DIGI- JA VÄESTÖTIETO-VIRASTO

# VARMENNEPOLITIIKKA SUOMEN VALTION JUURIVARMENTAJAA VARTEN

OID: 1.2.246.517.1.10.301
OID: 1.2.246.517.1.10.351

1.6.2021

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

## Dokumentinhallinta

| | |
|---|---|
| Omistaja | |
| Laatinut | Ville Aarnio |
| Tarkastanut | |
| Hyväksynyt | Mikko Pitkänen |

## Version hallinta

| versionro | mitä tehty | pvm/henkilö |
|---|---|---|
| v 1.0 | Versio 1.0 | 1.6.2021/VA |

# Sisällysluettelo

# VARMENNEPOLITIIKKA SUOMEN VALTION JUURIVARMENTAJAA VARTEN

Määritelmät ja lyhenteet

Määritelmät

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

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

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

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

Julkisen avaimen menetelmä: Tietoturvapalvelu, esimerkiksi henkilön sähköinen tunnistaminen, joka tuotetaan käyttämällä julkista ja yksityistä avainta, varmenteita ja epäsymmetristä salausta.

Juurivarmentaja: Organisaatio, joka myöntää varmentajan varmenteet ja laatii toimintaansa kuvaavan varmennepolitiikan sekä varmennuskäytännön. Digi- ja väestötietovirasto toimii tämän varmennuskäytännön mukaisena juurivarmentajana.

Luottava osapuoli: Taho, joka luottaa (relying party, luottava taho) varmenteen tietoihin ja käyttää varmennetta erilaisiin turvapalveluihin, kuten todennus, luottamuksellisuus ja allekirjoituksen varmistaminen, silloin kun varmenteeseen liittyvä Varmentajan allekirjoitus täsmää.

OID: Object Identifier, yksilöivä tunnus. Tämän varmennuskäytännön yksikäsitteinen tunnus OID on osa jokaisen juurivarmentajan myöntämän varmentajan varmenteen tietosisältöä.

Lyhenteet

| | |
|---|---|
| ARL | Authority Revocation List |
| CA | Certification Authority |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |

| | |
|---|---|
| CRL | Certificate Revocation List |
| ECC | Elliptic curve cryptography |
| FINEID | Finnish Electronic Identification |
| FIPS | Federal Information Processing Standard |
| HSM | Hardware Security Module |
| HST | Henkilön sähköinen tunnistaminen |
| HTTP | Hypertext Transfer Protocol |
| ISO 27001 | ISO IEC 27001 |
| LDAP | Lightweight Directory Access Control |
| OCSP | Online Certificate Status Protocol, suorakäyttöinen varmenteen tilan palauttava palvelu |
| OID | Object Identifier |
| PDS | PKI Disclosure Statement, varmennekuvaus |
| PKI | Public Key Infrastructure |
| RSA | Rivest, Shamir, Adleman |
| SIM | Subscriber Identity Module |
| DVV | Digi- ja väestötietovirasto |

# 1 Johdanto

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.fineid.fi.

Tätä varmennepolitiikkaa sovelletaan juurivarmentajan (DVV Gov. Root CA – G3 RSA ja DVV Gov. Root CA – G3 ECC) myöntäessä varmentajan varmenteita.

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

## 1.1 Yleistä

Digi- ja väestötietovirasto tarjoaa tietoturvallisuuden tasoltaan korkealaatuisia sähköisten luottamuspalveluiden ja tunnistamisen varmenteita ja niihin liittyviä palveluja.

Digi- ja väestötietovirasto (DVV) toimii valtiovarainministeriön hallinnonalalla. DVV on henkilörekisteriä ylläpitävä viranomainen, jonka väestötietojärjestelmästä ja 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), laki sähköisestä lääkemääräyksestä (61/2007). DVV on tarjonnut varmenteisiin perustuvia allekirjoitus- ja tunnistusvälineitä sekä verkkosivujen varmenteita vuodesta 1999 lähtien ja toiminut eurooppalaisen yhteisesti hyväksyttävän tason allekirjoitusvarmentajana 31.3.2003 lukien. Digi- ja väestötietovirasto tarjoaa myös muita luottamuspalveluita.

Digi- ja väestötietoviraston varmennetietojärjestelmä ja varmennepalvelut perustuvat julkisen avaimen järjestelmään (Public Key Infrastructure eli PKI). DVV:n varmenneinfrastruktuuri muodostuu varmennejärjestelmästä, varmennekortteihin 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.

Digi- ja väestötietovirasto on Suomen valtion juurivarmenneviranomainen ja hyväksyy julkaisemansa varmennepolitiikan mukaisesti Digi- ja väestötietoviraston myöntämät ja allekirjoittamat varmenteet.

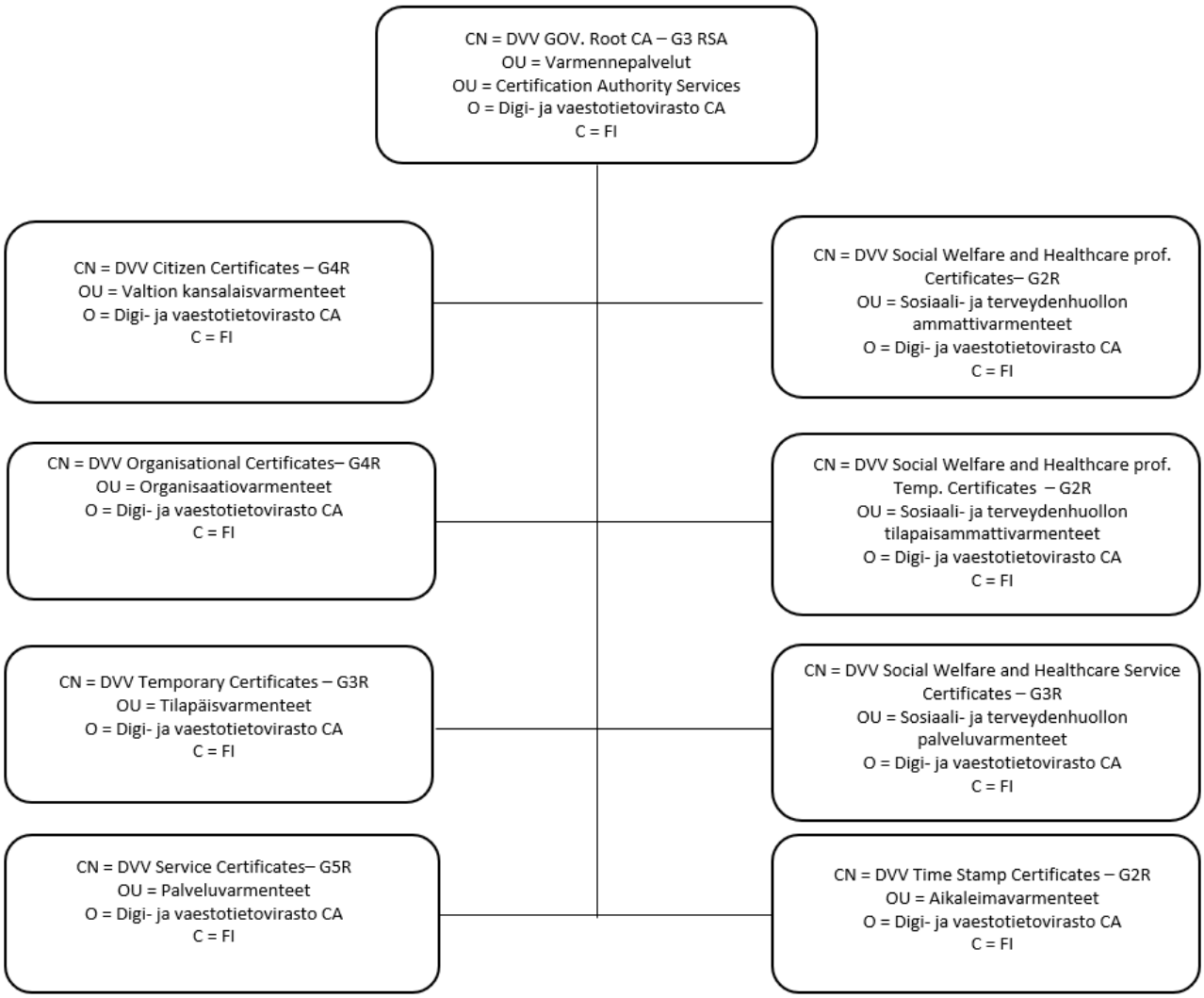
Digi- ja väestötietovirasto luo Suomen valtion juurivarmenteen. Suomen valtion juurivarmenteeseen perustuva luottamusrakenne on hierarkkinen. Digi- ja väestötietovirasto hyväksyy julkaisemansa varmennepolitiikan mukaisesti Digi- ja väestötietoviraston myöntämät ja allekirjoittamat varmenteet. Varmentaja voi olla joko julkinen tai yksityinen organisaatio.

Digi- ja väestötietoviraston varmennetoiminta perustuu tunnistus- ja luottamuspalveluista säädettyyn Euroopan parlamentin ja neuvoston asetukseen (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (Asetus).

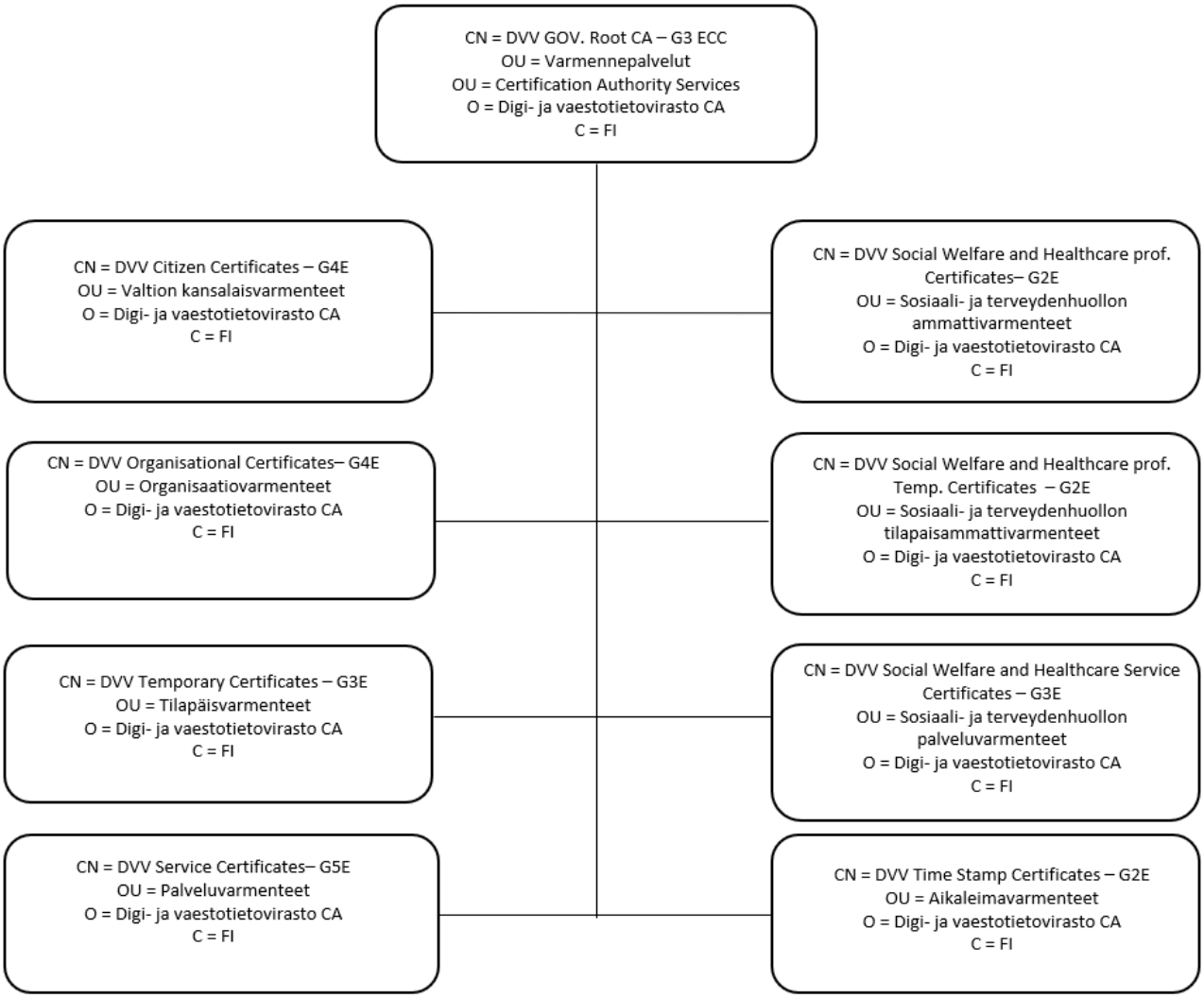
Digi- ja väestötietoviraston luottamuspalvelut täyttävät eIDAS-asetuksessa asetettujen vaatimusten lisäksi hyväksytyn luottamuspalvelun tarjoajaa koskevan standardin EN 319 401 sekä varmenteita tarjoavan hyväksytyn luottamuspalvelun tarjoajaa koskevan standardin EN 319 411-1 vaatimukset.

Digi- ja väestötietoviraston myöntämät varmenteet ovat vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) mukaisia luottamuspalveluita ja vahvan sähköisen tunnistamisen välineitä. DVV myöntää myös muita henkilö- ja ohjelmistovarmenteita samassa varmentajan luotettavassa järjestelmässä. Tämä asiakirja kuvaa niitä periaatteita, joita juurivarmentaja noudattaa

myöntäessään varmentajan varmenteita joko Digi- ja väestötietovirastolle tai muulle organisaatiolle. Juurivarmentaja ei myönnä loppukäyttäjän varmenteita. Loppukäyttäjän varmenteita myöntävät juurivarmentajan varmentamat varmentajat, joilla jokaisella on oma varmennepolitiikkansa ja omat varmennuskäytäntönsä.




Kuva 1. Varmennehierarkia RSA




Kuva 2: Varmennehierarkia ECC

Varmennehierarkia on seuraava

Juurivarmenne:

- Digi- ja väestötietoviraston juurivarmenne
    - CN = DVV Gov. Root CA – G3 RSA
    - OID: 1.2.246.517.1.10.301
    - CN= DVV Gov. Root CA – G3 ECC
    - OID: 1.2.246.517.1.10.351
- Varmentajan varmenteet
    - Valtion kansalaisvarmenteet
        - CN = DVV Citizen Certificates - G4R
        - OID: 1.2.246.517.1.10.301.1
        - CN = DVV Citizen Certificates - G4E
        - OID: 1.2.246.517.1.10.351.1
    - Organisaatiovarmenteet
        - CN = DVV Organisational Certificates - G4R
        - OID: 1.2.246.517.1.10.301.2
        - CN = DVV Organisational Certificates - G4E
        - OID: 1.2.246.517.1.10.351.2
    - Palveluvarmenteet
        - CN = DVV Service Certificates - G5R
        - OID: 1.2.246.517.1.10.301.4
        - CN = DVV Service Certificates - G5E
        - OID: 1.2.246.517.1.10.351.4
    - Sosiaali- ja terveydenhuollon ammattivarmenteet
        - CN = DVV Social Welfare and Healthcare Prof. Certificates - G2R
        - OID: 1.2.246.517.1.10.301.5

- CN = DVV Social Welfare and Healthcare Prof. Certificates - G2E
- OID: 1.2.246.517.1.10.351.5

- Sosiaali- ja terveydenhuollon palveluvarmenteet
  - CN = DVV Social Welfare and Healthcare Service Certificates - G3R
  - OID: 1.2.246.517.1.10.301.7
  - CN = DVV Social Welfare and Healthcare Service Certificates - G3E
  - OID: 1.2.246.517.1.10.351.7
- Aikaleimavarmenteet
  - CN = DVV Time Stamp Certificates - G2R
  - OID: 1.2.246.517.1.10.301.8
  - CN = DVV Time Stamp Certificates - G2E
  - OID: 1.2.246.517.1.10.351.8

CN = VRK Gov. Root CA

OID: 1.2.246.517.1.10.1

- Tilapäisvarmenteet
  - CN = DVV Temporary Certificates - G3R
  - OID: 1.2.246.517.1.10.301.3
  - CN = DVV Temporary Certificates - G3E
  - OID: 1.2.246.517.1.10.351.3
- Sosiaali- ja terveydenhuollon tilapäisammattivarmenteet
  - CN = DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2R
  - OID: 1.2.246.517.1.10.301.6
  - CN = DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2E
  - OID: 1.2.246.517.1.10.351.6

Varmentajan varmenne sisältää varmentajan julkisen avaimen, nimen, varmenteen käyttötarkoituksen sekä muut varmenteen käytön kannalta välttämättömät tiedot. Varmenteen tiedot on sähköisesti allekirjoitettu juurivarmentajan yksityisellä avaimella. Tämän varmennepolitiikan mukainen varmentajan varmenne perustuu julkisen avaimen järjestelmään.

Varmentajan varmenteessa olevaa julkista avainta vastaavalla yksityisellä avaimella allekirjoitetaan sähköisesti kaikki myönnettävät loppukäyttäjän varmenteet sekä sulkulistat. Varmentajan varmenteeseen luottava osapuoli voi todentaa sen aitouden ja eheyden juurivarmenteen avulla.

Digi- ja väestötietoviraston varmennepolitiikka ja varmennuskäytäntöasiakirjat on yksilöity yksikäsitteisin tunnuksin (OID).

Digi- ja väestötietovirasto laatii erillisen varmennepolitiikan juurivarmentajalle sekä (erilliset varmennuskäytännöt vai yhden) jokaista juurivarmentajan myöntämää varmentajan varmennetta varten.

Varmennepolitiikka kuvaa Digi- ja väestötietoviraston varmennetoiminnassa käytettävät menettelytavat, käyttöehdot, vastuiden jaon ja muut varmennetoimintaan liittyvät näkökulmat yleisellä tasolla. Varmennuskäytäntö kuvaa noudatettavat menettelytavat yksityiskohtaisesti.

## 1.2 Tunnistetiedot

Tämän varmennepolitiikan nimi on Varmennepolitiikka Suomen valtion juurivarmentajaa varten, jonka yksiselitteinen tunnus on OID 1.2.246.517.1.10.301 ja 1.2.246.517.1.10.351.

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

## 1.3 Juurivarmentaja ja varmentajan varmenteiden sovellusalueet

Juurivarmentaja tuottaa varmennepalvelut tässä varmennepolitiikassa mainituin ehdoin ja vastaa niiden toimivuudesta juurivarmentajan vastuita kuvaavan luvun 2.2.1 mukaisesti. Juurivarmentaja vastaa koko varmentajan varmennejärjestelmän toimivuudesta, myös käyttämiensä rekisteröijien ja teknisten toimittajien osalta. Tämän varmennepolitiikan on rekisteröinyt Digi- ja väestötietovirasto. Digi- ja väestötietovirasto on Suomen valtion juurivarmenneviranomainen. Varmenteet myöntää Digi- ja väestötietovirasto, joka henkilörekisteriä ylläpitävä, suomi.fi -palveluita sekä varmennepalveluita tuottava viranomainen, jonka lain väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista mukainen tehtävä on tuottaa varmennepalveluita sähköiseen asiointiin. Digi- ja väestötietoviraston varmennepalvelu jakaantuu toiminnallisesti seuraaviin osa-alueisiin:

### 1.3.1 Juurivarmentaja

Juurivarmentajan tehtävänä on:

- myöntää varmentajan varmenteita
- huolehtia myöntämiensä varmenteiden tietosisällön virheettömyydestä
- tarjota varmennepolitiikan ja varmennuskäytännön mukaisia varmenne ja hakemistopalveluita sekä sulkulistapalveluita
- huolehtia varmenteiden sulkemisesta ja varmenteiden sulkulistojen julkaisemisesta.

### 1.3.2 Rekisteröijä

Juurivarmentaja vastaa kaikista varmentajan varmenteiden rekisteröijätehtävistä.

Rekisteröijä tunnistaa varmentajan varmenteen hakijan varmennuskäytännön mukaisella tavalla

### 1.3.3 Hakemistopalvelu

Hakemistopalvelu on julkinen Internetpalvelu, josta on saatavilla kaikki juurivarmentajan myöntämät varmentajan varmenteet sekä uusin sulkulista. Hakemistopalvelu on julkisessa palvelussa saatavilla ldap.fineid.fi – palvelimella.

### 1.3.4 Varmentajan varmenteen haltijaorganisaatio

Tämä varmennepolitiikka kuvaa juurivarmentajan menettelytapoja, kun se myöntää varmentajan varmenteita Digi- ja väestötietoviraston tai muun organisaation käyttöön.

Varmentajan varmenteen haltijaorganisaation tulee noudattaa juurivarmentajan varmennepolitiikkaa ja varmennuskäytäntöä.

### 1.3.5 Varmentajan varmenteeseen luottaminen

Varmentajan varmenteeseen luottava osapuoli on henkilö tai organisaatio, joka luottaa varmentajan varmenteen tietoihin. Varmentajan varmenteeseen luottavan osapuolen on tarkistettava, että varmenne on voimassa ja että varmentajan varmenne ei ole sulkulistalla.

### 1.3.6 Varmentajan varmenteen käyttäminen

Tämän varmennepolitiikan mukaisesti juurivarmentaja myöntää varmentajan varmenteita siten, kuin varmennuskäytännössä on kyseessä olevaa varmentajan varmennetta koskien kuvattu. Varmentajan varmenteen käyttötarkoitus on esimerkiksi kansalaisvarmenteita myöntävien varmenteiden allekirjoittaminen ja sulkulistan allekirjoittaminen.

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

## 1.4 Yhteystiedot

### 1.4.1 Varmennepolitiikkaa hallinnoiva organisaatio

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

Tämän varmennepolitiikan mukaiset tekijänoikeudet kuuluvat Digi- ja väestötietovirastolle.

### 1.4.2 Yhteyshenkilö

Tätä varmennepolitiikkaa 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.fineid.fi

# 2 Yhteiset ehdot

Tämä varmennepolitiikka astuu voimaan 1.6.2021. Varmennepolitiikan muutosmenettely ja julkaiseminen on kuvattu tämän asiakirjan luvussa 8.

## 2.1 Velvollisuudet

### 2.1.1 Juurivarmentajan velvollisuudet

- Juurivarmentaja noudattaa toiminnassaan voimassaolevaa lainsäädäntöä.
- Juurivarmentaja toimii huolellisesti, luotettavasti ja asianmukaisesti.
- Juurivarmentajalla on riittävät tekniset taidot, ja taloudelliset voimavarat sekä mahdollisuus vahingonkorvausvastuun kattamiseksi.
- Digi- ja väestötietovirasto voi myöntää varmenteen myös omiin tarkoituksiinsa. Tällöin se noudattaa samoja vaatimuksia kuin muut organisaatiot.
- Juurivarmentaja vastaa kaikista varmennetoiminnan osa-alueista, myös juurivarmentajan apunaan käyttämien teknisten toimittajien ja henkilöiden tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta.
- Juurivarmentaja laatii ja ylläpitää varmennepolitiikan, joka kuvaa varmentajan varmenteen myöntämisessä, ylläpidossa ja hallinnoinnissa käytettävät menettelytavat, käyttöehdot, vastuiden jaon ja muut varmentajan varmenteen käyttöön liittyvät näkökulmat yleisellä tasolla.
- Juurivarmentaja laatii ja ylläpitää varmennuskäytäntöjä, jotka kuvaavat, miten juurivarmentaja soveltaa varmennepolitiikkaa.
- Juurivarmentaja noudattaa varmennepolitiikan ja varmennuskäytännön vaatimuksia.
- Juurivarmentaja julkaisee varmennepolitiikan ja varmennuskäytännön yleisesti saataville.
- Juurivarmentaja pitää palveluksessaan riittävästi henkilökuntaa, jolla on varmennepalvelujen tuottamisen edellyttämä asiantuntemus, kokemus ja pätevyys.
- Juurivarmentaja käyttää luotettavia järjestelmiä ja tuotteita, jotka on suojattu oikeudettomalta käytöltä.

- Juurivarmentaja pitää yleisesti saatavilla juurivarmennetta ja varmennetoimintaa koskevat tiedot, joiden perusteella juurivarmentajan toiminta ja luotettavuus voidaan arvioida.
- Juurivarmentaja noudattaa rekisteröinnissä varmennepolitiikkaa ja varmennuskäytäntöä.
- Juurivarmentaja tunnistaa varmentajan varmennetta hakevan organisaation luotettavasti varmennuskäytännössä kuvatulla tavalla siten, että hakijan tiedot tulevat huolellisesti tarkastetuiksi.
- Juurivarmentaja huolehtii tietojen huolellisesta käsittelystä ja luottamuksellisuudesta.

### 2.1.2 Varmentajan varmenteen haltijaorganisaatiota koskevat velvollisuudet

Varmentajan varmenteen käyttötarkoitus on kuvattu kyseessä olevassa varmennuskäytännössä. Varmennetta saa käyttää vain sen käyttötarkoituksen mukaisesti.

Varmentajan varmenteen haltijaorganisaatio vastaa siitä, että varmennetta haettaessa ilmoitetut tiedot ovat oikeita.

Varmentajan varmenteen haltijaorganisaation on säilytettävä yksityinen avaimensa turvallisessa ympäristössä ja pyrittävä estämään sen katoaminen, joutuminen ulkopuolisten käsiin, muuttaminen tai luvaton käyttö.

Varmentajan varmenteen haltijaorganisaation on ilmoitettava juurivarmentajalle välittömästi, jos sillä on tieto tai epäilys siitä, että varmentajan varmenteen haltijan yksityinen avain on paljastunut. Tällöin juurivarmentaja sulkee kyseisen varmentajan varmenteen ja julkaisee sen sulkulistalle.

### 2.1.3 Varmentajan varmenteeseen luottavaa osapuolta koskevat velvollisuudet

Juurivarmentaja noudattaa varmennepolitiikkaa ja varmennuskäytäntöä myöntäessään varmentajan varmenteita.

Varmentajan varmenteeseen luottava osapuoli voi vilpittömässä mielessä luottaa varmentajan varmenteeseen tarkistettuaan, että varmentajan varmenne on voimassa ja että se ei ole sulkulistalla. Varmentajan varmenteeseen luottavalla osapuolella on velvollisuus tarkistaa varmenteet sulkulistalta ennen hyväksymistä. Varmentajan varmenteen voimassaolon luotettavuuden varmistamiseksi varmenteeseen luottavan osapuolen on noudatettava alla esitettyjä sulkulistan tarkistustoimia.

Jos varmentajan varmenteeseen luottava osapuoli noutaa sulkulistan hakemistosta, sen on varmistettava sulkulistan aitous ja eheys tarkistamalla sulkulistan sähköinen allekirjoitus. Lisäksi on tarkistettava sulkulistan voimassaoloaika.

Mikäli uusinta sulkulistaa ei voida saada hakemistosta laitteiston tai hakemistopalvelun toimintahäiriön vuoksi, mitään varmennetta ei pidä hyväksyä, mikäli viimeisen saadun sulkulistan voimassaoloaika on päättynyt. Kaikki varmentajan varmenteiden ja loppukäyttäjän varmenteiden hyväksymiset tämän voimassaoloajan jälkeen tapahtuvat varmentajan varmenteeseen luottavan osapuolen omalla riskillä.

### 2.1.4 Varmentajan varmenteen julkaisemiseen liittyvät velvollisuudet

Varmentajan varmenteet julkaistaan yleisesti saatavilla olevassa julkisessa hakemistossa ja suljetut varmentajan varmenteet sulkulistalla, josta varmenteeseen luottavan osapuolen on tarkistettava varmenteen voimassaolotieto.

## 2.2 Vastuut

### 2.2.1 Juurivarmentajan vastuut

Digi- ja väestötietovirasto vastaa juurivarmentajana koko varmennejärjestelmän turvallisuudesta. Juurivarmentaja vastaa toimeksiantona hankkimistaan palveluista samoin kuin olisi itse tuottanut palvelun.

Juurivarmentaja vastaa siitä, että varmentajan varmenne on käytettävissä luovutushetkestä alkaen varmentajan varmenteen voimassaoloajan, ellei varmennetta ole asetettu sulkulistalle.

Juurivarmentaja vastaa siitä, että varmentajan varmenne on luovutettu sopimuksen mukaisesti organisaatiolle, joka on tunnistettu varmentajan varmenteelta edellytettävällä tavalla.

Juurivarmentaja vastaa siitä, että sulkulistalle viedään oikea varmentajan varmenne ja että se ilmestyy tässä varmennuskäytännössä mainitussa ajassa sulkulistalle.

### 2.2.2 Rekisteröijän vastuut

Varmentajan varmenteen rekisteröijänä toimii juurivarmentaja. Juurivarmentaja vastaa rekisteröinnin osalta tämän luvun mukaisista vahingonkorvausvastuista.

Digi- ja väestötietovirasto voi myöntää varmenteen myös omiin tarkoituksiinsa. Tällöin se noudattaa samoja vaatimuksia kuin muut organisaatiot.

### 2.2.3 Varmentajan varmenteen haltijaorganisaation vastuut

Varmentajan varmenteen haltijaorganisaatio on vastuussa varmenteen käytöstä, sillä tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista.

Varmentajan varmenteen haltijaorganisaation vastuu varmenteen käyttämisestä päättyy, kun se on ilmoittanut juurivarmentajalle varmentajan varmenteen myöntämistä koskevan sopimuksen mukaiset tiedot varmenteen sulkemiseksi. Varmentajan varmenteen haltijaorganisaation vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

### 2.2.4 Varmentajan varmenteeseen luottavan osapuolen vastuut

Varmentajan varmenteeseen luottava osapuoli ei voi luottaa varmenteeseen vilpittömässä mielessä, mikäli varmenteen voimassaoloa ei ole tarkastettu sulkulistalta. Varmentajan varmenteen hyväksyminen mainitussa tapauksessa vapauttaa Digi- ja väestötietoviraston vastuusta. Varmentajan varmenteeseen luottavan osapuolen on tarkistettava, että myönnetty varmenne vastaa käyttötarkoitustaan.

### 2.2.5 Vastuiden rajoitukset

Juurivarmentaja ei vastaa varmentajan varmenteen haltijaorganisaation yksityisen avaimen paljastumisen seurauksena syntyvistä vahingoista ja kustannuksista, ellei paljastuminen välittömästi johdu juurivarmentajan toiminnasta.

Juurivarmentaja ei vastaa varmentajan varmenteen haltijaorganisaatiolle aiheutuneista välillisistä tai seurannaisvahingoista. Juurivarmentaja ei myöskään vastaa varmentajan varmenteeseen luottavan osapuolen tai varmenteen haltijaorganisaation muun sopimuskumppanin mahdollisesti kärsimistä välillisistä tai seurannaisvahingoista.

Juurivarmentaja ei vastaa yleisten tietoliikenneyhteyksien eikä tietoverkkojen, esimerkiksi Internetin toimivuudesta eikä siitä, jos oikeustoimen suorittaminen estyy varmentajan varmenteen haltijaorganisaation käyttämän laitteen tai ohjelmiston toimimattomuudesta eikä siitä, että varmentajan varmennetta käytetään vastoin sen käyttötarkoitusta.

Juurivarmentajalla on oikeus kehittää edelleen varmennepalvelua. Juurivarmentaja ei ole velvollinen korvaamaan varmentajan varmenteen haltijaorganisaatiolle tai varmenteeseen luottavalle osapuolelle tällaisesta juurivarmentajan kehittämistyöstä aiheutuvia kustannuksia.

Juurivarmentajalla on oikeus keskeyttää varmennepalvelu muutos tai huoltotoimien ajaksi. Sulkulistaa koskevista muutoksista tai huoltotöistä ilmoitetaan etukäteen.

Juurivarmentaja ei vastaa varmenteeseen pohjautuvan verkkopalvelun tai sovelluksen virheistä tai niistä aiheutuvista kustannuksista.

Varmentajan varmenteen haltijaorganisaation vastuu varmenteen käyttämisestä päättyy, kun organisaation edustaja on ilmoittanut juurivarmentajalle tarvittavat tiedot varmenteen sulkemiseksi. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

## 2.3 Taloudellinen vastuu

### 2.3.1 Juurivarmentaja

Juurivarmentajalla on toimintaansa liittyen vahingonkorvausvastuu, joka perustuu yhteistyösopimuksiin sekä säädetyn oikeuden mukaisiin velvoitteisiin.

### 2.3.2 Muut osapuolet

Varmentajan varmenteeseen luottava osapuoli voi luottaa varmenteeseen ja sillä tehtyihin toimiin, jos hän on tarkastanut, ettei varmennetta ole asetettu sulkulistalle eikä varmenteen voimassaoloaika ole umpeutunut ja varmenteen allekirjoitus on tarkistettu. Juurivarmentaja vastaa varmentajan varmenteesta ennen varmenteen ilmoittamista sulkulistalle sen mukaisesti kuin se on sitoutunut tässä varmennepolitiikassa ja varmentajan varmennetta koskevassa varmennuskäytännössä.

### 2.3.3 Juurivarmentajan taloushallinto

Juurivarmentajana toimivan Digi- ja väestötietoviraston tuottamat varmennepalvelut ovat sellaisen taloushallinnollisen järjestelmän ja valvonnan piirissä kuin on erikseen säädetty. Digi- ja väestötietovirasto on valtiovarainministeriön alaisuudessa toimiva nettobudjetoitu virasto, jonka kustannuksista noin kaksi kolmasosaa katetaan kerätyillä maksuilla. Digi- ja väestötietoviraston taloushallinnon järjestäminen perustuu valtion taloutta ohjaaviin lakeihin ja asetuksiin sekä valtiovarainministeriön ja Valtiokonttorin määräyksiin. Valtiontalouden tarkastusvirasto tarkastaa Digi- ja väestötietoviraston toimintaa säännönmukaisesti. Lisäksi toiminnan tuloksellisuutta kuvataan vaikuttavuuden, taloudellisuuden ja tuottavuuden näkökulmasta.

## 2.4 Tulkinta ja täytäntöönpano

### 2.4.1 Sovellettava lainsäädäntö

Juurivarmentaja noudattaa varmennepalvelutoiminnassaan voimassaolevaa Suomen lainsäädäntöä.

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

### 2.4.2 Erimielisyyksien ratkaiseminen

Juurivarmentaja vastaa varmenteita myöntäessään siitä, että varmentajan varmenteet täyttävät tässä varmennepolitiikassa esitetyt vaatimukset.

Mahdolliset erimielisyydet ratkaistaan Suomen oikeusjärjestyksen mukaisesti. Valitusten ja riitojen ratkaisussa sekä hallinnollisessa valvonnassa ja lainkäytössä noudatetaan voimassaolevaa lainsäädäntöä.

## 2.5 Maksut

Tässä kappaleessa on määritelty Digi- ja väestötietoviraston myöntämän varmentajan varmenteen käyttöön liittyvät maksut.

### 2.5.1 Varmentajan varmenteen myöntäminen ja uusiminen

Varmentajan varmennetta haetaan Digi- ja väestötietovirastosta. Varmenne myönnetään aina uuden hakemuksen perusteella noudattaen varmennuskäytännössä määriteltyä tunnistamismenettelyä. Varmentajan varmenteen hinta perustuu kulloinkin voimassaolevaan Digi- ja väestötietoviraston palveluhinnaston mukaiseen vuosimaksuun.

### 2.5.2 Varmentajan varmenteen käyttöön liittyvät maksut

Juurivarmentaja ei erikseen veloita varmentajan varmenteen haltijaa varmenteiden, sulkupalvelun tai julkisen hakemiston käytöstä. Varmentajan varmenteen hinta perustuu kulloinkin voimassa olevaan Digi- ja väestötietoviraston palveluhinnaston mukaiseen vuosimaksuun.

Yksittäiset verkkopalveluntarjoajat saattavat veloittaa erikseen oman palvelunsa käytöstä.

### 2.5.3 Varmentajan varmenteen sulkulistamerkintään liittyvät maksut

Varmentajan varmenteen ilmoittaminen sulkulistalle on maksutonta. Myös sulkulistojen noutaminen hakemistosta sekä varmentajan varmenteiden voimassaolon tarkistaminen sulkulistalta on maksutonta.

## 2.6 Tietojen julkaiseminen ja saatavuus

### 2.6.1 Varmentajan varmenteen tietojen julkaiseminen

Juurivarmentaja julkaisee kaikki varmentajan varmenteet ja sulkulistat yleisesti saatavilla olevassa julkisessa hakemistossa. Digi- ja väestötietovirasto julkaisee varmennepolitiikan, varmennuskäytännöt, varmennekuvauksen sekä muut julkiset varmennepalvelujen tuottamiseen liittyvät dokumentit verkkosivuillaan.

### 2.6.2 Julkaisutiheys

Varmentajan varmenne julkaistaan julkisessa hakemistossa ja se on hakemistossa koko voimassaolonsa ajan. Juurivarmentaja julkaisee suljettuja varmentajan varmenteita koskevan sulkulistan, joka on voimassa yhden vuoden julkaisemisestaan. Tämä sulkulista päivitetään kerran vuodessa tai tarpeen mukaan uudella sulkulistalla.

### 2.6.3 Tietojen saatavuus

Hakemisto ja sulkulistatiedot ovat yleisesti saatavilla. Digi- ja väestötietoviraston julkaisemat FINeID-määritykset, varmennepolitiikat ja varmennuskäytännöt ovat saatavilla sen verkkosivuilla.

### 2.6.4 Tietovarastot

Juurivarmentajana toimivan Digi- ja väestötietoviraston julkaisemat tiedot ovat saatavilla sen verkkosivuilla. Varmennejärjestelmän tiedot, jotka eivät ole julkisia, on talletettu Digi- ja väestötietoviraston tietovarastoon. Varmentajan tiedot arkistoidaan juurivarmentajan voimassaolevan arkistosäännön mukaisesti.

## 2.7 Tietoturvatarkastus

### 2.7.1 Tarkastusten tiheys

Juurivarmentaja Digi- ja väestötietovirasto tekee tietoturvatarkastuksen myöntämänsä varmentajan varmenteen haltijaorganisaation toimitiloihin, laitteisiin ja toimintaan tarkoituksenmukaisella tavalla. Tarkastus tehdään vähintään kerran vuodessa ja aina, kun uusi sopimuskausi alkaa. Tarkastusmenettelyssä Digi- ja väestötietovirasto noudattaa ISO 27001 –tietoturvastandardin mukaisia menettelytapoja.

Tarkastuksen avulla selvitetään, että toimiiko varmentaja sopimuksen mukaisesti ottaen huomioon tietoturvastandardien vaatimukset. Pääsääntöisesti varmentajaa arvioidaan ISO 27001 –standardin mukaisesti.

## 2.8 Tietojen julkaiseminen

### 2.8.1 Juurivarmentajan julkaisemat tiedot

Varmennejärjestelmän tietoja ei julkaista eikä luovuteta edelleen, ellei tietojen luovuttaminen perustu henkilötietolain, viranomaisten julkisuudesta annetun lain, lain väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista tai vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain säännöksiin tietojen luovuttamisesta, tai varmentajan varmennepolitiikassa tai varmennuskäytännössä määriteltyihin tarkoituksiin.

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

Varmentajan varmenteen voimassaolon alkamis- ja päätymisajankohta on merkitty varmenteeseen. Kesken voimassaoloajan suljetut varmentajan varmenteet julkaistaan yleisesti saatavilla olevalla sulkulistalla.

Viranomaisille luovutettavat tiedot määritellään voimassaolevan lainsäädännön mukaisesti.

Varmennejärjestelmän tietoja luovutetaan ainoastaan tässä luvussa mainittuihin tarkoituksiin

### 2.8.2 Muut tiedon luovuttamiseen liittyvät periaatteet

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

Digi- ja väestötietovirasto noudattaa henkilötietojen käsittelyssä henkilötietolakia sekä erityislainsäädäntöä. Digi- ja väestötietovirasto on valmistellut käytännesäännöt sekä tietojen luovuttamisen, että varmennetoiminnan yhteydessä tapahtuvasta henkilötietojen käsittelystä. Henkilötietojen käsittelyssä noudatetaan erityistä huolellisuutta.

## 2.9 Immateriaalioikeudet

Digi- ja väestötietovirasto omistaa kaikki varmenteisiin ja dokumentaatioon liittyvät tiedot sekä myöntämänsä varmenteet teknisten toimitussopimusten mukaisesti. Digi- ja väestötietovirasto omistaa täydet omistus ja käyttöoikeudet tähän varmennuskäytäntöön ja varmentajan varmennepolitiikkaan.

# 3 Varmentajan varmenteen hakijan tunnistaminen

## 3.1 Rekisteröinti

Luvuissa 4.1.4.3. esitetään ne käytännöt ja toimintaprosessit, joita noudatetaan varmentajan varmenteen hakijoiden tunnistamisessa ja todentamisessa.

Varmentajan varmenteen hakijan oikeudet ja velvollisuudet on mainittu varmentajan varmenteen haltijaorganisaation ja juurivarmentajan välisessä sopimuksessa varmentajan varmenteen tuottamiseksi.

Sopimuksessa mainitaan selkeästi, että varmentajan varmenteen hakija hyväksyy varmentajan varmenteen luomisen ja julkaisun julkisessa hakemistossa. Samalla hakija hyväksyy varmentajan varmenteen käyttöön liittyvät säännöt ja ehdot sekä yksityisen avaimen huolellisesta säilyttämisestä sekä mahdollisen väärinkäytön tai yksityisen avaimen paljastumisen ilmoittamisesta.

Varmentajan varmenteen hakija vastaa siitä, että kaikki varmenteen kannalta olennaiset tiedot, jotka varmenteen hakija on antanut varmentajalle tai rekisteröijälle, ovat oikeita.

### 3.1.1 Nimeämiskäytännöt

Juurivarmentaja on:

Digi- ja väestötietoviraston juurivarmentajat ovat:

CN (Common name) = DVV Gov. Root CA – G3 RSA

OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Digi- ja vaestotietovirasto CA

C (Country) = FI

ja

CN (Common name) = DVV Gov. Root CA – G3 ECC

OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Digi- ja vaestotietovirasto CA

C (Country) = FI

Juurivarmentaja allekirjoittaa varmentajan varmenteen ja se sijoitetaan julkiseen hakemistoon.

Varmentajan varmenteen haltijaa koskevat tiedot määrittelevät varmenteen haltijaorganisaation yksikäsitteisesti.

### 3.1.2 Yksityisten avainten toimittaminen varmentajan varmenteen haltijalle

Varmentajan varmenteen hakija luo yksityisen ja julkisen avaimen. Varmentajan varmenteen hakijan velvollisuus on säilyttää yksityinen avaimensa turvallisessa ympäristössä ja estettävä sen katoaminen, joutuminen ulkopuolisten käsiin, muuttaminen tai luvaton käyttö.

## 3.2 Avainparin uusiminen

Varmentajan varmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmentajan varmennetta ensi kertaa haettaessa. Kun varmentajan varmenteen haltija uusii yksityisen avaimensa, se vaatii aina uuden rekisteröitymisen, uuden sopimuksen ja uuden varmentajan varmenteen.

## 3.3 Sulkupyynnön tekeminen

Varmentajan varmenteen haltija voi halutessaan saada varmentajan varmenteen suljettavaksi ennen varmentajan varmenteen voimassaoloajan päättymistä.

Varmentajan varmenteen haltijaorganisaation edustajan on ilmoitettava juurivarmentajalle toimitussopimuksessa mainitulla tavalla välittömästi, jos on tiedossa tai oletettavissa, että varmentajan varmenteen yksityinen avain on paljastunut. Tällöin juurivarmentaja sulkee ko. varmenteen. Varmentajan varmenteen sulkupyynnön tekee ensisijaisesti varmentajan varmenteen haltija, jos varmenteen väärinkäyttö on tullut mahdolliseksi. Sulkupyynnön voi tehdä myös rekisteröijä tai juurivarmentaja.

# 4 Toiminnalliset vaatimukset

## 4.1 Varmentajan varmenteen hakeminen

Varmentajan varmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa ja varmentajan varmenteen hakijana toimivan organisaation kanssa tehtävässä sopimuksessa. Sopimuksen allekirjoittaa varmentajan varmenteen haltijaorganisaation toimivaltainen edustaja. Sopimuksessa on mainittu kummankin osapuolen oikeuksista ja velvollisuuksista. Hakemusasiakirjan ja käyttöehtojen mukaisesti varmentajan varmenteen hakija vahvistaa allekirjoituksellaan annettujen tietojen oikeellisuuden sekä hyväksyy varmenteen luomisen ja julkaisun hakemistossa. Samalla varmenteen hakija hyväksyy varmenteen ilmoittamisen sulkulistalle, jos väärinkäytön mahdollisuus on olemassa.

## 4.2 Varmentajan varmenteen myöntäminen

Varmentaja myöntää Varmentajan varmenteen hyväksyessään varmentajan varmennetta koskevan hakemuksen ja allekirjoittamalla siihen liittyvän varmentajan varmennetta koskevan toimitussopimuksen.

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

## 4.3 Varmentajan varmenteen vastaanottaminen

Myönnetty varmentajan varmenne toimitetaan asiakkaalle sopimuksen mukaisesti.

## 4.4 Varmentajan varmenteen voimassaoloaika ja sulkeminen

### 4.4.1 Varmentajan varmenteen sulkemisen edellytykset

Varmentajan varmenteen haltijan on ilmoitettava varmentajalle välittömästi, jos on tiedossa tai epäiltävissä, että varmentajan varmenteen yksityinen avain on paljastunut. Tällöin juurivarmentaja sulkee ko. varmenteen. Varmentajan varmenteen haltijaorganisaation toimivaltainen edustaja on määritelty juurivarmentajan ja varmentajan varmenteen haltijaorganisaation välisessä sopimuksessa.

Suljettuja varmentajan varmenteita ei voi palauttaa käyttöön.

Juurivarmentaja sulkee myöntämänsä Varmentajan varmenteet, mikäli varmenteen tietosisällössä havaitaan virhe tai tiedossa on varmentajan varmenteen yksityisen avaimen paljastuminen tai sen perusteltu uhka tai varmentajan varmenteen haltijaorganisaation kanssa tehtyä sopimusta ei ole noudatettu tai sen voimassaolo on päättynyt.

Juurivarmentaja voi sulkea yksityisellä avaimellaan allekirjoitetut Varmentajan varmenteet, mikäli on syytä epäillä juurivarmentajan yksityisten avainten paljastuneen tai joutuneen vääriin käsiin.

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

Mikäli Digi- ja väestötietoviraston varmentajan varmenteiden myöntämisessä käyttämä yksityinen avain tai muu tekninen menetelmä on paljastunut tai tullut muutoin käyttökelvottomaksi, Digi- ja väestötietoviraston on ilmoitettava tapahtuneesta kaikille varmentajan varmenteen haltijaorganisaatioille ja loppukäyttäjille asianmukaisella tavalla.

Juurivarmentaja voi sulkea varmentajan varmenteen erityisestä syystä.

Varmentajan varmenteen sulkeminen toteutetaan välittömästi sulkupyynnön saavuttua ja kun varmentajan varmenteen sulkeminen on vahvistettu.

### 4.4.2 Sulkulistan julkaisutiheys

Varmentajan varmenne julkaistaan julkisessa hakemistossa ja se on hakemistossa koko voimassaolonsa ajan. Varmentaja julkaisee sulkulistan, joka on voimassa yhden vuoden ajan julkaisemisestaan. Tämä sulkulista päivitetään kerran vuodessa uudella sulkulistalla.

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.

Varmentajan varmenteeseen luottavan osapuolen velvollisuudet on kuvattu luvussa 2.

### 4.4.3 Varmentajan varmenteen haltijan yksityisen avaimen paljastumista koskevat erityisvaatimukset

Varmentajan varmenteen haltijan vastuulla on suojata yksityisen avaimensa käyttö huolehtimalla kaikin keinoin yksityisestä avaimestaan käyttöehdoissa mainitulla tavalla. Varmentajan varmenteen haltijaorganisaation on välittömästi otettava yhteyttä juurivarmentajaan, mikäli se epäilee, että sopimusehtojen vastainen käyttö on tullut mahdolliseksi.

## 4.5 Järjestelmän valvonta

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

## 4.6 Varmentajan varmenteisiin liittyvien tietojen arkistointi

### 4.6.1 Talletettava aineisto

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

Varmuuskopiot varastoidaan fyysisesti erilliseen tilaan alkuperäisistä tiedoista.

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

Juurivarmentaja varmistaa arkistojen tavoitettavuuden ja lukukelpoisuuden siinäkin tapauksessa, että juurivarmentajan toiminta keskeytyy tai päättyy.

## 4.7 Toiminnan jatkumisen hallinta ja poikkeustapausten käsittely

Juurivarmentajalla on jatkuvuus ja valmiussuunnitelma, joka mahdollistaa juurivarmentajan toiminnan jatkuvuuden. Juurivarmentajan toimet poikkeustapausten käsittelyn osalta on kuvattu varmennuskäytännössä.

## 4.8 Juurivarmentajan toiminnan lakkauttaminen

Juurivarmentajan lakkauttamisena pidetään tilannetta, jossa kaikki juurivarmentajan ja Varmentajan varmenteiden myöntämiseen, ylläpitoon ja hallinnointiin liittyvät palvelut lakkautetaan pysyvästi. Juurivarmentajan lakkauttamisella ei tarkoiteta tilannetta,

jossa juurivarmennuspalvelu siirretään organisaatiolta toiselle. Juurivarmentajan toimet poikkeustapausten käsittelyn osalta on kuvattu varmennuskäytännössä.

# 5 Fyysiset, toiminnalliset ja henkilöstöturvallisuuteen liittyvät vaatimukset

Juurivarmentajana toimivalle Digi- ja väestötietovirastolle on myönnetty tietoturvasertifikaatti. Digi- ja väestötietoviraston tietoturvallisuusratkaisut täyttävät standardin ISO 27001 vaatimukset.

Digi- ja väestötietovirasto käyttää teknisiä toimittajia juurivarmentajan tietoteknisten tehtävien hoitamiseen. Juurivarmentaja vastaa varmentajana varmennetuotannon turvallisuudesta ja toiminnasta asianmukaisella tavalla sen kaikilla osa-alueilla. Juurivarmentajan toimet poikkeustapausten käsittelyn osalta on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Muun organisaation kuin juurivarmentajan myöntäessä loppukäyttäjän varmenteita varmentajan varmenteeseen perustuen organisaatio noudattaa lisäksi kyseessä olevan organisaation omia tieto-turvallisuuslinjauksia.

# 6 Tekniset turvajärjestelyt

## 6.1 Avainparin luominen ja tallettaminen

### 6.1.1 Avainparin luominen

Juurivarmentajan 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. Juurivarmentaja ei julkaise todennäköisyyteen käytettyä tarkkuutta ja menetelmää.

Juurivarmentaja luo yksityiset allekirjoitusavaimensa ja yksityisiä allekirjoitusavaimiaan vastaavat julkiset avaimensa. Avaimia säilytetään juurivarmentajan hallinnoimissa avaintenhallintalaitteissa (HSM).

### 6.1.2 Avainten pituudet

Juurivarmentajan varmenteiden allekirjoittamiseen käytetty juurivarmentajan yksityinen avain sekä yksityistä avainta vastaava julkinen avain ovat 4096-bittisiä RSA-avaimia.

Varmentajan varmenteen haltijan yksityisen ja julkisen avaimen pituudet on kuvattu varmennuskäytännössä.

### 6.1.3 Avainten käyttötarkoitukset

Avaimen käyttöä koskeva kenttä (key usage) varmenteissa määrittelee varmentajan varmenteeseen liittyvän yksityisen ja julkisen avaimen käyttötarkoituksen.

## 6.2 Yksityisen avaimen suojaus

Juurivarmentajan yksityisiä avaimia säilytetään juurivarmentajan hallinnoimissa turvamoduuleissa, jotka täyttävät tarvittavan turvallisuusstandardin vaatimukset.

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

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

Varmentajan varmenteen haltijan on säilytettävä yksityinen avaimensa turvallisessa ympäristössä ja pyrittävä estämään sen katoaminen, joutuminen ulkopuolisten käsiin, muuttaminen tai luvaton käyttö.

Varmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa avaintenhallintalaitteissa.

Juurivarmentajan 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.

## 6.3 Muut avaintenhallintaan liittyvät seikat

Juurivarmentaja arkistoi kaikki varmentamansa julkiset avaimet.

Varmentajan varmenteen käyttöaika määritellään varmenteen toimittamista koskevassa sopimuksessa. Varmentajan varmenne voidaan sulkea voimassaoloaikansa kuluessa, jos sopimuksen ehtoja ei noudateta tai on muita erityisiä tässä varmennuskäytännössä esitettyjä syitä sulkea varmenne.

## 6.4 Tietokoneiden käyttöön ja niihin pääsyyn liittyvät turvallisuusvaatimukset

Juurivarmentajan 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.

Juurivarmentajan varmennejärjestelmän laitteistot ovat ympärivuorokautisessa valvonnassa.

## 6.5 Varmennejärjestelmän elinkaaren hallinta

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

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

## 6.6 Tietoverkon turvallisuus

Juurivarmentajan 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 varmentajan varmennejärjestelmään liittyvissä tehtävissä. Verkko on jaettu loogisiin verkon osiin, joiden välisiä yhteyksiä rajoitetaan.

## 6.7 Turvamoduulin käytön valvonta

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

Moduuli kerää lokitietoa tapahtumista.

# 7 Varmentajan varmenne ja sulkulistaprofiilit

## 7.1 Varmentajan varmenteiden tekniset tiedot

Juurivarmenteen ja varmentajan varmenteiden tietosisällöt on kuvattu dokumentissa FINEID S2. Dokumentti on saatavilla juurivarmentajan verkkosivuilla www.fineid.fi.

## 7.2 Sulkulistaprofiili

Juurivarmentajan julkaisemien sulkulistojen tietosisällöt on kuvattu dokumentissa FINEID S2. Dokumentti on saatavilla juurivarmentajan verkkosivuilla www.fineid.fi.

# 8 Määritysasiakirjojen hallinta

## 8.1 Määritysten muuttaminen

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

## 8.2 Julkaiseminen ja tiedottaminen

Juurivarmentaja julkaisee varmennepolitiikan ja varmennuskäytännön, jotka ovat saatavilla internet sivustolla www.fineid.fi.

Juurivarmentajan julkiset varmenteiden tuotantoon liittyvät määritykset ovat saatavilla samoilla internetsivustoilla.

Tietoteknisten toimittajien kanssa tehdyt varmenteiden toimittamista koskevat sopimukset sekä tuotantojärjestelmien kuvaukset ja tuotteisiin liittyvät määritykset ovat luottamuksellisia.

## 8.3 Varmennepolitiikan muutos ja hyväksymismenettely

Digi- ja väestötietovirasto hyväksyy juurivarmentajan sekä varmentajan varmennetta koskevan varmennepolitiikan, että varmennuskäytännöt. Juurivarmentajan asiakirjoja voidaan muuttaa Digi- ja väestötietoviraston sisäisin muutosmenettelyin.

Digi- ja väestötietovirasto ilmoittaa muutoksista hyvissä ajoin ennen niiden voimaantuloa omilla verkkosivuillaan.

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