DIGI- JA VÄESTÖTIETO-VIRASTO

Varmennepolitiikka

Suomen sirullisten matkustusasiakirjojen ja oleskelulupa-asiakirjojen allekirjoitusvarmennetta varten

OID: 1.2.246.517.2.10.5

CERTIFIED SFS ORGANIZATION ISO 9001

kiwa ISO/IEC 27001

Sisällysluettelo

Määritelmät ja lyhenteet

Määritelmät

Allekirjoitusvarmenne: Varmenne, jota vastaavalla yksityisellä avaimella allekirjoitetaan digitaalisesti matkustusasiakirjan ja oleskelulupa-asiakirjan etäluettavalle sirulle talletettava data.

Allekirjoitusvarmenteen hakija: Oikeushenkilö, joka hakee allekirjoitusvarmennetta ja joka tunnistetaan hakemisen yhteydessä luotettavasti. Oikeushenkilö on Suomen valtio, jota passilain mukaan edustaa Poliisihallitus ja ulkomaalaislain mukaan Maahanmuuttovirasto.

Allekirjoitusvarmenteen haltija: Oikeushenkilö, jonka yksilöintitiedot ja julkinen avain on varmennettu varmentajan sähköisellä allekirjoituksella ja jonka hallussa varmenteeseen liittyvä yksityinen avain on. Oikeushenkilö on Suomen valtio, jota passilain mukaan edustaa Poliisihallitus ja ulkomaalaislain mukaan Maahanmuuttovirasto.

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

Digitaalinen allekirjoitus: Sähköinen allekirjoitus varmistaa allekirjoitettujen tietojen aitouden ja eheyden, ts. varmistaa tietojen alkuperän ja sen, ettei tietoja ole muutettu matkustusasiakirjan ja oleskelulupa-asiakirjan valmistamisen jälkeen.

ECC-algoritmi ja ECC-avain: ECC-algoritmi on eräs yleisesti käytetty julkisen avaimen algoritmi. Allekirjoitusvarmenteeseen liittyvät yksityinen ja julkinen avaimet ovat ECC-avaimia.

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

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

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

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

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

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. Allekirjoitusvarmenteeseen liittyvät yksityinen ja julkinen avaimet ovat RSA-avaimia.

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

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

Suomen sirullinen matkustusasiakirja: Poliisin myöntämä yleinen matkustusasiakirja, jonka tekniseen osaan on talletettu sirun tietosisällön aitouden ja eheyden varmistava allekirjoitusvarmenne.

Suomen sirullinen oleskelulupa-asiakirja: Poliisin tai Maahanmuuttoviraston myöntämä oleskelulupa-asiakirja, jonka tekniseen osaan on talletettu sirun tietosisällön aitouden ja eheyden varmistava allekirjoitusvarmenne.

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, joka 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 hyväksyttyjä varmenteita yleisölle tarjoavan varmentajan on velvollisuus pitää. Tiedot on säilytettävä vähintään 10 vuoden ajan varmenteen voimassaolon päättymisestä.

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. Varmentajalla tarkoitetaan Digi- ja väestötietovirastoa.

Varmentajan varmenne: Varmentajan itsensä myöntämä varmentajan yksityistä avainta vastaavan julkisen avaimen sisältävä varmenne, jonka avulla varmentajan myöntämien muiden varmenteiden sähköisen allekirjoituksen aitous tarkistetaan. Varmentajan varmenne sisältää mm. varmentajan nimen, sijaintimaan ja julkisen avaimen.

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

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.

Yksilöivä tunnus (OID): Tunnus, jolla yksilöidään mm. varmenteen myöntänyt organisaatio ja varmennuskäytäntö, jonka mukaisesti varmenne on myönnetty. OID-tunnus on osa varmenteen tietosisältöä.

Yksityinen avain: Julkisen avaimen menetelmässä epäsymmetrisessä salauksessa käytettävän avainparin yksityinen osa. Yksityinen allekirjoitusavain on talletettu varmenteen haltijan hallinnoimaan tietojärjestelmään.

Lyhenneluettelo

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

1. Johdanto

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

Tätä varmennepolitiikkaa sovelletaan Digi- ja väestötietoviraston myöntämään sirullisten matkustusasiakirjojen ja oleskelulupa-asiakirjojen allekirjoitusvarmenteeseen (jäljempänä allekirjoitusvarmenne), joka myönnetään passilaissa (671/2006) ja ulkomaalaislaissa (301/2004) määritellyille viranomaisille.

1.1. Yleistä

Varmenne on sähköinen todistus, joka liittää allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistaa varmenteen haltijan henkilöllisyyden. Tämän varmennepolitiikan mukainen allekirjoitusvarmenne perustuu julkisen avaimen järjestelmään ja menetelmiin. Varmentajan varmenteen ja allekirjoitusvarmenteiden tiedot on sähköisesti allekirjoitettu Varmentajan yksityisellä avaimella. Tämän varmennepolitiikan mukaisten allekirjoitusvarmenteiden tietosisältö on määritelty varmennuskäytännössä. Varmennuskäytäntö on salainen mutta siitä julkaistaan julkinen tiivistelmä.

Sirullisten matkustusasiakirjojen ja oleskelulupa-asiakirjojen allekirjoitusvarmenteen käyttötarkoitus on matkustusasiakirjan ja oleskelulupa-asiakirjan sirulle talletettavien tietojen digitaalisen allekirjoituksen todentaminen. Digitaalinen allekirjoitus varmistaa allekirjoitettujen tietojen aitouden ja eheyden, ts. varmistaa tietojen alkuperän ja sen, ettei tietoja ole muutettu matkustusasiakirjan ja oleskelulupa-asiakirjan valmistamisen jälkeen. Varmentajan varmenteella tarkistetaan allekirjoitusvarmenteiden aitous. Varmenteiden tietojen oikeellisuuden takaa Digi- ja väestötietovirasto.

Digi- ja väestötietoviraston varmennepolitiikalla ja varmennuskäytännöllä on molemmilla yksilöivä tunnuksensa (OID).

Varmentajan toimintoja ovat varmenne-, hakemisto- ja sulkupalveluiden tuottaminen sekä rekisteröinti. 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.

1.2. Tunnistetiedot

Tämän varmennepolitiikan nimi on Varmennepolitiikka Suomen sirullisten matkustusasiakirjojen ja oleskelulupa-asiakirjojen allekirjoitusvarmennetta varten, jonka OID on 1.2.246.517.2.10.5.

Varmennepolitiikka ja varmennuskäytännön julkinen tiivistelmä ovat saatavilla osoitteesta http://www.dvv.fi.

1.3. Varmentaja ja varmenteiden sovellusalueet

Varmentaja tuottaa varmennepalvelut tässä varmennepolitiikassa mainituin ehdoin ja vastaa niiden toimivuudesta Allekirjoitusvarmenteen haltijalle Varmentajan vastuita kuvaavan luvun

2.2.1 mukaisesti. Varmentaja vastaa koko varmennejärjestelmän toimivuudesta, myös käyttämiensä teknisten toimittajien osalta.

Tämän varmennepolitiikan on rekisteröinyt Digi- ja väestötietovirasto. Se on henkilörekisteriä ylläpitävä viranomainen, jonka passilain ja ulkomaalaislain mukainen tehtävä on tuottaa varmennepalveluita Suomen sirullisiin matkustusasiakirjoihin ja oleskelulupa-asiakirjoihin.

1.3.1. Varmentaja

Varmentajan tehtävänä on:

- tarjota passilain ja ulkomaalaislain tarkoittamia varmennepolitiikan ja varmennuskäytännön mukaisia varmenne-, hakemisto, sulku- ja rekisteröintipalveluita
- tunnistaa Allekirjoitusvarmenteen hakija
- huolehtia varmenteiden tietosisällön virheettömyydestä
- huolehtia varmenteiden sulkemisesta ja varmenteiden sulkulistojen julkaisemisesta
- noudattaa varmenteen haltijan tietojen käsittelyssä hyvää tietosuojan tasoa sekä hyvää tietojenkäsittelytapaa.

1.3.2. Rekisteröijä

Allekirjoitusvarmenteen rekisteröinti tapahtuu noudattaen luvun 3 mukaista menettelytapaa. Tarkempi menettelytapa kuvataan varmennuskäytännössä.

- Rekisteröijä toimii Varmentajan toimeksiannosta ja vastuulla.
- Rekisteröijä noudattaa Varmentajan varmennepolitiikkaa ja varmennuskäytäntöä.
- Rekisteröijä tunnistaa Allekirjoitusvarmenteen hakijan varmennuskäytännön mukaisella tavalla. Rekisteröijä noudattaa Varmentajan kanssa sovittuja rekisteröintiin liittyviä menettelytapoja.

1.3.3. Sulkupalvelu

Varmenteiden sulkupalvelu sulkee Allekirjoitusvarmenteet, jotka Allekirjoitusvarmenteen haltija haluaa suljettavaksi ennen niiden voimassaoloajan päättymistä. Suljetut Allekirjoitusvarmenteet toimitetaan sulkulistalle.

1.3.4. Hakemistopalvelu

Hakemistopalvelu on julkinen Internet-palvelu, josta on saatavilla kaikki Varmentajan myöntämät ja hakemistossa julkaistavat Varmentajan varmenteet, allekirjoitusvarmenteet sekä sulkulistat. Hakemistopalvelu on saatavissa osoitteesta ldap://ldap.fineid.fi. CSCA-varmenteet, sulkulistat, passien DS-varmenteet, henkilökorttien DS-varmenteet ja oleskelulupien DS-varmenteet julkaistaan hakemistopalvelussa.

1.3.5. ICAO PKD

ICAO:n julkisen avaimen hakemisto (ICAO PKD) on keskitetty tietovarasto, jonka avulla jaetaan tietoja, joita tarvitaan sähköisten koneellisesti luettavien matkustusasiakirjojen (eMRTD), kuten passien, henkilökorttien ja allekirjoitettujen viivakoodien (Visible Digital Seals) todentamiseen. CSCA-varmenteet, sulkulistat sekä asiakirjavarmenteet julkaistaan ICAO PKD -hakemistopalvelussa.

1.3.6. Allekirjoitusvarmenteen haltija

Tämän varmennepolitiikan mukaiset Allekirjoitusvarmenteet myönnetään Suomen valtiolle, jonka edustajia ovat Poliisihallitus ja Maahanmuuttovirasto.

Allekirjoitusvarmenteen haltijan tulee noudattaa Varmentajan varmennepolitiikkaa ja varmennuskäytäntöä.

1.3.7. Varmenteeseen luottava osapuoli

Varmenteeseen luottava osapuoli on henkilö tai organisaatio, joka luottaa varmenteen tietoihin ja joka käyttää varmennetta sähköisen allekirjoituksen tarkistamiseen.

Varmenteeseen luottavan osapuolen on tarkastettava, että käytettävä varmenne on voimassa, varmenne ei ole sulkulistalla ja että varmenneketju on eheä.

1.3.8. Varmenteen käyttäminen

Digi- ja väestötietovirasto noudattaa tätä varmennepolitiikkaa myöntäessään allekirjoitusvarmenteen. Varmentajan varmenteiden ja allekirjoitusvarmenteiden haltijoiden ja varmenteisiin luottavien osapuolien tulee toimia tämän varmennepolitiikan mukaisesti.

Tämän varmennepolitiikan mukaista allekirjoitusvarmennetta käytetään sähköisen allekirjoituksen tarkistamiseen.

Varmennepolitiikka ja varmennuskäytäntö sisältävät vaatimuksia, jotka koskevat Varmentajan, rekisteröijän, Allekirjoitusvarmenteen haltijan ja varmenteisiin luottavan osapuolen velvoitteita sekä lainsäädäntöön ja mahdollisten erimielisyyksien ratkaisuun liittyviä kysymyksiä.

1.4. Yhteystiedot

1.4.1. Varmennepolitiikkaa hallinnoiva organisaatio

Tämän varmennepolitiikan on rekisteröinyt Digi- ja väestötietovirasto. Se on henkilörekisteriä ylläpitävä viranomainen, jonka väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2009) mukainen tehtävä on tuottaa muiden tehtäviensä lisäksi varmennettuja sähköisen asioinnin palveluita sekä passilain ja ulkomaalaislain mukaisesti varmenteita Suomen sirullisiin matkustusasiakirjoihin ja oleskelulupa-asiakirjoihin. Digi- ja väestötietovirasto vastaa tämän varmennepolitiikan hallinnoinnista ja päivityksistä.

Tämän varmennepolitiikan mukaiset tekijänoikeudet kuuluvat Digi- ja väestötietovirastolle.

1.4.2. Yhteystiedot

Tätä varmennepolitiikkaa koskevat kysymykset lähetetään seuraavaan osoitteeseen:

Digi- ja väestötietovirasto	kirjaamo@dvv.fi
PL 00531 (Lintulahdenkuja 2)	Puh. +358 295 536 000
00581 Helsinki	Fax. +358 295 535 555
Y-tunnus: 0245437-2	

Varmennepolitiikkaan liittyviin kysymyksiin vastaa Digi- ja väestötietoviraston Varmennepalvelut-yksikkö.

2. Yleiset ehdot

Tämän varmennepolitiikan voimaantuloajankohta on 27.5.2011 (v 1.0). Varmennepolitiikan muutosmenettely ja julkaiseminen on kuvattu tämän asiakirjan kohdassa 8. Kohtaan 8 sisältyy myös versionhallinta, josta käy ilmi varmennepolitiikkaan 27.5.2011 jälkeen tehdyt muutokset.

2.1. Velvollisuudet

2.1.1. Varmentajan velvollisuudet

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

2.1.2. Rekisteröijää koskevat velvollisuudet

- Rekisteröijä noudattaa rekisteröinnin yhteydessä varmennepolitiikkaa ja varmennuskäytäntöä.
- Rekisteröijä tunnistaa Allekirjoitusvarmenteen hakijan edustajan henkilökohtaisesti ja luotettavasti varmennuskäytännössä kuvatulla tavalla siten, että hakijan yksilöintitiedot ja muut varmenteen myöntämisessä tarpeelliset tiedot tulevat huolellisesti tarkastetuiksi.
- Rekisteröijä huolehtii rekisteröintitietojen huolellisesta käsittelystä ja luottamuksellisuudesta.
- Rekisteröijä noudattaa Varmentajan kanssa sovittuja rekisteröintiin liittyviä menettelytapoja.

2.1.3. Allekirjoitusvarmenteen haltijaa koskevat velvollisuudet

- Allekirjoitusvarmenteen käyttötarkoitus ja -ehdot on määritelty tässä varmennepolitiikassa ja varmennuskäytännössä. Allekirjoitusvarmennetta saa käyttää vain sen käyttötarkoituksen ja -ehtojen mukaisesti.
- Allekirjoitusvarmenteen haltija vastaa siitä, että varmennetta haettaessa ilmoitetut tiedot ovat oikeita.
- Allekirjoitusvarmenteen haltija on vastuussa varmenteen käytöstä.
- Allekirjoitusvarmenteen haltijan vastuulla on estää hänelle kuuluvan yksityisen avaimen käyttäminen käyttötarkoituksen vastaisella tavalla huolehtimalla siitä tässä asiakirjassa ja varmennuskäytännössä mainitulla tavalla.
- Allekirjoitusvarmennetta vastaavan yksityisen avaimen häviämisestä tai väärinkäytön mahdollisuudesta tulee ilmoittaa viipymättä Varmentajalle luvussa 4.4 kuvatulla tavalla.

2.1.4. Varmenteisiin luottavaa osapuolta koskevat velvollisuudet

Varmenteisiin luottavan osapuolen on noudatettava varmennepolitiikkaa ja varmennuskäytäntöä.

Varmenteisiin luottava osapuoli voi vilpittömässä mielessä luottaa varmenteeseen, kun hän on tarkistanut, että varmenne on voimassa, että se ei ole sulkulistalla ja että varmenneketju on eheä. Varmenteisiin luottavalla osapuolella on velvollisuus tarkistaa varmenteet sulkulistalta. Varmenteen voimassaolon luotettavuuden varmistamiseksi varmenteisiin luottavan osapuolen on noudatettava alla esitettyjä sulkulistan tarkistustoimia.

Jos varmenteisiin 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, varmennetta ei pidä hyväksyä, mikäli viimeisen saadun sulkulistan voimassaoloaika on päättynyt. Kaikki Allekirjoitusvarmenteen hyväksymiset tämän voimassaoloajan jälkeen tapahtuvat varmenteisiin luottavan osapuolen omalla riskillä.

2.1.5. Allekirjoitusvarmenteen julkaisemiseen liittyvät velvollisuudet

Allekirjoitusvarmenteet julkaistaan yleisesti saatavilla olevassa julkisessa hakemistossa ja suljetut allekirjoitusvarmenteet sulkulistalla, josta varmenteeseen luottavan osapuolen on tarkistettava sen voimassaolotieto.

2.2. Vastuut

2.2.1. Varmentajan vastuut

Digi- ja väestötietovirasto vastaa Varmentajana koko varmennejärjestelmän turvallisuudesta. Varmentaja vastaa toimeksiantona hankkimistaan palveluista samoin kuin olisi itse tuottanut palvelun. Digi- ja väestötietoviraston, Poliisihallituksen ja Maahanmuuttoviraston vahingonkorvausvastuusta on sovittu Digi- ja väestötietoviraston ja Poliisihallituksen sekä Digi- ja väestötietoviraston ja Maahanmuuttoviraston välisillä sopimuksilla

Digi- ja väestötietovirasto vastaa siitä, että allekirjoitusvarmenne on luotu noudattaen varmennepolitiikassa sekä varmennuskäytännössä esitettyjä menettelyjä ja Allekirjoitusvarmenteen hakijan antamien tietojen mukaisesti. Väestörekisterikeskus vastaa niistä tiedoista, jotka se on tallettanut Allekirjoitusvarmenteeseen.

Digi- ja väestötietoviraston vastaa siitä, että kun Allekirjoitusvarmennetta käytetään asianmukaisesti, se on käytettävissä luovutushetkestä koko sen voimassaoloajan, ellei sitä ole asetettu sulkulistalle. Allekirjoitusvarmenne on luovutettu henkilölle, joka on tunnistettu varmennuskäytännössä kuvatulla tavalla.

Allekirjoittaessaan Allekirjoitusvarmenteen yksityisellä avaimellaan Varmentaja vakuuttaa tarkistaneensa Allekirjoitusvarmenteessa olevat tiedot varmennepolitiikassa ja varmennuskäytännössä esitettyjen menettelyjen mukaisesti.

Varmentaja vastaa siitä, että sulkulistalle viedään oikea Allekirjoitusvarmenne ja että se ilmestyy tässä varmennepolitiikassa mainitussa ajassa sulkulistalle.

2.2.2. Rekisteröijän vastuut

Allekirjoitusvarmenteen rekisteröijänä toimii Digi- ja väestötietovirasto. Rekisteröinnin osalta noudatetaan tässä varmennepolitiikassa ja siihen liittyvässä varmennuskäytännössä kuvattuja toimintatapoja ja vastuita.

2.2.3. Allekirjoitusvarmenteen haltijan vastuut

Allekirjoitusvarmenteen haltija on vastuussa oman toimintansa taloudellisista ja oikeudellisista seuraamuksista.

Allekirjoitusvarmenteen haltijan vastuu sen käyttämisestä päättyy, kun tämä on ilmoittanut sulkupalveluun tarvittavat tiedot Allekirjoitusvarmenteen sulkemiseksi ja saatuaan sulkupyynnön vastaanottaneelta henkilöltä sulkemista koskevan ilmoituksen. Vastuun katkaisemiseksi sulkupyyntö on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

2.2.4. Allekirjoitusvarmenteeseen luottavan osapuolen vastuut

Allekirjoitusvarmenteeseen luottava osapuoli ei voi luottaa siihen vilpittömässä mielessä, mikäli Allekirjoitusvarmenteen voimassaoloa ei ole tarkastettu sulkulistalta ja mikäli varmenneketjun eheyttä ei ole tarkistettu. Allekirjoitusvarmenteen hyväksyminen mainitussa tapauksessa vapauttaa Digi- ja väestötietoviraston ja Allekirjoitusvarmenteen haltijan vastuusta. Allekirjoitusvarmenteeseen luottavan osapuolen on tarkistettava, että myönnettyä Allekirjoitusvarmennetta on käytetty sen käyttötarkoituksen mukaisesti.

2.2.5. Vastuiden rajoitukset

Digi- ja väestötietoviraston, Poliisihallituksen ja Maahanmuuttoviraston vahingonkorvausvastuusta on sovittu Digi- ja väestötietoviraston ja Poliisihallituksen sekä Digi- ja väestötietoviraston ja Maahanmuuttoviraston välisillä sopimuksilla. Muissa tilanteissa Digi- ja väestötietoviraston, Poliisihallituksen ja Maahanmuuttoviraston vastuu on rajoitettu osoitettuihin välittömiin vahinkoihin. Välittöminä vahinkoina korvataan kuitenkin enintään 10.000 euroa vahinkotapahtumaa tai toisiinsa liittyviä vahinkotapahtumia kohden.

Digi- ja väestötietovirasto ei vastaa Allekirjoitusvarmenteen haltijan yksityisen avaimen paljastumisen seurauksena syntyvistä vahingoista, ellei paljastuminen johdu Digi- ja väestötietoviraston välittömästä toiminnasta.

Digi- ja väestötietovirasto ei vastaa Allekirjoitusvarmenteeseen luottavan osapuolen tai Allekirjoitusvarmenteen haltijan muun sopimuskumppanin mahdollisesti kärsimistä välillisistä tai seurannaisvahingoista.

Digi- ja väestötietovirasto ei vastaa yleisten tietoliikenneyhteyksien eikä tietoverkkojen toimivuudesta eikä siitä, jos Allekirjoitusvarmenteen käyttäminen estyy Allekirjoitusvarmenteen

haltijan tai luottavan osapuolen käyttämän laitteen tai ohjelmiston toimimattomuudesta eikä siitä, että Allekirjoitusvarmennetta käytetään vastoin sen käyttötarkoitusta.

Varmentajalla on oikeus keskeyttää palvelu muutos- ja huoltotoimien ajaksi. Mikäli keskeytyksellä on merkitystä Allekirjoitusvarmenteen hakijalle, tulee siitä sopia yhteisesti Poliisihallituksen ja Maahanmuuttoviraston kanssa. Sulkulistaa koskevista muutoksista tai huoltotöistä ilmoitetaan etukäteen.

Varmentajalla on oikeus kehittää edelleen varmennepalvelua. Allekirjoitusvarmenteeseen luottavan osapuolen on vastattava tämän vuoksi aiheutuvista omista kustannuksistaan, eikä Varmentaja ole velvollinen korvaamaan Allekirjoitusvarmenteeseen luottavalle osapuolelle tällaisesta varmennepalvelun kehittämistyöstä aiheutuvista kustannuksista. Varmentajan, Poliisihallituksen ja Maahanmuuttoviraston välillä kehitystoimenpiteistä ja –kustannuksista sovitaan erikseen.

Varmentaja ei vastaa Allekirjoitusvarmenteen käytöstä johtuvista toimista, virheistä tai niistä aiheutuvista kustannuksista.

2.3. Taloudellinen vastuu

2.3.1. Varmentaja

Tässä varmennepolitiikassa kuvattujen varmennepalveluiden tuottamiseen liittyvä Digi- ja väestötietoviraston vahingonkorvausvastuu määräytyy kulloinkin sovellettavan sopimuksen perusteella ja soveltuvin osin vahingonkorvauslain (412/1974) säännösten mukaisesti.

Digi- ja väestötietoviraston, Poliisihallituksen ja Maahanmuuttoviraston vahingonkorvausvastuusta on sovittu Digi- ja väestötietoviraston ja Poliisihallituksen sekä Digi- ja väestötietoviraston ja Maahanmuuttoviraston välisillä sopimuksilla Muissa tilanteissa Digi- ja väestötietoviraston, Poliisihallituksen ja Maahanmuuttoviraston vastuu on rajoitettu osoitettuihin välittömiin vahinkoihin. Välittöminä vahinkoina korvataan kuitenkin enintään 10.000 euroa vahinkotapahtumaa tai toisiinsa liittyviä vahinkotapahtumia kohden.

2.3.2. Muut osapuolet

Allekirjoitusvarmenteeseen luottava osapuoli voi luottaa varmenteisiin, jos hän on tarkastanut, ettei niitä ole asetettu sulkulistalle eikä niiden voimassaoloaika ole päättynyt, varmenneketju on eheä eikä hänellä ole muita syitä perustellusti epäillä niiden käytön oikeellisuutta.

Luottava osapuoli on vastuussa Allekirjoitusvarmenteen hyödyntämisestä ja sen hyödyntämiseen liittyvistä oikeustoimista ja niihin liittyvistä taloudellisista ja oikeudellisista seuraamuksista.

2.3.3. Varmentajan taloushallinto

Digi- ja väestötietoviraston tuottamat varmennepalvelut ovat sellaisen taloushallinnollisen järjestelmän ja valvonnan piirissä kuin on erikseen säädetty.

2.4. Tulkinta ja täytäntöönpano

2.4.1. Sovellettava lainsäädäntö ja viranomaissuositukset

Tämän varmennepolitiikan mukaisesti myönnetty Allekirjoitusvarmenne täyttää passilain ja ulkomaalaislain vaatimukset sekä noudattaa Kansainvälisen siviili-ilmailujärjestön (ICAO) suosituksia muutamia asian luonteesta johtuvia poikkeuksia lukuun ottamatta. Poikkeukset on kuvattu yksityiskohtaisesti Varmennuskäytännön tiivistelmässä.

Tässä varmennepolitiikassa kuvattujen varmennepalveluiden tuottamiseen liittyvä Digi- ja väestötietoviraston vahingonkorvausvastuu määräytyy kulloinkin sovellettavan sopimuksen perusteella ja soveltuvin osin vahingonkorvauslain säännösten mukaisesti.

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

Digi- ja väestötietoviraston vastaa siitä, että Allekirjoitusvarmenteet on luotu noudattaen varmennepolitiikassa ja varmennuskäytännössä esitettyjä menettelyjä ja Allekirjoitusvarmenteen hakijan antamien tietojen mukaisesti.

2.4.2. Erimielisyyksien ratkaiseminen

Digi- ja väestötietovirasto vastaa varmenteita myöntäessään siitä, että Allekirjoitusvarmenne täyttää tässä varmennepolitiikassa esitetyt vaatimukset. Mahdolliset erimielisyydet ratkaistaan Suomen oikeusjärjestyksen mukaisesti.

2.5. Maksut

Tässä luvussa on määritelty Allekirjoitusvarmenteen käyttöön liittyvät maksut.

2.5.1. Allekirjoitusvarmenteen myöntäminen ja uusiminen

Allekirjoitusvarmennetta haetaan sen mukaisesti kuin varmennuskäytännössä on kuvattu.

Allekirjoitusvarmenteet on hinnoiteltu Digi- ja väestötietoviraston ja Poliisihallituksen sekä Digi- ja väestötietoviraston ja Maahanmuuttoviraston välisten sopimusten mukaisesti.

2.5.2. Allekirjoitusvarmenteen käyttöön liittyvät maksut

Varmentaja veloittaa Allekirjoitusvarmenteen haltijaa Allekirjoitusvarmenteiden, sulkupalvelun tai julkisen hakemiston käytöstä Digi- ja väestötietoviraston ja Poliisihallituksen sekä Digi- ja väestötietoviraston ja Maahanmuuttoviraston välisten sopimusten mukaisesti.

2.5.3. Allekirjoitusvarmenteen sulkulistamerkintään liittyvät maksut

Allekirjoitusvarmenteen ilmoittamisesta sulkulistalle, sulkulistojen noutamisesta hakemistosta sekä Allekirjoitusvarmenteen voimassaolon tarkistamisesta sulkulistalta veloitetaan Digi- ja väestötietoviraston ja Poliisihallituksen sekä Digi- ja väestötietoviraston ja Maahanmuuttoviraston välisten sopimusten mukaisesti.

2.6. Varmentajan tietojen julkaiseminen ja saatavuus

2.6.1. Varmentajan tietojen julkaiseminen

Varmentaja julkaisee kaikki julkaistavaksi tarkoitetut Varmentajan varmenteet, Allekirjoitusvarmenteet ja sulkulistat yleisesti saatavilla olevassa julkisessa hakemistossa. Varmentaja julkaisee varmennepolitiikan ja varmennuskäytännön tiivistelmän.

2.6.2. Julkaisutiheys

Allekirjoitusvarmenne julkaistaan julkisessa hakemistossa heti sen luomisen jälkeen ja se on hakemistossa koko voimassaolonsa ajan. Varmentaja julkaisee sulkulistan, joka on voimassa 40 vuorokautta julkaisemisestaan. Tämä sulkulista päivitetään 30:n vuorokauden välein uudella sulkulistalla.

2.6.3. Tietojen saatavuus

Hakemisto- ja sulkulistatiedot ovat yleisesti saatavilla osoitteesta ldap://ldap.fineid.fi. Tarkempi kuvaus hakemistopalvelusta on varmennuskäytännön tiivistelmässä. Sulkulista on myös saatavissa Allekirjoitusvarmenteessa ilmoitetusta sähköpostiosoitteesta. Varmennepolitiikat ja varmennuskäytännön tiivistelmä ovat niin ikään saatavilla Varmentajan www-sivuilla.

2.6.4. Tietovarastot

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

2.7. Tietoturvatarkastus

Poliisihallitus, sisäasiainministeriön poliisiosasto ja Maahanmuuttovirasto voivat tarkastaa Varmentajan toiminnan Digi- ja väestötietoviraston ja Poliisihallituksen sekä Digi- ja väestötietoviraston ja Maahanmuuttoviraston välisten sopimusten mukaisesti.

Digi- ja väestötietovirasto tarkastaa teknisten toimittajiensa toimitilat, laitteet ja toiminnan tarkoituksenmukaisella tavalla.

2.7.1. Tarkastusten tiheys

Digi- ja väestötietovirasto tarkastaa teknisten toimittajiensa toiminnan vuosittain tai tarvittaessa.

2.7.2. Tarkastaja

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

2.7.3. Tarkastuksen kohteet ja kattavuus

Tarkastuksen kohteet määräytyvät tietoturvastandardin ISO/IEC 27001, Digi- ja väestötietoviraston tietoturvapolitiikan tai teknisten toimitussopimusten mukaisesti.

Tarkastettavia tietoturvallisuuden ominaisuuksia ovat luottamuksellisuus, eheys ja käytettävyys.

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

Tarkastuksissa otetaan huomioon hallinnollisen tietoturvallisuuden lisäksi palveluntoimittajat.

2.7.4. Poikkeamista johtuvat toimenpiteet

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

2.7.5. Tarkastuksen tuloksesta tiedottaminen

Tarkastuksen tuloksesta tiedotetaan lain, tietoturvastandardin ISO/IEC 27001, Digi- ja väestötietoviraston tietoturvapolitiikan ja voimassa olevien toimitussopimusten mukaisesti. Sisäiseen käyttöön tarkoitettu yksityiskohtainen määrämuotoinen tarkastustulos on luottamuksel-

linen eikä siitä anneta tietoja julkisuuteen. Määrämuotoiset raportit laaditaan erikseen organisaation ulkopuoliseen käyttöön.

Digi- ja väestötietovirasto tiedottaa tarkastuksen tuloksista Poliisihallitukselle, sisäasiainministeriöön ja Maahanmuuttovirastolle.

2.8. Tietojen julkisuus

2.8.1. Varmentajan julkaisemat tiedot

Varmennejärjestelmän tiedot ovat luottamuksellisia, elleivät ne perustu tietosuojalain (1050/2018), viranomaisten toiminnan julkisuudesta annetun lain (621/1999) säännöksiin tietojen luovuttamisesta tai varmennepolitiikassa tai varmennuskäytännössä määriteltyihin tarkoituksiin.

2.8.2. Julkiset tiedot

Julkisen hakemiston ja sulkulistan tiedot ovat julkisia, samoin varmennuskäytännön tiivistelmä ja varmennepolitiikassa määritellyt tiedot.

2.8.3. Allekirjoitusvarmenteen voimassaolon päättymiseen tai sulkemiseen liittyvät tiedot

Allekirjoitusvarmenteen voimassaoloaika on merkitty Allekirjoitusvarmenteeseen. Kesken voimassaoloajan suljetut Allekirjoitusvarmenteet julkaistaan yleisesti saatavilla olevalla sulkulistalla.

2.8.4. Viranomaisille luovutettavat tiedot

Viranomaisille luovutettavat tiedot määritellään voimassa olevan lainsäädännön mukaisesti.

2.8.5. Muut tiedot

Varmennejärjestelmän tietoja ei luovuteta kuin edellä tässä kappaleessa mainittuihin tarkoituksiin.

2.8.6. Allekirjoitusvarmenteen haltijan pyynnöstä tapahtuva tiedon luovuttaminen

Allekirjoitusvarmenteen haltijalla on oikeus saada itseään koskevia tietoja voimassa olevan lainsäädännön ja Digi- ja väestötietoviraston ja Poliisihallituksen sekä Digi- ja väestötietoviraston ja Maahanmuuttoviraston välisten sopimusten mukaisesti.

2.8.7. 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 tietosuojalakia sekä erityislainsäädäntöä. Digi- ja väestötietovirasto on valmistellut käytännesäännöt sekä tietojen luovuttamisesta että varmennetoiminnan yhteydessä tapahtuvasta henkilötietojen käsittelystä. Henkilötietojen käsittelyssä noudatetaan erityistä huolellisuutta.

2.9. Immateriaalioikeudet

Digi- ja väestötietovirasto omistaa Allekirjoitusvarmenteisiin ja dokumentaatioon liittyvät tiedot teknisten toimitussopimusten mukaisesti. Digi- ja väestötietovirastolla on täydet omistus- ja käyttöoikeudet tähän varmennepolitiikkaan.

3. Allekirjoitusvarmenteen hakijan tunnistaminen

3.1. Rekisteröinti

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

Allekirjoitusvarmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa, joka muodostaa varmenteen hakijan kanssa tehtävän toimeksiannon varmenteen hakemisesta.

3.1.1. Nimeämiskäytännöt

Sirullisten matkustusasiakirjojen Allekirjoitusvarmenteiden varmentaja on:

CN (Common name) = CSCA Finland

OU (Organizational unit) = VRK

O (Organization) = Finland

C (Country) = FI

Allekirjoitusvarmenteen haltijan nimeämiskäytäntö on kuvattu yksityiskohtaisesti varmennuskäytännössä. Allekirjoitusvarmenteella olevat tiedot määrittelevät varmenteen haltijan yksikäsitteisesti.

3.2. Avainparin uusiminen

Allekirjoitusvarmenteen julkista avainta ei voi uusia. Uuden avainparin muodostaminen edellyttää uutta Allekirjoitusvarmennetta.

Allekirjoitusvarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

3.3. Avainparin uusiminen Allekirjoitusvarmenteen sulkulistalle asettamisen jälkeen

Allekirjoitusvarmenteen julkista avainta ja sitä vastaavaa yksityistä avainta ei voi uusia. Uuden avainparin muodostaminen edellyttää uutta Allekirjoitusvarmennetta.

Allekirjoitusvarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

4. Toiminnalliset vaatimukset

4.1. Allekirjoitusvarmenteen hakeminen

Allekirjoitusvarmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa, joka muodostaa Allekirjoitusvarmenteen hakijan kanssa tehtävän sopimuksen. Hakemusasiakirjassa on tiedot kummankin osapuolen oikeuksista ja velvollisuuksista. Hakemusasiakirjassa mainitaan selkeästi, että Allekirjoitusvarmenteen hakija vahvistaa allekirjoituksellaan annettujen tietojen oikeellisuuden sekä hyväksyy Allekirjoitusvarmenteen luomisen ja julkaisun julkisessa hakemistossa.

Allekirjoitusvarmenteen hakija vastaa siitä, että kaikki Allekirjoitusvarmenteen kannalta olennaiset tiedot, jotka Allekirjoitusvarmenteen hakija on antanut Varmentajalle ovat oikeita. Allekirjoitusvarmenteen haltijan on käytettävä Allekirjoitusvarmennetta vain sen käyttötarkoitusten mukaisesti.

4.2. Allekirjoitusvarmenteen myöntäminen

Varmentaja myöntää Allekirjoitusvarmenteen hyväksyessään varmennehakemuksen.

Varmentaja vastaa myöntäessään Allekirjoitusvarmenteen, että sen tietosisältö on hyväksytyn hakemuksen mukainen.

4.3. Allekirjoitusvarmenteen toimittaminen Allekirjoitusvarmenteen hakijalle

Allekirjoitusvarmenne noudetaan henkilökohtaisesti rekisteritoimipisteestä tai se toimitetaan sähköisesti allekirjoitettuna sähköpostin välityksellä Allekirjoitusvarmenteen hakijan kanssa sovittuun osoitteeseen.

4.4. Allekirjoitusvarmenteen sulkeminen

4.4.1. Allekirjoitusvarmenteen sulkemisen edellytykset

Allekirjoitusvarmenne on asetettava sulkulistalle, kun on syytä epäillä väärinkäyttöä esimerkiksi yksityisen avaimen paljastumisen vuoksi. Sulkupyyntö on tehtävä välittömästi sen jälkeen, kun epäilys väärinkäytön mahdollisuudesta on syntynyt.

4.4.2. Sulkupyynnön tekijä ja tunnistaminen

Allekirjoitusvarmenteen sulkupyynnön tekevät nimetyt Allekirjoitusvarmenteen haltijaorganisaation edustajat.

Allekirjoitusvarmenteen sulkemisen perusteet, ajankohta ja suorittajan tiedot talletetaan.

Allekirjoitusvarmenteen haltija voi halutessaan saada Allekirjoitusvarmenteen suljettavaksi ennen sen voimassaoloajan päättymistä.

Kaikki sulkupyynnöt, sulkemisen perusteet, sulkupyynnön tekijän tunnistustapa ja pyyntöä seuranneet Varmentajan toimenpiteet arkistoidaan.

Allekirjoitusvarmenteen sulkeminen on kuvattu yksityiskohtaisesti varmennuskäytännössä.

4.4.3. Sulkutapahtuma

Allekirjoitusvarmenne suljetaan kolmen arkivuorokauden kuluessa sulkupyynnön vastaanottamisesta.

Allekirjoitusvarmenteen sulkeminen ja sen vaikutukset on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Sulkupalvelu ilmoittaa Allekirjoitusvarmenteen sulkupyynnön tekijälle Allekirjoitusvarmenteen sulkemisesta.

Allekirjoitusvarmenteiden sulkeminen Digi- ja väestötietoviraston pyynnöstä

Digi- ja väestötietovirasto sulkee myöntämänsä Allekirjoitusvarmenteet, mikäli niiden tietosisällössä havaitaan virhe, ja Allekirjoitusvarmenteen haltija hyväksyy sulkemisen.

Edellä mainitun mukaisesti Digi- ja väestötietovirasto voi sulkea käyttämällään yksityisellä avaimella allekirjoitetut varmenteet, mikäli on syytä epäillä Digi- ja väestötietoviraston yksityisen avaimen paljastuneen tai joutuneen vääriin käsiin.

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

Mikäli Digi- ja väestötietoviraston varmenteiden luonnissa käyttämä yksityinen avain tai muu tekninen menetelmä on paljastunut tai tullut muutoin käyttökelvottomaksi, Digi- ja väestötietoviraston on ilmoitettava tapahtuneesta Allekirjoitusvarmenteen haltijalle asianmukaisella tavalla.

4.4.4.Sulkulistan julkaisutiheys

Tieto varmenteen viennistä sulkulistalle on julkisesti saatavilla viimeistään kolmen arkivuorokauden kuluttua siitä, kun sulkupyyntö on todettu päteväksi ja hyväksytty. Sulkulista on voimassa 40 vuorokautta julkaisemisestaan. Tämä sulkulista päivitetään 30:n vuorokauden välein uudella sulkulistalla. Uusi sulkulista julkaistaan viimeistään voimassa olevan sulkulistan voimassaolon päättymisajankohtaan mennessä.

Sulkulista sisältää seuraavan sulkulistan julkaisuajankohdan.

4.4.5. Sulkulistatarkistukseen liittyvät vaatimukset

Varmenteisiin luottavan osapuolen velvollisuudet on kuvattu luvussa 2.1.4.

4.4.6. Suorakäyttöinen varmenteen tilan tarkistaminen

Varmentaja ei toistaiseksi tarjoa suorakäyttöistä varmenteen tilan tarkistuspalvelua eli OCSP-palvelua.

4.4.7. Suorakäyttöiseen varmenteen tilan tarkistamiseen liittyvät vaatimukset

Varmentaja ei toistaiseksi tarjoa suorakäyttöistä varmenteen tilan tarkistuspalvelua.

4.5. Järjestelmän valvonta

Järjestelmän valvonta on kuvattu varmennuskäytännössä.

4.6. Allekirjoitusvarmenteisiin liittyvien tietojen arkistointi

4.6.1. Talletettava aineisto

Arkistoinnissa sovelletaan yleislakina arkistolain (831/1994) säännöksiä. Oikeus tietojensaantiin määräytyy viranomaisten toiminnan julkisuudesta annetun lain mukaisesti. Varmennerekisterin tiedot säilytetään 10 vuoden ajan varmenteiden voimassaolon päättymisestä.

Varmentajan arkistoimat tiedot on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Arkistotiedot säilytetään Varmentajana toimivaa viranomaista koskevien säännösten mukaisesti.

4.6.2. Arkistojen suojaus

Arkistoitava tieto säilytetään korkean turvatason tiloissa, joissa on pääsynvalvonta.

4.6.3. Arkistotietojen varmistusmenettelyt

Varmuuskopiot varastoidaan fyysisesti erilliseen tilaan alkuperäisistä tiedoista.

4.6.4. Arkistotietojen hankinta- ja varmistusmenetelmät

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

4.7. Toiminnan jatkuvuuden hallinta ja poikkeustapausten käsittely

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

Poikkeustapauksiin varautuminen on kuvattu varmennuskäytännössä.

4.7.1. Varmentajan yksityinen avain paljastunut tai Varmentajan varmenne on suljettu

Varmentaja ilmoittaa jokaisessa varmennuskäytännössä ne toimenpiteet, joihin Allekirjoitusvarmenteen haltijan, varmenteeseen luottavan osapuolen ja rekisteröijien ja Varmentajan työntekijöiden on ryhdyttävä, mikäli Varmentajan yksityinen avain on paljastunut tai tullut muutoin käyttökelvottomaksi.

4.7.2. 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/IEC 27001 – tietoturvasertifikaatin, joka asettaa vaatimukset Digi- ja väestötietoviraston toiminnalle myös mahdollisen katastrofin tapahduttua.

4.8. Varmentajan toiminnan lakkauttaminen

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

Varmentaja ilmoittaa varmennepalveluiden lakkauttamisesta varmennuskäytännössä 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 viimeisten 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 tietojen arkistoinnista sekä noudattaa muutoinkin arkistolain säännöksiä tietojen arkistoinnin osalta.

5. Fyysiset, toiminnalliset ja henkilöstöturvallisuuteen liittyvät vaatimukset

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

5.1. Fyysiseen turvallisuuteen liittyvät järjestelyt

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

Yksityiskohtainen kuvaus turvallisuuteen liittyvistä järjestelyistä on kuvattu varmennuskäytännössä.

5.1.1. Sijainti ja rakennusten ominaisuudet

Varmentajan järjestelmät sijaitsevat korkean turvatason konesalitiloissa ja täyttävät tietokonekeskuksille annetut turvallisuutta koskevat ohjeet ja määräykset.

Toimitilaturvallisuus on toteutettu siten, että asiattomien pääsy toimitiloihin on estetty.

5.1.2. Fyysinen pääsy toimitilaan

Toimitiloihin, joissa tehdään varmennejärjestelmän tuotannollisia tehtäviä, on valvottu pääsy. Kulunvalvontajärjestelmä havaitsee sekä luvallisen että luvattoman sisäänmenon. Konesalitiloihin vaaditaan henkilön tunnistautuminen, jolloin henkilö tunnistetaan ja pääsyoikeudet tarkistetaan sekä tapahtumat rekisteröidään. Konesalitiloja vartioidaan vuorokauden ympäri.

5.1.3 Varajärjestelyt

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

Tärkeiden laitteiden varaosien saanti ja huolto on varmistettu.

5.2. Toiminnalliset vaatimukset

5.2.1. Vastuunjako

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

5.2.2. Tehtäviin vaadittavien henkilöiden lukumäärä

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

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

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

Järjestelmän käyttämiseen vaaditaan yhden tehtävään oikeutetun henkilön läsnäolo.

Allekirjoitusvarmenteen rekisteröiminen ja hakijan tunnistaminen vaatii yhden henkilön läsnäolon.

5.2.3. Tehtäväkohtainen tunnistaminen

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

5.3. Henkilöturvallisuus

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

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

5.3.1. Henkilökuntaa koskevan taustaselvityksen tekeminen

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

5.3.2. Taustaselvityksen tekemisessä noudatettava menettely

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

Turvallisuusselvitysmenettely on kuvattu yksityiskohtaisesti varmennuskäytännössä.

5.3.3. Koulutukseen liittyvät vaatimukset

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

5.3.4. Asiantuntemuksen ja osaamisen ylläpito

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

5.3.5. Tehtäväkiertoon liittyvät vaatimukset

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

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

5.3.6. 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).

5.3.7. Organisaatiota edustava henkilökunta

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

5.3.8. Henkilökunnan käyttöön annettavat asiakirjat

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

6. Tekniset turvajärjestelyt

Tekniset turvajärjestelyt on kuvattu yksityiskohtaisesti varmennuskäytännössä.

6.1. Avainparin luominen ja tallettaminen

6.1.1. Avainparin luominen

Varmentaja luo yksityisen allekirjoitusavaimensa ja yksityistä allekirjoitusavaintaan vastaavan julkisen avaimen. Varmentajan yksityistä avainta säilytetään turvamoduulissa.

Varmenteen haltijan avainpari luodaan Poliisihallituksen ja Maahanmuuttoviraston yhteisesti hallinnoimissa tiloissa. Avainparia säilytetään FIPS 140-2 luokan 3 mukaisessa turvamoduulissa. Yksityinen avain on asetettu luku- ja kirjoitussuojattuun tilaan.

6.1.2. Yksityisen avaimen luovuttaminen Allekirjoitusvarmenteen hakijalle

Allekirjoitusvarmenteen haltija luo ja säilyttää yksityisen avaimensa turvamoduulissa.

6.1.3. Allekirjoitusvarmenteen haltijan julkisen avaimen toimittaminen Varmentajalle

Allekirjoitusvarmenteen hakija toimittaa rekisteröijälle luomansa varmennepyynnön, jossa allekirjoitusvarmenteen hakijan tiedot yhdistetään kyseessä olevaan julkiseen avaimeen. Allekirjoitusvarmenne luodaan varmennepyynnön perusteella.

Allekirjoitusvarmenne sisältää allekirjoitusvarmenteen haltijan julkisen avaimen.

6.1.4. Varmentajan julkisen avaimen jakelu Allekirjoitusvarmenteen haltijalle

Varmentajan varmenne sisältää Varmentajan julkisen avaimen. Varmentajan varmenne talletetaan julkiseen hakemistoon.

6.1.5. Avainten pituudet

Allekirjoitusvarmenteen allekirjoittamiseen käytetty Varmentajan yksityinen avain sekä sitä vastaava julkinen avain ovat 512-bittisiä ECC-avaimia.

Allekirjoitusvarmenteen haltijan yksityinen ja julkinen avain ovat 512-bittisiä ECC-avaimia.

6.1.6. Avainten käyttötarkoitukset

Varmenteen tietosisällössä käyttötarkoituksen määräävä kenttä määrittelee varmenteisiin liittyvän avaimen käyttötarkoituksen (esimerkiksi digitaalinen allekirjoitus). Avaimen käyttö rajataan vain käyttötarkoitukseensa, digitaaliseen allekirjoitukseen tarkoitettua avainta tulee siis käyttää vain tähän tarkoitukseen.

Varmentajan varmenne:

Käyttötarkoitus: Varmenteiden ja sulkulistojen allekirjoitus.

Varmenteen haltijan allekirjoitusvarmenne:

Käyttötarkoitus: Digitaalinen allekirjoitus

Sekä Varmentajan varmenne että Allekirjoitusvarmenne poikkeavat joiltakin osin ICAO:n suosituksista. Poikkeukset on kuvattu tarkemmin Varmennuskäytännössä.

6.2. Varmentajan yksityisen avaimen suojaus

6.2.1. Turvamoduulia koskevat standardit

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

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

6.2.2. Varmentajan yksityisen avaimen käsittelyyn osallistuva henkilökunta

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

6.2.3. Varmentajan yksityisen avaimen tallettaminen

Varmentaja säilyttää yksityisen avaimensa turvamoduulissa ja pyrkii estämään sen katoamisen, joutumisen ulkopuolisten käsiin, muuttamisen tai luvattoman käytön.

6.2.4. Yksityisen avaimen varmuuskopio

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

6.2.5. Yksityisen avaimen arkistointi

Varmentajan yksityisiä avaimia säilytetään Varmentajan hallinnoimissa turvamoduuleissa.

6.2.6. Yksityisen avaimen hallinnointi turvamoduuleissa

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

Yksityisen avaimen hallinnointi on kuvattu yksityiskohtaisesti varmennuskäytännössä.

6.3. Muut avaintenhallintaan liittyvät seikat

6.3.1. Julkisen avaimen arkistointi

Varmentaja arkistoi kaikki varmentamansa julkiset avaimet.

6.3.2. Julkisten ja yksityisten avainten voimassaoloaika

Allekirjoitusvarmenteen voimassaoloaika on viisi vuotta kolme kuukautta. Allekirjoitusvarmenne voidaan sulkea sen voimassaoloaikana. Allekirjoitusvarmennetta voidaan käyttää allekirjoituksen todentamiseen varmenteen vanhenemisen tai sulkemisen jälkeen, jos varmennettu allekirjoitus on luotu ennen varmenteen sulkemista tai vanhenemisaikaa.

6.4. Tietokoneiden käyttöön ja niihin pääsyyn liittyvät turvallisuusvaatimukset

6.4.1. Laitteistoturvallisuus

Varmennejärjestelmän laitteistoina käytetään vain käyttötarkoitukseensa sopivia laitteistoja.

Yksityiskohtainen menettely on kuvattu varmennuskäytännössä.

6.5. Varmennejärjestelmän elinkaaren hallinta

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

6.5.1. Järjestelmän kehittämiseen liittyvä valvonta

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

6.5.2. Turvallisuuden hallinta

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

6.6. Tietoverkon turvallisuus

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

Tarkempi kuvaus tietoverkon turvallisuudesta on kuvattu varmennuskäytännössä.

6.7. Turvamoduulin käytön valvonta

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

Yksityiskohtainen menettely on kuvattu varmennuskäytännössä.

7. Varmenne- ja sulkulistaprofiilit

7.1. Varmenteiden tekniset tiedot

Varmentajan varmenteen ja Allekirjoitusvarmenteen haltijan varmenteen tietosisällöt on kuvattu varmennuskäytännön tiivistelmässä.

7.2. Sulkulistaprofiili

Varmentajan julkaiseman sulkulistan tietosisältö on kuvattu varmennuskäytännön tiivistelmässä.

8. Määritysasiakirjojen hallinta

8.1. Määritysten muuttaminen

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

8.2. Varmennepolitiikan muutos- ja hyväksymismenettely

Digi- ja väestötietovirasto hyväksyy sekä Allekirjoitusvarmennetta koskevan varmennepolitiikan että varmennuskäytännöt. Asiakirjoja voidaan muuttaa Digi- ja väestötietoviraston, Poliisihallituksen, Maahanmuuttoviraston ja ulkoministeriön yhteisellä päätöksellä.

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 Allekirjoitusvarmenteen haltijan ja luottaviin osapuoliin, voidaan muuttaa ilmoittamalla niistä 14 päivää aikaisemmin.

8.3. Versionhallinta

Varmennepolitiikka Suomen sirullisten matkustusasiakirjojen ja oleskelulupa-asiakirjojen Allekirjoitusvarmenteita varten, v 1.2.

Versio	**Päivämäärä**	**Kuvaus / muutokset**
v 1.0	27.5.2011	Hyväksytty versio 1.0.
v 1.1	02.11.2023	Viraston nimimuutokset lisätty. Teknisisä tietoja päivitetty, mm. 512-bittinen ECC-avain. Vanhentuneita lakipykäliä päivitetty.
v 1.2	1.2.2024	Poliisihallituksen kommentit huomioitu.