DIGI- JA VÄESTÖTIETO-VIRASTO

Varmennekäytäntö tila-päisvarmennetta varten

OID: 1.2.246.517.1.10.204.1

15.9.2023

15.9.2023

Dokumentinhallinta

Omistaja	
Laatinut	Tuire Saaripuu, Auli Jukkola
Tarkastanut	
Hyväksynyt	Mikko Pitkänen

Version hallinta

versionro	mitä tehty	pvm/henkilö
v 1.0	Hyväksytty versio 1.0.	3.5.2018
v 1.1	Hyväksytty versio 1.1, viraston nimenmuutos.	1.1.2020
v 1.2	Päivitetty versio, saavutettavuusominaisuudet	6.5.2021
v 1.3	Päivitetty versio ja linkit varmennepolitiikkasivulle	23.9.2022/SK
v 1.5	Päivitetty versio, editoriaaliset muutokset, otsikkonumerointi, otsikoiden tasot ja sisällysluettelo korjattu, päivitetty tiedot RSA-avaimista, PUK-koodi korjattu aktivointitunnusluvuksi, ajokortti poistettu tunnistamisasiakirjoista, faxin numero poistettu yhteystiedoista. Versionumeroinnissa siirrytty yhtenäisyyden vuoksi suoraan versioon 1.5, 1.4 jätetty välistä.	15.9.2023/AJ

15.9.2023

Sisällys

15.9.2023

15.9.2023

Määritelmät ja lyhenteet

Määritelmät

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

Aktivointitunnusluku: Aktivointitieto, joka on varmenteen haltijan henkilökohtainen tunnusluku, jolla voi aktivoida ja määritellä omat, henkilökohtaiset PIN-tunnusluvut. Aktivointitunnuslukua voi lisäksi käyttää lukkiutuneen PIN-tunnusluvun vapauttamiseen.

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

ECC-algoritmi ja ECC-avain: ECC-algoritmi kattaa erilaiset elliptisten käyrien salausmenetelmiin liittyvät algoritmit, jotka toteuttavat julkisen avaimen salausjärjestelmän. ECC-avaimella on RSA-avainparin tapaan julkinen ja yksityinen avain.

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

Julkinen avain: Julkisen avaimen menetelmässä epäsymmetrisessä salauksessa käytettävän avainparin julkinen osa. Varmentaja varmentaa sähköisellä allekirjoituksellaan julkisen avaimen kuulumisen varmenteen haltijalle. Julkinen avain on osa varmenteen tietosisältöä.

Julkisen avaimen järjestelmä: Tietoturvainfrastruktuuri, jossa tietoturvapalveluita tuotetaan julkisen avaimen menetelmillä.

Julkisen avaimen menetelmä: Tietoturvapalvelu, esimerkiksi henkilön sähköinen tunnistaminen, joka tuotetaan käyttämällä julkisia ja yksityisiä avaimia, varmenteita ja epäsymmetristä salausta.

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

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

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

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

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

OCSP: Online Certificate Status Protocol, suorakäyttöinen varmenteen tilan palauttava palvelu.

Organisaatiovarmenne: Digi- ja väestötietoviraston luonnolliselle henkilölle myöntämä laatuvarmenne, 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.

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

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

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

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

Terveydenhuollon ammattihenkilö: Henkilö, joka terveydenhuollon ammattihenkilöistä annetun lain nojalla on saanut ammatinharjoittamisoikeuden (laillistettu ammattihenkilö) tai ammatinharjoittamisluvan (luvan saanut ammattihenkilö) sekä henkilö, jolla lain nojalla on oikeus käyttää asetuksella säädettyä terveydenhuollon ammattihenkilön ammattinimikettä (nimikesuojattu ammattihenkilö) ja joka on rekisteröity terveydenhuollon ammattihenkilöiden keskusrekisteriin.

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

Terveydenhuollon henkilöstö: terveydenhuollon ammattihenkilöistä annetussa laissa (559/1994) tarkoitettu terveydenhuollon palvelujen antajien henkilöstö, jotka eivät ole terveydenhuollon ammattihenkilöitä. Kyseiseen henkilöstöryhmään kuuluu esimerkiksi terveydenhuollon toimintayksikön tuki-, toimisto- ja tietopalveluhenkilöstö. Terveydenhuollon palvelujen antajaorganisaatiossa työskentelevä henkilö, joka ei ole terveydenhuollon ammattihenkilö.

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

Terveydenhuollon opiskelija: Laillistetun ammattihenkilön tehtävissä voi valtioneuvoston asetuksella säädetyin edellytyksin toimia tilapäisesti myös kyseiseen ammattiin opiskeleva kyseistä ammattia itsenäisesti harjoittamaan oikeutetun laillistetun ammattihenkilön johdon ja valvonnan alai-

sena. Opiskelijaan sovelletaan tällöin soveltuvin osin, mitä säädetään terveydenhuollon ammattihenkilöstä. Lääketieteen, hammaslääketieteen ja farmasian opiskelijat saavat terveydenhuollon ammattikortin. Muuhun terveydenhuollon ammattiin opiskeleva, asetuksella säädetyt työskentelyn edellytykset täyttävä opiskelija saa organisaatiokohtaisen terveydenhuollon henkilöstökortin.

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

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

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

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

Varmenne: Sähköinen todistus, jonka avulla henkilö voidaan todentaa ja tietoja salata ja joka liittää allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistaa allekirjoittajan. Varmenne sisältää siihen liittyvän varmennuskäytännön yksilöivän tunnuksen.

Varmennejärjestelmä: Tietotekninen järjestelmä, jonka avulla luodaan varmenteet ja allekirjoitetaan sulkulistat.

Varmennekuvaus: Asiakirja sisältää varmennepolitiikan ja varmennuskäytännön keskeiset kohdat.

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

Varmennerekisteri: Rekisteri, jota varmenteita yleisölle tarjoava varmentaja ylläpitää. Tiedot säilytetään vähintään 5 vuoden ajan varmenteen voimassaolon päättymisestä.

Varmennetietojärjestelmä: Tietotekninen järjestelmä, joka koostuu varmennejärjestelmistä, tietoliikenteestä, varmennehakemistosta ja sulkulistapalvelusta, neuvonta- ja sulkupalvelusta sekä varmenteiden ja korttien hallinnoinnista. Varmennuskäytännön yksilöivä tunnus on osa varmenteen tietosisältöä.

Varmennuskäytäntö: Kuvaus miten varmentaja toteuttaa varmennepolitiikkaa. Jokaisella varmennuskäytännöllä on yksilöivä tunnuksensa.

15.9.2023

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

Varmentajan varmenne: Sisältää varmentajan nimen, sijaintimaan ja julkisen avaimen.

Varmentajan yksityinen avain: Varmentajan myöntämien varmenteiden ja sen julkaisemien sulkulistojen allekirjoittamiseen käyttämä yksityinen avain.

Varmenteen hakija: Henkilö, joka hakee tilapäisvarmennetta ja joka tunnistetaan hakemisen yhteydessä luotettavasti.

Varmenteen haltija: Henkilö, jonka henkilöllisyys ja julkinen avain on varmennettu varmentajan sähköisellä allekirjoituksella, ja jonka hallussa varmenteeseen liittyvät yksityiset avaimet ovat.

Varmenteen haltijan todentamis- ja salausvarmenne: Varmennetta käytetään henkilön sähköiseen tunnistamiseen ja tiedon salaukseen. Varmenteen haltija käyttää yksityistä todentamis- ja salausavaintaan sähköiseen tunnistautumiseen ja salatun tiedon tai viestin salauksen purkuun. Avaimen käyttämiseen tarvitaan perustunnusluku (PIN 1).

Varmenteen käyttö ja käyttötarkoitus: Tässä dokumentissa varmenteen käyttö on nimitys sekä itse varmenteen että siihen liittyvien avainten käytölle.

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

15.9.2023

Lyhenneluettelo

CA	Certification Authority, varmentaja
CP	Certificate Policy, varmennepolitiikka
CPS	Certification Practice Statement, varmennuskäytäntö
CRL	Certificate Revocation List, sulkulista
ECC	Elliptic Curve Cryptography, elliptisten käyrien salausmenetelmä, eräs julkisen avaimen algoritmi
FINEID	Finnish Electronic Identification
HSM	Hardware Security Module, turvamoduuli
HST	Henkilön sähköinen tunnistaminen
HTTP	Hypertext Transport Protocol
ISO 27001	ISO/IEC 27001
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol, suorakäyttöinen varmenteen tilan palauttava palvelu
OID	Object Identifier, yksilöivä tunnus
PDS	PKI Disclosure Statement, varmennekuvaus
PIN	Personal Identification Number, PIN-tunnus
PKI	Public Key Infrastructure, julkisen avaimen järjestelmä
RSA	Rivest, Shamir, Adleman, eräs julkisen avaimen algoritmi, epäsymmetrinen algoritmi
DVV	Digi- ja väestötietovirasto

15.9.2023

1 Johdanto

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

Tätä varmennuskäytäntöä sovelletaan varmentajana toimivan Digi- ja väestötietoviraston tilapäisvarmenteeseen.

Tilapäisvarmenne on varmenne, joka tukee varmentajan myöntämän organisaatiovarmenteen, OID: 1.2.246.517.1.10.203, käyttöä.

1.1 Yleistä

Varmenne on sähköinen todistus, joka liittää allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistaa varmenteen haltijan henkilöllisyyden. Varmenteen tiedot on sähköisesti allekirjoitettu varmentajan yksityisellä avaimella. Tämän varmennuskäytännön mukainen varmenne perustuu julkisen avaimen järjestelmään ja menetelmiin. Tämän varmennuskäytännön mukaisen varmenteen tietosisältö on määritelty laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista.

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

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

Varmentaja yksilöi varmenteen haltijan yksilöivän tunnuksen avulla, joka on myös osa varmenteen tietosisältöä. Tunnus on sähköistä asiointia varten erikseen luotu tekninen tunnistetieto, joka ei sisällä henkilöön liittyviä tunnistetietoja.

Tilapäisvarmenne voidaan tallentaa erilaisille toimikorteille.

Varmentajan 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.

Varmentaja 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 sisä-

markkinoilla ja direktiivin 1999/93/EY kumoamisesta annettua asetusta (Asetus) sovelletaan luottamuspalveluiden allekirjoitusvarmenteiden osalta 1.7.2016 alkaen. Tässä asiakirjassa määritellään menettelytapavaatimukset, jotka koskevat Asetuksen mukaisesti tunnistus- ja allekirjoitusvarmenteita myöntävien varmentajien toimintaa ja hallintokäytäntöjä. Tässä asiakirjassa esitetyissä menettelytapavaatimuksissa kuvataan turvallisen allekirjoituksen luomisvälineen käyttö.

Varmentaja on Asetuksen mukainen varmennepalvelujen tarjoaja, joka myöntää varmenteita.

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

Varmentaja on toiminut myös terveydenhuollon lakisääteisenä varmentajana 1.12.2010 alkaen ja toimii lisäksi sosiaalihuollon lakisääteisenä varmentajana 1.4.2015 alkaen sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä koskevaan lakiin tehtyjen muutosten johdosta (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 (304/2019) nojalla). Varmentajan Varmennepalvelut toiminto vastaa viraston varmennetoiminnasta.

1.2 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 tilapäisvarmennetta varten, jonka OID on 1.2.246.517.1.10.204.1.

Tämä varmennuskäytäntö viittaa Varmennepolitiikkaan tilapäisvarmennetta varten, jonka OID on 1.2.246.517.1.10.204.

Varmentaja 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.dvv.fi/cps.

1.3 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 varmentaja. Varmentaja on henkilörekisteriä ylläpitävä viranomainen, jonka väestötietojärjestelmästä ja Digi- ja väestötieto-

viraston varmennepalveluista annetun lain (304/2019) ja sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007) ja laissa sähköisestä lääkemääräyksestä (61/2007) mukainen tehtävä on tuottaa muiden tehtäviensä lisäksi varmennettuja sähköisen asioinnin palveluita. Varmentaja varmennepalvelu jakaantuu toiminnallisesti seuraaviin osa-alueisiin:

1.3.1 Varmentaja

Varmentajan tehtävänä on:

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

1.3.2 Rekisteröijä

Tilapäisvarmenteen rekisteröinti tapahtuu noudattaen vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaista ja tässä varmennuskäytäntöasiakirjassa kuvattua menettelytapaa.

Varakortilla olevien tilapäisvarmenteiden rekisteröijänä toimii varmentajan 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 periaatteita.
- Varmentaja valvoo, että asiakasorganisaatio noudattaa rekisteröintiä koskevia sopimuksessa mainittuja ehtoja ja vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain rekisteröintiä koskevia säännöksiä.
- Rekisteröijä käyttää rekisteröintiin, varakorttien tilaamiseen ja sulkemiseen varmentajan tarjoamaa tilaus- ja hallintajärjestelmää.

1.3.3 Varakortin tai mikrosirun valmistaja ja yksilöijä

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

1.3.4 Sulkupalvelu

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

1.3.5 Tilapäisvarmenteiden tietojen julkaiseminen

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

1.3.6 Varmenteen haltija

Tämän varmennuskäytännön mukaisia tilapäisvarmenteita voidaan myöntää vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaisesti tunnistetuille henkilöille tai sosiaali- ja terveydenhuollon henkilöstön tai sosiaali- ja terveydenhuollon toimijoiden ollessa kyseessä tilapäisvarmenteita voidaan sen lisäksi luovuttaa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa lain (159/2007) ja lain sähköisestä lääkemääräyksestä (61/2007) sekä niiden nojalla annetuissa säädöksien ja niiden nojalla asetettujen vaatimuksien mukaisesti. Sosiaali- ja terveydenhuollon henkilöstön ja sosiaali- ja terveydenhuollon toimijoiden tilapäisvarmenteen haltijana voi olla ainoastaan sosiaali- ja terveydenhuollon henkilöstö tai sosiaali- ja terveydenhuollon toimija.

Varmenteen haltijan tulee noudattaa varmentajan varmennepolitiikkaa ja varmennuskäytäntöä.

1.3.7 Varmenteeseen luottava osapuoli

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

15.9.2023

1.3.8 Varmenteen käyttäminen

Varmentaja noudattaa tätä varmennuskäytäntöä myöntäessään tilapäisvarmenteita. Varmenteen haltijoiden ja varmenteeseen luottavien osapuolien tulee toimia tämän varmennuskäytännön mukaisesti.

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

Varmennepolitiikka ja varmennuskäytäntö sisältävät vaatimuksia, jotka koskevat varmentajan, rekisteröijän, varmenteen haltijan ja varmenteeseen luottavan osapuolen velvoitteita sekä lainsäädäntöön ja mahdollisten erimielisyyksien ratkaisuun liittyviä kysymyksiä.

1.4 Yhteystiedot

1.4.1 Varmennuskäytäntöä hallinnoiva organisaatio

Tämän varmennepolitiikan on rekisteröinyt varmentaja. Se on henkilörekisteriä ylläpitävä viranomainen, jonka väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (304/2019) mukainen tehtävä on tuottaa muiden tehtäviensä lisäksi varmennettuja sähköisen asioinnin palveluita. Varmentaja vastaa tämän varmennepolitiikan hallinnoinnista ja päivityksistä.

Tämän varmennuskäytännön mukaiset tekijänoikeudet kuuluvat varmentajalle.

1.4.2 Yhteyshenkilö

Tätä varmennuskäytäntöä koskevat kysymykset lähetetään seuraavaan osoitteeseen:

Digi- ja väestötietovirasto

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

00531 Helsinki kirjaamo@dvv.fi

Y-tunnus: 0245437-2

Digi- ja väestötietovirasto (DVV) Varmennepalvelut

PL 123

00531 Helsinki

www.dvv.fi

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

15.9.2023

2 Yleiset ehdot

Tämä varmennepolitiikka astuu voimaan kansisivulla mainittuna ajankohtana. Varmennuskäytännön muutosmenettely ja julkaiseminen on kuvattu tämän asiakirjan kohdassa 8.

2.1 Velvollisuudet

2.1.1 Varmentajaa koskevat velvollisuudet

- Digi- ja väestötietovirastolla on lakisääteinen tehtävä toimia varmentajana.
- Asiakasorganisaatio vastaa omalta osaltaan varmenteiden sulkemisesta varmentajan ja asiakasorganisaation välisen sopimuksen mukaisesti.
- Asiakasorganisaation on tarkastettava loppukäyttäjiä koskevien tietojen oikeellisuus varmentajan ja asiakasorganisaation välisen sopimuksen mukaisesti.
- Varmentaja noudattaa toiminnassaan voimassa olevaa lainsäädäntöä.
- Varmentaja toimii huolellisesti, luotettavasti ja asianmukaisesti.
- Varmentajalla on riittävät tekniset taidot, ja taloudelliset voimavarat sekä mahdollisuus vahingonkorvausvastuun kattamiseksi.
- Varmentaja vastaa kaikista varmennetoiminnan osa-alueista, myös varmentajan apunaan käyttämien teknisten toimittajien tai henkilöiden, kuten rekisteröijien ja kortinvalmistajien tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta.
- Varmentaja laatii ja ylläpitää varmennepolitiikkaa, joka kuvaa tilapäisvarmenteiden myöntämisessä, ylläpidossa ja hallinnoinnissa käytettävät menettelytavat, käyttöehdot, vastuiden jaot ja muut tilapäisvarmenteen käyttöön liittyvät näkökulmat yleisellä tasolla.
- Varmentaja laatii ja ylläpitää varmennuskäytäntöjä, jotka kuvaavat, miten varmentaja soveltaa varmennepolitiikkaa.
- Varmentaja noudattaa varmennepolitiikkaa ja varmennuskäytäntöä.
- Varmentaja julkaisee varmennepolitiikan ja varmennuskäytännön yleisesti saataville.
- Varmentaja pitää palveluksessaan riittävästi henkilökuntaa, jolla on varmennepalvelujen tuottamisen edellyttämä asiantuntemus, kokemus ja pätevyys.
- Varmentaja käyttää luotettavia järjestelmiä ja tuotteita, jotka on suojattu oikeudettomalta käytöltä.
- Varmentaja pitää yleisesti saatavilla varmennetta ja varmennetoimintaa koskevat tiedot, joiden perusteella varmentajan toiminta ja luotettavuus voidaan arvioida.
- 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. Varmenteita saa käyttää vain sen käyttötarkoituksen mukaisesti todentamiseen, tiedon salaamiseen tai sähköiseen allekirjoittamiseen.
- Tilapäisvarmenteen haltija vastaa siitä, että tilapäisvarmenteita haettaessa ilmoitetut tiedot ovat oikeita.
- Tilapäisvarmenteen haltija on vastuussa tilapäisvarmenteen käytöstä, tilapäisvarmenteella tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista.
- Tilapäisvarmenneen haltija säilyttää mikrosirulla olevan yksityisen avaimensa ja sen käyttämiseen tarvittavan tunnusluvun erillään sekä pyrkii estämään yksityisen avaimensa katoamisen, joutumisen ulkopuolisten käsiin, muuttamisen tai luvattoman käytön. Mikrosirun luovuttaminen tai PIN-tunnuksen paljastaminen toiselle henkilölle esim. lainaamalla vapauttaa varmentajan ja tilapäisvarmenteeseen luottavan osapuolen mikrosirun käyttämisestä mahdollisesti aiheutuvista vastuista.
- Tilapäisvarmennetta käsitellään ja suojataan samalla huolellisuudella kuin muita vastaavia mikrosiruja, kortteja tai asiakirjoja, kuten esimerkiksi luottokortteja, henkilökorttia ja passia. Henkilökohtaiset PIN-tunnukset on säilytettävä fyysisesti eri paikassa kuin tilapäisvarmenteen ja yksityisen avaimen sisältävä mikrosiru.
- Tilapäisvarmenteen sisältävän varakortin häviämisestä tai väärinkäytön mahdollisuudesta tulee ilmoittaa viipymättä varmenteen haltijan organisaation rekisteröijälle, joka sulkee varmenteen korttien tilaus- ja hallinnointijärjestelmässä.

2.1.4 Varmenteeseen luottavaa osapuolta koskevat velvollisuudet

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

Varmenteeseen luottavan osapuolen on noudatettava varmennepolitiikkaa ja varmennuskäytäntöä.

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

Jos tilapäisvarmenteeseen luottava osapuoli kopioi sulkulistan hakemistosta, sen on varmistettava sulkulistan aitous tarkistamalla sulkulistan varmentajan sähköinen allekirjoitus. Lisäksi on tarkistettava sulkulistan voimassaoloaika.

Mikäli uusinta sulkulistaa ei voida saada hakemistosta laitteiston tai hakemistopalvelun toimintahäiriön vuoksi, tilapäisvarmennetta ei pidä hyväksyä, mikäli viimeisen saadun sulkulistan voimassaoloaika on päättynyt. Kaikki tilapäisvarmenteen hyväksymiset tämän voimassaoloajan jälkeen tapahtuvat tilapäisvarmenteeseen luottavan osapuolen omalla riskillä.

2.1.5 Varmenteen julkaisemiseen liittyvät velvollisuudet

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

2.2 Vastuut

2.2.1 Varmentajan vastuut

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

Varmentaja vastaa siitä, että tilapäisvarmenne on luotu noudattaen laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista, varmennepolitiikassa sekä varmennuskäytännössä esitettyjä menettelyjä ja varmenteen hakijan antamien tietojen mukaisesti ja että se täyttää laeissa määritellyt varmentajan vahingonkorvausvastuut tai jos kyseessä on sosiaali- ja terveydenhuollon henkilöstölle tai sosiaali- ja terveydenhuollon toimijoille luotava tilapäisvarmenne, niin edellisten lisäksi noudatetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007) ja laissa sähköisestä lääkemääräyksestä (61/2007) sekä niiden nojalla annettuja säädöksiä ja niiden nojalla asetettuja vaatimuksia. Varmentaja vastaa ainoastaan niistä tiedoista, jotka se on tallettanut varmenteeseen.

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

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

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

15.9.2023

2.2.2 Rekisteröijän vastuut

Tilapäisvarmenteen rekisteröijänä toimii rekisteröintipiste, joka rekisteröi varmenteen hakijan varmentajan lukuun erikseen tätä toimintaa varten solmitun sopimuksen perusteella. Rekisteröijä vastaa suorittamastaan rekisteröinnistä ja varmenteen sulkemisesta. Rekisteröinnin osalta noudatetaan laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista ja varmennuskäytännössä kuvattuja vaatimuksia tai jos kyseessä on sosiaali- ja terveydenhuollon henkilöstölle tai sosiaali- ja terveydenhuollon toimijoille luotava tilapäisvarmenne, niin edellisten lisäksi noudatetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007) ja laissa sähköisestä lääkemääräyksestä (61/2007) sekä niiden nojalla annettuja säädöksiä ja niiden nojalla asetettuja vaatimuksia.

2.2.3 Varmenteen haltijan vastuut

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

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

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

2.2.4 Tilapäisvarmenteeseen luottavan osapuolen vastuut

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

2.2.5 Vastuiden rajoitukset

Varmentajaa koskevat lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) mukaiset säännökset sekä soveltuvin osin vahingonkorvauslain (412/1974) säännökset.

Varmentaja ei vastaa PIN-tunnuksen ja varmenteen haltijan yksityisen avaimen paljastumisen seurauksena syntyvistä vahingoista, ellei paljastuminen välittömästi johdu varmentajan välittömästä toiminnasta.

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

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

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

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

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

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

2.3 Taloudellinen vastuu

2.3.1 Varmentaja

Varmentajaa koskevat lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) mukaiset säännökset sekä soveltuvin osin vahingonkorvauslain (412/1974) säännökset.

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

2.3.2 Muut osapuolet

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

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

2.3.3 Varmentajan taloushallinto

Varmentajan tuottamat varmennepalvelut ovat sellaisen taloushallinnollisen järjestelmän ja valvonnan piirissä kuin on erikseen säädetty. Digi- ja väestötietovirasto on valtiovarainministeriön alaisuudessa toimiva virasto.

Varmentajan 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.

15.9.2023

2.4 Tulkinta ja täytäntöönpano

2.4.1 Sovellettava lainsäädäntö

Varmentajaa koskevat lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) mukaiset säännökset sekä soveltuvin osin vahingonkorvauslain (412/1974) säännökset. Jos kyseessä on sosiaali- ja terveydenhuollon henkilöstölle tai terveydenhuollon toimijoille luotava tilapäisvarmenne, niin edellisten lisäksi noudatetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007) ja laissa sähköisestä lääkemääräyksestä (61/2007) sekä niiden nojalla annettuja säädöksiä ja niiden nojalla asetettuja vaatimuksia.

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

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

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

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

Varmentaja vastaa siitä, että tilapäisvarmenteet on luotu noudattaen laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista, varmennepolitiikassa ja varmennuskäytännössä esitettyjä menettelyjä. Lisäksi tilapäisvarmenne luodaan varmenteen hakijan antamien tietojen mukaisesti tai jos kyseessä on sosiaali- ja terveydenhuollon henkilöstö tai sosiaali- ja terveydenhuollon toimijoille luotava tilapäisvarmenne, niin edellisten lisäksi noudatetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007) ja laissa sähköisestä lääkemääräyksestä (61/2007) sekä niiden nojalla annettuja säädöksiä ja niiden nojalla asetettuja vaatimuksia.

Varmentajan toimintaa valvoo vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukainen valvontaelin Traficom, joka antaa tarvittavat toimintaa koskevat määräykset ja suositukset.

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

Valitusten ja riitojen ratkaisussa sekä hallinnollisessa valvonnassa ja lainkäytössä noudatetaan voimassa olevaa lainsäädäntöä.

2.4.2 Erimielisyyksien ratkaiseminen

Varmentaja vastaa varmenteita myöntäessään siitä, että varmenteet täyttävät tässä varmennuskäytännössä sekä tilapäisvarmennetta koskevassa varmennepolitiikassa esitetyt vaatimukset. Mahdolliset erimielisyydet ratkaistaan Suomen oikeusjärjestyksen mukaisesti.

15.9.2023

2.5 Maksut

Tässä kappaleessa on määritelty tilapäisvarmenteen käyttöön liittyvät maksut.

2.5.1 Tilapäisvarmenteen myöntäminen ja uusiminen

Tilapäisvarmennetta haetaan sen mukaisesti kuin varmennuskäytännössä on kuvattu.

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

Tilapäisvarmenteet on hinnoiteltu voimassa olevan varmentajan liiketaloudellisia suoritteita koskevan hinnaston mukaisesti.

2.5.2 Tilapäisvarmenteen käyttöön liittyvät maksut

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

2.5.3 Tilapäisvarmenteen sulkulistamerkintään liittyvät maksut

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

2.5.4 Muut maksut

Neuvontapalvelun käytöstä peritään erillinen maksu voimassa olevan hinnaston mukaisesti.

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

Tilapäisvarmenteen käyttöehdot luovutetaan tilapäisvarmennetta vastaanotettaessa tilapäisvarmenteen haltijalle.

2.6 Tietojen julkaiseminen ja saatavuus

2.6.1 Varmentajan tietojen julkaiseminen

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

2.6.2 Julkaisutiheys

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

2.6.3 Tietojen saatavuus

Hakemisto- ja sulkulistatiedot ovat yleisesti saatavilla. Varmentajan julkaisemat julkiset FINEID-määritykset ovat saatavilla varmentajan www-sivuilla. Varmennepolitiikat ja varmennuskäytännöt ovat niin ikään saatavilla varmentajan www-sivuilla.

2.6.4 Tietovarastot

Varmentajan julkaisemat tiedot ovat saatavilla varmentajan www-sivuilla ja tämän varmennuskäytännön mukaisesti julkisessa hakemistossa.

Varmennejärjestelmän luottamukselliset tiedot on talletettu varmentajan omaan, luottamukselliseen tietovarastoon. Varmentajan tiedot arkistoidaan voimassa olevien arkistosäännösten mukaisesti.

Henkilötietojen käsittelyyn kiinnitetään erityistä huolellisuutta ja varmentaja on julkaissut varmennepalveluiden tuottamisesta erityiset henkilötietolain mukaiset käytännesäännöt. Varmentaja on valmistellut myös varmennejärjestelmän henkilötietolain mukaisen rekisteriselosteen henkilötietojen käsittelyn osalta.

2.7 Tietoturvatarkastus

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

2.7.1 Tarkastusten tiheys

Varmentaja tarkastaa teknisten toimittajiensa toimitilat ja laitteet ja toiminnan tarkoituksenmukaisella tavalla. Tarkastus tehdään vähintään kerran vuodessa ja aina, kun uusi sopimuskausi alkaa. Tarkastusmenettelyssä varmentaja 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 mukaisesti.

2.7.2 Tarkastaja

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

2.7.3 Tarkastuksen kohteet ja kattavuus

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

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

Tarkastuksessa verrataan politiikkaa, varmennuskäytäntöä ja soveltamisohjeita koko varmenneorganisaation ja -järjestelmän toimintaan. Varmentaja 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:

- Henkilöstöturvallisuus – työnjaot ja työtehtävät
- Fyysinen turvallisuus
- Varmentajan avaimiin liittyvä turvallisuus
- Varmenteiden 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

2.7.4 Poikkeamista johtuvat toimenpiteet

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

2.7.5 Tarkastuksen tuloksesta tiedottaminen

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

Varmentaja tiedottaa tarkastuksen tuloksista muun muassa Traficomille.

2.8 Tietojen julkaiseminen

2.8.1 Varmentajan julkaisemat tiedot

Varmennejärjestelmän tiedot ovat luottamuksellisia, elleivät ne perustu henkilötietolain, viranomaisten toiminnan julkisuudesta annetun lain, väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (304/2019) tai vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain säännöksiin tietojen luovuttamisesta tai varmennepolitiikassa tai varmennuskäytännössä määriteltyihin tarkoituksiin.

2.8.2 Julkiset tiedot

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

2.8.3 Tilapäisvarmenteen voimassaolon päättymiseen tai keskeyttämiseen liittyvät tiedot

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

2.8.4 Viranomaisille luovutettavat tiedot

Viranomaisille luovutettavat tiedot määritellään voimassa olevan lainsäädännön mukaisesti.

2.8.5 Muut tiedot

Varmennejärjestelmän tietoja ei luovuteta kuin edellä tässä kappaleessa mainittuihin tarkoituksiin.

2.8.6 Varmenteen haltijan pyynnöstä tapahtuva tiedon luovuttaminen

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

2.8.7 Muut tiedon luovuttamiseen liittyvät periaatteet

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

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

2.9 Immateriaalioikeudet

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

3 Varmenteen hakijan tunnistaminen

3.1 Rekisteröinti

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

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

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

Kun varmentaja myöntää tilapäisvarmenteen, se samalla hyväksyy varmennehakemuksen.

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

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

3.1.1 Nimeämiskäytännöt

Varmentajan juurivarmentaja on:

CN (Common name) = VRK Gov. Root CA

OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Vaestorekisterikeskus CA

S (State) = Finland

C (Country) = FI

Varmentajan tilapäisvarmenteiden varmentaja on:

CN (Common name) = VRK CA for Temporary Certificates - G2

OU (Organizational unit) = Tilapaisvarmenteet

O (Organization) = Vaestorekisterikeskus CA

C (Country) = FI

Varmenteen haltijan nimeämiskäytäntö tilapäisvarmenteissa:

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 Principal Name) = UPN-nimi

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

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

3.1.2 Yksityisten avainten toimittaminen varmenteen haltijalle

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

Tilapäisvarmenteen sisältävä varakortti luovutetaan varmenteen haltijalle vain henkilökohtaisesti tämän käydessä varmentajaa edustavan rekisteröijän luona. Tilapäisvarmenteen haltijan on osoitettava henkilöllisyytensä tavalla, joka vastaa hakemusvaiheessa noudatettua menettelyä. Tunnistustapa merkitään hakemuslomakkeeseen, jonka asiakkaan lisäksi allekirjoittaa myös varakortin luovuttava rekisteröijä.

3.2 Avainparin uusiminen

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

Tilapäisvarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

3.3 Avainparin uusiminen varmenteen sulkulistalle asettamisen jälkeen

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

Tilapäisvarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

3.4 Sulkupyynnön tekijän tunnistaminen

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

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

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

Kaikki sulkemiseen liittyvät sähköiset toimenpiteet arkistoidaan.

4 Toiminnalliset vaatimukset

4.1 Varmenteen hakeminen

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

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

Tilapäisvarmennetta haetaan käymällä henkilökohtaisesti rekisteröijänä toimivassa rekisteröintipisteessä. Varmennetta haettaessa henkilöllisyys tarkistetaan voimassa olevasta, poliisin myöntämästä henkilöllisyyden osoittavasta asiakirjasta, joita ovat 1.3.1999 jälkeen myönnetty henkilökortti ja passi. Hyväksyttäviä tunnistamisasiakirjoja ovat myös Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä voimassa oleva passi tai henkilökortti ja muun valtion viranomaisen myöntämä voimassa oleva passi.

Tieto tunnistustavasta merkitään hakemuslomakkeeseen ja rekisteröintipisteen virkailija vahvistaa omalla allekirjoituksellaan, että henkilöllisyyden tunnistus on tapahtunut.

4.2 Varmenteen myöntäminen

Varmentaja myöntää tilapäisvarmenteen hyväksyessään varmennehakemuksen.

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

4.3 Varmenteen vastaanottaminen

Tilapäisvarmennetta haetaan käymällä henkilökohtaisesti rekisteröintipisteellä. Tilapäisvarmenteen sisältävä varakortti yksilöidään ja luovutetaan kortinhaltijalle rekisteröintipisteellä.

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

4.4 Varmenteen voimassaolon päättyminen ja keskeyttäminen

4.4.1 Varmenteen sulkemisen edellytykset

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

4.4.2 Sulkupyynnön tekijä

Varmenteen sulkemisen tekee varmenteen haltijan organisaation rekisteröijä.

4.4.3 Sulkutapahtuma

Varmenteen sulkeminen voidaan tehdä varmentajan tarjoaman korttien tilaus- ja hallinnointijärjestelmän kautta

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

4.4.4 Tilapäisvarmenteen sulkeminen

Varmenteen haltija on vastuussa varmenteiden sulkemisesta. Tilapäisvarmenne voidaan sulkea, jolloin sen käyttö estyy. Sen sijaan kortin teknisellä alustalla mahdollisesti olevia muita sovelluksia voidaan edelleen käyttää niiden käyttötarkoitusten mukaisesti.

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

Suljettuja varmenteita ei voi palauttaa käyttöön.

4.4.5 Varmenteen sulkeminen varmentajan toimesta

Varmentaja ei suorita varmenteiden sulkemista muissa kuin seuraavissa tapauksissa:

- Varmentaja sulkee myöntämänsä varmenteet, mikäli varmenteiden tietosisällössä havaitaan virhe.
- Varmentaja voi sulkea yksityisellä avaimellaan allekirjoitetut varmenteet, mikäli on syytä epäillä varmentajan 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 varmentajan varmenteiden luonnissa käyttämä yksityinen avain tai muu tekninen menetelmä on paljastunut tai tullut muutoin käyttökelvottomaksi, varmentajan on ilmoitettava tapahtuneesta kaikille kortinhaltijoille ja Traficomille asianmukaisella tavalla.
- Varmentaja voi sulkea varmenteen myös muusta erityisestä syystä.

4.4.6 Sulkutapahtuman ajoitus

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

4.4.7 Varmenteen voimassaolon keskeyttämiseen liittyvät vaatimukset

Tilapäisvarmenteiden voimassaoloa ei voi keskeyttää tilapäisesti.

4.4.8 Keskeyttämispyynnön tekijä

Tilapäisvarmenteiden voimassaoloa ei voi keskeyttää tilapäisesti.

4.4.9 Keskeyttämispyynnön tekeminen

Tilapäisvarmenteiden voimassaoloa ei voi keskeyttää tilapäisesti.

4.4.10 Keskeyttämisajan rajoitukset

Tilapäisvarmenteiden voimassaoloa ei voi keskeyttää tilapäisesti.

4.4.11 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 voimassa olevan sulkulistan voimassaolon päättymisajankohtaan mennessä.

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

4.4.12 Sulkulistatarkistukseen liittyvät vaatimukset

Varmenteeseen luottavan osapuolen velvollisuudet on kuvattu luvussa 2.1.4.

4.4.13 Suorakäyttöinen varmenteen tilan tarkistaminen

Varmentaja tarjoaa suorakäyttöisen varmenteen tilan tarkistuspalvelun eli OCSP-palvelun. Varmentaja julkaisee suljetuista varmenteista sulkulistan.

4.4.14 Suorakäyttöiseen varmenteen tilan tarkistamiseen liittyvät vaatimukset

Varmentaja tarjoaa suorakäyttöisen varmenteen tilan tarkistuspalvelun.

4.4.15 Varmenteen haltijan yksityisen avaimen paljastumista koskevat erityisvaatimukset

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

4.5 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.

4.6 Varmenteisiin liittyvien tietojen arkistointi

4.6.1 Talletettava aineisto

Arkistoinnissa sovelletaan yleislakina arkistolain (831/1994) säännöksiä. Oikeus tietojensaantiin määräytyy viranomaisen toiminnan julkisuudesta annetun lain (621/1999) mukaisesti. Varmenteiden arkistoinnin osalta sovelletaan lisäksi, mitä sähköisen asioinnin lainsäädännössä on arkistoinnista määrätty.

Varmennerekisterin tiedot säilytetään vähintään 5 vuoden ajan varmenteiden voimassaolon päättymisestä tai jos kyseessä on sosiaali- ja terveydenhuollon henkilöstölle tai sosiaali- ja terveydenhuollon toimijoille luotava tilapäisvarmenne, niin edellisten lisäksi noudatetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007) ja laissa sähköisestä lääkemääräyksestä (61/2007) sekä niiden nojalla annettuja säädöksiä ja niiden nojalla asetettuja vaatimuksia.

Varmentaja arkistoi seuraavat tiedot:

a) Hakijan allekirjoittaman hakemuslomakkeen sekä tositteen varakortin ja siihen liittyvien yleisten käyttöehtojen vastaanottamisesta.
b) Myönnetyt varmenteet, niiden tietosisällöt 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) Voimassa oleva 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.

Arkistotiedot säilytetään viranomaista koskevien säännösten mukaisesti.

4.6.2 Arkistojen suojaus

Arkistoitava tieto säilytetään korkean turvatason tiloissa, joissa on pääsynvalvonta.

4.6.3 Arkistotietojen varmistusmenettelyt

Varmuuskopiot varastoidaan fyysisesti erilliseen tilaan alkuperäisistä tiedoista.

4.6.4 Arkistotietojen hankinta- ja varmistusmenetelmät

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.

4.7 Toiminnan jatkumisen hallinta ja poikkeustapausten käsittely

Varmentajalla on jatkuvuus- ja valmiussuunnitelma, joka mahdollistaa varmentajan toiminnan jatkuvuuden.

4.7.1 Varmentajan yksityinen avain on 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:

- 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.

- Varmentaja luo uuden avaimen luvun 6 mukaisesti.
- 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.
- Varmentaja arkistoi lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista mukaiset tiedot lain vaatimaksi ajaksi sekä noudattaa muutoinkin arkistolain säännöksiä tietojen arkistoinnin osalta.

4.7.2 Turvallisuuden vaarantuminen luonnonmullistuksen tai muun katastrofin seurauksena

Varmentajan turvapolitiikassa on otettu huomioon ulkoisen turvallisuuden vaarantumisen aiheuttamat toimenpiteet. Varmentaja on saanut ISO/IEC 27001 -tietoturvasertifikaatin, joka asettaa vaatimukset varmentajan toiminnalle myös mahdollisen katastrofin tapahduttua. Varmenteiden myöntämisen ja ylläpidon yhteydessä varmentaja noudattaa kohdassa 4.7 mainittuja menettelytapoja.

4.8 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:

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

15.9.2023

5 Fyysiset, toiminnalliset ja henkilöstöturvallisuuteen liittyvät vaatimukset

Varmentajalle on myönnetty tietoturvasertifikaatti, joka varmentaa, että varmentajan tietoturvallisuus täyttää standardin ISO/IEC 27001 vaatimukset.

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

Varmentaja noudattaa hyvää tiedonhallintatapaa. Varmenteiden tarjoamiseen liittyvät palvelut on organisoitu varmentajan 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

Varmentaja käyttää varmennetuotannon rekisteröintiin ja tietoteknisiin tehtäviin teknisiä toimittajia. Varmentaja 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 läsnä ollessa.

Varmentajan yksityisen avaimen peruuttaminen on mahdollista vain kahden oikeutetun henkilön valvonnassa.

Varmentajan yksityisen avaimen turvamoduulin alustuksessa on läsnä vähintään kaksi järjestelmän ylläpitotehtäviin oikeutettua henkilöä.

Järjestelmän käyttämiseen vaaditaan yhden tehtävään oikeutetun henkilön läsnäolo.

Tilapäisvarmenteen rekisteröiminen ja tunnistaminen vaatii yhden henkilön läsnäolon.

5.2.3 Tehtäväkohtainen tunnistaminen

Tilapäisvarmenteen rekisteröijä:

Rekisteröijä tunnistetaan käyttäjätunnuksella. Rekisteröijänä toimii organisaatio, jonka kanssa varmentaja on tehnyt rekisteröintiä koskevan sopimuksen.

Varmennejärjestelmän ylläpitäjä:

Tunnistetaan henkilökohtaisella järjestelmän hallintaan tarkoitetulla hallintakortilla. Järjestelmän ylläpitäjiä ovat varmennejärjestelmän toimittajan järjestelmäasiantuntijat sekä varmentajan tehtävään valtuutetut henkilöt.

Varmennejärjestelmän käyttäjä:

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

5.3 Henkilöturvallisuus

Varmentaja vastaa varmennetoiminnasta. Tekniset toimittajat on hankittu kilpailuttamalla ja ne toimivat varmentajan vastuulla ja lukuun.

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

5.3.1 Henkilökuntaa koskevan taustaselvityksen tekeminen

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

5.3.2 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 sekä 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.

5.3.3 Koulutukseen liittyvät vaatimukset

Varmentajan henkilökunnan on oltava koulutettu siten, että tehtävän hoitaminen parhaalla mahdollisella tavalla on mahdollista. Varmentajalla on koulutussuunnitelma, jonka toteuttamisesta varmentaja vastaa.

5.3.4 Asiantuntemuksen ja osaamisen ylläpito

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

5.3.5 Tehtäväkiertoon liittyvät vaatimukset

Kun varmentajan tehtävissä suunnitellaan tehtäväkiertoa, tehtävät organisoidaan siten, että henkilö voi huolehtia uusista tehtävistään parhaalla mahdollisella tavalla. Tehtäväkierron toteuttamisessa on otettava huomioon hyvän tietojenhallintatavan säilyminen ja riittävän tehtäväkohtaisen osaamistason ylläpitäminen.

Myös tehtäväkierrossa noudatetaan varmentajan tietoturvapolitiikkaa ja tietoturvasuunnitelmaa sekä varmentajan muita yleisiä ohjeita.

5.3.6 Poikkeamista johtuvat toimenpiteet

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

5.3.7 Organisaatiota edustava henkilökunta

Henkilökuntaa rekrytoitaessa on huolehdittava siitä, että henkilökunta vastaa taidoiltaan tehtävän edellyttämiä vaatimuksia ja että henkilön taustaselvityksestä ei ilmene mitään sellaista, että henkilön tehtävät ovat ristiriidassa varmennepalveluiden tuottamisen kanssa.

5.3.8 Henkilökunnan käyttöön annettavat asiakirjat

Henkilökunnalla on aina käytössään varmentajan 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 140-2 tai 140-3 tason 3 vaatimukset.

Varmenteen haltija:

Avainten luominen tehdään suoraan varmennuksen yhteydessä. Yksityinen avain säilytetään luku- ja kirjoitussuojattuna varakortilla.

Varmentaja luo varmenteen haltijan avaimet turvallisesti.

6.1.2 Yksityisen avaimen luovuttaminen varmenteen haltijalle

Tilapäisvarmenteen loppukäyttäjä asettaa yksityisen avaimen käyttöön tarvittavat PIN-tunnusluvut tilaisvarmennetta myönnettäessä rekisteröintipisteellä. PIN-tunnuslukujen asettamisessa on huolehdittava tietoturvallisista käytännöistä ja siitä, etteivät PIN-tunnusluvut tule rekisteröijän tietoon.

Tilapäisvarmenteen haltijan on osoitettava henkilöllisyytensä tavalla, joka vastaa hakemusvaiheessa noudatettua menettelyä. Tunnistustapa merkitään hakemuslomakkeeseen, jonka asiakkaan lisäksi allekirjoittaa myös varakortin 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 julkinen avain on varmentajan varmenteessa, joka sijoitetaan varakortille. Varmentajan varmenteet ovat vapaasti levitettävissä ja saatavilla myös julkisesta hakemistosta sekä varmentajan www-palvelusta.

6.1.5 Avainten pituudet

Tilapäisvarmenteen allekirjoittamiseen käytetty Varmentajan yksityinen avain sekä yksityistä avainta vastaava julkinen avain ovat vähintään 4096-bittisiä RSA-avaimia ja vähintään 384-bittisiä ECC-avaimia.

Varmenteen haltijan yksityinen ja julkinen avain ovat vähintään 2048-bittisiä RSA-avaimia tai vähintään 384-bittisiä ECC-avaimia.

6.1.6 Avainten käyttötarkoitukset

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

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

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

Avainten luontivaiheessa avaimia ei ole vielä kohdistettu kenellekään henkilölle.

6.2.4 Yksityisen avaimen varmuuskopio

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

6.2.5 Yksityisen avaimen arkistointi

Varmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa.

6.2.6 Yksityisen avaimen hallinnointi turvamoduuleissa

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

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

6.4 Aktivointitieto

6.4.1 Aktivointitiedon luominen ja käyttöönotto

Tilapäisvarmenteen loppukäyttäjä asettaa PIN-tunnusluvut tilaisvarmennetta myönnettäessä rekisteröintipisteellä.

Loppukäyttäjän asettama, yksilöllinen PIN-tunnusluku siirretään kortille varakortin yksilöinnin yhteydessä rekisteröintipisteellä.

Aktivointitiedon luomisessa huolehditaan, ettei PIN-tunnusluku tule missään vaiheessa rekisteröijän tietoon.

6.4.2 Aktivointitiedon suojaus

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

6.4.3 Muut aktivointitietoon liittyvät seikat

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

Tilapäisvarmenne lukkiutuu ja sen käyttö estyy kolmen peräkkäisen väärän PIN-tunnuksen antamisen jälkeen. Lukkiutunutta PIN-tunnusta ei pysty vapauttamaan. Tällöin henkilölle tulee tehdä uusi varakortti.

15.9.2023

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.

6.6 Varmennejärjestelmän elinkaaren hallinta

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

6.6.1 Järjestelmän kehittämiseen liittyvä valvonta

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

6.6.2 Turvallisuuden hallinta

Varmentajan tietoturvallisuutta hallitaan varmentajan tietoturvapolitiikan ja standardin ISO/IEC 27001 mukaisesti.

6.7 Tietoverkon turvallisuus

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

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.

6.8 Turvamoduulin käytön valvonta

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

Turvamoduulin käyttöön tarvitaan aina hallintakortti 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.dvv.fi.

7.2 Sulkulistaprofiili

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

8 Määritysasiakirjojen hallinta

8.1 Määritysten muuttaminen

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

8.2 Julkaiseminen ja tiedottaminen

Varmentaja julkaisee varmennepolitiikan ja varmennuskäytännön, jotka ovat saatavilla internet-sivuilla www.dvv.fi/cps.

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

Varmentaja hyväksyy sekä tilapäisvarmennetta koskevan varmennepolitiikan että varmennuskäytännön. Asiakirjoja voidaan muuttaa varmentajan sisäisin muutosmenettelyin.

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

15.9.2023

Varmentaja 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 varmentajan mielestä eivät merkittävästi vaikuta varmenteiden haltijoihin ja luottaviin osapuoliin, voidaan muuttaa ilmoittamalla niistä 14 päivää aikaisemmin.