DIGI- JA VÄESTÖTIETO-VIRASTO

Varmennuskäytäntö

Digi- ja väestötietoviraston juurivarmennetta varten

OID: 1.2.246.517.1.10.201

15.9.2023

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

Dokumentinhallinta

Omistaja	
Laatinut	Tuire Saaripuu (TS), Ville Aarnio (VA), Jari Pirinen (JP)
Tarkastanut	
Hyväksynyt	Mikko Pitkänen

Version hallinta

versionro	mitä tehty	pvm/henkilö
v. 1.0	Hyväksytty versio 1.0., julkaistu 14.12.2017	14.12.2017/TS
v.1.1	Päivitetty versio	18.6.2019/TS
v 1.2	Päivitetty versio, viraston nimenmuutos.	1.1.2020/TS
v 1.3	Päivitetty versio, saavutettavuusominaisuudet	4.5.2021/VA
v 1.4	Päivitetty versio, linkit varmennepolitiikkaan	16.9.2022/VA
v 1.6	Päivitetty versionumeroksi 1.6 jotta se olisi linjassa muiden samanaikaisesti päivitettävien asiakirjojen kanssa. Muutettu kohdissa 4.4.1 ja 4.4.4 sana ’välittömästi’ sanaan ’viipymättä’. Muutettu voimaantulopäivä viittaukseksi kansisivun päiväykseen kohdassa 2.	15.9.2023/JP

Sisällysluettelo

Varmennuskäytäntö

Määritelmät ja lyhenteet

Määritelmät

Aktivointitieto: Sellainen luottamuksellinen tieto, jota tarvitaan RSA-avaimien lisäksi kryptografisten moduulien käyttöä varten (esimerkiksi perustunnusluku ja allekirjoitustunnusluku).

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.

Kansalaisvarmenne: Digi- ja väestötietoviraston luonnolliselle henkilölle myöntämä sähköisen asioinnin varmenne, joka on määritelty laissa väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista.

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.

PDS: PKI Disclosure Statement, varmennekuvaus. Asiakirjassa kuvataan pääpiirteissään varmentajan toiminnan keskeiset osa-alueet.

RSA-algoritmi: Eräs julkisen avaimen algoritmi, asymmetrinen algoritmi.

Rekisteröijä: Rekisteröijä tunnistaa varmenteen hakijan varmennepolitiikan / varmennuskäytännön mukaisesti juurivarmentajan toimeksiannosta.

Sulkulista: Luettelo kesken voimassaoloajan suljetuista varmenteista. Sulkulistalle vietyä varmennetta ei voi aktivoida uudelleen käyttöön. (Authority Revocation List, ARL).

Varmenne: Sähköinen todistus, joka liittää allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistaa allekirjoittajan.

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

Varmennekuvaus: Asiakirja sisältää varmennepolitiikan ja varmennuskäytännön keskeiset ratkaisut.

Varmennepolitiikka (CP): Asiakirja, jossa on kuvattu, kuinka juurivarmentaja myöntää varmentajan varmenteita. Asiakirjassa on kuvattu lisäksi mm. osapuolten vastuut. Varmennepolitiikan on oltava julkisesti saatavilla.

Varmennerekisteri: Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukainen rekisteri, jota yleisölle tarjoavan Varmentajan on velvollisuus pitää yllä säädetyn määräajan.

Varmennuskäytäntö (CPS): Tarkempi kuvaus siitä, miten juurivarmentaja toteuttaa varmennepolitiikkaa.

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

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

Varmentajan varmenne: Juurivarmentajan myöntämä varmentajan yksityistä avainta vastaavan julkisen avaimen sisältävä (CA-) varmenne, jonka avulla varmentajan sähköisen allekirjoituksen aitous tarkistetaan.

Varmenteen hakija: Organisaatio, joka hakee varmennetta ja joka tunnistetaan varmenteen hakemisen yhteydessä.

Varmenteen haltija: Organisaatio, jonka julkinen avain on varmennettu juurivarmentajan yksityisellä avaimella, ja jonka yksilöintitiedot ovat varmentajan varmenteessa.

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.

Lyhenteet

ARL	Authority Revocation List

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
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

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

Tätä varmennuskäytäntöä sovelletaan Digi- ja väestötietoviraston juurivarmentajan (VRK Gov. Root CA – G2) varmenteeseen.

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

1.1 Yleistä

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 laatii erillisen varmennepolitiikan jokaiselle myöntämälleen varmennetyypille sekä varmennuskäytännön jokaista eri teknistä alustaa koskien. Varmennepolitiikka kuvaa varmennetyypeittäin käytettävät menettelytavat, käyttöehdot, vastuiden jaon ja muut varmenteen käyttöön liittyvät näkökulmat yleisellä tasolla. Varmennuskäytäntö kuvaa noudatettavat menettelytavat yksityiskohtaisella tasolla. Jokaisella asiakirjalla on oma yksilöivä OID-tunnuksensa. Nämä asiakirjat ovat saatavilla sähköisesti osoitteessa www.dvv.fi/cps.

Digi- ja väestötietoviraston varmennetoiminta perustuu 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).

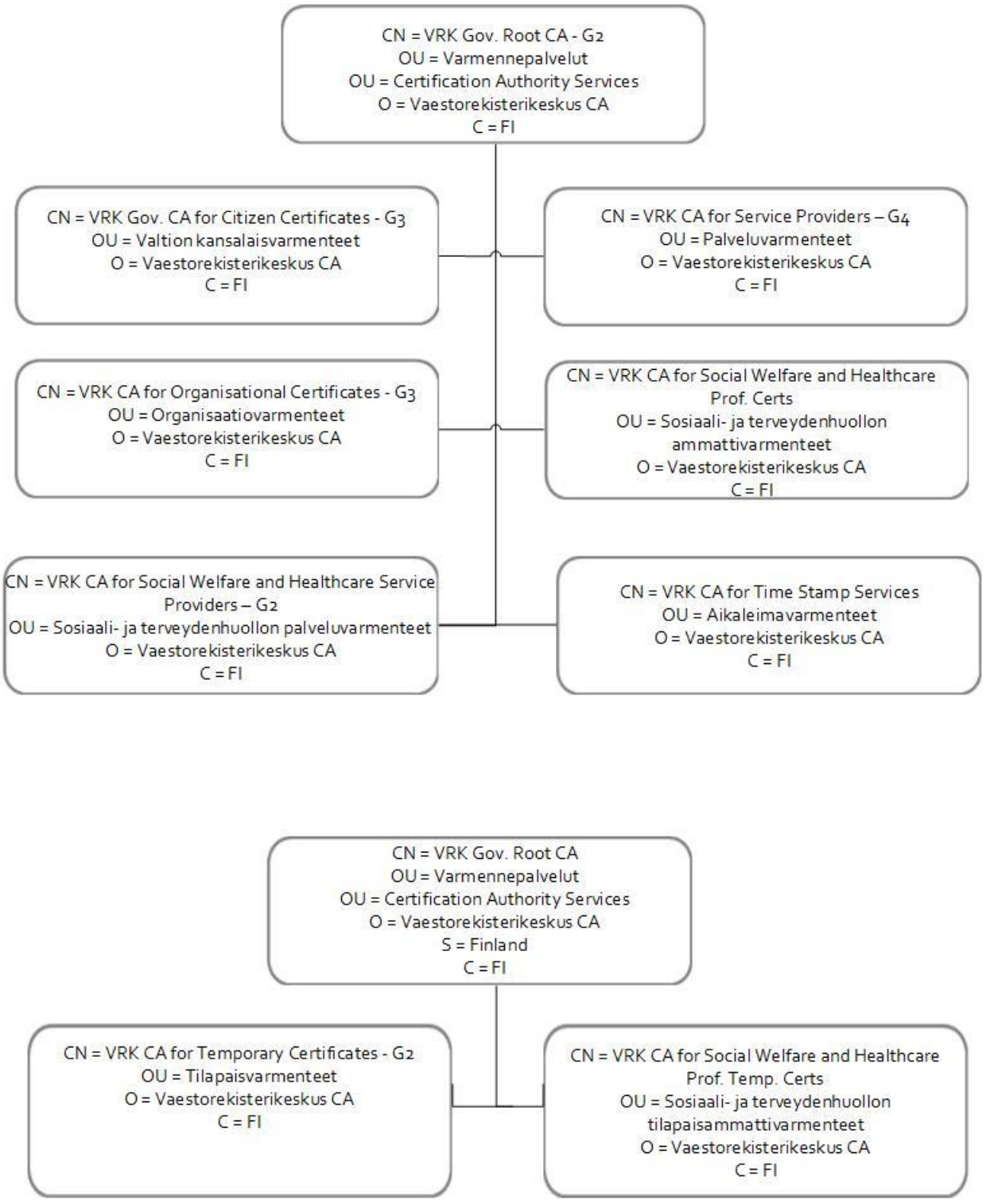
Digi- ja väestötietoviraston luottamuspalvelut täyttävät eIDAS-asetuksessa asetettujen vaati-musten lisäksi hyväksytyn luottamuspalvelun tarjoajaa koskevan standardin EN 319 401 sekä varmenteita tarjoavan hyväksytyn luottamuspalvelun tarjoajaa koskevan standardin EN 319 411-1 vaatimukset.

Digi- ja väestötietoviraston myöntämät varmenteet ovat vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) mukaisia allekirjoitusvarmenteita ja vahvan sähköisen tunnistamisen välineitä. DVV myöntää myös muita henkilö- ja ohjelmistovarmenteita samassa varmentajan luotettavassa järjestelmässä.

Digi- ja väestötietoviraston luottamusrakenne on hierarkkinen: Digi- ja väestötietovirastolla on yksi juurivarmentaja, joka myöntää varmenteet muille varmentajille. Varmentaja voi olla joko Digi- ja väestötietovirasto tai muu julkinen tai yksityinen organisaatio.

Digi- ja väestötietovirasto siirtyi 14.12.2017 uuden varmennejärjestelmän käyttöön. Digi- ja väestötietoviraston luottamusmalli on hierarkkinen: Digi- ja väestötietovirastolla on yksi juurivarmentaja, joka myöntää varmenteet muille varmentajille. Varmentaja voi olla joko Digi- ja väestötietovirasto tai muu julkinen tai yksityinen organisaatio.

Tämä asiakirja kuvaa niitä käytäntöjä, joita juurivarmentaja noudattaa myöntäessään varmenteen valtion kansalaisvarmenteita myöntävälle varmentajalle. Juurivarmentaja ei myönnä loppukäyttäjän varmenteita: niitä myöntävät juurivarmentajan varmentamat varmentajat, joilla jokaisella on oma varmennepolitiikka ja omat varmennekäytäntönsä.



Kuva 1: Varmennehierarkia

Varmentajan varmenne sisältää varmentajan julkisen avaimen, nimen, varmenteen käyttötarkoituksen, voimassaoloajan sekä muut varmenteen käytön kannalta

välttämättömät tiedot. Varmenteen tiedot on sähköisesti allekirjoitettu juurivarmentajan yksityisellä avaimella. Tämän varmennuskäytännön mukainen varmentajan varmenne perustuu julkisen avaimen järjestelmään.

Varmentajan varmenteessa olevaa julkista avainta vastaavalla yksityisellä avaimella allekirjoitetaan sähköisesti kaikki myönnettävät kansalaisvarmenteet 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 ja sekä erilliset varmennuskäytännöt jokaista juurivarmentajan myöntämää varmentajan varmennetta varten. Varmenne-politiikka kuvaa varmentajan varmennetoiminnassa käyttämät menettelytavat, käyttöehdot, vastuiden jaon ja muut varmennetoimintaan liittyvät näkökulmat yleisellä tasolla. Varmennuskäytäntö kuvaa noudatettavat menettelytavat yksityiskohtaisesti.

1.2 Tunnistetiedot

Tämän varmennuskäytännön nimi on Varmennuskäytäntö Digi- ja väestötietoviraston juurivarmennetta varten,

ja se viittaa seuraaviin alivarmenteiden varmennekäytäntöihin:

VRK Gov. CA for Citizen Certificates - G3, OID: 1.2.246.517.1.10.201.1

VRK CA for Organisational Certificates - G3, OID: 1.2.246.517.1.10.201.2

VRK CA for Temporary Certificates - G2, OID: 1.2.246.517.1.10.201.3

VRK CA for Service Providers - G4, OID: 1.2.246.517.1.10.201.4

VRK CA for Social Welfare and Healthcare Prof. Certs, OID: 1.2.246.517.1.10.201.5

VRK CA for Social Welfare and Healthcare Prof. Temp. Certs, OID: 1.2.246.517.1.10.201.6

VRK CA for Social Welfare and Healthcare Service Providers – G2, OID: 1.2.246.517.1.10.201.7

VRK CA for Time Stamp Services, OID: 1.2.246.517.1.10.201.8

Tämä varmennuskäytäntö viittaa Digi- ja väestötietoviraston juurivarmentajan politiikkaa varten, OID 1.2.246.517.1.10.201.

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

1.3 Juurivarmentaja ja varmentajan varmenteiden sovellusalueet

Juurivarmentaja tuottaa varmennepalvelut tässä varmennuskäytännössä mainituin ehdoin ja vastaa niiden toimivuudesta juurivarmentajan vastuita kuvaavan luvun 2.2.1 mukaisesti. Juurivarmentaja vastaa koko varmennejärjestelmän toimivuudesta, myös käyttämiensä rekisteröijien ja teknisten toimittajien osalta. Tämän varmennuskäytännön on rekisteröinyt Digi- ja väestötietovirasto, joka toimii myös tämän varmennuskäytännön mukaisena varmentajan varmenteen haltijana.

Digi- ja väestötietovirasto on henkilörekisteriä ylläpitävä 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 varmentajan varmenteiden sulkemisesta ja varmentajan varmenteiden sulkulistojen (ARL) 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 Internet-palvelu, josta on saatavilla kaikki juurivarmentajan myöntämät varmentajan varmenteet sekä uusin sulkulista. Hakemistopalvelu on saatavissa osoitteessa ldap://ldap.fineid.fi.

1.3.4 Varmentajan varmenteen haltijaorganisaatio

Tämän varmennuskäytännön mukainen varmentajan varmenne on myönnetty Digi- ja väestötietovirastolle kansalaisvarmenteen myöntämistä varten.

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 ja joka käyttää juurivarmentajan varmennetta

varmentajan varmenteen aitouden ja eheyden tarkistamiseen. Varmentajan varmenteeseen luottavan osapuolen on tarkistettava, että varmenne on voimassa ja varmenne ei ole sulkulistalla.

1.3.6 Varmentajan varmenteen käyttäminen

Tämän varmennuskäytännön mukaisen varmentajan varmenteen käyttötarkoituksia ovat: varmentajan 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 Varmennuskäytäntöä hallinnoiva organisaatio

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

Tämän varmennuskäytännön mukaiset tekijänoikeudet kuuluvat Digi- ja väestötietovirastolle.

1.4.2 Yhteyshenkilö

Tätä varmennuskäytäntöä koskevat kysymykset lähetetään seuraavaan osoitteeseen:

Digi- ja väestötietovirasto

PL 123 (Lintulahdenkuja 2)
00531 Helsinki
Y-tunnus: 0245437-2

Puh. +358 295 535 001
Fax. +358 9 876 4369
kirjaamo@dvv.fi

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

Digi- ja väestötietovirasto (DVV) Varmennepalvelut

PL 123

00531 Helsinki

www.dvv.fi

2 Yleiset ehdot

Tämä varmennuskäytäntö astuu voimaan asiakirjan kansisivulla mainittuna päivämääränä. Varmennuskäytännön 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.
- 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 käyttötarkoituksia ovat: kansalaisvarmenteiden allekirjoittaminen ja sulkulistan allekirjoittaminen. 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 estettävä 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 yksityinen avain on paljastunut. Tällöin juurivarmentaja sulkee kyseisen varmentajan varmenteen ja julkaisee sen sulkulistalla (ARL).

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 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.

Kun 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 varmentajan varmennetta eikä sillä myönnettyä 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.

Digi- ja väestötietovirasto vastaa siitä, että varmentajan varmenteet on luotu noudattaen lakia väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annettua lakia ja että se täyttää määritellyt varmentajan vahingonkorvausvastuut. Digi- ja väestötietovirasto vastaa ainoastaan niistä tiedoista, jotka se on tallettanut varmentajan varmenteeseen.

Digi- ja väestötietovirasto vastaa siitä, että varmentajan varmenne on käytettävissä luovutushetkestä alkaen varmentajan varmenteen voimassaoloajan, ellei varmennetta ole asetettu sulkulistalle.

Digi- ja väestötietovirasto vastaa siitä, että varmentajan varmenne on luovutettu sopimuksen mukaisesti organisaatiolle, joka on tunnistettu varmentajan varmenteelta edellytettävällä tavalla.

Allekirjoittaessaan varmentajan varmenteen yksityisellä avaimellaan juurivarmentaja vakuuttaa tarkistaneensa varmenteessa olevat tiedot juurivarmentajan varmennepolitiikassa ja varmennuskäytännössä esitettyjen menettelyjen mukaisesti.

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. Varmentajan varmennetta haetaan juurivarmentajalta tätä koskevan hakemuksen perusteella.

Juurivarmentaja noudattaa kaikissa toimissaan tässä luvussa mainittuja varmentajan vastuita.

Juurivarmentaja vastaa rekisteröinnin osalta tämän luvun mukaisista vahingonkorvausvastuista.

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 juurivarmentajan 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. Digi- ja väestötietovirasto 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. Sulku-listaa koskevista muutoksista tai huoltotöistä ilmoitetaan etukäteen.

Juurivarmentaja ei 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 ja tiedottanut siitä lisäksi tärkeimmille varmenneasiointiin liittyville yhteistyökumppaneilleen ja sidosryhmilleen. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

2.3 Taloudellinen vastuu

2.3.1 Juurivarmentaja

Digi- ja väestötietovirastoa koskee vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) annetun lain mukaiset vaatimukset. Eräin osin sovelletaan myös vahingonkorvauslain (412/1974) säännöksiä.

2.3.2 Muut osapuolet

Varmentajan varmenteeseen luottava osapuoli voi luottaa varmentajan 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 varmennepolitiikassa ja tässä 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 virasto. Digi- ja väestötietoviraston taloushallinnon hoito perustuu valtion taloutta ohjaaviin lakeihin ja asetuksiin sekä valtiovarainministeriön ja Valtiokonttorin määräyksiin. Valtiontalouden tarkastusvirasto hoitaa talouden valvonnan. Lisäksi toiminnan tuloksellisuutta kuvataan vaikuttavuuden, taloudellisuuden ja tuottavuuden näkökulmasta.

2.4 Tulkinta ja täytäntöönpano

2.4.1 Sovellettava lainsäädäntö

Juurivarmentaja noudattaa varmennepalvelutoiminnassaan voimassaolevaa Suomen lainsäädäntöä.

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

Juurivarmentaja noudattaa henkilötietolain (523/1999) mukaista henkilötietojen hyvää tietojenkäsittelytapaa ja viranomaisten julkisuudesta annetun lain (621/1999) mukaista hyvää tiedonhallintatapaa.

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 väestötietovirastoa koskee vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) annetun lain mukaiset vaatimukset. Eräin osin sovelletaan myös vahingonkorvauslain (412/1974) säännöksiä.

2.4.2 Erimielisyyksien ratkaiseminen

Juurivarmentaja vastaa varmenteita myöntäessään siitä, että varmentajan varmenteet täyttävät tässä varmennuskäytännössä sekä varmentajan varmennetta koskevassa 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 juurivarmentajan 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 tässä 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 voimassaolevaan juurivarmentajan 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 (ARL) 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 maksuttomassa, 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 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

Digi- ja väestötietoviraston julkaisemat tiedot ovat saatavilla sen verkkosivuilla. Varmennejärjestelmän tiedot, jotka eivät ole julkisia, on talletettu Digi- ja väestötietoviraston omaan tietovarastoon. Varmentajan tiedot arkistoidaan juurivarmentajan voimassaolevan arkistosäännön mukaisesti. Henkilötietojen käsittelyyn kiinnitetään erityistä huolellisuutta ja

Digi- ja väestötietovirasto on julkaissut varmennepalveluiden tuottamisesta erityiset henkilötietolain mukaiset käytännesäännöt. Digi- ja väestötietovirasto on valmistellut myös varmennejärjestelmän jokaiselta osa-alueelta henkilötietolain mukaisen rekisteriselosteen henkilötietojen käsittelyn osalta.

2.7 Tietoturvatarkastus

2.7.1 Tarkastusten tiheys

Digi- ja väestötietovirasto juurivarmentajana tekee tietoturvatarkastuksen teknisten toimittajiensa 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, toimiiko varmentaja sopimuksen mukaisesti ottaen huomioon tieto-turvastandardien vaatimukset. Pääsääntöisesti varmentajaa arvioidaan ISO 27001 –standardin mukaisesti.

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

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 laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä alle-kirjoituksista tai Digi- ja väestötietoviraston suorittaessa tarkastusta tietoturvastandardin ISO 27001, Digi- ja väestötietoviraston tietoturvapolitiikan tai teknisten toimitussopimusten mukaisesti.

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

Tarkastuksessa verrataan varmennepolitiikkaa, varmennuskäytäntöä ja teknisten toimittajien toimintaohjeita koko varmenneorganisaation ja -järjestelmän toimintaan. Digi- ja väestötietovirasto valvoo, että toimintaohjeet ovat yhdenmukaiset varmennepolitiikan kanssa.

Tarkastuksissa otetaan huomioon hallinnollisen tietoturvallisuuden lisäksi eri palveluntoimittajia mm. seuraavan jaottelun mukaisesti:

Sulkupalvelu:

- tietoliikenneturvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus

Varmennetuotanto:

- työnjaot ja kunkin tehtävät – henkilöstöturvallisuus
- fyysinen turvallisuus
- varmentajan yksityiseen avaimeen liittyvä turvallisuus
- varmentajan tuotantojärjestelmä ja varajärjestelmä
- tietoliikenneturvallisuus

Korttituotanto:

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

Hakemistopalvelu:

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

2.7.4 Poikkeamista johtuvat toimenpiteet

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

2.7.5 Tarkastuksen tuloksesta tiedottaminen

Tarkastuksen tuloksesta tiedotetaan lain, tietoturvastandardin ISO 27001, Digi- ja väestötietoviraston tietoturvapolitiikan ja voimassa olevien toimitussopimusten mukaisesti. Sisäiseen käyttöön tarkoitettu yksityiskohtainen määrämuotoinen tarkastustulos on luottamuksellinen eikä siitä anneta tietoja julkisuuteen. Määrämuotoiset raportit laaditaan erikseen organisaation ulkopuoliseen käyttöön.

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.

2.8.2 Julkiset tiedot

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

2.8.3 Varmentajan varmenteen voimassaolon päättymiseen tai keskeyttämiseen liittyvät tiedot

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

2.8.4 Viranomaisille luovutettavat tiedot

Viranomaisille luovutettavat tiedot määritellään voimassaolevan lainsäädännön mukaisesti.

2.8.5 Muut tiedot

Varmentajan varmennejärjestelmän tietoja ei luovuteta kuin edellä tässä luvussa mainittuihin tarkoituksiin.

2.8.6 Muut tiedon luovuttamiseen liittyvät periaatteet

Varmentajan luotettavuuden vuoksi on olennaista, että juurivarmentaja 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 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

Digi- ja väestötietoviraston juurivarmentaja on:

CN (Common name) = VRK Gov. Root CA – G2

OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Vaestorekisterikeskus 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 tekijän tunnistaminen

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

Sulkupyyntömenettely

Varmentajan varmenteen haltijaorganisaation edustajan on ilmoitettava juurivarmentajalle välittömästi, jos on tiedossa tai epäilys, että varmentajan varmenteen yksityinen avain on paljastunut. Tällöin juurivarmentaja sulkee ko. varmenteen. Varmentajan varmenteen sulkupyynnön tekee ensisijaisesti varmentajan varmenteen haltijaorganisaatio, 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 varmenteen haltijaorganisaation toimivaltainen edustaja. Sopimuksessa on mainittu kummankin osapuolen oikeuksista ja velvollisuuksista. Hakemusasiakirjassa ja käyttöehdoissa mainitaan selkeästi, että Varmentajan varmenteen hakija vahvistaa allekirjoituksellaan annettujen tietojen oikeellisuuden sekä hyväksyy varmenteen luomisen ja julkaisun julkisessa

hakemistossa. Samalla varmenteen hakija hyväksyy varmenteen ilmoittamisen sulkulistalle, jos väärinkäytön mahdollisuus on olemassa.

4.2 Varmentajan varmenteen myöntäminen

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

Juurivarmentaja 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 juurivarmentajalle 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.

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

4.4.2 Sulkupyynnön tekijä

Varmentajan varmenteen sulkupyynnön tekee ensisijaisesti varmenteen haltijan organisaation edustaja, jos varmentajan varmenteen väärinkäyttö on tullut mahdolliseksi. Varmentajan varmenteen voi sulkea myös rekisteröijä tai juurivarmentaja.

4.4.3 Sulkutapahtuma

Varmentajan varmenteen haltijaorganisaatio on vastuussa varmentajan varmenteen sulkemisesta. Varmentajan varmenne voidaan varmenteenhaltijan organisaation ilmoituksesta merkitä sulkulistalle, jolloin juurivarmentajan myöntämän varmentajan varmenteen käyttö estyy.

Varmentajan varmenne suljetaan ilmoittamalla varmentajan varmenteen haltijaorganisaation kanssa tehdyn toimitussopimuksen mukaisesti Digi- ja väestötietovirastolle osoitteeseen kirjaamo@vrk.fi. Varmentajan varmenteen haltijaorganisaation sopimuksen mukainen vastuu juurivarmentajaan nähden päättyy, kun sulkupyynnön mahdollistava yksilöivä ilmoitus on vastaanotettu. Samalla hetkellä päättyy varmentajan varmenteen haltijan vastuu varmentajan varmenteen käytöstä.

Suljettuja varmentajan varmenteita ei voi palauttaa käyttöön.

Digi- ja väestötietovirasto sulkee myöntämänsä varmentajan varmenteet, mikäli varmentajan 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.

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

Juurivarmentaja voi sulkea varmentajan varmenteen erityisestä syystä.

4.4.4 Sulkutapahtuman ajoitus

Varmentajan varmenteen sulkeminen toteutetaan viipymättä sulkupyynnön saavuttua.

4.4.5 Varmentajan varmenteen voimassaolon keskeyttäminen tilapäisesti

Varmentajan varmenteen voimassaoloa ei voi keskeyttää tilapäisesti.

4.4.6 Sulkulistan julkaisutiheys

Varmentajan varmenne julkaistaan julkisessa hakemistossa ja se on hakemistossa koko voimassaolonsa ajan. Juurivarmentaja 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 julkaisu-tiheyksillä ja pidennetyillä voimassaoloajoilla.

4.4.7 Sulkulistatarkistukseen liittyvät vaatimukset

Varmentajan varmenteeseen luottavan osapuolen velvollisuudet on kuvattu luvussa 2.

4.4.8 Suorakäyttöinen varmentajan varmenteen tilan tarkistaminen

Varmentajan varmenteet voi sulkea vain sopimuksessa tai tässä varmennuskäytännössä mainitulla tavalla rekisteröijän luona. Juurivarmentaja ei tarjoa suorakäyttöistä

varmenteen tilan tarkistuspalvelua eli OCSP-palvelua. Varmentaja julkaisee suljetuista varmenteista sulkulistan.

4.4.9 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. Varmentajan 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.

Lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista perustuvan varmennerekisterin tiedot säilytetään 10 vuoden ajan varmentajan varmenteiden voimassaolon päättymisestä.

Arkistotiedot säilytetään laatuvarmentajana toimivaa viranomaista koskevien säännösten mukaisesti.

4.6.2 Arkistojen suojaus

Juurivarmentaja säilyttää varmentajan varmenteen hakemiseen, henkilön tunnistamiseen ja varmentajan varmenteen luovutukseen liittyvät arkistoitavat asiakirjat asianmukaisissa tiloissa.

Arkistoitava tieto säilytetään turvallisissa tiloissa, joissa on pääsynvalvonta.

4.6.3 Arkistotietojen varmistusmenettelyt

Varmuuskopiot varastoidaan fyysisesti erilliseen tilaan alkuperäisistä tiedoista.

4.6.4 Arkistotietojen hankinta- ja varmistusmenetelmät

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.

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

4.7 Toiminnan jatkumisen hallinta ja poikkeustapausten käsittely

Juurivarmentajalla on jatkuvuus- ja valmiussuunnitelma, joka mahdollistaa juurivarmentajan toiminnan jatkuvuuden.

4.7.1 Juurivarmentajan yksityinen avain on paljastunut tai juurivarmentajan varmenne on suljettu

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

Tällaisessa tapauksessa juurivarmentaja joko lakkauttaa toimintansa luvussa 4.8 esitetyllä tavalla tai suorittaa seuraavat toimenpiteet:

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

b) Juurivarmentaja luo uuden avaimen luvun 6 mukaisesti.

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

4.7.2 Turvallisuuden vaarantuminen luonnonmullistuksen tai muun katastrofin seurauksena

Juurivarmentajana toimivan Digi- ja väestötietoviraston turvapolitiikassa on otettu huomioon ulkoisen turvallisuuden vaarantumisen aiheuttamat toimenpiteet. Digi- ja

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

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.

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

Ennen juurivarmentajan lakkauttamista suoritetaan vähintäänkin seuraavat toimenpiteet:

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

b) Juurivarmentaja lakkauttaa kaikki sopimuskumppaniensa valtuudet suorittaa kaikkien juurivarmenteiden myöntämisprosessiin liittyviä tehtäviä juurivarmentajan puolesta.

c) c) Juurivarmentaja varmistaa, että kohdassa 4.6 mainittu saatavuus juurivarmentajan arkistoihin säilyy juurivarmentajan lakkauttamisen jälkeenkin.

5 Fyysiset, toiminnalliset ja henkilöstöturvallisuuteen liittyvät vaatimukset

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

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

Juurivarmentaja noudattaa hyvää tiedonhallintatapaa. Varmenteiden tarjoamiseen liittyvät palvelut on organisoitu Digi- ja väestötietoviraston varmennepalvelut-toimintoina talon organisaatiorakenteen mukaisesti.

5.1 Fyysiseen turvallisuuteen liittyvät järjestelyt

5.1.1 Sijainti ja rakennusten ominaisuudet

Juurivarmentajan järjestelmät sijaitsevat turvallisissa konesalitiloissa ja täyttävät tietokonekeskuksille annetut turvallisuutta koskevat ohjeet ja määräykset.

Juurivarmentajan toimitilojen turvallisuus on toteutettu siten, että asiattomien pääsy toimitiloihin on estetty lukitsemalla toimitilat asianmukaisesti, käyttämällä toimitiloja jotka ovat vankkarakenteisia ja lujuudeltaan riittäviä. Konesalitiloissa on vältetty turhia ikkunoita ja niiden rakenteisiin on valittu kestäviä rakennusmateriaaleja.

5.1.2 Fyysinen pääsy toimitilaan

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

5.1.3 Sähkön syöttö ja ilmastointi

Juurivarmentajan varmennejärjestelmän konesalitilat on asianmukaisesti ilmastoitu. Tiloissa on varauduttu hallitsemattomiin sähkökatkoksiin kiinteistöihin rakennetuilla varavoimaratkaisuilla.

5.1.4 Paloturvallisuus

Juurivarmentajan varmennejärjestelmän konesalitiloissa on tarvittavat hälytysmekanismit tulipalon varalle, tarpeellinen alkusammutuskalusto sekä automaattiset sammutusjärjestelmät.

5.1.5 Tiedon säilytys

Juurivarmentajan arkistoitavat tiedot ja varmuuskopiot säilytetään eri tiloissa kuin juurivarmentajan laitteistot.

Juurivarmentajan tiedot on suojattu häviämiseltä, muuttamiselta ja luvattomalta käytöltä.

5.1.6 Tarpeettoman tietoaineiston käsittely

Juurivarmentajan turvaluokiteltu tietoaineisto hävitetään luotettavalla tavalla tuhoamalla.

5.1.7 Vesivahingot

Juurivarmentajan varmennejärjestelmän konesalitiloissa on asianmukaiset kosteuden havaitsevat ilmaisimet.

5.2 Toiminnalliset vaatimukset

5.2.1 Vastuunjako

Juurivarmentaja käyttää varmennetuotannon rekisteröintiin ja tietoteknisiin tehtäviin teknisiä toimittajia.

Juurivarmentajan tehtävät on jaettu seuraaviin vastuualueisiin:

- Tietoturvallisuusvastaava

- Rekisteröintivastaava
- Järjestelmän ylläpitäjä
- Järjestelmän käyttäjä
- Järjestelmän valvoja

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

5.2.2 Tehtäviin vaadittavien henkilöiden lukumäärä

Juurivarmentajan yksityisen avaimen luominen, aktivointi, varmuuskopiointi ja palauttaminen ovat kahden järjestelmän ylläpitotehtäviin oikeutetun henkilön läsnä ollessa tehtäviä toimenpiteitä. Samoin juurivarmentajan yksityisen avaimen peruuttaminen on mahdollista vain kahden oikeutetun henkilön valvonnassa. Kryptografisen moduulin alustuksessa on läsnä vähintään kaksi järjestelmän ylläpitotehtäviin oikeutettua henkilöä.

5.2.3 Tehtäväkohtainen tunnistaminen

Varmentajan varmenteen rekisteröijä: Rekisteröijänä toimii Digi- ja väestötietoviraston varmennetoiminnan rekisteröivä yksikkö.

Juurivarmentajan varmennejärjestelmän ylläpitäjä: Järjestelmän ylläpitäjä tunnistetaan henkilökohtaisella juurivarmentajan järjestelmän hallintaan tarkoitetulla hallintakortilla. Juurivarmentajan varmennejärjestelmän ylläpitäjiä ovat varmennejärjestelmän toimittajan järjestelmäasiantuntijat sekä Digi- ja väestötietoviraston tehtävään valtuuttamat henkilöt.

Juurivarmentajan varmennejärjestelmän käyttäjä: Järjestelmän käyttäjä tunnistetaan henkilökohtaisella järjestelmän käyttöön tarkoitetulla henkilökortilla. Juurivarmentajan varmennejärjestelmän käyttäjiä ovat konesalioperointi, teknisten varmennepyyntöjen käynnistäjät sekä sulkupalvelu.

5.3 Henkilöturvallisuus

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

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

Kilpailutuksen yhteydessä juurivarmentaja on arvioinut teknisten toimittajien avainasiantuntijoiden ja työntekijöiden pätevyyttä juurivarmentajan varmennepalvelun toteuttamiseen. Tietotekniset toimittajat ylläpitävät henkilöstönsä osaamista palvelutuotannossa käytettyjen laitteistojen, ohjelmistojen, menetelmien ja tietoturvallisuuden

osalta. Lisäksi tekniset toimittajat huolehtivat siitä, että henkilöstö tuntee varmennepalvelun tietojenkäsittelytehtävät palvelun edellyttämällä tavalla.

5.3.1 Henkilökuntaa koskevan taustaselvityksen tekeminen

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

5.3.2 Taustaselvityksen tekemisessä noudatettava menettely

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

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

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

5.3.3 Koulutukseen liittyvät vaatimukset

Juurivarmentajan 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

Digi- ja väestötietoviraston henkilökunnan koulutusta suunnitellaan ja ylläpidetään siten, että tehtävän hoitamiseen liittyvä asiantuntemus on aina tehtävän edellyttämällä tavalla parhaalla mahdollisella tasolla.

5.3.5 Tehtäväkiertoon liittyvät vaatimukset

Kun juurivarmentajan tehtävissä suunnitellaan tehtäväkiertoa, on tehtävät organisoitava siten, että henkilö voi huolehtia uusista tehtävistään parhaalla mahdollisella tavalla. Henkilöstön kierron suunnittelussa otetaan huomioon mm. tietoturvallisuuden asettamat vaatimukset, luottamuksellisuuden turvaaminen ja henkilötietojen hyvän käsittelyn periaatteet, jotka on kuvattu henkilötietojen käsittelyä koskevissa käytännesäännöissä. Myös tehtäväkierrossa noudatetaan juurivarmentajan tietoturvapolitiikkaa ja tietoturvasuunnitelmaa sekä juurivarmentajan 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 varmentajan varmennepalveluiden tuottamisen kanssa.

5.3.8 Henkilökunnan käyttöön annettavat asiakirjat

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

6 Tekniset turvajärjestelyt

6.1 Avainparin luominen ja tallettaminen

6.1.1 Avainparin luominen

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 generointi-menetelmä täyttävät laadulliset vaatimukset, joita ovat mm. algoritmin luotettavuus, generointimenetelmän toistamattomuus ja satunnaisluvun aito satunnaisuus. Juurivarmentaja ei julkaise todennäköisyyteen käytettyä tarkkuutta ja menetelmää.

Juurivarmentaja:

Juurivarmentaja luo yksityiset allekirjoitusavaimensa ja yksityisiä allekirjoitusavaimiaan vastaavat julkiset avaimensa. Avaimia säilytetään juurivarmentajan hallinnoimissa avaintenhallintalaitteissa (HSM). Avaintenhallintalaitteet täyttävät turvatasoltaan laatuvarmenteen tuottamiseksi vaadittavat edellytykset.

6.1.2 Yksityisen avaimen luovuttaminen varmentajan varmenteen hakijalle

Varmentajan varmenteen hakija luo itse yksityisen ja julkisen avaimensa.

6.1.3 Varmentajan varmenteen hakijan julkisen avaimen toimittaminen juurivarmentajalle

Varmentajan varmenteen hakija toimittaa rekisteröijälle luomansa varmennepyynnön, jonka perusteella varmentajan varmenne luodaan.

6.1.4 Juurivarmentajan julkisen avaimen jakelu varmentajan varmenteen haltijalle

Juurivarmentajan julkinen avain on varmentajan varmenteessa, joka on vapaasti levitettävissä ja saatavilla myös julkisesta hakemistosta sekä juurivarmentajan verkkopalvelusta.

6.1.5 Avainten pituudet

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

Varmentajan varmenteen haltijan yksityinen ja julkinen avain ovat 4096 –bittisiä RSA-avaimia.

6.1.6 Avainten käyttötarkoitukset

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

Juurivarmentajan varmenne:

Käyttötarkoitus: Varmentajan varmenteiden ja sulkulistojen allekirjoitus.

6.2 Yksityisen avaimen suojaus

6.2.1 Turvamoduulia koskevat standardit

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.

6.2.2 Juurivarmentajan yksityisen avaimen käsittelyyn osallistuva henkilökunta

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

6.2.3 Yksityisen avaimen luovutus luotetun osapuolen huostaan

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

6.2.4 Yksityisen avaimen varmuuskopio

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

6.2.5 Yksityisen avaimen arkistointi

Juurivarmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa avainten-hallintalaitteissa.

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

6.2.6 Yksityisen avaimen hallinnointi turvamoduulissa

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.

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

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

6.3 Muut avaintenhallintaan liittyvät seikat

6.3.1 Julkisen avaimen arkistointi

Juurivarmentaja arkistoi kaikki varmentamansa julkiset avaimet.

6.3.2 Julkisten ja yksityisten avainten käyttöaika

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 varmentajan varmenne.

6.4 Tietokoneiden käyttöön ja niihin pääsyyn liittyvät turvallisuusvaatimukset

6.4.1 Laitteistoturvallisuus

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.

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

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

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.

6.5.1 Järjestelmän kehittämiseen liittyvä valvonta

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

6.5.2 Turvallisuuden hallinta

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 juurivarmentajan 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 juurivarmentajan varmennejärjestelmään liittyvissä tehtävissä. Tarpeettomat verkkopalvelut on otettu pois käytöstä. Verkko on jaettu loogisiin verkon osiin, joiden välisiä yhteyksiä rajoitetaan. Käytössä on riittävät todentamis-, pääsynvalvonta- ja kiistämättömyysmenettelyt.

6.7 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.

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

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

7 Varmentajan varmenne- ja sulkulistaprofiilit

7.1 Varmenteiden tekniset tiedot

Juurivarmenteen tietosisällöt on kuvattu dokumentissa FINEID S2. Dokumentti on saatavilla juurivarmentajan verkkosivuilla, www.dvv.fi/cps.

7.2 Sulkulistaprofiili

Juurivarmentajan julkaisemien sulkulistojen tietosisällöt on kuvattu dokumentissa FINEID S2. Dokumentti on saatavilla juurivarmentajan verkkosivuilla, www.dvv.fi/cps.

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.dvv.fi/cps.

Juurivarmentajan julkiset varmenteiden tuotantoon liittyvät määritykset ovat saatavilla samoilla internet-sivustoilla.

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

8.3 Varmennuskäytännön 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

4.5.2021