunnistus luvussa 4.4.3 kuvatulla tavalla.

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 organisaatiovarmenteen hakija hakee varmennetta, hän hyväksyy samalla yleiset käyttöehdot.

Hakemusasiakirjassa ja käyttöohjeissa mainitaan selkeästi, että organisaatiovarmenteen hakija hyväksyy nimikirjoituksellaan annettujen tietojen oikeellisuuden sekä varmenteen luomisen ja julkaisun asiakasorganisaation kanssa tehdyn sopimuksen mukaisesti. Samalla hakija hyväksyy organisaatiovarmenteen käyttöön liittyvät säännöt ja ehdot sekä huolehtii organisaatiovarmenteen ja PIN-tunnusten säilyttämisestä sekä mahdollisen väärinkäytön tai varmenteiden / mikrosirun katoamisen ilmoittamisesta.

Varmentajan ja rekisteröijän, kortinvalmistajan sekä muiden varmennepalveluiden osa-alueita tuottavien toimittajien kesken on tehty sopimukset, jotka ilmaisevat kiistattomasti kummankin osapuolen oikeudet, vastuut ja velvoitteet.

Organisaatiovarmennetta haetaan käymällä henkilökohtaisesti rekisteröijänä toimivassa rekisteröintipisteessä. Varmennetta haettaessa henkilöllisyys tarkistetaan 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. Tieto tunnistustavasta merkitään hakemuslomakkeeseen ja rekisteröintipisteen virkailija vahvistaa omalla allekirjoituksellaan, että henkilöllisyyden tunnistus on tapahtunut. Asiakasorganisaation tehdyn sopimuksen mukaisesti varmennetta voidaan hakea myös Digi- ja väestötietoviraston 31.3.2003 jälkeen myöntämällä allekirjoitusvarmenteella.

4.2 Varmenteen myöntäminen

Varmentaja myöntää organisaatiovarmenteen hyväksyessään varmennehakemuksen.

Varmentaja vastaa myöntäessään organisaatiovarmenteen, että sen tietosisältö on oikea varmenteen luovuttamishetkellä.

4.3 Varmenteen vastaanottaminen

Organisaatiovarmenne toimitetaan varmenteen haltijalle organisaation kanssa tehdyn varmennepalveluiden toimittamista koskevan sovitun menettelytavan mukaisesti. Varmenteen haltijalle annetaan kortin käyttöön liittyvät yleiset käyttöehdot ja ohjeet.

Varmenteen hakijalle korostetaan kortin luovutushetkellä, että kortin sisällä teknisessä osassa luoduista yksityisistä allekirjoitusavaimista ei ole eikä niistä voi myöhemminkään valmistaa kopiota.

4.4 Varmenteen voimassaolon päättyminen ja keskeyttäminen

4.4.1 Varmenteen sulkemisen edellytykset

Organisaatiovarmenne on asetettava sulkulistalle, kun on syytä epäillä väärinkäyttöä esimerkiksi sen katoamisen tai anastamisen vuoksi. Organisaatiovarmenne voidaan sulkea soittamalla maksuttomaan sulkupalvelunumeroon. Sulkupyyntö on tehtävä välittömästi sen jälkeen, kun epäilys väärinkäytön mahdollisuudesta on syntynyt.

Organisaatiovarmenteen haltijan vastuulla on suojata hänelle kuuluvien yksityisten avaintensa ja niihin liittyvien PIN-tunnusten käyttäminen käyttöehtojen vastaiselta tavalta, huolehtimalla kortistaan ja tunnusluvuistaan käyttöehdoissa mainitulla tavalla.

4.4.2 Sulkupyynnön tekijä

Varmenteen sulkupyynnön tekee ensisijaisesti varmenteen haltija tai organisaation yhteyshenkilö. Mikäli soittaja on eri henkilö kuin suljettavan varmenteen haltija, tunnistetaan varmenteen haltijan lisäksi myös varmenteen sulkija.

Sulkupyynnön voi tehdä myös varmentaja, kortinvalmistaja tai rekisteröijä. Varmenteen sulkemista pyytäneen henkilön todentamiseen käytetty menetelmä kirjataan.

Varmenteen sulkemisen perusteet, ajankohta ja suorittajan tiedot talletetaan.

4.4.3 Sulkutapahtuma

Varmenteen sulkeminen voidaan tehdä seuraavilla tavoilla:

Puhelinsoitolla sulkupalveluun

Käymällä rekisteröijän luona

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

Organisaatiovarmenteen sulkeminen

Varmenteenhaltija on vastuussa varmenteiden sulkemisesta. Organisaatiovarmenne voidaan kortinhaltijan ilmoituksesta merkitä sulkulistalle, jolloin sen käyttö estyy. Sen sijaan kortin teknisellä alustalla mahdollisesti olevia muita sovelluksia voidaan edelleen käyttää niiden käyttötarkoitusten mukaisesti.

Varmenne suljetaan soittamalla maksuttomaan yleiseen sulkupalvelunumeroon +358 800 162 622 tai kuulovammaisten tekstipuhelinpalveluun +358 100 2288. Varmenteen haltijan vastuu päättyy, kun sulkemisen mahdollistava yksilöivä ilmoitus on vastaanotettu. Samalla hetkellä päättyy varmenteen haltijan vastuu varmenteen käytöstä. Tarvittaessa ilmoituksen voi tehdä myös muu henkilö, jolloin varmistetaan ilmoittajan henkilöllisyys ja yhteys peruutettavan toimikortin haltijaan.

Sulkupalvelu ilmoittaa varmenteen sulkupyynnön tekijälle saman puhelun aikana sulkupyynnön onnistumisesta.

Mikäli varmenteen haltijalle luovutetun varmenteen sulkupyynnön tekijä on eri henkilö kuin varmenteen haltija ja sulkupyyntö ei johdu varmenteen haltijan yhteydenotosta vamentajaan tai rekisteröijään, ilmoitetaan varmenteen sulkutapahtumasta myös kirjeitse varmenteen haltijalle.

Suljettuja varmenteita ei voi palauttaa käyttöön.

Varmenteen sulkeminen Digi- ja väestötietoviraston toimesta

Digi- ja väestötietovirasto sulkee varmenteet aina silloin, kun varmenteen haltijan kuolemasta on tullut tieto Digi- ja väestötietovirastolle.

Digi- ja väestötietovirasto sulkee myöntämänsä varmenteet, mikäli varmenteiden tietosisällössä havaitaan virhe.

Digi- ja väestötietovirasto voi sulkea 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.

4.4.4 Sulkutapahtuman ajoitus

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

4.4.5 Varmenteen voimassaolon keskeyttämiseen liittyvät vaatimukset

Organisaatiovarmenteiden voimassaoloa ei voi keskeyttää tilapäisesti, ellei Digi- ja väestötietoviraston ja asiakasorganisaation kanssa tästä menettelystä ole erikseen sovittu.

4.4.6 Keskeyttämispyynnön tekijä

Organisaatiovarmenteen voimassaoloa ei voi keskeyttää tilapäisesti, ellei Digi- ja väestötietoviraston ja asiakasorganisaation kanssa tästä menettelystä ole erikseen sovittu.

4.4.7 Keskeyttämispyynnön tekeminen

Organisaatiovarmenteen voimassaoloa ei voi keskeyttää tilapäisesti, ellei Digi- ja väestötietoviraston ja asiakasorganisaation kanssa tästä menettelystä ole erikseen sovittu.

4.4.8 Keskeyttämisajan rajoitukset

Organisaatiovarmenteen voimassaoloa ei voi keskeyttää tilapäisesti, ellei Digi- ja väestötietoviraston ja asiakasorganisaation kanssa tästä menettelystä ole erikseen sovittu.

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.

4.4.10 Sulkulistatarkistukseen liittyvät vaatimukset

Varmenteeseen luottavan osapuolen velvollisuudet on kuvattu luvussa 2.1.4.

4.4.11 Suorakäyttöinen varmenteen tilan tarkistaminen

Organisaatiovarmenne voidaan sulkea vain puhelimitse tai käymällä henkilökohtaisesti rekisteröijän luona. Varmentaja tarjoaa suorakäyttöisen varmenteen tilan tarkistuspalvelun eli OCSP-palvelun.

4.4.12 Suorakäyttöiseen varmenteen tilan tarkistamiseen liittyvät vaatimukset

Varmentaja tarjoaa suorakäyttöisen varmenteen tilatiedon tarkistuspalvelun.

4.4.13 Varmenteen haltijan yksityisen avaimen paljastumista koskevat erityisvaatimukset

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.

4.4.14 Järjestelmän valvonta

Varmentaja tallettaa järjestelmän valvontaa varten lokitietoa varmennetuotannon tapahtumista, varmennejärjestelmän käyttöoikeuksien hallinnasta, laitekokoonpanosta, varusohjelmista ja sovellusohjelmista muutoksineen, varmistuksista sekä niiden palautuksista. Varmentaja valvoo myös toimintaan liittyviä asiakirjoja. Havaituista poikkeamista raportoidaan sovitulla tavalla.

4.5 Allekirjoitusvarmenteisiin liittyvien tietojen arkistointi

4.5.1 Talletettava aineisto

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 arkistoi seuraavat tiedot:

a) Hakijan allekirjoittaman hakulomakkeen, tositteen toimikortin ja siihen liittyvien yleisten käyttöehtojen vastaanottamisesta.

b) Myönnetyt varmenteet, niiden tietosisältö ja elinkaaren hallintaan liittyvät lisätiedot siitä hetkestä, kun varmenteen voimassaoloaika on päättynyt tai siitä kun varmenne on suljettu.

c) Varmentajan yksityisen avaimen luomiseen ja uusintaan liittyvät tapahtumat.

d) Varmenteen sulkupyynnöt.

e) Julkiseen hakemistoon lähetetyt sulkulistat ja muu varmenteen sulkemiseen liittyvä tieto.

f) Voimassaoleva ja aikaisemmin julkaistut varmennepolitiikat ja niitä vastaavat varmennuskäytännöt.

g) Varmennejärjestelmän käyttäjiksi rekisteröityjen varmennejärjestelmän ylläpitäjien ja varmennejärjestelmän käyttäjien suorittamat toimenpiteet taltioidaan lokitiedostoihin.

h) Tarkastusraportit ja pöytäkirjat käsittäen Tietoturvatarkastukset ja järjestelmän auditoinnin.

i) Arkistotiedot säilytetään allekirjoitusvarmentajana toimivaa viranomaista koskevien säännösten mukaisesti.

4.5.2 Arkistojen suojaus

Arkistoitava tieto säilytetään korkean turvatason tiloissa, joissa on pääsynvalvonta.

4.5.3 Arkistotietojen varmistusmenettelyt

Varmuuskopiot varastoidaan fyysisesti erilliseen tilaan alkuperäisistä tiedoista.

4.5.4 Arkistotietojen hankinta- ja varmistusmenetelmät

Mikäli Varmentajan palvelu keskeytyy tai päättyy, Varmentajan tulee ilmoittaa kaikille asiakkailleen, että arkisto on edelleen tavoitettavissa. Kaikki kyselyt arkistoiduista tiedoista lähetetään varmentajalle tai varmentajan ennen toimintansa päättämistä ilmoittamalle taholle.

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

Arkistosta voidaan luovuttaa tietoa sen mukaisesti, kuin se on perusteltua varmenteen haltijan tai varmenteeseen luottavan osapuolen kannalta.

4.5.5 Toiminnan jatkumisen hallinta ja poikkeustapausten käsittely

Digi- ja väestötietovirastolla on jatkuvuus- ja valmiussuunnitelma, joka mahdollistaa Digi- ja väestötietoviraston toiminnan jatkuvuuden.

4.5.6 Varmentajan yksityinen avain paljastunut tai Varmentajan varmenne on suljettu

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

Tällaisessa tapauksessa varmentaja joko lakkauttaa toimintansa kohdassa 4.8 esitetyllä tavalla tai suorittaa seuraavat toimenpiteet:

a) Varmentaja ilmoittaa tapahtuneesta kaikille niille varmenteiden haltijoille, luottaville osapuolille sekä kaikille niille asiakkaille, joiden kanssa varmentajalla on sopimuksia tai jotka muuten ovat sellaisessa asemassa sopimussuhteen tai viranomaistoiminnan vuoksi sellaisessa suhteessa varmentajaan, että varmentajan on asiasta tiedotettava.

b) Varmentaja luo uuden avaimen luvun 6 mukaisesti.

c) Kaikki paljastuneella avaimella myönnetyt ja voimassa olevat varmenteet suljetaan yhdellä tai useammalla sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeisen suljetun varmenteen voimassaoloaika on päättynyt.

d) Varmentaja arkistoi vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain 38 § mukaiset tiedot lain vaatimaksi ajaksi sekä noudattaa muutoinkin arkistolain säännöksiä tietojen arkistoinnin osalta.

4.5.7 Turvallisuuden vaarantuminen luonnonmullistuksen tai muun katastrofin seurauksena

Digi- ja väestötietoviraston turvapolitiikassa on otettu huomioon ulkoisen turvallisuuden vaarantumisen aiheuttamat toimenpiteet. Digi- ja väestötietovirasto on saanut ISO/IEC 27001-tietoturvaseritifikaatin, joka asettaa vaatimukset Digi- ja väestötietoviraston toiminnalle myös mahdollisen katastrofin tapahduttua. Varmenteiden myöntämisen ja ylläpidon yhteydessä Digi- ja väestötietovirasto noudattaa kohdassa 4.7 mainittuja menettelytapoja.

4.5.8 Varmentajan toiminnan lakkauttaminen

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

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

Ennen varmentajan lakkauttamista suoritetaan vähintäänkin seuraavat toimenpiteet:

a) Kaikki myönnetyt ja voimassa olevat varmenteet suljetaan yhdellä tai useammalla sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeisen suljetun varmenteen voimassaoloaika on päättynyt.

b) Varmentaja lakkauttaa kaikki sopimuskumppaniensa valtuudet suorittaa varmenteiden myöntämisprosessiin liittyviä tehtäviä varmentajan puolesta.

c) Varmentaja varmistaa, että kohdassa 4.6 mainittu saatavuus varmentajan arkistoihin säilyy varmentajan lakkauttamisen jälkeenkin.

d) Varmentaja huolehtii vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain 38 § mukaisten tietojen arkistoinnista sekä noudattaa muutoinkin arkistolain säännöksiä tietojen arkistoinnin osalta.

5 Fyysiset, toiminnalliset ja henkilöstöturvallisuuteen liittyvät vaatimukset

Digi- ja väestötietovirastolle on myönnetty tietoturvasertifikaatti, joka varmentaa, että DVV:n tietoturvallisuus täyttää standardin ISO/IEC 27001 vaatimukset.

Digi- ja väestötietovirasto käyttää teknisiä toimittajia varmennepalvelun tietoteknisten tehtävien hoitamiseen. DVV vastaa varmentajana varmennetuotannon turvallisuudesta ja toiminnasta asianmukaisella tavalla sen kaikilla osa-alueilla.

Digi- ja väestötietovirastossa noudatetaan hyvää tiedonhallintatapaa. Varmenteiden tarjoamiseen liittyvät palvelut on organisoitu Digi- ja väestötietoviraston Varmennepalvelut toimintoon.

5.1 Fyysiseen turvallisuuteen liittyvät järjestelyt

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 Sähkön syöttö ja ilmastointi

Konesalitilat on asianmukaisesti ilmastoitu. Tiloissa on varauduttu hallitsemattomiin sähkökatkoksiin kiinteistöihin rakennetuilla varavoimaratkaisuilla.

5.1.4 Paloturvallisuus

Konesalitiloissa on tarvittavat hälytysmekanismit tulipalon varalle, tarpeellinen alkusammutuskalusto sekä automaattiset sammutusjärjestelmät.

5.1.5 Tiedon säilytys

Arkistoitavat tiedot ja varmuuskopiot säilytetään eri tiloissa kuin varmentajan laitteistot.

Tiedot on suojattu häviämiseltä, muuttamiselta ja luvattomalta käytöltä.

5.1.6 Tarpeettoman tietoaineiston käsittely

Turvaluokiteltu tietoaineisto hävitetään luotettavalla tavalla tuhoamalla.

5.1.7 Vesivahingot

Konesalitiloissa on asianmukaiset kosteuden havaitsevat ilmaisimet.

5.1.8 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

Digi- ja väestötietovirasto käyttää varmennetuotannon rekisteröintiin ja tietoteknisiin tehtäviin teknisiä toimittajia. Digi- ja väestötietovirasto toimii varmentajana, joka vastaa varmennetoiminnasta.

Varmentajan tehtävät on jaettu seuraaviin vastuualueisiin:

Tietoturvallisuusvastaava

Rekisteröintivastaava

Järjestelmän ylläpitäjä

Järjestelmän käyttäjä

Järjestelmän valvoja

Varmentajan ja teknisen toimittajan välillä on solmittu toimitussopimus, jossa toimittajan tehtävät, menetelmät ja vastuut sekä tietoturvallisuuden järjestäminen on kuvattu yksityiskohtaisesti.

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.

Organisaatiovarmenteen rekisteröiminen ja tunnistaminen vaatii yhden henkilön läsnäolon.

5.2.3 Tehtäväkohtainen tunnistaminen

Organisaatiovarmenteen rekisteröijä:

Rekisteröijänä toimii organisaatio, jonka kanssa Digi- ja väestötietovirasto on tehnyt rekisteröintiä koskevan sopimuksen.

Varmennejärjestelmän ylläpitäjä:

Tunnistetaan henkilökohtaisella järjestelmän hallintaan tarkoitetulla hallintakortilla. Järjestelmän ylläpitäjiä ovat varmennejärjestelmän toimittajan järjestelmäasiantuntijat sekä Digi- ja väestötietoviraston tehtävään valtuutetut henkilöt.

Varmennejärjestelmän käyttäjä:

Tunnistetaan henkilökohtaisella järjestelmän käyttöön tarkoitetulla toimikortilla. Varmennejärjestelmän käyttäjiä ovat konesalioperointi, teknisten varmennepyyntöjen käynnistäjät sekä sulkupalvelu.

5.2.4 Henkilöturvallisuus

Digi- ja väestötietovirasto toimii varmentajana, joka vastaa varmennetoiminnasta. Tekniset toimittajat on hankittu kilpailuttamalla ja ne toimivat Digi- ja väestötietoviraston vastuulla ja lukuun.

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

5.2.5 Henkilökuntaa koskevan taustaselvityksen tekeminen

Digi- ja väestötietovirasto teettää omasta henkilöstöstään sekä teknisten toimittajien varmenneympäristön kanssa työskentelevistä henkilöistä perusmuotoisen turvallisuusselvityksen.

5.2.6 Taustaselvityksen tekemisessä noudatettava menettely

Henkilökunnan työkokemus kartoitetaan työhönottovaiheessa ja henkilö täyttää Suojelupoliisille toimitettavan lomakkeen, jonka avulla henkilöön kohdistetaan turvallisuusselvitysmenettely.

Kaikkien Varmentajan, varmennepalveluiden ja hakemistopalveluiden tuottajien, sulkupalvelun ja kortinvalmistajan keskeisissä tehtävissä olevien henkilöiden tulee:

- täyttää Suojelupoliisille toimitettava lomake, jonka avulla henkilöihin kohdistetaan turvallisuusselvitysmenettely;
- pysytellä erossa heidän velvoitteidensa ja vastuidensa kanssa ristiriidassa olevista tehtävistä;
- olla henkilöitä, joiden ei tiedetä vapautetun mistään aikaisemmasta tehtävästä velvollisuuksiensa laiminlyönnin tai väärinkäytön takia;
- olla tehtäviensä hoitoon asianmukaisesti koulutettuja.

5.2.7 Koulutukseen liittyvät vaatimukset

Digi- ja väestötietoviraston henkilökunnan on oltava koulutettu siten, että tehtävän hoitaminen parhaalla mahdollisella tavalla on mahdollista. Digi- ja väestötietovirastossa on koulutussuunnitelma, jonka toteuttamisesta vastaa Digi- ja väestötietoviraston hallintoyksikkö.

5.2.8 Asiantuntemuksen ja osaamisen ylläpito

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

5.2.9 Tehtäväkiertoon liittyvät vaatimukset

Kun varmentajan tehtävissä suunnitellaan tehtäväkiertoa, on tehtävät organisoitava 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.

5.2.10 Poikkeamista johtuvat toimenpiteet

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

5.2.11 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.

5.2.12 Henkilökunnan käyttöön annettavat asiakirjat

Henkilökunnalla on aina käytössään Digi- ja väestötietoviraston laatu- ja turvallisuusasiakirjat.

6 Tekniset turvajärjestelyt

6.1 Avainparin luominen ja tallettaminen

6.1.1 Avainparin luominen

Avaimen luonti perustuu syötettyyn satunnaislukuun, joka on riittävän pitkä ja joka on saatu aikaan niin, että sitä on laskennallisesti mahdotonta jäljittää, vaikka tiedettäisiin milloin ja millä laitteistolla se on luotu. Lisäksi satunnaisluvun generointiin käytettävä algoritmi ja generointimenetelmä täyttävät laadulliset vaatimukset, joita ovat mm. algoritmin luotettavuus, generointimenetelmän toistamattomuus ja satunnaisluvun aito satunnaisuus. Varmentaja ei julkaise todennäköisyyteen käytettyä tarkkuutta ja menetelmää.

Varmentaja:

Varmentaja luo yksityiset allekirjoitusavaimensa ja yksityisiä allekirjoitusavaimiaan vastaavat julkiset avaimensa. Avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa. Ne täyttävät turvatasoltaan FIPS 140-1 tason 3 vaatimukset.

Varmenteen haltija:

Avainten luominen voidaan tehdä eräajona ennen varmennusta tai suoraan varmennuksen yhteydessä. Molemmissa tapauksissa yksityinen avain säilytetään luku- ja kirjoitussuojattuna toimikortilla.

Varmentaja luo varmenteen haltijan avaimet toimikortin sisällä. Yksityisistä allekirjoitusavaimista ei luoda kopiota.

6.1.2 Yksityisen avaimen luovuttaminen varmenteen haltijalle

Toimikortti, joka sisältää varmenteen haltijan yksityiset avaimet ja jonka aktivointitiedoksi tarvitaan alkuperäiset PIN-tunnukset, toimitetaan asiakkaalle siten, että se ei ole yhdessä PIN-tunnusten kanssa samassa paikassa ennen asiakkaalle luovuttamista. Tämä toteutetaan erillisten siirtoreittien avulla ja luovuttamalla kortti ja tunnusluvut eriaikaisesti.

Kortti luovutetaan kortin haltijalle henkilökohtaisesti Varmentajaa edustavan Rekisteröijän luona. Organisaatiovarmenteen haltijan on osoitettava henkilöllisyytensä tavalla, joka vastaa hakemusvaiheessa noudatettua menettelyä. Tunnistustapa merkitään vastaanottokuittiin, jonka asiakkaan lisäksi allekirjoittaa myös toimikortin luovuttava rekisteröijävirkailija.

6.1.3 Varmenteen haltijan julkisen avaimen toimittaminen varmentajalle

Julkisten avainten eheys suojataan varmennukseen asti. Kortinvalmistaja tekee avainten luonnin jälkeen varmennepyyntöjä varmennejärjestelmään. Varmennepyyntö sisältää julkisen avaimen ja muut varmenteen tiedot. Varmennepyyntöjärjestelmän ja varmenteiden luontijärjestelmän välinen tietoliikenneyhteys salataan ja varmennepyyntöjärjestelmän käynnistävät henkilöt tunnistetaan Varmentajan myöntämillä hallintakorteilla.

6.1.4 Varmentajan julkisen avaimen jakelu varmenteen haltijalle

Varmentajan varmenne sisältää varmentajan julkisen avaimen. Varmentajan varmenne talletetaan julkiseen hakemistoon. Varmenteen haltijan varmenne talletetaan asiakasorganisaation kanssa tekemän sopimuksen mukaisesti. Varmentajan varmenne on myös saatavilla myös julkisesta hakemistosta sekä varmentajan www-palvelusta.

6.1.5 Avainten pituudet

Organisaatiovarmenteiden allekirjoittamiseen käytetty Varmentajan yksityinen avain sekä yksityistä avainta vastaava julkinen avain ovat 4096 –bittisiä RSA-avaimia tai 384-bittisiä ECC avaimia.

Varmenteen haltijan yksityiset ja julkiset avaimet ovat vähintään 2048 –bittisiä RSA-avaimia. Digi- ja väestötietoviraston ja varmennepalveluita tilaavan organisaation välillä solmitun sopimuksen mukaisesti on mahdollista toteuttaa myös 4096-bittisiä RSA-avaimia ja 384-bittisiä ECC-avaimia.

6.1.6 Avainten käyttötarkoitukset

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

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 paljastumista ja luvatonta käyttöä vastaan. Varmentajan yksityisistä avaimista otetaan varmuuskopio kriittisen tietoturvallisuuden edellyttämällä tavalla.

6.2.2 Varmentajan yksityisen avaimen käsittelyyn osallistuva henkilökunta

Yksityisen avaimen luontiin vaaditaan vähintään kahden henkilön samanaikainen läsnäolo tai toiminnan aktivoiminen.

6.2.3 Yksityisen avaimen luovutus luotetun osapuolen huostaan

Kortinhaltijoiden yksityiset avaimet luodaan allekirjoitusvarmenteelta edellytettävällä tavalla turvallisesti. Kortinhaltijan itsensä luomia avainpareja ei hyväksytä. Yksityiset avaimet eivät ole siirrettävissä tai kopioitavissa toimikortilta. Varmentaja ja kortinvalmistaja eivät pääse käsittelemään varmentamiensa henkilöiden yksityisiä avaimia. Toimikorteilla olevilla allekirjoitusavaimilla ei ole ns. key escrow -toimintoa. Todentamis- ja salausvarmenteesta on Digi- ja väestötietoviraston ja varmennepalveluita tilaavan organisaation välillä solmitun sopimuksen mukaisesti mahdollisuus toteuttaa key escrow -toiminto. 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. Avainten käyttöä valvotaan erityisten, asiattomalta käytöltä suojattujen hallintakorttien avulla.

Varmentajan luotetuissa työtehtävissä toimivilla henkilöillä on hallussaan PIN-koodilla suojattu hallintakortti. Henkilön oikeus käyttää varmennejärjestelmää tai muita varmentamiseen liittyviä järjestelmiä todetaan näiden hallintakorttien avulla.

Kun varmentajan avaimen käyttö lopetetaan, avain hävitetään niin, ettei sitä ole mahdollista enää käyttää tai luoda uudelleen. Samalla hävitetään avaimen varmuuskopiot. Rikkoutuneiden laitteiden hävittämismenettelyt on hoidettu siten, että kyetään tuhoamaan sekä laitteisto- että ohjelmistopohjaisesti tallennetut yksityiset avaimet luotettavalla tavalla (riittävän usealla ylikirjoittamisella).

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

Organisaatiovarmenteen käyttöaika on sopimuksen mukainen, tavallisimmin kaksi-viisi vuotta. Varmenne voidaan sulkea voimassaoloaikansa kuluessa. Varmenteessa olevaa tietoa voidaan käyttää allekirjoituksen oikeellisuuden osoittamiseen varmenteen vanhenemisen tai sulkemisen jälkeen, jos varmennettu allekirjoitus on luotu ennen varmenteen sulkemista tai vanhenemisaikaa.

6.4 Aktivointitieto

6.4.1 Aktivointitiedon luominen ja käyttöönotto

Kortinvalmistaja luo avainten käytön mahdollistavat aktivointitiedot eli PIN-tunnukset. Yksilölliset PIN-tunnukset ja PUK-koodit lasketaan ja siirretään kortille ja salakirjoitettuna vastetiedostoon siirrettäväksi kortinvalmistajan tuotantojärjestelmään. Korttien toimituksen jälkeen niiden salakirjoitetut PIN-tunnukset ja PUK-koodit siirretään korttien valmistuksesta eriytetyn osaston haltuun, jossa PIN- ja PUK-kirjeet tulostetaan. Ne toimitetaan sovitun aikamäärän kuluttua korttien toimituksesta hakijan korttihakemuksessa ilmoittamaan jakeluosoitteeseen.

6.4.2 Aktivointitiedon suojaus

PIN-tunnukset on suojattu niin, ettei niitä voi lukea tai kopioida kortilta. Varmenteen haltijan vastuulla on suojata avaintensa käyttö toimikortilla huolehtimalla kortistaan ja tunnusluvuistaan käyttöehdoissa mainitulla tavalla.

6.4.3 Muut aktivointitietoon liittyvät seikat

Organisaatiovarmenteen haltijalle selvitetään, että hänellä on mahdollisuus vaihtaa alkuperäiset PIN-tunnukset uusiksi tunnuksiksi. PIN-tunnusluvun vaihto-ohjelma on maksutta kortinhaltijan käytettävissä osoitteessa www.fineid.fi.

Toimikortti lukkiutuu ja sen käyttö estyy kolmen peräkkäisen väärän PIN-tunnuksen antamisen jälkeen. Lukkiutunut PIN-tunnus vapautetaan uudelleen käyttöön yhdessä

rekisteröijän ja varmenteen haltijan kanssa. Lukituksen purkamisen jälkeen purkukoodit pyyhitään purkamiseen käytetyn järjestelmän muistista.

6.5 Tietokoneiden käyttöön ja niihin pääsyyn liittyvät turvallisuusvaatimukset

6.5.1 Laitteistoturvallisuus

Varmennejärjestelmän laitteistoina käytetään vain käyttötarkoitukseensa sopivia laitteistoja.

Laitteistoturvallisuus on toteutettu hyvän tietojenhallintatavan mukaisesti siten, että järjestelmän pettäessä voidaan siirtyä käyttämään varajärjestelmää vaarantamatta järjestelmän luottamuksellisuutta. Toiminnan jatkuvuuden kannalta tärkeiden laitteiden varaosien saanti on varmistettu.

Huoltomenettelykäytännössä ulkopuolisen henkilöstön pääsy palvelutuotannon vastuulla oleviin järjestelmiin ja tiloihin on estetty. Huoltokäynti on mahdollista ainoastaan teknisen toimitussopimuksen ja salassapitosopimuksen tehneelle tekniselle toimittajalle. Listaa hyväksytyistä teknisistä toimittajista pidetään yllä.

Huoltokäynnit ovat mahdollisia ainoastaan järjestelmän ylläpitäjän tai hänen valtuuttamansa henkilön valvonnassa.

Varmennejärjestelmän laitteistot ovat ympärivuorokautisessa valvonnassa.

6.5.2 Varmennejärjestelmän elinkaaren hallinta

Digi- ja väestötietovirasto pitää yllä tärkeysluokitusta varmennepalveluiden kohteista ja järjestelmistä, niiden varmistamisesta, priorisoinnista ja minimiylläpitotasosta.

6.5.3 Järjestelmän kehittämiseen liittyvä valvonta

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

6.5.4 Turvallisuuden hallinta

Digi- ja väestötietoviraston tietoturvallisuutta hallitaan Digi- ja väestötietoviraston tietoturvapolitiikan ja standardin ISO/IEC 27001 mukaisesti.

6.5.5 Tietoverkon turvallisuus

Tietoliikenneturvallisuus on toteutettu siten, että varmennejärjestelmän tietoverkko on yhtenäinen kokonaisuus, joka on eriytetty muista tietoverkoista ja jonka kriittiset osat on kahdennettu. Verkossa välitettävät viestit ja niiden lähettäjät tai vastaanottajat eivät paljastu asiaankuulumattomille osapuolille ilman erityistoimenpiteitä. Verkkoa käytetään vain varmennejärjestelmään liittyvissä tehtävissä. Tarpeettomat verkkopalvelut on otettu pois käytöstä. Verkko on jaettu loogisiin verkon osiin, joiden välisiä yhteyksiä rajoitetaan. Käytössä on riittävät todentamis- pääsynvalvonta- ja kiistämättömyysmenettelyt.

6.5.6 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.

Turvamoduulin käyttöön tarvitaan aina toimikortti henkilön tunnistamiseen ja käyttöoikeuksien todentamiseen. Moduulin saa aktiivitilaan vain järjestelmän käyttäjän henkilökohtaisella hallintakortilla.

Uuden käyttäjätasoisen käyttöoikeuden luontiin tarvitaan kahden järjestelmän ylläpitäjätasoisen henkilön läsnäolo ja vastaavat henkilökohtaiset hallintakortit. Moduuli kerää lokitietoa tapahtumista.

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 varmennuskäytäntöasiakirjoihin seuraavassa kuvatulla tavalla.

8.2 Julkaiseminen ja tiedottaminen

Varmentaja julkaisee varmennepolitiikan ja varmennuskäytännön, jotka ovat saatavilla internet-sivuilla 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

Digi- ja väestötietovirasto hyväksyy sekä organisaatiovarmennetta koskevan varmennepolitiikan että varmennuskäytännön. 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.

[Yksikkö] / Aarnio Ville

31.3.2021