DIGI- JA VÄESTÖTIETO-VIRASTO

VARMENNUSKÄYTÄNTÖ KANSALAIS-VARMENNE

Digi- ja väestötietoviraston henkilökortilla olevaa kansalaisvarmennetta varten v. 1.0

OID: 1.2.246.517.1.10.202.1

13.3.2023

[Yksikkö] / Kytölä Sanni

13.3.2023

Dokumentinhallinta

Omistaja	
Laatinut	Tuire Saaripuu
Tarkastanut	
Hyväksynyt	Joonas Kankaanrinne

Version hallinta

versionro	mitä tehty	pvm/henkilö
v.1.0	Hyväksytty versio 1.0, eIDAS-asetuksen mukainen asiakirja	3.5.2018 TS
v 1.1	Päivitetty versio, viraston nimenmuutos, julkaiseminen.	1.1.2020 TS
v 1.2	Päivitetty versio	6.5.2021
v 1.3	Päivitetty versio ja linkit varmennepolitiikkasivulle	21.9.2022/SK
v 1.4	Tarkennettu aktivointitunnusluvun määritelmää. Tarkennettu ISO IEC 27001 -standardin määritelmää. Päivitetty linkit.	8.3.2023/AG

Sisällysluettelo

1 Määritelmät ja lyhenteet

1.1 Määritelmät

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

Aktivointitunnusluku: Kansalaisvarmenteen käyttäjä saa kortin käyttämistä varten haltuunsa henkilökohtaisen aktivointitunnusluvun, jonka jälkeen käyttäjä voi aktivoida ja määritellä omat, henkilökohtaiset PIN-tunnuslukunsa. Aktivointiprosessin jälkeen käyttäjä pystyy käyttämään henkilökorttiaan sähköisessä asioinnissa. Aktivointitunnuslukua voidaan 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 allekirjoitusvarmenne sekä 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.

Henkilökortti: Poliisin myöntämä henkilöllisyystodistus, jonka tekniseen osaan on talletettu kortinhaltijan kansalaisvarmenne.

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.

Kansalaisvarmenne: Digi- ja väestötietoviraston luonnolliselle henkilölle myöntämä allekirjoitusvarmenne, jonka tietosisältö on määritelty laissa Digi- ja väestötietoviraston varmennepalveluista (661/2009).

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

Allekirjoitusvarmenne: Varmenne, 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.

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

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

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

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

Osa kansalaisvarmenteeseen liittyvistä avainpareista on 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.

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

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 10 vuoden ajan varmenteen voimassaolon päättymisestä.

Varmennetietojärjestelmä: Tietotekninen järjestelmä, joka koostuu varmennejärjestelmistä, tietoliikenteestä, varmennehakemistosta ja sulkulistapalvelusta, neuvonta- ja sulkupalvelusta sekä varmenteiden ja korttien hallinnoinnista.

Varmennuskäytännön yksilöivä tunnus on osa varmenteen tietosisältöä.

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

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

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

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

Varmenteen hakija: Henkilö, joka hakee kansalaisvarmennetta 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.

1.2 Lyhenneluettelo

CA	Certification Authority, varmentaja
CP	Certificate Policy, varmennepolitiikka
CPS	Certification Practise Statement, varmennuskäytäntö
CRL	Certificate Revocation List, sulkulista
FINEID	Finnish Electronic Identification
HSM	Hardware Security Module, turvamoduuli
HST	Henkilön sähköinen tunnistaminen
HTTP	Hypertext Transfer Protocol
ISO 27001	ISO IEC 27001, Kansainvälinen standardi tietoturvan hallinnalle
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol, suorakäyttöinen varmenteen tilatiedon tarkistamispalvelu
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
SATU	Sähköinen asiointitunnus
SIM	Subscriber Identity Module
DVV	Digi- ja väestötietovirasto

2 Johdanto

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

Tätä varmennuskäytäntöä sovelletaan henkilökortilla olevaan Digi- ja väestötietoviraston kansalaisvarmenteeseen, joka myönnetään väestötietojärjestelmään rekisteröidyille Suomen kansalaisille ja Suomessa pysyvästi asuville ulkomaalaisille.

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

2.1 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 varmennuskäytännön mukainen varmenne perustuu julkisen avaimen järjestelmään ja menetelmiin. Tämän varmennuskäytännön mukaisten varmenteiden tietosisältö on määritelty laissa Digi- ja väestötietoviraston varmennepalveluista (661/2009) ja vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun laissa (617/2009).

Digi- ja väestötietovirasto (DVV) toimii valtiovarainministeriön hallinnonalalla. DVV on henkilörekisteriä ylläpitävä viranomainen, jonka Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2009) mukainen tehtävä on tuottaa varmennettuja sähköisen asioinnin palveluita. Digi- ja väestötietovirasto toimii myös sosiaali- ja terveydenhuollon lakisääteisenä varmentajana 1.12.2010 alkaen (laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) ja laki sähköisestä lääkemääräyksestä (61/2007). Digi- ja väestötietoviraston Varmennepalvelut- toiminto vastaa viraston varmennetoiminnasta. DVV on tarjonnut varmennepohjaisia allekirjoitus- ja tunnistusvälineitä vuodesta 1999 lähtien ja toiminut laatuallekirjoitusvarmentajana 31.3.2003 lukien.

DVV:n varmennetietojärjestelmä ja varmennepalvelut perustuvat julkisen avaimen järjestelmään (Public Key Infrastructure eli PKI). DVV:n varmenneinfrastruktuuri muodostuu varmennejärjestelmästä, kortteihin sisältyvien varmennetietojen toimittajasta, sulkulistasta, neuvontapalvelusta ja hakemistopalvelusta. DVV:n toimintoja varmentajana ovat varmenne-, hakemisto- ja sulkupalveluiden tuottaminen, rekisteröinti sekä

varmenteen sisältävän kortin valmistus ja yksilöinti. DVV vastaa koko varmennejärjestelmän toimivuudesta, myös käyttämiensä rekisteröijien ja teknisten toimittajien osalta. 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. Jokaisella asiakirjalla on oma yksilöivä OID-tunnuksensa. Nämä asiakirjat ovat saatavilla sähköisesti osoitteessa www.dvv.fi.

Varmentajana toimiva Digi- ja väestötietovirasto yksilöi varmenteen haltijan sähköisen asiointitunnuksen (SATU) avulla, joka on myös osa varmenteen tietosisältöä. Sähköinen asiointitunnus on sähköistä asiointia varten erikseen luotu laissa Digi- ja väestötietoviraston varmennepalveluista (661/2009) määritelty tekninen tunnistetieto, joka ei sisällä henkilöön liittyviä tunnistetietoja.

Kansalaisvarmenne voidaan myöntää ja tallettaa erilaisille teknisille alustoille eli mikrosiruille kuten henkilökortille, sirulliselle pankin maksukortille ja mobiilipäätelaitteen SIM-kortille. Tämä varmennuskäytäntö on kuvaus henkilökortilla olevasta kansalaisvarmenteesta.

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. Asetuksen sääntelyyn liittyvät vaatimuksen on saatettu voimaan Suomen lainsäädäntöön lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) annetulla muutoksella 1.7.2016. Lailla säädetään vahvan sähköisen tunnistamisen palvelujen tarjoamisesta sekä sähköisestä allekirjoituksesta ja niiden oikeusvaikutuksista. Henkilökortista on säädetty henkilökorttilaissa (663/2016).

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

Kansalaisvarmenne koostuu kolmesta eri varmenteesta, joilla on kaksi eri käyttötarkoitusta: todentaminen- ja salaus sekä sähköiset allekirjoitukset. Todentamisvarmenne on mainitun lain mukainen vahvan sähköisen tunnistamisen väline. Allekirjoitusvarmenteet ovat vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaisia sähköisiä allekirjoitusvälineitä. Toinen saman vaatimustason täyttävistä allekirjoitusvarmenteista on toteutettu RSA-algoritmiin ja toinen ECC-algoritmiin perustuen. Varmenteen haltija voi käyttää kumpaa tahansa näistä varmenteista sähköisiin allekirjoituksiin.

Tämä varmennuskäytäntö kuvaa Asetukseen perustuvan, vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaisen sähköisen allekirjoituksen allekirjoitusvarmenteen myöntämiseen, tuottamiseen ja vastuun jakoon liittyviä yksityiskohtaisia vaatimuksia. Tämän varmennuskäytännön mukaisesti myönnettäviä allekirjoitusvarmenteita voi käyttää sellaisten sähköisten allekirjoitusten

vahvistamisessa, jotka vastaavat hyväksytyiltä sähköisten allekirjoitusten varmenteilta ja luontivälineiltä edellytettäviä vaatimuksia kuten Asetuksen 28 ja 29 artiklassa säädetään. Tunnistusvarmenteen taso täyttää Asetuksen ja sen nojalla annetun varmuustasoasetuksen mukaisesti vaatimustason ”korkea”.

Tämä asiakirja kuvaa myös kansalaisvarmenteeseen 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.

2.2 Tunnistetiedot

Tämän varmennuskäytännön nimi on Varmennuskäytäntö henkilökortilla olevaa kansalaisvarmennetta varten, jonka OID on 1.2.246.517.1.10.202.1.Tämä varmennuskäytäntö viittaa Varmennepolitiikkaan Digi- ja väestötietoviraston kansalaisvarmennetta varten, OID 1.2.246.517.1.10.202.

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

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

2.3 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 Digi- ja väestötietovirasto. Digi- ja väestötietoviraston varmennepalvelu jakaantuu toiminnallisesti seuraaviin osa-alueisiin:

2.3.1 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 tilatiedon oikeellisuudesta sekä varmenteiden sulkulistojen julkaisemisesta
- noudattaa varmenteen haltijoiden henkilötietojen käsittelyssä hyvää tietosuojan tasoa sekä hyvää tietojenkäsittelytapaa.

2.3.2 Rekisteröijä

Henkilökortilla olevan kansalaisvarmenteen rekisteröijänä toimii poliisi.

- Rekisteröijä toimii varmentajan toimeksiannosta ja vastuulla.
- Rekisteröijä noudattaa varmentajan varmennepolitiikkaa ja varmennuskäytäntöä.
- Rekisteröijä tunnistaa varmenteen hakijan varmennuskäytännön mukaisella tavalla
- Henkilökortilla olevan kansalaisvarmenteen korttialustan on tuottanut Poliisi.
- Rekisteröijänä toimiva Poliisi toimittaa henkilökortilla olevan kansalaisvarmenteen hakemiseen liittyvät henkilön tunnistamiseen liittyvät tiedot, joiden perusteella kansalaisvarmenne luodaan.

2.3.3 Toimikortin valmistaja ja yksilöijä

- Valmistaja toimii varmenteen, siihen liittyvien avainparien ja aktivointitietojen osalta varmentajan toimeksiannosta ja vastuulla ja yhteistyösopimuksen mukaisesti.
- Valmistaja noudattaa varmentajan varmennepolitiikkaa ja varmennuskäytäntöä.
- Toimikortit yksilöidään rekisteröijän toimittamien tietojen mukaisesti.

2.3.4 Sulkupalvelu

Varmenteiden sulkupalvelu sulkee varmenteet, jotka varmenteen haltija tai varmentaja haluaa suljettavaksi ennen varmenteen voimassaoloajan päättymistä. Suljetut varmenteet toimitetaan sulkulistalle. Syy henkilökortilla olevan kansalaisvarmenteen sulkemiseen voi olla esimerkiksi henkilökortin katoaminen.

2.3.5 Hakemistopalvelu

Hakemistopalvelu on julkinen Internet-palvelu, josta on saatavilla kaikki varmentajan myöntämät kansalaisvarmenteen tunnistusvarmenteet sekä varmentajan varmenteet sekä sulkulista. Hakemistopalvelu on saatavissa osoitteesta ldap://ldap.fineid.fi.

2.3.6 Varmenteen haltija

Tämän varmennuskäytännön mukainen kansalaisvarmenne voidaan myöntää Suomen kansalaiselle tai kotikuntalain (201/1994) mukaisesti Suomessa vakinaisesti asuvalle ulkomaalaiselle, jonka henkilötiedot on talletettu väestötietojärjestelmään.

Varmenteen haltijan tulee noudattaa varmentajan varmennepolitiikkaa ja varmennuskäytäntöä.

2.3.7 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.

2.3.8 Varmenteen käyttäminen

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

2.4 Yhteystiedot

2.4.1 Varmennuskäytäntöä hallinnoiva organisaatio

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

Tämän varmennuskäytännön mukaiset tekijänoikeudet kuuluvat Digi- ja väestötietovirastolle.

2.4.2 Yhteyshenkilö

Varmennuskäytäntöön liittyviin kysymyksiin sekä näihin asiakirjoihin liittyvästä viestinnästä vastaa Digi- ja väestötietoviraston kirjaamo, sähköpostiosoite kirjaamo@dvv.fi.

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

Digi- ja väestötietovirasto (DVV) Varmennepalvelut

PL 123

00531 Helsinki

www.dvv.fi

3 Yleiset ehdot

Tämä varmennuskäytäntö astuu voimaan 13.3.2023. Varmennuskäytännön muutosmenettely ja julkaiseminen on kuvattu tämän asiakirjan kohdassa 8.

3.1 Velvollisuudet

3.1.1 Varmentajan velvollisuudet

- Digi- ja väestötietovirastolla on lakisääteinen tehtävä toimia varmentajana.
- Varmentaja noudattaa toiminnassaan voimassaolevaa lainsäädäntöä.
- Varmentaja toimii huolellisesti, luotettavasti ja asianmukaisesti.
- Varmentajalla on riittävät tekniset taidot ja taloudelliset voimavarat varmennetoiminnan asianmukaiseksi järjestämiseksi sekä mahdollisen vahingonkorvausvastuun kattamiseksi.
- Varmentaja vastaa kaikista varmennetoiminnan osa-alueista, myös varmentajan apunaan käyttämien teknisten toimittajien ja henkilöiden, kuten rekisteröijien ja kortinvalmistajien tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta.
- Varmentaja laatii ja ylläpitää varmennepolitiikkaa, joka kuvaa kansalaisvarmenteen myöntämisessä, ylläpidossa ja hallinnoinnissa käytettävät menettelytavat, käyttöehdot, vastuiden jaot ja muut kansalaisvarmenteen käyttöön liittyvät näkökulmat yleisellä tasolla.
- Varmentaja laatii ja ylläpitää varmennuskäytäntöjä, jotka kuvaavat, miten varmentaja soveltaa varmennepolitiikkaa.
- Varmentaja noudattaa varmennepolitiikan ja varmennuskäytännön vaatimuksia.

- 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.

3.1.2 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.

3.1.3 Varmenteen haltijaa koskevat velvollisuudet

- Varmenteen käyttötarkoitus on määritelty kunkin varmenteen varmennepolitiikassa, varmennuskäytännössä sekä varmenteen haltijan käyttöohjeissa. Varmennetta saa käyttää vain sen käyttötarkoituksen mukaisesti sähköiseen allekirjoitukseen, todentamiseen tai tiedon salaamiseen.
- Kansalaisvarmenteen haltija vastaa siitä, että kansalaisvarmennetta haettaessa ilmoitetut tiedot ovat oikeita.
- Kansalaisvarmenteen haltija on vastuussa henkilökortin ja sillä olevan kansalaisvarmenteen käytöstä, niillä tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista. Allekirjoitusvarmenteen osalta noudatetaan, mitä Asetuksessa on määrätty.

- Kansalaisvarmenteen haltija säilyttää yksityiset avaimensa ja niiden käyttämiseen tarvittavat tunnusluvut erillään sekä pyrkii estämään yksityisten avaintensa katoamisen, joutumisen ulkopuolisten käsiin, muuttamisen tai luvattoman käytön. Henkilökortin luovuttaminen tai aktivointitunnuksen paljastaminen toiselle henkilölle esim. lainaamalla vapauttaa varmentajan ja kansalaisvarmenteeseen luottavan osapuolen kortin käyttämisestä mahdollisesti aiheutuvista vastuista.

- Kansalaisvarmenteen sisältävää henkilökorttia käsitellään ja suojataan samalla huolellisuudella kuin muita vastaavia kortteja tai asiakirjoja, kuten esimerkiksi luottokortteja, ajokorttia ja passia. Henkilökohtaiset aktivointitunnukset on säilytettävä fyysisesti eri paikassa kuin henkilökortti.

- Kansalaisvarmenteen ja henkilökortin 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.

3.1.4 Kansalaisvarmenteeseen luottavaa osapuolta koskevat velvollisuudet

Varmenteeseen luottavan osapuolen velvollisuus on varmistaa, että varmennetta käytetään käyttötarkoituksensa mukaisesti. Henkilökortilla olevan kansalaisvarmenteen allekirjoitusvarmenteen käyttötarkoitus on sähköinen allekirjoitus. Todennus- ja salausvarmenteen käyttötarkoitus on henkilön todentaminen ja tiedon salaus.

Varmenteeseen luottavan osapuolen on noudatettava varmennepolitiikkaa ja varmennuskäytäntöä.

Kansalaisvarmenteeseen luottava osapuoli voi vilpittömässä mielessä luottaa kansalaisvarmenteeseen, kun hän on tarkistanut, että ***kansalaisvarmenne on voimassa.*** Kansalaisvarmenteeseen luottavalla osapuolella on velvollisuus tarkistaa varmenteet sulkulistalta. Varmenteen voimassaolo voidaan tarkistaa suorakäyttöisestä varmenteen tilatiedon tarkistuspalvelusta eli OCSP-palvelusta. Kansalaisvarmenteen voimassaolon luotettavuuden varmistamiseksi kansalaisvarmenteeseen luottavan osapuolen on noudatettava alla esitettyjä sulkulistan tarkistustoimia.

Jos kansalaisvarmenteeseen 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, kansalaisvarmennetta ei pidä hyväksyä, mikäli viimeisen saadun sulkulistan voimassaoloaika on päättynyt. Kaikki kansalaisvarmenteen hyväksymiset tämän voimassaoloajan jälkeen tapahtuvat kansalaisvarmenteeseen luottavan osapuolen omalla riskillä.

3.1.5 Kansalaisvarmenteen julkaisemiseen liittyvät velvollisuudet

Kansalaisvarmenteen tunnistusvarmenteet julkaistaan yleisesti saatavilla olevassa julkisessa hakemistossa ja suljetut kansalaisvarmenteet sulkulistalla, josta varmen-

teeseen luottavan osapuolen on tarkistettava sen voimassaolotieto. Varmenteen voimassaolo voidaan tarkistaa suorakäyttöisestä varmenteen tilatiedon tarkistuspalvelusta eli OCSP-palvelusta.

3.2 Vastuut

3.2.1 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 kansalaisvarmenne on luotu noudattaen laissa Digi- ja väestötietoviraston varmennepalveluista (661/2009), laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista, laissa sähköisestä asioinnista viranomaistoiminnassa ja varmennepolitiikassa sekä varmennuskäytännössä esitettyjä menettelyjä ja varmenteen hakijan antamien tietojen mukaisesti. Digi- ja väestötietovirasto vastaa ainoastaan niistä tiedoista, jotka se on tallettanut kansalaisvarmenteeseen.

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

Allekirjoittaessaan kansalaisvarmenteen yksityisellä avaimellaan varmentaja vakuuttaa tarkistaneensa kansalaisvarmenteessa olevat henkilötiedot varmennepolitiikassa ja varmennuskäytännössä esitettyjen menettelyjen mukaisesti.

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

3.2.2 Rekisteröijän vastuut

Henkilökortin rekisteröijänä toimii poliisi, joka rekisteröi varmenteen hakijan varmentajana toimivan Digi- ja väestötietoviraston lukuun. Poliisin toimista rekisteröinnin yhteydessä on tarkemmin säädetty henkilökorttilaissa.

3.2.3 Kansalaisvarmenteen haltijan vastuut

Kansalaisvarmenne on haltijansa sähköinen henkilöllisyys eikä sitä tämän vuoksi saa luovuttaa toisen henkilön käytettäväksi.

Kansalaisvarmenteen haltija on vastuussa sen käytöstä, sillä tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista.

Henkilökortin jättäminen lukijalaitteeseen saattaa mahdollistaa kortin väärinkäytön. Lopettaessaan pääteistunnon tai jättäessään päätelaitteen valvomatta kansalaisvarmenteen haltijan vastuulla on ottaa henkilökortti pois lukijalaitteesta ja sulkea käytetyt sovellukset asianmukaisesti.

Henkilökortilla olevan kansalaisvarmenteen haltijan vastuu kansalaisvarmenteen käyttämisestä päättyy, kun hän on ilmoittanut sulkupalveluun tarvittavat tiedot kansalaisvarmenteen sulkemiseksi ja saatuaan puhelun vastaanottaneelta virkailijalta sulkemista koskevan ilmoituksen. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

3.2.4 Kansalaisvarmenteeseen luottavan osapuolen vastuut

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

3.2.5 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).

Sähköisestä henkilökortista on säädetty henkilökorttilaissa ja Digi- ja väestötietoviraston myöntämistä varmenteista on säädetty Digi- ja väestötietoviraston varmennepalveluista annetussa laissa (661/2009). Hallinnon asioinnista on säädetty myös sähköisestä asioinnista viranomaistoiminnassa annetussa laissa (13/2003).

Digi- ja väestötietovirasto ei vastaa aktivointitunnusten ja kansalaisvarmenteen haltijan yksityisten avainten paljastumisen seurauksena syntyvistä vahingoista, ellei paljastuminen välittömästi johdu Digi- ja väestötietoviraston välittömästä toiminnasta.

Digi- ja väestötietovirasto vastaa kansalaisvarmenteen haltijalle ja kansalaisvarmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Digi- ja väestötietoviraston välittömästä toiminnasta.

Digi- ja väestötietovirasto ei vastaa kansalaisvarmenteen haltijalle aiheutuneista välillisistä tai seurannaisvahingoista. Digi- ja väestötietovirasto ei myöskään vastaa kansalaisvarmenteeseen luottavan osapuolen tai henkilökortin 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 kansalaisvarmenteen haltijan käyttämän laitteen tai ohjelmiston toimimattomuudesta eikä siitä, että kansalaisvarmennetta 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. Kansalaisvarmenteen haltijan tai kansalaisvarmenteeseen luottavan osapuolen on vastattava tämän vuoksi aiheutuvista omista kustannuksistaan eikä varmentaja ole velvollinen korvaamaan kansalaisvarmenteen haltijalle tai kansalaisvarmenteeseen luottavalle osapuolelle tällaisesta varmentajan kehittämistyöstä aiheutuvista kustannuksista.

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

Henkilökortin haltijan vastuu sillä olevan kansalaisvarmenteen käyttämisestä päättyy, kun hän on ilmoittanut sulkupalveluun tarvittavat tiedot kansalaisvarmenteen sulkemiseksi ja saatuaan puhelun vastaanottaneelta virkailijalta ilmoituksen kansalaisvarmenteen sulkulistalle viemisestä. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

3.3 Taloudellinen vastuu

3.3.1 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 kansalaisvarmenteeseen luottavalle osapuolelle enintään välittömistä vahingoista, mikäli vahinko johtuu Digi- ja väestötietoviraston toiminnasta.

3.3.2 Muut osapuolet

Kansalaisvarmenteeseen luottava osapuoli voi luottaa kansalaisvarmenteen ja sähköisen allekirjoituksen oikeellisuuteen, jos hän on tarkastanut, ettei kansalaisvarmennetta ole asetettu sulkulistalle eikä varmenteen voimassaoloaika ole päättynyt eikä hänellä ole muita syitä perustellusti epäillä varmenteen käytön oikeellisuutta. Varmenteen voimassaolo voidaan tarkistaa suorakäyttöisestä varmenteen tilatiedon tarkistuspalvelusta eli OCSP-palvelusta.

Varmentaja vastaa kansalaisvarmenteesta sen mukaisesti kuin varmentaja on sitoutunut tässä varmennuskäytännössä ja kansalaisvarmennetta koskevassa varmennepolitiikassa.

3.3.3 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.

3.4 Tulkinta ja täytäntöönpano

3.4.1 Sovellettava lainsäädäntö

Tämän varmennuskäytännön mukaisesti myönnetty allekirjoitusvarmenne täyttää 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 annetun asetuksen allekirjoitusvarmenteelle asettamat vaatimukset.

Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009) on säädetty allekirjoitusvarmenteella tehdyistä sähköisistä luottamuspalveluista. Henkilökortista on säädetty henkilökorttilaissa ja Digi- ja väestötietoviraston myöntämistä varmenteista on säädetty laissa Digi- ja väestötietoviraston varmennepalveluista (661/2009).

Varmennepalveluiden tuottamiseen liittyvä Digi- ja väestötietoviraston vahingonkorvausvastuu määräytyy vahingonkorvauslain (412/1974) säännösten mukaisesti. Digi- ja väestötietovirastoa koskevat myös vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun (617/2009) ja sähköisestä asioinnista viranomaistoiminnassa annetun lain (13/2003) mukaiset vaatimukset.

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 tietojenhallintatapaa. 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 Poliisilta. Tässä toiminnassa Digi- ja väestötietovirasto noudattaa julkisen hallinnon yhteispalvelusta annetussa laissa (2007/223) noudatettuja säännöksiä.

Digi- ja väestötietoviraston asemasta on säädetty laissa Digi- ja väestötietovirastosta (304/2019). Allekirjoitusvarmentajia valvoo Suomessa Traficom.

Digi- ja väestötietovirasto vastaa siitä, että henkilökortilla oleva kansalaisvarmenne on luotu noudattaen laissa Digi- ja väestötietoviraston varmennepalveluista (661/2009), laissa sähköisistä luottamuspalveluista, laissa sähköisestä asioinnista

viranomaistoiminnassa ja varmennepolitiikassa esitettyjä menettelyjä ja henkilökortin 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. Digi- ja väestötietoviraston varmennetoimintaa valvoo Traficom ja henkilötietojen käsittely osalta Digi- ja väestötietovirasto noudattaa henkilötietolakia. Digi- ja väestötietovirasto on myös jatkuvassa yhteistyössä henkilötietojen käsittelyn osalta Tietosuojavaltuutetun kanssa.

Valitusten ja riitojen ratkaisussa sekä hallinnollisessa valvonnassa ja lainkäytössä noudatetaan voimassaolevaa lainsäädäntöä. Allekirjoitusvarmenteiden tuotannossa huomioon on otettava erityisesti laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista.

3.4.2 Erimielisyyksien ratkaiseminen

Digi- ja väestötietovirasto vastaa kansalaisvarmenteita myöntäessään siitä, että kansalaisvarmenne täyttävää tässä varmennuskäytännössä sekä kansalaisvarmennetta koskevassa varmennepolitiikassa esitetyt vaatimukset.

Mahdolliset erimielisyydet ratkaistaan Suomen oikeusjärjestyksen mukaisesti. Valitusten ja riitojen ratkaisussa sekä hallinnollisessa valvonnassa ja lainkäytössä noudatetaan voimassaolevaa lainsäädäntöä. Allekirjoitusvarmenteen tuotannossa on huomioon otettava erityisesti laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista.

3.5 Maksut

Tässä kappaleessa on määritelty henkilökortilla olevan kansalaisvarmenteen käyttöön liittyvät maksut.

3.5.1 Kansalaisvarmenteen myöntäminen ja uusiminen

Henkilökortilla oleva kansalaisvarmenne haetaan poliisin toimipisteestä. Henkilökortilla oleva kansalaisvarmenne myönnetään aina uuden hakemuksen perusteella noudattaen henkilökorttilaissa määriteltyä tunnistamismenettelyä. Henkilökortin hankintahinta määräytyy kulloisenkin valtiovarainministeriön asetuksen Digi- ja väestötietoviraston suoritteista mukaisesti.

3.5.2 Kansalaisvarmenteen käyttöön liittyvät maksut

Varmentaja ei erikseen veloita kansalaisvarmenteen haltijaa kansalaisvarmenteen, sulkupalvelun tai julkisen hakemiston käytöstä. Yksittäiset verkkopalveluntarjoajat saattavat veloittaa oman palvelunsa käytöstä. Kansalaisvarmenteiden käyttö ei vaadi erillistä ilmoitusta tai lupaa varmentajalta.

3.5.3 Kansalaisvarmenteen sulkulistamerkintään liittyvät maksut

Kansalaisvarmenteen ilmoittaminen sulkulistalle on maksutonta. Myös sulkulistojen noutaminen hakemistosta sekä kansalaisvarmenteen voimassaolon tarkistaminen sulkulistalta on maksutonta.

3.5.4 Muut maksut

Neuvontapalvelun käytöstä peritään erillinen maksu voimassaolevan hinnaston mukaisesti.

Jos palveluntarjoaja haluaa järjestää tietohuoltopalvelun kansalaisvarmenteen haltijan 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.

3.6 Tietojen julkaiseminen ja saatavuus

3.6.1 Varmentajan tietojen julkaiseminen

Varmentaja julkaisee kaikki kansalaisvarmenteen tunnistusvarmenteetja sulkulistat maksuttomassa, yleisesti saatavilla olevassa julkisessa hakemistossa. Varmentaja julkaisee varmennepolitiikan, varmennuskäytännöt, varmennekuvauksen (PDS) sekä muut julkiset varmennepalvelujen tuottamiseen liittyvät dokumentit www-sivuillaan, www.dvv.fi/cps.

3.6.2 Julkaisutiheys

Tunnistusvarmenne julkaistaan julkisessa hakemistossa heti, kun se on luotu, ja se on hakemistossa koko voimassaolonsa ajan. Varmentaja julkaisee sulkulistan, joka on voimassa kahdeksan tuntia julkaisemisestaan. Tämä sulkulista päivitetään kerran tunnissa uudella sulkulistalla.

3.6.3 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.

3.6.4 Tietovarastot

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

3.7 Tietoturvatarkastus

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

3.7.1 Tarkastusten tiheys

Digi- ja väestötietovirasto tekee tietoturvatarkastuksen teknisten toimittajiensa toimitiloista, laitteista ja toiminnasta 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.

3.7.2 Tarkastaja

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

3.7.3 Tarkastuksen kohteet ja kattavuus

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

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

Tarkastus kattaa Traficomin antamat määräykset varmentajan toiminnan tietoturvallisuudesta.

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
- 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

3.7.4 Poikkeamista johtuvat toimenpiteet

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

3.7.5 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.

3.8 Tietojen julkaiseminen

3.8.1 Varmentajan julkaisemat tiedot

Varmennejärjestelmän tiedot ovat luottamuksellisia, elleivät ne perustu henkilötietolain, viranomaisten julkisuudesta annetun lain, Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2009) tai vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain säännöksiin tietojen luovuttamisesta tai varmentajan varmennepolitiikassa tai varmennuskäytännössä määriteltyihin tarkoituksiin.

3.8.2 Julkiset tiedot

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

3.8.3 Kansalaisvarmenteen voimassaolon päättymiseen tai keskeyttämiseen liittyvät tiedot

Kansalaisvarmenteen voimassaoloaika on merkitty kansalaisvarmenteeseen. Kesken voimassaoloajan suljetut kansalaisvarmenteet julkaistaan yleisesti saatavilla olevalla sulkulistalla.

3.8.4 Viranomaisille luovutettavat tiedot

Viranomaisille luovutettavat tiedot määritellään voimassaolevan lainsäädännön mukaisesti.

3.8.5 Muut tiedot

Varmennejärjestelmän tietoja ei luovuteta kuin edellä tässä kappaleessa mainittuihin tarkoituksiin.

3.8.6 Varmenteen haltijan pyynnöstä tapahtuva tiedon luovuttaminen

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

3.8.7 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.

3.9 Immateriaalioikeudet

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

4 Varmenteen hakijan tunnistaminen

4.1 Rekisteröinti

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

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.

Hakemusasiakirjassa ja käyttöehdoissa mainitaan selkeästi, että kansalaisvarmenteen hakija vahvistaa allekirjoituksellaan annettujen tietojen oikeellisuuden sekä hyväksyy kansalaisvarmenteen luomisen ja julkaisun julkisessa hakemistossa. Samalla hakija hyväksyy kansalaisvarmenteen käyttöön liittyvät säännöt ja ehdot sekä huolehtii kansalaisvarmenteen ja niiden aktivointitunnusten säilyttämisestä sekä mahdollisen väärinkäytön tai kortin katoamisen ilmoittamisesta.

Varmentajan ja rekisteröijän, kortinvalmistajan sekä muiden varmennepalveluiden osa-alueita tuottavien toimittajien kesken on laadittu sopimus, joka ilmaisee kiistattomasti kaikkien osapuolten oikeudet, vastuut ja velvoitteet.

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

Kun Varmentaja myöntää kansalaisvarmenteen, se samalla hyväksyy varmennehakemuksen.

Kansalaisvarmenteen hakija voi halutessaan tallettaa sähköpostiosoitteen sekä varmenteeseen että väestötietojärjestelmään. Sähköpostiosoite merkitään sekä varmenteeseen että väestötietojärjestelmään hakijan ilmoittamassa muodossa. Kansalaisvarmenteeseen merkitty sähköpostiosoite talletetaan julkiseen hakemistoon samoin kuin muu tunnistussvarmenteen tietosisältö. Sähköpostiosoitetta ei voi muuttaa kansalaisvarmenteen voimassaoloaikana.

Kansalaisvarmenteen käyttäminen sähköisissä verkkopalveluissa edellyttää tähän tarvittavan kortinlukijaohjelmiston hankkimista. Digi- ja väestötietoviraston Internetsivuilta www.dvv.fi voi varmenteen haltija ladata käyttöönsä sen käyttämisessä tarvittavan kortinlukijaohjelmiston, jonka avulla on myös mahdollista vaihtaa henkilökortilla olevat PIN-tunnukset.

Kansalaisvarmenteen haltijan vastuulla on estää hänelle kuuluvien yksityisten avaintensa ja niihin liittyvien aktivointitunnusten käyttäminen käyttöehtojen vastaisella tavalla huolehtimalla kortistaan ja tunnusluvuistaan käyttöehdoissa mainitulla tavalla.

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

4.1.1 Nimeämiskäytännöt

Digi- ja väestötietoviraston juurivarmentaja on:

CN = VRK Gov. Root CA - G2

OU = Varmennepalvelut

OU = Certification Authority Services

O = Vaestorekisterikeskus CA

C = FI

Digi- ja väestötietoviraston kansalaisvarmenteiden varmentaja on:

CN (Common name) = VRK Gov. CA for Citizen Qualified Certificates - G3

OU (Organizational unit) = Valtion kansalaisvarmenteet

O (Organization) = Vaestorekisterikeskus CA

C (Country) = FI

Varmenteen haltijan nimeämiskäytäntö kansalaisvarmenteissa:

2.5.4.5 (Serial Number) = Sähköinen asiointitunnus (SATU)

SN (Surname) = Sukunimi

G (Given name) = Etunimi

CN (Common name) = Sukunimi Etunimi SATU

C (Country) = FI

E (EmailAddress) = Sähköpostiosoite (valinnainen)

Varmentajan julkinen avain sijoitetaan varmentajan varmenteeseen, julkiseen hakemistoon ja kansalaisvarmenteen haltijan toimikortille. Kansalaisvarmenteen sisältävään henkilökorttiin on henkilön visuaalista tunnistamista varten yksilöity kortinhaltijan valokuva ja allekirjoitusnäyte. Kansalaisvarmenteella olevat tiedot määrittelevät kansalaisvarmenteen haltijan yksikäsitteisesti. Varmentaja selvittää tarvittaessa varmenteen hakijan virallisen henkilöllisyyden.

4.1.2 Yksityisten avainten toimittaminen kansalaisvarmenteen haltijalle

Kansalaisvarmenteeseen liittyvät, kortin teknisessä osassa luodut yksityiset avaimet toimitetaan kansalaisvarmenteen hakijalle kortin luovutuksen yhteydessä. Teknisessä osassa luoduista yksityisistä avaimista ei ole eikä niistä voi myöhemminkään valmistaa kopiota.

Kansalaisvarmenteen sisältävä henkilökortti luovutetaan kansalaisvarmenteen hakijalle varmentajaa edustavan rekisteröijän kanssa sovitun menettelyn mukaisesti.

Henkilökortin käyttö sähköisessä asioinnissa edellyttää aktivointia aktivointitunnusluvun avulla. Aktivointitunnusluvun avulla käyttäjä pystyy aktivoimaan saamansa henkilökortin. Kun henkilökorttia käytetään ensimmäisen kerran sähköisessä asioinnissa esimerkiksi omalla kotitietokoneellaan, käynnistetään kortinlukijaohjelmiston toimesta automaattisesti henkilökortin aktivointiprosessi. Tämän prosessin aikana käyttäjältä ensin kysytään aktivointitunnusluku, jonka jälkeen käyttäjä voi aktivoida ja määritellä omat, henkilökohtaisen PIN-tunnuslukunsa. Aktivointiprosessin jälkeen käyttäjä pystyy käyttämään henkilökorttiaan sähköisessä asioinnissa.

Aktivoituja tunnuslukuja on kaksi. Perustunnusluku, jonka avulla käyttäjä kontrolloi henkilökortin ylläpitoa ja sähköistä tunnistautumista. Allekirjoitustunnusluku, jonka avulla käyttäjä voi tehdä sähköisen allekirjoituksen.

Mikäli käyttäjä antaa tunnusluvun viisi kertaa väärin, kortti lukittuu eikä tunnusluvun suojaamaa toimintoa voi enää käyttää. Perustunnusluvun lukittuminen estää kaikkien tunnusluvun suojaamien sovellutusten käytön. Allekirjoitustunnusluvun lukittuminen estää sähköisen allekirjoituksen käytön. Lukkiutuneet tunnusluvut vapautetaan aktivointitunnusluvulla.

4.2 Avainparin uusiminen

Kansalaisvarmenteella olevia julkisia avaimia ja sirulla olevia yksityisiä avaimia ei voi uusia. Uusien avainparien muodostaminen edellyttää uutta kansalaisvarmennetta.

Kansalaisvarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

4.3 Avainparin uusiminen varmenteen sulkulistalle asettamisen jälkeen

Kansalaisvarmenteella olevia julkisia avaimia ja sirulla olevia yksityisiä avaimia ei voi uusia. Uusien avainparien muodostaminen edellyttää uutta kansalaisvarmennetta.

Kansalaisvarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

4.4 Sulkupyynnön tekijän tunnistaminen

Kansalaisvarmenteen haltija voi halutessaan saada varmenteen suljettavaksi ennen kansalaisvarmenteen voimassaoloajan päättymistä.

4.5 Sulkupyyntömenettely

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

Sulkupyyntö on tehtävä välittömästi, kun on syytä epäillä kansalaisvarmenteen väärinkäyttöä esimerkiksi katoamisen tai anastamisen vuoksi. Kansalaisvarmenne voidaan sulkea soittamalla maksuttomaan yleiseen sulkupalvelunumeroon +358 800 162 622.

Kaikki sulkupyynnöt, sulkemisen perusteet, sulkupyynnön tekijän tunnistustapa ja pyyntöä seuranneet varmentajan toimenpiteet arkistoidaan. Sulkupyyntöjä koskevat puhelut nauhoitetaan.

4.6 Kansalaisvarmenteen sulkupyynnön tekijän tunnistaminen

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

Kansalaisvarmenteen haltijan tunnistetietojen perusteella saadaan selville sulkupyynnön mahdollistava kansalaisvarmenteen yksilöivä tieto.

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

5 Toiminnalliset vaatimukset

5.1 Kansalaisvarmenteen hakeminen

Kansalaisvarmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa ja ennen kansalaisvarmennehakemuksen allekirjoittamista annettavissa yleisissä käyttöohjeissa, jotka muodostavat kansalaisvarmenteen hakijan kanssa tehtävän sopimuksen. Hakemusasiakirjassa on tiedot kummankin osapuolen oikeuksista ja velvollisuuksista. Kun kansalaisvarmenteen hakija hakee varmennetta, hän hyväksyy samalla yleiset käyttöehdot.

Hakemusasiakirjassa ja käyttöohjeissa mainitaan selkeästi, että kansalaisvarmenteen hakija vahvistaa allekirjoituksellaan annettujen tietojen oikeellisuuden sekä hyväksyy varmenteen luomisen ja julkaisun julkisessa hakemistossa. Samalla hakija hyväksyy kansalaisvarmenteen käyttöön liittyvät säännöt ja ehdot sekä huolehtii kansalaisvarmenteen ja aktivointitunnusten säilyttämisestä sekä mahdollisen väärinkäytön tai varmenteiden/henkilökortin katoamisen ilmoittamisesta.

Varmentajan ja rekisteröijän, kortinvalmistajan sekä muiden varmennepalveluiden osa-alueita tuottavien toimittajien kesken on laadittu sopimus, joka ilmaisee kiistattomasti kummankin osapuolen oikeudet, vastuut ja velvoitteet.

Kansalaisvarmennetta haetaan käymällä henkilökohtaisesti rekisteröijänä toimivan poliisiviranomaisen luona tai muussa rekisteröintipisteessä. Kansalaisvarmennetta haettaessa henkilöllisyys tarkistetaan poliisin myöntämästä henkilöllisyyden osoittavasta asiakirjasta, joita ovat henkilökortti ja passi. Hyväksyttäviä tunnistamisasiakirjoja ovat myös Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä voimassa oleva passi tai henkilökortti ja muun valtion viranomaisen myöntämä voimassa oleva passi. Jos hakijalla ei ole em. asiakirjoja, poliisi tunnistaa hakijan henkilöllisyyden muilla tavoin. Tieto tunnistustavasta merkitään hakemuslomakkeeseen ja rekisteröintipisteen virkailija vahvistaa omalla allekirjoituksellaan, että henkilöllisyyden tunnistus on tapahtunut.

Henkilön esittämiä tietoja verrataan Väestötietojärjestelmän tietoihin.

5.2 Kansalaisvarmenteen myöntäminen

Varmentaja myöntää kansalaisvarmenteen hyväksyessään varmennehakemuksen.

Varmentaja vastaa myöntäessään kansalaisvarmenteen, että sen tietosisältö on oikea sen luovuttamishetkellä.

5.3 Kansalaisvarmenteen vastaanottaminen

Kansalaisvarmenne voidaan noutaa henkilökohtaisesti rekisteritoimipisteestä.

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

Kansalaisvarmenteen haltija voi ladata Digi- ja väestötietoviraston www-sivuilta kortinlukijaohjelmiston, jolla kansalaisvarmennetta voidaan käyttää sähköisissä asiointipalveluissa.

5.4 Kansalaisvarmenteen voimassaoloaika ja varmenteen sulkeminen

5.4.1 Kansalaisvarmenteen sulkemisen edellytykset

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

Kansalaisvarmenteen haltijan vastuulla on suojata hänelle kuuluvien yksityisten avaintensa ja niihin liittyvien aktivointitunnusten käyttäminen käyttöehtojen vastaiselta tavalta, huolehtimalla henkilökortistaan ja tunnusluvuistaan käyttöehdoissa mainitulla tavalla.

5.4.2 Sulkupyynnön tekijä

Kansalaisvarmenteen sulkupyynnön tekee ensisijaisesti sen haltija. Mikäli soittaja on eri henkilö kuin suljettavan varmenteen haltija, tunnistetaan haltijan lisäksi myös soittaja.

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

Varmenteen sulkemisen perusteet, ajankohta ja suorittajan tiedot talletetaan.

5.4.3 Sulkutapahtuma

Kansalaisvarmenteen sulkeminen voidaan tehdä seuraavilla tavoilla:

a) Puhelinsoitolla sulkupalveluun

b) Käymällä rekisteröijän luona

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

5.4.4 Henkilökortin peruuttaminen

Poliisi peruuttaa henkilökortin aina kortinhaltijan sitä pyytäessä. Alaikäiselle annettu henkilökortti peruutetaan myös silloin, jos alaikäisen huoltaja peruuttaa suostumuksensa. Henkilökortti voidaan peruuttaa, jos se on kadonnut, anastettu, turmeltunut, sen merkintöjä on muutettu tai sitä käyttää oikeudettomasti muu kuin se, jolle henkilökortti on annettu. Henkilökortti voidaan lisäksi peruuttaa, jos kansalaisvarmenteeseen tarkoitettuja tietoja on muutettu. Poliisi tekee ilmoituksen sulkupalveluun peruuttamansa henkilökortin kansalaisvarmenteiden sulkemiseksi aina henkilökortin voimassaolon aikana sekä voimassaoloajan päätyttyä aina silloin, kun henkilökortti on kadonnut tai anastettu. Mikäli henkilökortin haltija haluaa tehdä sulkuilmoituksen kansalaisvarmenteen sulkemiseksi ennen peruutuksen tekemistä, hänen on itse tehtävä ilmoitus sulkupalveluun.

5.4.5 Kansalaisvarmenteen käytön estäminen muilla tavoilla

Kortinhaltija on vastuussa kansalaisvarmenteen sulkemisesta. Kansalaisvarmenne voidaan kortinhaltijan ilmoituksesta merkitä sulkulistalle, jolloin Digi- ja väestötietoviraston myöntämän kansalaisvarmenteen käyttö estyy. Sen sijaan kortin teknisellä alustalla mahdollisesti olevia muita sovelluksia voidaan edelleen käyttää niiden käyttötarkoitusten mukaisesti. Kansalaisvarmenteiden käytön estäminen ei vaikuta henkilökortin hyväksyttävyyteen henkilökorttina ja Suomen kansalaisella matkustusasiakirjana.

Kansalaisvarmenne suljetaan soittamalla sulkupalvelunumeroon. Kansalaisvarmenteen haltijan vastuu päättyy, kun sulkupyynnön mahdollistava yksilöivä ilmoitus on vastaanotettu. Samalla hetkellä päättyy kansalaisvarmenteen haltijan vastuu kansalaisvarmenteen käytöstä. Tarvittaessa ilmoituksen voi tehdä myös muu henkilö, jolloin varmistetaan ilmoittajan henkilöllisyys ja yhteys peruutettavan henkilökortin haltijaan.

Sulkupalvelu ilmoittaa kansalaisvarmenteen sulkupyynnön tekijälle saman puhelun aikana sulkupyynnön onnistumisesta.

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

Suljettua varmennetta ei voi palauttaa käyttöön.

5.4.6 Henkilökortin käytön estäminen henkilökorttina ja Suomen kansalaisella matkustusasiakirjana

Kortinhaltija voi tehdä henkilökortin katoamisesta tai anastuksesta ilmoituksen poliisille. Poliisi tekee ilmoituksesta merkinnän poliisin henkilökorttirekisteriin eikä korttia hyväksytä henkilökorttina tai matkustusasiakirjana. Poliisi ilmoittaa myös katoamiseen ja anastamiseen liittyvän ilmoituksen yhteydessä kortin teknisessä osassa olevan kansalaisvarmenteen sulkulistalle. Kortinhaltijan ilmoitettua henkilökorttinsa löytymisestä poliisille löytymisestä tehdään merkintä henkilökorttirekisteriin. Henkilökortti

hyväksytään merkinnän jälkeen henkilökorttina tai Suomen kansalaisella matkustusasiakirjana.

Uuden henkilökortin luovuttamisen yhteydessä poliisivirkailija leikkaa rauenneen henkilökortin oikeasta alakulmasta valokuvan kohdalta kulman pois. Henkilökortin haltija voi kuitenkin käyttää tällä tavoin kelpaamattomaksi tehtyä korttia salaamiensa asiakirjojen ja tiedostojen hallintaan sekä hyödyntää edelleen kortille mahdollisesti itse tallettamiaan sovelluksia ja tietoja.

5.4.7 Kansalaisvarmenteen sulkeminen Digi- ja väestötietoviraston toimesta

Digi- ja väestötietovirasto sulkee kansalaisvarmenteen aina silloin, kun kansalaisvarmenteen haltijan kuolemasta on tullut tieto Digi- ja väestötietovirastolle. Digi- ja väestötietovirasto tekee tätä koskevan ilmoituksen kuolleen kansalaisvarmenteen haltijan oikeudenomistajille. Digi- ja väestötietovirasto voi sulkea yksityisellä avaimellaan allekirjoitetut kansalaisvarmenteet, mikäli on syytä epäillä Digi- ja väestötietoviraston yksityisten avainten paljastuneen tai joutuneen vääriin käsiin.

Digi- ja väestötietovirasto sulkee myöntämänsä kansalaisvarmenteet, mikäli kansalaisvarmenteen tietosisällössä havaitaan virhe.

Kaikki paljastuneella avaimella myönnetyt ja voimassa olevat kansalaisvarmenteet on suljettava yhdellä tai useammalla sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeisen suljetun kansalaisvarmenteen voimassaoloaika on päättynyt.

Mikäli Digi- ja väestötietoviraston kansalaisvarmenteiden 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 kansalaisvarmenteen erityisestä syystä.

5.4.8 Sulkutapahtuman ajoitus

Kansalaisvarmenteen sulkeminen toteutetaan välittömästi sulkupyynnön yhteydessä.

5.4.9 Varmenteen voimassaolon keskeyttämiseen liittyvät vaatimukset

Kansalaisvarmenteen voimassaoloa ei voi keskeyttää tilapäisesti. Suljettua kansalaisvarmennetta ei voi palauttaa käyttöön.

5.4.10 Keskeyttämispyynnön tekijä

Kansalaisvarmenteen voimassaoloa ei voi keskeyttää tilapäisesti.

5.4.11 Keskeyttämispyynnön tekeminen

Kansalaisvarmenteen voimassaoloa ei voi keskeyttää tilapäisesti.

5.4.12 Keskeyttämisajan rajoitukset

Kansalaisvarmenteen voimassaoloa ei voi keskeyttää tilapäisesti.

5.4.13 Sulkulistan julkaisutiheys

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

Sulkulista sisältää seuraavan sulkulistan julkaisuajankohdan.

Uusi sulkulista julkaistaan viimeistään voimassaolevan sulkulistan voimassaolon päättymisajankohtaan mennessä.

Järjestelmäpäivityksissä ja muissa poikkeavissa tilanteissa DVV voi julkaista sulkulistoja eri julkaisutiheyksillä ja pidennetyillä voimassaoloajoilla.

5.4.14 Sulkulistatarkistukseen liittyvät vaatimukset

Varmenteeseen luottavan osapuolen velvollisuudet on kuvattu luvussa 2.1.4.

5.4.15 Suorakäyttöinen varmenteen tilan tarkistaminen

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

5.4.16 Suorakäyttöiseen varmenteen tilan tarkistamiseen liittyvät vaatimukset

Varmentaja tarjoaa suorakäyttöisen varmenteen tilan tarkistuspalvelun.

5.4.17 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.

5.5 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.

5.6 Kansalaisvarmenteisiin liittyvien tietojen arkistointi

5.6.1 Talletettava aineisto

Arkistoinnissa sovelletaan yleislakina arkistolain (831/1994) säännöksiä. Oikeus tietojensaantiin määräytyy viranomaisen toiminnan julkisuudesta annetun lain (621/ 1999)

mukaisesti. Kansalaisvarmenteiden arkistoinnissa osalta sovelletaan lisäksi, mitä sähköisen asioinnin lainsäädännössä on arkistoinnista määrätty. Varmennerekisterin tiedot säilytetään 10 vuoden ajan kansalaisvarmenteiden voimassaolon päättymisestä. Varmentajan arkistoi seuraavat tiedot:

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

b) Poliisin myöntämän henkilökortin tiedot kerätään poliisin ylläpitämään henkilökorttirekisteriin josta vastaa poliisi

c) Myönnetyt kansalaisvarmenteet, niiden tietosisältö ja elinkaaren hallintaan liittyvät lisätiedot siitä hetkestä, kun kansalaisvarmenteen voimassaoloaika on päättynyt tai siitä kun kansalaisvarmenne on suljettu.

d) Varmentajan yksityisen avaimen luomiseen ja uusintaan liittyvät tapahtumat

e) Kansalaisvarmenteen sulkupyynnöt

f) Julkiseen hakemistoon lähetetyt sulkulistat ja muu kansalaisvarmenteen sulkemiseen liittyvä tieto

g) Voimassaoleva ja aikaisemmin julkaistut varmennepolitiikat ja niitä vastaavat varmennuskäytännöt

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

i) Tarkastusraportit ja pöytäkirjat käsittäen tietoturvatarkastukset ja järjestelmän auditoinnin

Arkistotiedot säilytetään varmentajana toimivaa viranomaista koskevien säännösten mukaisesti.

5.6.2 Arkistojen suojaus

Poliisi säilyttää henkilökortin hakemiseen, henkilön tunnistamiseen ja kortin luovutukseen liittyvät arkistoitavat asiakirjat asianmukaisissa tiloissa.

Arkistoitava tieto säilytetään korkean turvatason tiloissa, joissa on pääsynvalvonta.

5.6.3 Arkistotietojen varmistusmenettelyt

Varmuuskopiot varastoidaan fyysisesti erilliseen tilaan alkuperäisistä tiedoista.

5.6.4 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.

5.7 Toiminnan jatkumisen hallinta ja poikkeustapausten käsittely

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

5.7.1 Varmentajan yksityinen avain paljastunut tai Varmentajan varmenne on suljettu

Varmentaja ilmoittaa jokaisessa varmennuskäytännössä ne toimenpiteet, joihin varmenteen haltijoiden, varmenteeseen luottavien osapuolten ja 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 kohdan 6 mukaisesti.

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

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

5.7.2 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 27001
-tietoturvasertifikaatin, joka asettaa vaatimukset Digi- ja väestötietoviraston toiminnalle myös mahdollisen katastrofin tapahduttua. Kansalaisvarmenteiden myöntämisen ja ylläpidon yhteydessä Digi- ja väestötietovirasto noudattaa tietoturvallisuuden noudattamisesta määriteltyjä menettelytapoja.

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 4.8. 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 lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista mukaisten tietojen arkistoinnista sekä noudattaa muutoinkin arkistolain säännöksiä tietojen arkistoinnin osalta.

6 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.

6.1 Fyysiseen turvallisuuteen liittyvät järjestelyt

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.

6.1.1 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 lukitsemalla toimitilat riittävän tehokkaasti, käyttämällä toimitiloja jotka ovat vankkarakenteisia ja lujuudeltaan riittäviä. Konesalitiloissa on vältetty turhia ikkunoita ja niiden rakenteisiin on valittu kestäviä rakennusmateriaaleja.

6.1.2 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.

6.1.3 Sähkön syöttö ja ilmastointi

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

6.1.4 Paloturvallisuus

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

6.1.5 Tiedon säilytys

Arkistoitavat tiedot ja varmuuskopiot säilytetään eri tiloissa kuin varmentajan laitteistot.

Tieto on suojattu häviämiseltä, muuttamiselta ja luvattomalta käytöltä.

6.1.6 Tarpeettoman tietoaineiston käsittely

Turvaluokiteltu tietoaineisto hävitetään luotettavalla tavalla tuhoamalla.

6.1.7 Vesivahingot

Konesalitiloissa on asianmukaiset kosteuden havaitsevat ilmaisimet.

6.1.8 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.

6.2 Toiminnalliset vaatimukset

6.2.1 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.

6.2.2 Tehtäviin vaadittavien henkilöiden lukumäärä

Varmentajan yksityisen avaimen luominen, aktivointi, varmuuskopiointi ja palauttaminen ovat kahden järjestelmän ylläpitotehtäviin oikeutetun henkilön läsnä ollessa tehtäviä toimenpiteitä. Samoin 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.

Henkilökortilla olevien kansalaisvarmenteen rekisteröiminen ja tunnistaminen vaatii yhden henkilön läsnäolon. Tehtävän suorittaa poliisi.

6.2.3 Tehtäväkohtainen tunnistaminen

Henkilökortilla olevan kansalaisvarmenteen rekisteröijä

Rekisteröijänä toimii poliisi ns. yhteispalvelusopimuksen perusteella.

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 henkilökortilla. Varmennejärjestelmän käyttäjiä ovat konesalioperointi, teknisten varmennepyyntöjen käynnistäjät sekä sulkupalvelu.

6.3 Henkilöturvallisuus

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

Digi- ja väestötietoviraston varmennepalvelun henkilökunnalta edellytetään työtehtävien edellyttämää koulutustasoa ja varmennetoiminnan tuntemusta. Asiantuntijat seuraavat jatkuvasti alan kehitystä Suomessa ja Euroopassa sekä toimivat alan asiantuntijatehtävissä.

Kilpailutuksen yhteydessä varmentaja on arvioinut teknisten toimittajien avainasiantuntijoiden ja työntekijöiden pätevyyttä varmennepalvelun toteuttamiseen. Tietotekniset toimittajat ylläpitävät henkilöstönsä osaamista palvelutuotannossa käytettyjen laitteistojen, ohjelmistojen, menetelmien ja tietoturvallisuuden osalta. Lisäksi tekniset toimittajat huolehtivat siitä, että henkilöstö tuntee varmennepalvelun tietojenkäsittelytehtävät palvelun edellyttämällä tavalla.

6.3.1 Henkilökuntaa koskevan taustaselvityksen tekeminen

Digi- ja väestötietovirasto teettää omasta henkilöstöstään sekä teknisten toimittajien varmenneympäristön kanssa työskentelevistä henkilöistä perusmuotoisen turvallisuusselvityksen, jonka tekee suojelupoliisi. Digi- ja väestötietovirasto pidättää itsellään oikeuden olla hyväksymättä teknisen toimittajan työntekijää tehtävään, jossa työskennellään varmennejärjestelmän kanssa.

6.3.2 Taustaselvityksen tekemisessä noudatettava menettely

Henkilökunnan työkokemus kartoitetaan työhönottovaiheessa ja henkilö täyttää suojelupoliisille toimitettavan lomakkeen, jonka avulla henkilöön kohdistetaan perusmuotoinen turvallisuusselvitys.

Kaikkien varmentajan, varmennepalveluiden ja hakemistopalveluiden tuottajien, sulkulistan, ja kortinvalmistajan keskeisissä tehtävissä olevien henkilöiden tulee:

- täyttää suojelupoliisille toimitettava lomake, jonka avulla henkilöihin kohdistetaan perusmuotoinen turvallisuusselvitys
- 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

6.3.3 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.

6.3.4 Asiantuntemuksen ja osaamisen ylläpito

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

6.3.5 Tehtäväkiertoon liittyvät vaatimukset

Kun varmentajan tehtävissä suunnitellaan tehtäväkiertoa, on tehtävät organisoitava siten, että henkilö voi huolehtia uusista tehtävistään parhaalla mahdollisella tavalla. Henkilöstön kierron suunnittelussa otetaan huomioon mm. tietoturvallisuuden asettamat vaatimukset, luottamuksellisuuden turvaaminen ja henkilötietojen hyvän käsittelyn periaatteet, jotka on kuvattu Digi- ja väestötietoviraston henkilötietojen käsittelyä koskevissa käytännesäännöissä.

Myös tehtäväkierrossa noudatetaan Digi- ja väestötietoviraston tietoturvapolitiikkaa ja tietoturvasuunnitelmaa sekä Digi- ja väestötietoviraston muita yleisiä ohjeita.

6.3.6 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).

6.3.7 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.

6.3.8 Henkilökunnan käyttöön annettavat asiakirjat

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

7 Tekniset turvajärjestelyt

7.1 Avainparin luominen ja tallettaminen

7.1.1 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 henkilökortilla.

Varmentaja luo varmenteen haltijan avaimet henkilökortin mikrosirulla. Yksityisistä avaimista ei luoda kopiota.

7.1.2 Yksityisen avaimen luovuttaminen varmenteen hakijalle

Henkilökortti, joka sisältää kansalaisvarmenteen hakijan yksityiset avaimet ja jonka aktivointitiedoksi tarvitaan alkuperäiset aktivointitunnukset, toimitetaan hakijalle siten, että se ei ole yhdessä henkilökortin kanssa samassa paikassa ennen hakijalle luovuttamista. Tämä toteutetaan erillisten siirtoreittien avulla ja luovuttamalla kortti ja tunnukset eriaikaisesti.

Kansalaisvarmenteen sisältävä henkilökortti luovutetaan varmenteen hakijalle varmentajaa edustavan rekisteröijän kanssa sovitun menettelyn mukaisesti.

7.1.3 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.

7.1.4 Varmentajan julkisen avaimen jakelu varmenteen haltijalle

Varmentajan julkinen avain on varmentajan varmenteessa, joka sijoitetaan henkilökortille. Varmentajan varmenteet ovat vapaasti levitettävissä ja saatavilla myös julkisesta hakemistosta sekä varmentajan www-palvelusta.

7.1.5 Avainten pituudet

Kansalaisvarmenteen allekirjoittamiseen käytetty varmentajan yksityinen avain sekä sitä vastaava julkinen avain ovat 4096-bittisiä RSA-avaimia.

Varmenteen haltijan yksityiset ja julkiset avaimet ovat vähintään 2048 -bittisiä RSA-avaimia.

7.1.6 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, https://dvv.fi/fineid-maaritykset.

Varmenteen haltijan todentamis- ja salausvarmenne:

Käyttötarkoitus: Sähköisen henkilöllisyyden todentaminen tai avaintenvaihto.

Varmenteen haltijan allekirjoitusvarmenne:

Käyttötarkoitus: Sähköinen allekirjoitus

7.2 Yksityisen avaimen suojaus

7.2.1 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.

7.2.2 Varmentajan yksityisen avaimen käsittelyyn osallistuva henkilökunta

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

7.2.3 Yksityisen avaimen luovutus luotetun osapuolen huostaan

Varmentajan yksityiset avaimet eivät ole siirrettävissä tai kopioitavissa.

7.2.4 Yksityisen avaimen varmuuskopio

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

7.2.5 Yksityisen avaimen arkistointi

Varmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa.

7.2.6 Yksityisen avaimen hallinnointi turvamoduulissa

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 aktivointitunnuksella suojattu hallintakortti. Henkilön oikeus käyttää varmennejärjestelmää tai muita varmentamiseen liittyviä järjestelmiä todennetaan 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).

7.3 Muut avaintenhallintaan liittyvät seikat

7.3.1 Julkisen avaimen arkistointi

Varmentaja arkistoi kaikki varmentamansa julkiset avaimet.

7.3.2 Julkisten ja yksityisten avainten käyttöaika

Henkilökortilla olevan kansalaisvarmenteen voimassaoloaika on viisi vuotta. Varmenne voidaan sulkea sen voimassaoloaikana. Allekirjoitusvarmennetta voidaan käyttää allekirjoituksen todentamiseen varmenteen vanhenemisen tai sulkemisen jälkeen, jos varmennettu allekirjoitus on luotu ennen varmenteen sulkemista tai vanhenemisaikaa.

7.4 Aktivointitieto

7.4.1 Aktivointitiedon luominen ja käyttöönotto

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

7.4.2 Aktivointitiedon suojaus

Aktivointitunnukset on suojattu niin, ettei niitä voi lukea tai kopioida kortilta. Kansalaisvarmenteen haltijan vastuulla on suojata avaintensa käyttö henkilökortilla huolehtimalla kortistaan ja tunnusluvuistaan käyttöehdoissa mainitulla tavalla.

7.4.3 Muut aktivointitietoon liittyvät seikat

Kansalaisvarmenteen haltijalle selvitetään, että hänellä on mahdollisuus vaihtaa alkuperäiset PIN-tunnukset uusiksi tunnuksiksi. Aktivointitunnusten vaihto-ohjelma on maksutta kortinhaltijan saatavissa osoitteessa www.dvv.fi.

PIN-tunnus lukkiutuu ja henkilökortilla olevien varmenteiden käyttö estyy viiden peräkkäisen väärän tunnuksen antamisen jälkeen. Lukkiutunut aktivointitunnus vapautetaan uudelleen käyttöön henkilökohtaisen käynnin yhteydessä poliisilaitoksen lupapalvelupisteessä. Tässä yhteydessä hakijan henkilöllisyys tarkistetaan.

Aktivointitunnus toimitetaan hakijan ilmoittamaan osoitteeseen viikon kuluessa tilauksesta. Varmenteen haltija avaa lukittuneen korttinsa itse kortinlukijaohjelmiston avulla. Tämä ohjelma lisätietoineen on saatavissa osoitteesta www.dvv.fi.

7.5 Tietokoneiden käyttöön ja niihin pääsyyn liittyvät turvallisuusvaatimukset

7.5.1 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.

7.6 Varmennejärjestelmän elinkaaren hallinta

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

7.6.1 Järjestelmän kehittämiseen liittyvä valvonta

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

7.6.2 Turvallisuuden hallinta

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

7.7 Tietoverkon turvallisuus

Tietoliikenneturvallisuus on toteutettu siten, että varmennejärjestelmän tietoverkko on yhtenäinen kokonaisuus, joka on eriytetty muista tietoverkoista asianmukaisella tavalla 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.

7.8 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 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.

8 Varmenne- ja sulkulistaprofiilit

8.1 Varmenteiden tekniset tiedot

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

8.2 Sulkulistaprofiili

Varmentajan julkaisemien sulkulistojen tietosisällöt on kuvattu dokumentissa FINEID S2. Dokumentti on saatavilla varmentajan www-sivuilla, https://dvv.fi/fineid-maaritykset.

9 Määritysasiakirjojen hallinta

9.1 Määritysten muuttaminen

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

9.2 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.

9.3 Varmennuskäytännön muutos- ja hyväksymismenettely

Digi- ja väestötietovirasto hyväksyy sekä kansalaisvarmennetta koskevan varmennepolitiikan että varmennuskäytännöt. Asiakirjoja voidaan muuttaa Digi- ja väestötietoviraston sisäisin muutosmenettelyin.

Digi- ja väestötietovirasto ilmoittaa muutoksista hyvissä ajoin ennen niiden voimaantuloa sekä Traficomille että omilla www-sivuillaan.

Digi- ja väestötietovirasto pitää asiakirjoista versionhallintaa sekä arkistoi kaikki varmennepolitiikka- ja varmennuskäytäntöasiakirjat. Typografiset korjaukset ja yhteystietojen muutokset ovat mahdollisia välittömästi.

1. Kaikkia varmennepolitiikan ja varmennuskäytännön kohtia voidaan muuttaa ilmoittamalla tulevista pääasiallisista muutoksista 30 päivää ennen muutosten voimaan astumista.

2. Kohtia, jotka Digi- ja väestötietoviraston mielestä eivät merkittävästi vaikuta varmenteiden haltijoihin ja luottaviin osapuoliin, voidaan muuttaa ilmoittamalla niistä 14 päivää aikaisemmin ennen muutosten voimaantuloa.

[Yksikkö] / Aarnio Ville

6.5.2021