VARMENNUSKÄYTÄNTÖ

Väestörekisterikeskuksen sosiaali- ja terveydenhuollon palvelinvarmennetta asiointikäyttöön varten
OID: 1.2.246.517.1.10.10.2

Väestörekisterikeskus

VRK/DiPa 1.2.2018

DOKUMENTINHALLINTA	
Omistaja	
Laatinut	Saaripuu Tuire
Tarkastanut	
Hyväksynyt	Kankaanrinne Joonas

VERSION HALLINTA		
versionro	mitä tehty	pvm/henkilö
v 1.0	Hyväksytty versio 1.0.	15.09.2016
v 1.1	Editoriaaliset muutokset	15.09.2016
v 1.2	EIDAS-luottamuspalvelut	01.12.2017
v 1.3	Editoriaaliset korjaukset, eIDAS auditointi	01.02.2018

VRK/DiPa 1.2.2018

Sisällysluettelo

1 Yleistä 5
2 Viiteluettelo 5
2.1 Ohjeelliset viitteet 5
2.2 Tietoa antavat viitteet 6
3 Määritelmät ja lyhenteet 6
3.1 Määritelmät 6
3.2 Lyhenteet 8
4 Yleiskäsitteet 9
4.1 Varmentaja 9
4.2 Varmennepalvelut 10
4.2.1 Rekisteröijä 10
4.2.2 Sulkupalvelu 11
4.2.3 Hakemistopalvelu 11
4.3 Varmennepolitiikka ja varmennuskäytäntö 11
4.3.1 Tarkoitus 11
4.3.2 Yksityiskohtaisuus 11
4.3.3 Lähestymistapa 12
4.3.4 Muut varmentajan julkaisemat asiakirjat 12
4.4 Tilaaja ja allekirjoittaja 12
5 Johdanto varmennepolitiikka-asiakirjoihin 12
5.1 Yleistä 12
5.2 Yksilöintitunnukset 13
5.3 Käyttäjäyhteisö ja sovellettavuus 14
5.4 Vaatimustenmukaisuus 14
5.4.1 Yleistä 14
5.4.2 Vaatimustenmukaisuuden vaatimukset 15
6 Velvollisuudet, vastuut ja vastuiden rajoitukset 15
6.1 Varmentajan velvollisuudet 15
6.2 Varmenteen tilaajaa ja haltijaa koskevat velvollisuudet 16
6.3 Varmenteeseen luottavaa osapuolta koskevat velvollisuudet 17
6.4 Vastuut ja vastuiden rajoitukset 18

7 . Varmentajan toimintaa koskevat vaatimukset 20
7.1 Varmennuskäytäntö 20
7.2 Julkisen avaimen järjestelmässä käytettävien avainten elinkaaren hallinta 21
7.2.1 Varmentajan avaimen luominen 21
7.2.2 Varmentajan avaimen tallennus, varmuuskopiointi ja palauttaminen 21
7.2.3 Varmentajan julkisen avaimen jakelu 22
7.2.4 Vara-avainjärjestelmä 22
7.2.5 Varmentajan avaimen käyttö 22
7.3 Julkisen avaimen järjestelmässä käytettävien varmenteiden elinkaaren hallinta 23
7.3.1 Allekirjoittajan rekisteröinti 23
7.3.2 Varmenteen uusiminen, sen avainparin vaihtaminen ja varmenteen päivittäminen 24
7.3.3 Varmenteiden luominen 25
7.3.4 Käyttöehtojen jakelu 26
7.3.5 Varmenteiden jakelu 27
7.3.6 Varmenteen sulkeminen ja asettaminen keskeytystilaan 27
7.4 Varmentajan johtamis- ja toimintakäytännöt 30
7.4.1 Turvallisuuden hallinta 30
7.4.2 Varantojen luokittelu ja hallinta 30
7.4.3 Henkilöstö ja tietoturva 30
7.4.4 Fyysinen ja ympäristön turvallisuus 32
7.4.5 Toiminnan hallinta 32
7.4.6 Järjestelmiin pääsyn hallinta 33
7.4.7 Luotettavien järjestelmien käyttöönotto ja ylläpito 33
7.4.8 Liiketoiminnan jatkuvuuden hallinta ja häiriötilanteiden käsittely 33
7.4.9 Varmentajan toiminnan lakkauttaminen 34
7.4.10 Sovellettava lainsäädäntö 34
7.5 Organisaatioon liittyvät vaatimukset 36
8 . Määrittelypuitteet muita varmennepolitiikka-asiakirjoja varten 37
8.1 Määritysasiakirjojen hallinta 37
8.2 Lisävaatimukset 38
8.3 Vaatimustenmukaisuus 38

VRK/DiPa 1.2.2018

VARMENNUSKÄYTÄNTÖ

1 Yleistä

Tässä asiakirjassa määritellään Väestörekisterikeskuksen - jatkossa varmentaja (Certification Authority) – julkisen avaimen menetelmän (Public Key Infrastructure; PKI) mukaisten varmentamistoimintojen edellytykset ja tämän asiakirjan soveltuvuusalue sekä rajaukset. Tämän asiakirjan sisältämät periaatteet määritellään käytännön tasolla tämän varmennuskäytännön lisäksi muissa tätä asiakirjaa täydentävissä menettelytapaohjeissa.

Tässä asiakirjassa noudatetaan ETSI TS 102 042 v 2.4.1:n (OVCP) linjauksia palveluvarmenteen osalta.

2 Viiteluettelo

2.1 Ohjeelliset viitteet

Varmentajan PKI:n perusteiden rakentamisessa on tukeuduttu seuraaviin säädöksiin, standardeihin ja ohjeisiin:

Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)

Laki viranomaisten toiminnan julkisuudesta (621/1999)

Laki turvallisuusselvityksistä (177/2002)

IETF RFC 3647 Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework (11/2003)

ETSI TS 102 042 V 2.4.1: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates (2013-02)

VAHTI 5/2004: Valtionhallinnon keskeisten tietojärjestelmien turvaaminen

ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management.

Dokumentin tulkinnassa käytetään seuraavia periaatteita:

1. Varmennepolitiikan otsikot ja alaotsikot ovat pääasiassa kansainvälisen standardoinnin [RFC 3647] suomennettuja suosituksia. Dokumenttia tulkittaessa itse teksti on etusijalla otsikoihin nähden.

2. Yleisenä ehtona varmentajalle on tämän varmennuskäytännön kaikkien varmentajaa koskevien vaatimusten täyttäminen.

2.2 Tietoa antavat viitteet

Seuraavassa mainittavat dokumentit eivät ole välttämättömiä tämän asiakirjan käytön kannalta, mutta niistä on käyttäjälle apua tietyillä aihealueilla. Ellei viite ole tarkka, sovelletaan dokumentin viimeisintä versiota (tarkistukset mukaan luettuina).

3 Määritelmät ja lyhenteet

3.1 Määritelmät

Attribuuttitieto: ammattihenkilön yksilöintiin ja ammattioikeuksien todentamiseen tarvittavat, pysyväisluonteiset tiedot.

Avainpari: Julkisen avaimen menetelmissä käytettävät, toisiinsa liittyvät avaimet, joista toinen on julkinen ja toinen yksityinen. Avainten käyttötarkoitus on määritelty varmenteessa. Kts. kappale 4.3

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

Hakemistopalvelu: Julkinen Internet-palvelu, josta on saatavilla kaikki varmentajan myöntämät varmenteet sekä varmentajan varmenteet sekä sulkulistat
Julkinen avain: Julkisen avaimen menetelmässä epäsymmetrisessä salauksessa käytettävän avainparin julkinen osa. Varmentaja varmentaa sähköisellä allekirjoituksellaan julkisen avaimen kuulumisen varmenteen haltijalle. Julkinen avain on osa varmenteen tietosisältöä.

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

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

Luottava osapuoli: Taho, joka luottaa varmenteen tietoihin ja käyttää varmennetta erilaisiin tietoturvapalveluihin, kuten varmenteen haltijan sähköiseen tunnistamiseen ja sähköisen allekirjoituksen todentamiseen. Kts. RFC 3647

Palvelinvarmenne: Palveluvarmenne, jolla tunnistetaan palvelin ja muodostetaan SSL-/TLS-salattu tietoliikenneyhteys palvelinten välille. Esimerkiksi www-palvelimen käyttöön tarkoitettu varmenne, jonka avulla käyttäjä voi varmistua palvelimen luotettavuudesta. Julkisen avaimen järjestelmää käyttävän palveluntuottajan julkisesta avaimesta ja tunnistetiedoista muodostettu tietokokonaisuus, jonka varmentaja on muodostanut ja allekirjoittanut yksityisellä avaimellaan.

Palvelinvarmenne asiointikäyttöön: Tiedostopohjainen varmenne, jota on tarkoitus käyttää esimerkiksi yhteisen sähköpostilaatikon sisältämien salattujen viestien vastaanottamiseen sekä

lähettämiseen. Tiedosto sisältää sekä varmenteet että niihin liittyvän yksityisen ja julkisen avaimen.

Palveluvarmenne: Yhteinen nimitys palvelin- ja sähköpostipalveluvarmenteille.

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

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

Suojattu käyttäjälaite: laite, joka säilyttää käyttäjän yksityisen avaimen, suojelee tätä avainta vaarantumiselta ja suorittaa allekirjoitus- tai salauksenpurkutoimintoja käyttäjän puolesta.

Sulkulista (CRL): Varmentajan sähköisesti allekirjoittama ja julkaisema luettelo kesken voimassaoloajan suljetuista varmenteista ja niiden sulkuajankohdista. Sulkulistasta ilmenee sen ja sitä seuraavan sulkulistan julkaisuajankohta. Suljetut varmenteet viedään sulkulistalle. Kts. ITU-T Suositus X.509.

Sulkupalvelu: Varmentajan palvelu, jossa Varmentaja ottaa vastaan varmenteiden sulkupyynnöt, sulkee varmenteet ja välittää tiedon varmenteen sulkemisesta varmennejärjestelmään.

Sähköinen allekirjoitus: sähköiseen viestiin liitetty PKI-allekirjoitus, jonka avulla voidaan luotettavasti todentaa viestin sisältö ja viestin allekirjoittajan henkilöllisyys.

Varmenne: Sähköinen todistus, joka liittää allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistaa allekirjoittajan. Varmenne sisältää siihen liittyvän varmennuskäytännön yksilöivän tunnuksen.

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

Varmennekuvaus: Asiakirja sisältää varmennepolitiikan ja varmennuskäytännön keskeiset kohdat.

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

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

Varmennuskäytännön yksilöivä tunnus on osa varmenteen tietosisältöä.

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

Varmentaja: Varmenteita myöntävä organisaatio, joka vastaa varmenteiden tuottamisesta sekä laatii toimintaansa kuvaavan varmennepolitiikan sekä varmennuskäytännön. Kts. kappale 4.1

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

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

Varmenteen hakija: Yksityinen tai julkinen organisaatio tai yksittäinen henkilö, joka hakee varmennetta ja joka tunnistetaan hakemisen yhteydessä luotettavasti.

Varmenteen haltija: Yksityinen tai julkinen organisaatio tai yksittäinen henkilö, jonka tiedot ja julkinen avain on varmennettu varmentajan sähköisellä allekirjoituksella, ja jonka hallussa varmenteeseen liittyvä yksityinen avain on.

Varmenteen käyttö ja käyttötarkoitus: Tässä dokumentissa varmenteen käyttö on nimitys sekä itse varmenteen että siihen liittyvien avainten käytölle. Esimerkiksi varmenteen käytöllä sähköisessä allekirjoituksessa tarkoitetaan sekä yksityisen avaimen käyttöä allekirjoituksessa että julkisen avaimen ja varmenteen käyttöä allekirjoituksen todentamisessa.

Yksityinen avain: Julkisen avaimen menetelmässä epäsymmetrisessä salauksessa käytettävän avainparin yksityinen osa. Varmenteen haltijan yksityinen avain talletetaan turvalliseen ympäristöön sen suojaamiseksi oikeudettomalta käytöltä.

3.2 Lyhenteet

CA Certification Authority, varmentaja

CP Certificate Policy, varmennepolitiikka

CPS Certification Practise Statement, varmennuskäytäntö

CRL Certificate Revocation List, sulkulista

CSP Certification Service Provider, varmentaja

FINEID Finnish Electronic Identification, suomalainen sähköinen tunnistusjärjestelmä

HSM Hardware Security Module, turvamoduuli

HTTP Hypertext Transfer Protocol

ISO 27001, ISO/IEC 27001

LDAP Lightweight Directory Access Protocol

OID Object Identifier, yksilöivä tunnus

OCSP-palvelu: Online Certificate Status Protocol. Palvelu, jolla voidaan tarkistaa varmenteen reaaliaikainen tilatieto.

PDS PKI Disclosure Statement, varmennekuvaus

PKI Public Key Infrastructure, julkisen avaimen järjestelmä

RSA Rivest, Shamir, Adleman, eräs julkisen avaimen algoritmi, epäsymmetrinen algoritmi

SSL Secure Socket Layer

TLS Transport Layer Security

VRK Väestörekisterikeskus

4 Yleiskäsitteet

4.1 Varmentaja

Varmentajaksi kutsutaan varmenteita myöntävää ja luovaa tahoa, jonka toimintaan varmennepalvelujen käyttäjät (eli tilaajat ja varmenteeseen luottavat osapuolet) luottavat. Varmentaja on kokonaisvastuussa kohdassa 4.2 määriteltyjen varmennepalvelujen tarjoamisesta. Varmentaja on yksilöity varmenteessa varmenteen myöntäjäksi, ja laatuvarmenteet allekirjoitetaan sen yksityisellä avaimella.

Varmentaja voi käyttää varmennepalvelussaan muita osapuolia, jotka tarjoavat palvelun osia. Varmentaja säilyy kuitenkin aina kokonaisvastuussa ja varmistaa, että tässä asiakirjassa määritellyt menettelytapavaatimukset täyttyvät. Varmentaja voi esimerkiksi hankkia alihankintana kaikki osapalvelut, myös varmenteiden luomispalvelun. Varmenteiden allekirjoittamiseen käytettävä avain kuitenkin määritellään kuitenkin varmentajalle kuuluvaksi, ja varmentajalla säilyy kokonaisvastuu tässä asiakirjassa määriteltyjen vaatimusten täyttämisestä.

Varmentaja myöntää varmenteita ja täyttää seuraavat ehdot:

- Varmentaja sitoutuu noudattamaan varmennepolitiikan ehtoja.
- Varmentaja laatii varmennuskäytännön ja muita varmennepolitiikkaa täydentäviä menettelytapaohjeita.
- Varmentaja pitää yllä riittävät taloudelliset valmiudet turvatakseen varmennepolitiikassa ja varmennuskäytännössä määritellyn toiminnan. Varmentaja vastaa varmennetoiminnasta ja siihen liittyvistä riskeistä ja edellyttää varmennejärjestelmän toimittajien suojautuvan toimintaan liittyviltä riskeiltä asianmukaisin riskienhallintakeinoin.
- Varmentaja pitää yllä rekisteriä hyväksymistään rekisteröijistä.
- Varmentaja päättää ristiinvarmentamisesta yhteistyössä toisten varmentajien kanssa.

- Varmentaja vastaa luomiensa avainparien elinkaaresta (luominen, tallennus, varmuuskopiointi, julkaiseminen ja käytöstä poistaminen) sekä sulkulistojen julkaisemisesta

Varmentaja sitoutuu:

1. tarjoamaan varmenne-, hakemisto- ja sulkupalveluja, jotka on määritelty varmennepolitiikassa;
2. tarjoamaan tämän varmennekäytännön luvuissa 4-6 kuvatut hallinta- ja seurantatoiminnot;
3. tunnistamaan luotettavasti varmenteen hakijan;
4. myöntämään varmenteita yhdenmukaisesti tämän varmennuskäytännöne kanssa;
5. noudattamaan voimassaolevia lakeja, asetuksia ja niiden nojalla annettuja määräyksiä ja ohjeita sekä tukemaan varmenteiden käyttäjien ja varmenteisiin luottavien osapuolten oikeuksia;
6. huolehtimaan siitä, että riittävät ja varmennuskäytännön mukaiset riippumattomat tarkastukset tulevat suoritetuiksi;
7. vastaamaan varmentajan toimivuudesta; ja
8. noudattamaan kaikkia varmennepolitiikan sekä tämän varmennuskäytännön ehtoja.

Varmentaja voi halutessaan tarjota varmennejärjestelmään liittyviä lisätoimintoja tai -palveluja.

Varmentaja vastaa, että varmenteen sisältämä informaatio on tämän varmennuskäytännön mukainen.

4.2 Varmennepalvelut

4.2.1 Rekisteröijä

Varmennepolitiikan mukaisesti toimivan rekisteröijän on täytettävä seuraavat ehdot:

- Rekisteröijä sitoutuu noudattamaan tämän varmennuskäytännön vaatimuksia.
- Rekisteröijän on oltava varmentajan hyväksymä ja rekisteröimä.
- Rekisteröijä vastaa varmenteiden hakijoiden tunnistamisesta.
- Rekisteröijä vastaa rekisteröintipisteen henkilökunnan luotettavuudesta. Rekisteröijä hankkii palvelukseen otettavan henkilön luotettavuudesta varmentajan edellyttämät selvitykset sekä huolehtii valtuuttamansa henkilökunnan jatkuvasta luotettavuudesta. Varmentaja hyväksyy rekisteröintipisteen henkilökunnan rekisteröijän toimittamien selvitysten perusteella.

Varmennepolitiikan mukaisen rekisteröijän tulee sitoutua:

1. noudattamaan voimassa olevaa lainsäädäntöä ja sen nojalla annettuja määräyksiä ja ohjeita;
2. tarjoamaan tämän varmennuskäytännön luvuissa 4-6 vaaditut hallinta- ja seurantatoiminnot;
3. suorittamaan varmenteen hakijan tunnistamismenettelyn tämän varmennuskäytännön lukujen 4-6 ja varmennepolitiikan mukaisesti sekä toimittamaan hakijan tiedot varmentajalle varmenteen luontia varten;
4. täyttämään sovitut toimeksiannot ja tukemaan varmenteiden käyttäjien ja varmenteisiin luottavien osapuolten oikeuksia; ja
5. noudattamaan kaikkia varmennepolitiikan sekä tämän varmennuskäytännön rekisteröintipalveluun liittyviä ehtoja.

Rekisteröijä voi tarjota varmentajan hyväksymiä lisätoimintoja tai -palveluja. Rekisteröijä kantaa vastuun kaikista antamistaan rekisteröintipalveluista. Palveluvarmenteen rekisteröijänä toimii Väestörekisterikeskus.

4.2.2 Sulkupalvelu

Varmenteiden sulkupalvelu sulkee palveluvarmenteet, jotka varmenteen haltija tai varmentaja haluaa suljettavaksi ennen varmenteen voimassaoloajan päättymistä. Suljetut palveluvarmenteet toimitetaan sulkulistalle. Syy palveluvarmenteiden sulkemiseen voi olla esimerkiksi varmenteen haltijan yksityisen avaimen paljastuminen tai epäily sen paljastumisesta.

4.2.3 Hakemistopalvelu

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

4.3 Varmennepolitiikka ja varmennuskäytäntö

4.3.1 Tarkoitus

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

4.3.2 Yksityiskohtaisuus

Varmennuskäytännössä kuvataan varmennepolitiikkaa tarkemmin käytäntöjä, joita varmentaja toteuttaa varmenteiden myöntämisessä ja muussa hallinnoinnissa. Siinä määritellään, kuinka

tietty varmentaja täyttää varmennepolitiikassa määritetyt tekniset sekä organisaatioon ja menettelyihin liittyvät vaatimukset.

4.3.3 Lähestymistapa

Varmennepolitiikka ja varmennuskäytäntö ovat lähestymistavoiltaan hyvin erilaisia. Varmennepolitiikka on määritelty tietyn varmentajan toimintaympäristön yksityiskohdista riippumatta. Varmennuskäytäntö sen sijaan laaditaan nimenomaan varmentajan organisaatiorakenteen, toimintatapojen, toimitilojen ja tietoteknisen ympäristön mukaisesti. Varmennepolitiikan määrittelijänä voi olla varmennepalvelujen käyttäjä, mutta varmennuskäytännön määrittelee aina varmenteiden tarjoaja.

4.3.4 Muut varmentajan julkaisemat asiakirjat

Varmennepolitiikan ja varmennuskäytännön lisäksi varmentaja voi julkaista muita varmentajan toimintaa koskevia asiakirjoja. Tällaiset käyttöehdot voivat sisältää monenlaisia kaupallisia ehtoja tai liittyä muun muassa tiettyyn julkisen avaimen järjestelmään. Vaikka tällaisista ehdoista ei välttämättä ilmoiteta asiakkaalle, niitä saatetaan silti soveltaa asiassa.

Varmennekuvaus on varmentajan käyttöehtojen osa, joka liittyy julkisen avaimen järjestelmän toimintaan. Varmentajan olisi syytä asettaa varmennekuvaus sekä tilaajien että varmenteeseen luottavien osapuolien saataville.

4.4 Tilaaja ja allekirjoittaja

"Tilaajalla" tarkoitetaan varmentajalta varmenteita hakevaa, varmentajaan sopimussuhteessa olevaa tahoa (yksityinen tai julkinen organisaatio tai yksityinen henkilö). "Allekirjoittajalla" tarkoitetaan tahoa, jolle varmenne on myönnetty (yksityinen tai julkinen organisaatio tai yksityinen henkilö). Tilaaja on vastuussa julkiseen avaimeen perustuvaan varmenteeseen liittyvän yksityisen avaimen käytöstä. Allekirjoittaja taas on henkilö, joka voidaan todentaa yksityisellä avaimella ja joka hallitsee yksityisen avaimen käyttöä.

Kun varmenteita myönnetään yksilöille heidän omaan käyttöönsä, sama taho voi olla sekä tilaaja että allekirjoittaja. Muissa tapauksissa, kuten silloin kun varmenteita myönnetään työntekijöitä varten, tilaaja ja allekirjoittaja ovat eri tahoja. Esimerkiksi työnantaja voi olla tilaaja ja työntekijä allekirjoittaja.

Tässä asiakirjassa käytetään näitä kahta käsitettä tämän eron ilmentämiseksi, silloin kun se on tarpeen. Kaikissa tapauksissa kyseinen ero ei kuitenkaan ole aivan selvä.

5 Johdanto varmennepolitiikka-asiakirjoihin

5.1 Yleistä

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

Varmennuskäytäntöä sovelletaan Väestörekisterikeskuksen palveluvarmenteeseen. Palvelinvarmenne on Väestörekisterikeskuksen myöntämä varmenne, jolla varmennetaan palveluntarjoajan - yksityisen tai julkisen organisaation tai yksittäisen henkilön - palvelin tai palvelu.

Varmenne on joukko tietoa, joka liittää todentamisen tai tiedon salaamisen yhteydessä todentamistiedot varmenteen haltijaan ja vahvistaa palveluvarmenteen haltijan. Varmenteen tiedot on sähköisesti allekirjoitettu varmentajan yksityisellä avaimella. Tämän varmennuskäytännön mukainen varmenne perustuu julkisen avaimen menetelmään (PKI). Palvelinvarmenne asiointikäyttöön on tiedostopohjainen, sähköpostin salaukseen ja allekirjoittamiseen tarkoitettu, PKCS #12 –tiedostomuodossa toimitettava varmenne.

Palvelinvarmenteita voidaan käyttää sekä julkishallinnon että yksityissektorin palveluiden tunnistamisessa. Palvelinvarmenteen avulla palvelun käyttäjä voi varmistua palvelun tarjoajan oikeellisuudesta.

Väestörekisterikeskuksen varmennuskäytännöllä on oma yksilöivä tunnuksensa (OID).

Varmentajan toimintoja ovat varmenne-, hakemisto- ja sulkupalveluiden tuottaminen sekä rekisteröinti. Nämä toiminnot on kuvattu tarkemmin luvussa 4.2

5.2 Yksilöintitunnukset

Varmenteessa on kaksi yksilöivää tunnistetta (OID). Toinen tunniste kertoo, mitä ETSI TS 102 042:n varmennepolitiikkaa noudatetaan varmenteessa ja toinen varmennuskäytännön yksilöivän tunnisteen.

Lisäksi varmennepolitiikalla on oma VRK:n yksilöivä tunniste, joka määrittelee varmennepolitiikan.

Yksilöivät tunnisteet ovat:

Noudatettavan ETSI TS 102 042 politiikan OID (OVCP): 0.4.0.2042.1.7 [itu-t(0), identified-organization(4), etsi(0), other-certificate-policies(2042), policy-identifiers(1), ovcp (7)]

Väestörekisterikeskuksen sosiaali- ja terveydenhuollon palvelinvarmenne asiointikäyttöä varten, varmennuskäytännön OID:1.2.246.517.1.10.10.2.

VRK:n sosiaali- ja terveydenhuollon palveluvarmenteet, varmennepolitiikan OID: 1.2.246.517.1.10.10.

Varmennepolitiikka, sen varmennekuvaus ja varmennuskäytännöt ovat saatavilla osoitteesta http://www.fineid.fi/.

VRK/DiPa 1.2.2018

5.3 Käyttäjäyhteisö ja sovellettavuus

Tämän varmennuskäytännön mukaisen palvelinvarmenteen asiointikäyttöön käyttötarkoituksia ovat: sähköpostin allekirjoitus ja salaus, salatun sähköpostin vastaanottaminen (email Protection). Varmennetta voidaan käyttää käyttötarkoituksensa mukaisesti rajoituksitta hallinnollisissa sekä yksityisen organisaation tai henkilön tarjoamissa sovelluksissa ja palveluissa.

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

5.4 Vaatimustenmukaisuus

5.4.1 Yleistä

Varmentaja tuottaa varmennepalvelut varmennuskäytännössä mainituin ehdoin ja vastaa niiden toimivuudesta varmenteen haltijalle. Varmentaja vastaa koko varmennejärjestelmän toimivuudesta, myös käyttämiensä rekisteröijien ja teknisten toimittajien osalta. Tämän varmennuskäytännön on rekisteröinyt Väestörekisterikeskus. Varmennepolitiikka-asiakirjat julkaistaan www.fineid.fi -sivuilla, josta ne ovat kaikkien saatavilla. Varmentajan toimintaa auditoidaan vuosittain ja silloin, kun järjestelmään on tehty merkittäviä muutoksia. Varmenneauditointiraportin voi saada pyydettäessä.

Tietoturvatarkastus

Väestörekisterikeskus tekee tietoturvatarkastuksen teknisten toimittajiensa toimitiloihin, laitteisiin ja toimintaan tarkoituksenmukaisella tavalla.

Väestörekisterikeskuksen tietoturvatarkastuksen tekee ulkopuolinen tarkastaja, joka on varmentajasta riippumaton taho.

Tarkastuksen kohteet määräytyvät Väestörekisterikeskuksen suorittaessa tarkastusta tietoturvastandardin ISO 27001, Väestörekisterikeskuksen tietoturvapolitiikan tai teknisten toimitussopimusten mukaisesti. Tarkastettavia tietoturvallisuuden ominaisuuksia ovat mm. luottamuksellisuus, eheys ja käytettävyys.

Tarkastuksessa verrataan varmennepolitiikkaa, varmennuskäytäntöä, soveltamisohjeita ja niiden yhteensopivuutta ETSI TS 102 042 -standardiin koko varmenneorganisaation ja -järjestelmän osalta.

Poikkeamista johtuvat toimenpiteet

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

Tarkastuksen tuloksesta tiedottaminen

Tarkastuksen tuloksesta tiedotetaan lain, tietoturvastandardin ISO 27001, Väestörekisterikeskuksen 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.

Tarkastusaineiston arkistointi

Varmentaja arkistoi tarkastusraportit ja pöytäkirjat käsittäen tietoturvatarkastukset ja järjestelmän auditoinnin. Arkistotiedot säilytetään varmentajana toimivaa viranomaista koskevien säännösten mukaisesti.

Varmentajan toimintaa koskevat suunnitelmat ja politiikat sekä varmentajaa koskevat velvollisuudet poikkeus- ja häiriötilanteissa kuvataan kohdassa 7.4.8. Toiminnan jatkumisen hallinta ja poikkeustapausten käsittely

5.4.2 Vaatimustenmukaisuuden vaatimukset

Varmentajan velvollisuudet on kuvattu kohdassa 6.1. Varmentajan toiminta täyttää kohdan 6.1. mukaiset vaatimukset. Lisäksi varmentajan toiminta ja toiminnan valvonta täyttävät kohdassa 7 yksilöidyt vaatimukset.

6 Velvollisuudet, vastuut ja vastuiden rajoitukset

6.1 Varmentajan velvollisuudet

Varmentaja vastaa koko varmennejärjestelmän toimivuudesta, myös käyttämiensä rekisteröijien ja teknisten toimittajien osalta.

- Väestörekisterikeskuksella on lakisääteinen tehtävä toimia varmentajana.
- Varmentaja noudattaa toiminnassaan voimassaolevaa lainsäädäntöä.
- Varmentaja toimii huolellisesti, luotettavasti ja asianmukaisesti.
- Varmentajalla on riittävät tekniset taidot ja taloudelliset voimavarat varmennetoiminnan asianmukaiseksi järjestämiseksi sekä mahdollisen vahingonkorvausvastuun kattamiseksi.
- Varmentaja vastaa kaikista varmennetoiminnan osa-alueista, myös varmentajan apunaan käyttämien teknisten toimittajien ja henkilöiden tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta.
- Varmentaja laatii ja ylläpitää varmennepolitiikkaa, joka kuvaa palveluvarmenteen myöntämisessä, ylläpidossa ja hallinnoinnissa käytettävät menettelytavat, käyttöehdot, vastuiden jaon ja muut palveluvarmenteen käyttöön liittyvät näkökulmat yleisellä tasolla.

- Varmentaja laatii ja ylläpitää varmennuskäytäntöjä, jotka kuvaavat, miten varmentaja soveltaa varmennepolitiikkaa.
- Varmentaja noudattaa varmennepolitiikan ja varmennuskäytännön vaatimuksia.
- Varmentaja julkaisee varmennepolitiikan ja varmennuskäytännön yleisesti saataville.
- Varmentaja pitää palveluksessaan riittävästi henkilökuntaa, jolla on varmennepalvelujen tuottamisen edellyttämä asiantuntemus, kokemus ja pätevyys.
- Varmentaja käyttää luotettavia järjestelmiä ja tuotteita, jotka on suojattu oikeudetto-malta käytöltä.
- Varmentaja pitää yleisesti saatavilla varmenteita ja varmennetoimintaa koskevat tiedot, joiden perusteella varmentajan toiminta ja luotettavuus voidaan arvioida.

Rekisteröijää koskevat velvollisuudet

Palveluvarmenteen rekisteröijänä toimii Väestörekisterikeskus.

- Rekisteröijä noudattaa rekisteröinnin yhteydessä varmennepolitiikkaa ja varmennuskäy-täntöä.
- Rekisteröijä tunnistaa palveluvarmenteen hakijan luotettavasti varmennuskäytännössä kuvatulla tavalla siten, että hakijan henkilöllisyys, oikeus hakea palveluvarmennetta sekä muut palveluvarmenteen myöntämisessä tarpeelliset hakijaan liittyvät tiedot tulevat huolellisesti tarkastetuiksi.
- Rekisteröijä huolehtii tietojen huolellisesta käsittelystä ja luottamuksellisuudesta.
- Rekisteröijä noudattaa varmentajan kanssa sovittuja rekisteröintiin liittyviä menettely-tapoja.

6.2 Varmenteen tilaajaa ja haltijaa koskevat velvollisuudet

- Palveluvarmenteen haltija on vastuussa siitä, että varmennetta käytetään palveluvar-mennehakemuksessa ilmoitettujen käyttötarkoitusten, varmennepolitiikan, varmennus-käytännön sekä varmenteen haltijaa sitovien sopimusehtojen mukaisesti.
- Väestörekisterikeskus voi myöntää palveluvarmenteen myös omiin tarkoituksiinsa. Täl-löin se noudattaa samoja vaatimuksia kuin muut organisaatiot.
- Varmenteen haltija (palveluntarjoaja) vastaa siitä, että varmennetta haettaessa ilmoite-tut tiedot ovat oikeita.
- Varmenteen haltijan on säilytettävä yksityinen avaimensa turvallisessa ympäristössä ja pyrittävä estämään sen katoaminen, joutuminen ulkopuolisten käsiin, muuttaminen tai luvaton käyttö.

- Varmenteen haltijan on ilmoitettava varmentajalle välittömästi, jos on tiedossa tai epäilys, että varmenteen haltijan yksityinen avain on paljastunut tai varmenteen tietosisältö on virheellinen. Tällöin varmentaja sulkee kyseessä olevan varmenteen eikä samaa yksityistä avainta voida enää käyttää uuden varmenteen tekemiseen.

- Palveluvarmenteen haltijan vastuu varmenteen käyttämisestä päättyy, kun hän on ilmoittanut Varmentajalle tarvittavat tiedot varmenteen sulkemiseksi ja saatuaan puhelun vastaanottaneelta henkilöltä sulkemista koskevan ilmoituksen. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

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

Mikäli Väestörekisterikeskuksen varmenteiden luonnissa käyttämä yksityinen avain tai muu tekninen menetelmä on paljastunut tai tullut muutoin käyttökelvottomaksi, Väestörekisterikeskuksen on ilmoitettava tapahtuneesta kaikille varmenteen haltijoille ja Viestintävirastolle asianmukaisella tavalla.

Palveluvarmenteen hakija toimittaa rekisteröijälle varmennettavalla palvelimellaan luomansa varmennepyynnön, jonka perusteella palveluvarmenne luodaan.

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

Palveluvarmenteen yksityisen ja julkisen avaimen pituus on varmenteen hakijan päätettävissä. Väestörekisterikeskuksen myöntämän palveluvarmenteen avainpituus on vähintään 2048 bittiä.

6.3 Varmenteeseen luottavaa osapuolta koskevat velvollisuudet

Palveluvarmenteeseen luottavan osapuolen velvollisuus on varmistaa, että varmennetta käytetään käyttötarkoituksensa mukaisesti.

Palveluvarmenteeseen luottavan osapuolen on noudatettava varmennepolitiikkaa ja varmennuskäytäntöä.

Palveluvarmenteeseen luottava osapuoli voi vilpittömässä mielessä luottaa palveluvarmenteeseen, kun hän on tarkistanut, että varmenne on voimassa ja että se ei ole sulkulistalla. Palveluvarmenteeseen luottavalla osapuolella on velvollisuus tarkistaa varmenne sulkulistalta. Palveluvarmenteen voimassaolon luotettavuuden varmistamiseksi palveluvarmenteeseen luottavan osapuolen on noudatettava alla esitettyjä sulkulistan tarkistustoimia.

Jos palveluvarmenteeseen 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 varmenteiden hyväksymiset tämän voimassaoloajan jälkeen tapahtuvat palveluvarmenteeseen luottavan osapuolen omalla riskillä.

6.4 Vastuut ja vastuiden rajoitukset

Varmentajan vastuut

Väestörekisterikeskus noudattaa varmennepalvelutoiminnassaan voimassaolevaa Suomen lainsäädäntöä.

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

Väestörekisterikeskus vastaa siitä, että palveluvarmenteet on luotu noudattaen varmennepolitiikassa sekä varmennuskäytännössä esitettyjä menettelyjä ja varmenteen hakijan antamien tietojen mukaisesti. Väestörekisterikeskus vastaa ainoastaan niistä tiedoista, jotka se on tallettanut palveluvarmenteeseen.

Varmennepalveluiden tuottamiseen liittyvä Väestörekisterikeskuksen vahingonkorvausvastuu määräytyy voimassa olevien yhteistyösopimusten ja vahingonkorvauslain (412/1974) mukaisesti.

Väestörekisterikeskus vastaa siitä, että palveluvarmenne on käytettävissä luovutushetkestä alkaen koko sen voimassaoloajan, ellei varmennetta ole asetettu sulkulistalle.

Väestörekisterikeskus vastaa siitä, että palveluvarmenne on luovutettu hakijalle, joka on tunnistettu palveluvarmenteelta edellytettävällä tavalla.

Allekirjoittaessaan palveluvarmenteen yksityisellä avaimellaan varmentaja vakuuttaa tarkistaneensa varmenteessa olevat tiedot palveluvarmennepolitiikassa ja varmennuskäytännössä esitettyjen menettelyjen mukaisesti.

Varmentaja vastaa siitä, että sulkulistalle viedään oikea palveluvarmenne ja että se ilmestyy varmennuskäytännössä mainitussa ajassa sulkulistalle.

Rekisteröijän vastuut

Palveluvarmenteen rekisteröijänä toimii Väestörekisterikeskus tai sen sopimuskumppani Väestörekisterikeskuksen vastuulla ja lukuun.

Varmenteen haltijan vastuut

Palveluvarmenteen haltija on vastuussa siitä, että varmennetta käytetään palveluvarmennehakemuksessa ilmoitettujen käyttötarkoitusten mukaisesti.

VRK/DiPa 1.2.2018

Palveluvarmenteen haltijan vastuu varmenteen käyttämisestä päättyy, kun hän on ilmoittanut Varmentajalle tarvittavat tiedot varmenteen sulkemiseksi ja saatuaan puhelun vastaanottaneelta henkilöltä sulkemista koskevan ilmoituksen. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

Varmenteeseen luottavan osapuolen vastuut

Palveluvarmenteeseen luottava osapuoli ei voi luottaa varmenteen oikeellisuuteen vilpittömässä mielessä, mikäli varmenteen voimassaoloa ei ole tarkastettu sulkulistalta. Palveluvarmenteen hyväksyminen mainitussa tapauksessa vapauttaa Väestörekisterikeskuksen vastuusta. Palveluvarmenteeseen luottavan osapuolen on tarkistettava, että myönnetty varmenne vastaa käyttötarkoitustaan siinä toiminnossa, jossa sitä on käytetty.

Vastuiden rajoitukset

Väestörekisterikeskus ei vastaa varmenteen haltijan yksityisen avaimen paljastumisen seurauksena syntyvistä vahingoista ja kustannuksista, ellei paljastuminen välittömästi johdu Väestörekisterikeskuksen toiminnasta.

Väestörekisterikeskus vastaa varmenteen haltijalle ja varmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Väestörekisterikeskuksen välittömästä toiminnasta, kuitenkin enintään 15 % edeltävän 3 kuukauden varmennelaskutuksen määrästä (VRK:lle tuloutettava osuus).

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

Väestörekisterikeskus ei vastaa yleisten tietoliikenneyhteyksien eikä tietoverkkojen, esimerkiksi Internetin, toimivuudesta eikä siitä, jos toiminnon suorittaminen estyy palveluvarmenteen haltijan käyttämän laitteen tai ohjelmiston toimimattomuudesta eikä siitä, että palveluvarmennetta käytetään vastoin sen käyttötarkoitusta.

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

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

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

Varmenteen haltijan vastuu varmenteen käyttämisestä päättyy, kun hän tai varmenteen haltijan organisaation edustaja on ilmoittanut varmentajalle tarvittavat tiedot varmenteen sulkemiseksi ja saatuaan puhelun vastaanottaneelta henkilöltä sulkemista koskevan ilmoituksen. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

7 . Varmentajan toimintaa koskevat vaatimukset

Varmentajan on toteutettava seuraavat vaatimukset täyttävät hallintakeinot.

Näihin sisältyvät rekisteröintipalvelujen tarjoaminen, varmenteiden luominen, varmenteiden jakelu, varmenteiden sulkeminen ja sulkutilasta tiedottaminen (katso kohta 4.2). Jos vaatimus liittyy varmentajan tiettyyn palvelualueeseen, se esitetään vastaavien alaotsikoiden alla. Mikäli seuraavassa ei yksilöidä yhtään palvelualuetta tai jos mainitaan "varmentaja yleisesti", vaatimus koskee varmentajan yleistä toimintaa.

Näiden menettelytapavaatimusten tarkoituksena ei ole rajoittaa varmentajan palveluista veloittamista.

Esitettävät vaatimukset koskevat turvallisuustavoitteita sekä niiden saavuttamiseen käytettäviä hallintakeinoja, joiden osalta esitetään yksityiskohtaisia vaatimuksia, mikäli se on katsottu tavoitteiden täyttymisen kannalta tarpeelliseksi

7.1 Varmennuskäytäntö

Varmentaja laatii varmennuskäytännön ja muita varmennepolitiikkaa täydentäviä menettelytapaohjeita. Varmentaja vastaa siitä, että varmennepolitiikat, varmennuskäytännöt ja varmennekuvaukset ovat julkisesti saatavilla osoitteesta www.fineid.fi.

Palveluvarmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa ja yleisissä käyttöehdoissa, jotka muodostavat varmenteen hakijan kanssa tehtävän sopimuksen.

Hakemusasiakirjassa ja käyttöehdoissa mainitaan selkeästi, että palveluvarmenteen hakija hyväksyy nimikirjoituksellaan annettujen tietojen oikeellisuuden sekä palveluvarmenteen luomisen ja julkaisun julkisessa hakemistossa. Samalla hakija hyväksyy palveluvarmenteen käyttöön liittyvät säännöt ja ehdot sekä mahdollisen väärinkäytön tai yksityisen avaimen paljastumisen ilmoittamisesta.

Varmentaja määrittelee ja hyväksyy varmennuskäytäntöasiakirjat.

Varmentaja vastaa, että sen varmennetoiminta ja varmennuskäytäntö noudattavat tätä varmennepolitiikkaa.

Varmentajan toiminta tarkastetaan vähintään kerran vuodessa. Tarkastuksessa verrataan varmennepolitiikkaa ja varmennuskäytäntöä varmentajan koko toimintaan. Varmentaja ryhtyy viivytyksettä havaittujen poikkeamien vaatimiin toimenpiteisiin tilanteen korjaamiseksi.

Varmennetoiminnassa ja varmenteissa käytetyt algoritmit ja muut tekniset yksityiskohdat on kuvattu luvussa 7.2.

7.2 Julkisen avaimen järjestelmässä käytettävien avainten elinkaaren hallinta

7.2.1 Varmentajan avaimen luominen

Varmentaja luo yksityiset allekirjoitusavaimensa ja yksityisiä allekirjoitusavaimiaan vastaavat julkiset avaimensa. Varmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa, jotka täyttävät tarvittavan turvallisuusstandardin vaatimukset.

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

Avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa. Ne täyttävät turvatasoltaan FIPS 140-1 tason 3 vaatimukset.

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

Palveluvarmenteen yksityisen ja julkisen avaimen pituus on varmenteen hakijan päätettävissä. Väestörekisterikeskuksen myöntämän palveluvarmenteen avainpituus on vähintään 2048 bittiä.

Varmentaja luo uuden avainparin ja varmentajan varmenteen viimeistään viisi vuotta ja kolme kuukautta ennen edellisen varmentajan varmenteen voimassaoloajan päättymistä. Varmentajan varmenne toimitetaan julkiseen hakemistoon luvun 7.3.5 mukaisesti.

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

7.2.2 Varmentajan avaimen tallennus, varmuuskopiointi ja palauttaminen

Varmentajan yksityiset avaimet on suojattu paljastumiselta ja luvattomalta käytöltä.

Avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa. Ne täyttävät turvatasoltaan FIPS 140-1 tason 3 vaatimukset.

Varmentajan yksityisestä avaimesta on varmuuskopio.

Varmentajan varmuuskopioidun yksityisen avaimen turvallisuusominaisuudet ja säilytys vastaavat varmentajan alkuperäisen yksityisen avaimen turvallisuusvaatimuksia kaikissa tilanteissa.

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

7.2.3 Varmentajan julkisen avaimen jakelu

Varmentajan julkisen avaimen sisältävän varmentajan varmenteen voi hakea julkisesta hakemistosta tai varmentajan ylläpitämästä palvelusta. Varmentaja julkaisee julkisen avaimensa yleisesti saatavilla olevassa julkisessa hakemistossa ldap://ldap.fineid.fi ja www-sivuillaan http://www.fineid.fi.

7.2.4 Vara-avainjärjestelmä

Allekirjoittajan yksityisiä allekirjoitusavaimia ei säilytetä salauksen purkamisen ja varmuuskopioinnin mahdollistavalla tavalla, jolloin valtuutetut tahot voisivat tietyissä tilanteissa purkaa salauksen hyödyntämällä yhden tai useamman osapuolen antamia tietoja

7.2.5 Varmentajan avaimen käyttö

Varmenteen tietosisällössä käyttötarkoituksen määräävä kenttä määrittelee varmenteisiin liittyvän avaimen käyttötarkoituksen.

Varmentajan varmenteella allekirjoitetaan ainoastaan palveluvarmenteita ja niihin liittyviä sulkulistoja. Tekninen kuvaus on FINEID S 2-määrityksessä.

Varmentajan varmenteen voimassaolon päätyttyä turvamodulissa olevat varmentajan yksityiset avaimet tuhotaan, eikä niitä käytetä uudelleen.

Varmentajan yksityiset avaimet säilytetään turvamoduuleissa salattuna.

Varmentajan yksityisten avainten aktivointi tapahtuu tehtävään oikeutettujen henkilöiden toimesta turvamoduuleissa hallintakorttien avulla. Varmentajan yksityisten avainten käyttö estetään tehtävään oikeutettujen henkilöiden toimesta hallintakorttien avulla tai kytkemällä varmentajan yksityiset avaimet sisältävästä turvamoduulista virta pois.

Varmentajalla on oikeus siirtää varmentajan yksityiset avaimet toiseen turvamoduuliin alkuperäisen laitteiston huoltoa tai vaihtamista varten.

Varmentajan yksityiset avaimet tuhotaan niiden voimassaoloajan päättymisen jälkeen. Vain varmentaja voi tuhota varmentajan yksityiset avaimet. Varmentajan lakkautuksen yhteydessä varmentajan yksityiset avaimet sekä niiden kopiot tuhotaan.

Varmentaja luo tarvittaessa varmenteen haltijan avainparin. Tällöin varmenne sekä siihen liittyvä avainpari ja salasana toimitetaan varmenteen haltijalle siten, ettei ulkopuolisten ole mahdollista saada niitä haltuunsa.

Avainparien turvallinen luomis- ja tallentamisprosessi estää avaimen paljastumisen avaimen luomiseen käytettävän järjestelmän ulkopuolelle.

VRK/DiPa 1.2.2018

7.3 Julkisen avaimen järjestelmässä käytettävien varmenteiden elinkaaren hallinta

7.3.1 Allekirjoittajan rekisteröinti

Varmentajan on varmistettava, että allekirjoittajat tunnistetaan ja todennetaan asianmukaisesti ja että allekirjoittajan varmennepyynnöt ovat täydellisiä, paikkansapitäviä ja asianmukaisesti valtuutettuja.

Palveluvarmenteen haltijan nimeämisessä käytetään varmenteen hakijan ilmoittamia ja rekisteröijän tarkistamia hakijan virallisia nimi- ja muita tietoja.

Attribuuttien joukko, josta muodostuu varmenteeseen kohteen nimitietue, on ainutkertainen ja yksilöi asianomaisen varmenteen haltijan. Kaikkien palveluvarmenteiden haltijaorganisaatioiden on toimittava omilla nimillään.

Varmenteen haltijan yksityiset avaimet luodaan varmenteen haltijan tai tämän teknisen toimittajan palvelimessa, kun kyseessä on palvelin- tai järjestelmäallekirjoitusvarmenne. Kun kyseessä on sähköpostipalveluvarmenne, varmentaja luo avainparin sekä varmenteen ja toimittaa ne varmenteen haltijalle.

Varmenteen hakijan edustaman organisaation todentaminen

Palveluvarmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa ja yleisissä käyttöehdoissa, jotka muodostavat varmenteen hakijan kanssa tehtävän sopimuksen.

Hakemusasiakirjassa ja käyttöehdoissa mainitaan selkeästi, että palveluvarmenteen hakija hyväksyy nimikirjoituksellaan annettujen tietojen oikeellisuuden sekä palveluvarmenteen luomisen ja mahdollisen julkaisun julkisessa hakemistossa. Samalla hakija hyväksyy palveluvarmenteen käyttöön liittyvät säännöt ja ehdot sekä mahdollisen väärinkäytön tai yksityisen avaimen paljastumisen ilmoittamisesta.

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

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

Kun varmentaja myöntää palveluvarmenteen, se samalla hyväksyy varmennehakemuksen.

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

Palveluvarmennetta haetaan lomakkeella, joka voidaan ladata ja tulostaa verkkosivuilta http://www.fineid.fi

Ennen varmenteen myöntämistä varmentaja tarkistaa hakijan tiedot mm. kaupparekisteristä. Jos hakija on yritys tai organisaatio, palveluvarmennehakemuksen liitteenä toimitetaan enintään kolme kuukautta vanha kaupparekisteriote silloin, kun palveluvarmennetta haetaan ensimmäistä kertaa. Lisäksi toimitetaan valtakirja, mikäli varmenteen hakija (atk-yhdyshenkilö tms.) toimii yrityksen / organisaation puolesta. Kaupparekisteriotetta ei toimiteta uudelleen varmenteen uusimisen yhteydessä, vaan Väestörekisterikeskus tarkistaa yrityksen tiedot Yritys- ja yhteisötietojärjestelmästä (YTJ). Kaupparekisteriotetta ei vaadita valtion, kuntien ja seurakuntien viranomaisilta. Hakijalla olevat .fi-päätteiset domain-nimet ja tieto niiden hallinnasta tulee olla VRK:n saatavilla hakemusta käsiteltäessä.

Jos hakija on yksityishenkilö, hakija toimittaa palveluvarmennehakemuksen henkilökohtaisesti varmentajalle, jolloin hakijan henkilöllisyys tarkistetaan poliisin myöntämästä henkilöllisyyden osoittavasta asiakirjasta, joita ovat henkilökortti, passi ja 1.10.1990 jälkeen annettu ajokortti.

Hyväksyttäviä tunnistamisasiakirjoja ovat myös Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä voimassa oleva passi tai henkilökortti, Euroopan talousalueen jäsenvaltion viranomaisen 1.10.1990 jälkeen myöntämä voimassa oleva ajokortti ja muun valtion viranomaisen myöntämä voimassa oleva passi.

Palveluvarmenne myönnetään enintään 27 kuukaudeksi.

Varmenteen uusiminen noudattaa samaa hakumenettelyä kuin alkuperäinen hakemus, kuitenkin ilman kaupparekisteriotteen toimittamista. Varmenteen hinta perustuu Väestörekisterikeskuksen palveluhinnaston mukaiseen vuosimaksuun.

Varmentaja myöntää palveluvarmenteen hyväksyessään varmennehakemuksen.

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

Myönnetty palveluvarmenne toimitetaan asiakkaalle sopimuksen mukaan.

7.3.2 Varmenteen uusiminen, sen avainparin vaihtaminen ja varmenteen päivittäminen

Varmenne tulee uusia varmenteen tietosisältöön vaikuttavien varmenteen haltijan tietojen muuttuessa. Tällöin varmenteen haltijan tulee ottaa yhteyttä varmentajaan ja hakea uutta palveluvarmennetta

Mikäli varmenteen haltijan yksityisen avaimen käyttö estyy, tulee kyseiseen avaimeen liitetty varmenne uusia.

Varmenteen uusimista voi hakea vain varmenteen haltijaorganisaation tai sen valtuuttaman tahon edustaja.

Varmenteiden uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

Varmenteen tietosisältöä ei voi muuttaa varmenteen luonnin jälkeen. Varmenteen tietosisältöön vaikuttavien tietojen muuttuessa varmenteen haltijan tulee hakea uutta palveluvarmennetta.

Palveluvarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa. Kun varmenteen haltija uusii yksityisen avaimensa, se vaatii aina uuden rekisteröitymisen, uuden varmennehakemuksen ja uuden palveluvarmenteen

7.3.3 Varmenteiden luominen

Varmenteen tietosisältö on kuvattu FINEID S2 -määrityksessä, joka löytyy www.fineid.fi -sivuilta.

Varmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa, jotka täyttävät FIPS 140-1 tai 140-2 tason 3 asettamat vaatimukset. Varmentajan yksityiset avaimet on suojattu paljastumiselta ja luvattomalta käytöltä.

Juurivarmentaja allekirjoittaa varmentajan varmenteen ja se sijoitetaan julkiseen hakemistoon.

Nimeämiskäytännöt:

CN (Common name) = VRK Gov. Root CA

OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Vaestorekisterikeskus CA

S (State) = Finland

C (Country) = FI

Väestörekisterikeskuksen palvelinvarmenteiden varmentaja on:

CN (Common name) = VRK CA for Social Welfare and Health Care Service Providers

OU (Organizational unit) = Sosiaali- ja terveydenhuollon palveluvarmenteet

O (Organization) = Vaestorekisterikeskus CA

C (Country) = FI

Varmenteen haltijan nimeämiskäytäntö palvelinvarmenteissa asiointikäyttöön (pakolliset kentät):

E = Sähköpostiosoite (esim. webmaster@yritys.fi)

C = Valtio (Fi)

CN = Sähköpostin käyttötarkoitus

SerialNumber = Organisaation Y-tunnus

O (Organization) = Organisaation nimi (esim. Yritys Oyj)

Valinnaiset kentät:

OU (Organizational Unit) = Organisaatioyksikkö (esim. ”Tietohallinto”)

L (Locality name) = Kaupunki tai kunta (esim. ”Helsinki”)

S (State or province name) = Maa (”Suomi”)

Varmentajan varmenteen haltijaa koskevat tiedot määrittelevät varmenteen haltijaorganisaation yksikäsitteisesti.

Varmentajan yksityisten avainten aktivointi tapahtuu tehtävään oikeutettujen henkilöiden toimesta turvalaskentalaitteiston hallintakorttien avulla.

Varmenteen haltijan yksityiset avaimet on suojattu paljastumiselta ja luvattomalta käytöltä varmenteen haltijan tietojärjestelmässä. Vain tietojärjestelmässä suoritettavilla sisäisillä komennoilla on pääsy yksityisiin avaimiin.

Jotta yksityisiin avaimiin liittyvä komento suoritetaan, tulee kyseisen avaimen olla aktivoitu oikealla salasanalla.

Arkistoitava tieto säilytetään korkean tason turvatiloissa, joissa on pääsynvalvonta.

Varmentajan julkisen avaimen sisältävän varmentajan varmenteen voi hakea julkisesta hakemistosta tai varmentajan ylläpitämästä palvelusta.

7.3.4 Käyttöehtojen jakelu

Varmentajan on varmistettava, että käyttöehdot asetetaan tilaajien ja varmenteeseen luottavien osapuolten saataville

Varmentajan julkisen avaimen sisältävän varmentajan varmenteen voi hakea julkisesta hakemistosta tai varmentajan ylläpitämästä palvelusta.

Varmentaja tiedottaa muista kuin luvussa 8 mainituista varmennepolitiikkaan liittyvistä muutoksista www-sivustollaan (www.fineid.fi) vähintään 30 päivää ennen muutoksen voimaanastumista.

Varmentaja julkaisee kaikki palveluvarmenteet ja sulkulistat maksuttomassa, yleisesti saatavilla olevassa julkisessa hakemistossa. Varmentaja julkaisee varmennepolitiikan, varmennuskäytännöt, varmennekuvauksen sekä muut julkiset varmennepalvelujen tuottamiseen liittyvät dokumentit www-sivuillaan http://www.fineid.fi.

Tietojen saatavuus

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

Tietovarastot

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

7.3.5 Varmenteiden jakelu

Varmenne toimitetaan sopimuksen mukaisesti tai julkaistaan julkisessa hakemistossa heti, kun se on luotu, ja se on hakemistossa koko voimassaolonsa ajan. Varmentaja julkaisee sulkulistan, joka on voimassa kaksi vuorokautta julkaisemisestaan. Tämä sulkulista päivitetään tunnin välein.

Hakemisto- ja sulkulistatiedot ovat yleisesti saatavilla ldap://ldap.fineid.fi.

7.3.6 Varmenteen sulkeminen ja asettaminen keskeytystilaan

Varmenteen sulkeminen ja määräaikainen sulkeminen

Varmentaja ylläpitää varmenteiden sulkupalvelua. Tiedot suljetuista varmenteista julkaistaan sulkulistan avulla, jonka varmentaja allekirjoittaa ja joka julkaistaan julkisessa hakemistossa. Varmennetta ei voi sulkea määräajaksi.

Varmentaja ei ilmoita varmenteen haltijalle varmenteen sulkemisesta.

Varmenteen sulkemisen edellytykset

Varmenne suljetaan kun:

- varmenteen haltija pyytää sulkemista
- varmenteen haltijan varmenteen tietosisältöön vaikuttavat tiedot ovat muuttuneet

- varmenteeseen liittyvä yksityinen avain on kadonnut tai paljastunut
- varmenteen haltijaorganisaatio on lopettanut toimintansa.

Varmennetta ei saa käyttää tai yrittää käyttää sen jälkeen, kun sitä koskeva sulkupyyntö on tehty.

Kuka voi vaatia varmenteen sulkemista

Varmenteen sulkemista voivat vaatia:

- palveluvarmenteen haltijaorganisaation edustaja;
- palveluvarmenteen haltija
- varmentaja kohdan 6.2 edellytysten täyttyessä.

Varmenteen sulkuprosessi

Varmenteen haltija esittää varmenteen sulkupyynnön varmentajalle. Ilmoitus tehdään:

1. puhelimitse
2. henkilökohtaisesti rekisteröintipisteessä tai
3. kirjallisesti varmentajalle.

Varmentaja sulkee viran puolesta varmenteet:

- varmenteen haltijaorganisaation toiminnan päättyessä.

Varmenteen sulkemisesta kirjataan seuraavat tiedot:

- palveluvarmenteen yksilöivät tiedot
- peruutuspyynnön tekijän henkilötiedot
- peruutuspyynnön tekijän organisaatio
- peruutuspyynnön tekijän tunnistamistapa
- peruutuspyynnön ajankohta
- peruutuspyynnön syy

- peruutuspyynnön vastaanottajan henkilötiedot
- mahdolliset muut varmenteen haltijan ilmoittamat lisätiedot
- avainparin paljastumisajankohta, varmenteen haltijaorganisaation toiminnan päättymisaika tms.
- varmenteen sulkijan henkilötiedot
- varmenteen sulkemisen ajankohta.

Varmentaja ei lähetä varmenteen haltijalle erillistä vahvistusta varmenteen sulkemisesta. Varmenteen sulkemiseen liittyvät tiedot säilytetään 5 vuotta sulkuajankohdasta.

Varmenteen haltijan velvollisuus tehdä sulkupyyntö

Varmenteen haltijan tulee viipymättä tehdä varmenteen sulkupyyntö varmentajalle, kun luvussa 6.2 kuvatut varmenteen sulkemisen edellytykset täyttyvät.

Varmenteen sulkupyynnön käsittelyaika

Varmentaja käsittelee varmenteen sulkupyynnöt viipymättä.

Varmenteeseen luottavan osapuolen velvollisuus tarkistaa varmenteen voimassaolo.

Luottavan osapuolen vastuulla on tarkistaa ennen varmenteen hyväksymistä, että varmenne on voimassa eikä sitä ole suljettu. On myös mahdollista tarkistaa varmenteen reaaliaikainen tilatieto OCSP-palvelusta.

Luottavan osapuolen vastuulla on voimassa olevan sulkulistan tarkistaminen. Varmenteeseen ei tule luottaa, ellei luottava osapuoli ole suorittanut tilatiedon tarkistusta.

Sulkulistan julkaisutiheys

Päivitetty sulkulista julkaistaan tunnin välein.

Sulkulistasta ilmenee seuraavan sulkulistan suunnitelman mukainen julkaisuajankohta. Uusi sulkulista voidaan julkaista myös ennen suunnitelman mukaista julkaisuajankohtaa.

Sulkulistan voimassaolon enimmäisaika

Päivitetty sulkulista on voimassa enintään 48 tuntia. Jokaisessa sulkulistassa on mainittu voimassaolon päättymisajankohta.

Palveluvarmenteen haltija voi halutessaan saada varmenteen suljettavaksi ennen varmenteen voimassaoloajan päättymistä.

Sulkupyyntömenettely

Palveluvarmenteen haltijan tai varmenteenhaltijaorganisaation toimivaltaisen edustajan on ilmoitettava Väestörekisterikeskuksen Varmennepalvelut-yksiköön, jos on tiedossa tai epäilys siitä, että varmenteen haltijan yksityinen avain on paljastunut. Ilmoitus tehdään puhelimitse virka-aikana numeroon 0295 535 001, faksilla numeroon 09 876 4369 tai sähköpostitse Väestörekisterikeskuksen myöntämällä laatuvarmenteella allekirjoitettuna osoitteeseen kirjaamo@vrk.fi. Ilmoituksessa on oltava seuraavat tiedot: ilmoittajan nimi ja organisaatio, suljettavan palveluvarmenteen sarjanumero. Ilmoituksen saatuaan varmentaja sulkee ko. varmenteen. Kun varmenteen haltija on tehnyt sulkupyynnön varmentajalle ja saanut sulkemisesta vahvistuksen (puhelun aikana, faksilla tai sähköpostitse ilmoitustavasta riippuen), varmenteen haltijan vastuu varmenteen käytöstä päättyy.

7.4 Varmentajan johtamis- ja toimintakäytännöt

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

7.4.1 Turvallisuuden hallinta

Väestörekisterikeskuksen tietoturvallisuutta hallitaan Väestörekisterikeskuksen tietoturvapolitiikan ja standardin ISO 27001 mukaisesti.

7.4.2 Varantojen luokittelu ja hallinta

Väestörekisterikeskus on valtiovarainministeriön alaisuudessa toimiva virasto, jonka tuottamat varmennepalvelut ovat sellaisen taloushallinnollisen järjestelmän ja valvonnan piirissä kuin on erikseen säädetty. Väestörekisterikeskuksen 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.

Väestörekisterikeskus vastaa julkisen hallinnon IT-hankintojen yleisten sopimusehtojen (JIT 2007) mukaisesti siitä että sillä on riittävät taloudelliset voimavarat varmennetoiminnan asianmukaiseksi järjestämiseksi sekä mahdollisen vahingonkorvausvastuun kattamiseksi.

7.4.3 Henkilöstö ja tietoturva

Väestörekisterikeskus toimii varmentajana, joka vastaa varmennetoiminnasta. Tekniset alihankkijat on hankittu kilpailuttamalla ja ne toimivat Väestörekisterikeskuksen vastuulla ja lukuun.

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

Taustaselvityksen tekeminen

Väestörekisterikeskus teettää omasta henkilöstöstään sekä teknisten toimittajien varmenneympäristön kanssa työskentelevistä henkilöistä perusmuotoisen turvallisuusselvityksen.

Taustaselvityksen tekemisessä noudatettava menettely

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

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

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

Koulutukseen liittyvät vaatimukset

Väestörekisterikeskuksen henkilökunnan on oltava koulutettu siten, että tehtävän hoitaminen parhaalla mahdollisella tavalla on mahdollista. Väestörekisterikeskuksessa on koulutussuunnitelma, jonka toteuttamisesta vastaa Väestörekisterikeskuksen hallintoyksikkö.

Asiantuntemuksen ja osaamisen ylläpito

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

Tehtäväkiertoon liittyvät vaatimukset

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

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

Poikkeamista johtuvat toimenpiteet

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

Organisaatiota edustava henkilökunta

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

Henkilökunnan käyttöön annettavat asiakirjat

Henkilökunnalla on aina käytössään Väestörekisterikeskuksen laatu- ja turvallisuusasiakirjat.

7.4.4 Fyysinen ja ympäristön turvallisuus

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

Sijainti ja rakennusten ominaisuudet

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

Toimitilaturvallisuus on toteutettu siten että asiattomien pääsy toimitiloihin on estetty.

Fyysinen pääsy toimitilaan

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

Varajärjestelyt

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

Tärkeiden laitteiden varaosien saanti ja huolto on varmistettu.

7.4.5 Toiminnan hallinta

Väestörekisterikeskus käyttää varmennetuotannon rekisteröintiin ja tietoteknisiin tehtäviin teknisiä toimittajia. Väestörekisterikeskus toimii varmentajana, joka vastaa varmennetoiminnasta.

Varmentajan tehtävät on jaettu seuraaviin vastuualueisiin:

- Tietoturvallisuusvastaava
- Rekisteröintivastaava
- Järjestelmän ylläpitäjä

- Järjestelmän käyttäjä
- Järjestelmän valvoja

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

7.4.6 Järjestelmiin pääsyn hallinta

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

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

Järjestelmän käyttämiseen vaaditaan yhden tehtävään oikeutetun henkilön läsnäolo.

Palveluvarmenteen rekisteröiminen ja tunnistaminen vaatii yhden henkilön läsnäolon.

7.4.7 Luotettavien järjestelmien käyttöönotto ja ylläpito

Palvelinvarmenteen rekisteröijä: Rekisteröijänä toimii Väestörekisterikeskuksen Varmennepalvelut-yksikkö.

Varmennejärjestelmän ylläpitäjä: Tunnistetaan henkilökohtaisella järjestelmän hallintaan tarkoitetulla hallintakortilla. Järjestelmän ylläpitäjiä ovat varmennejärjestelmän toimittajan järjestelmäasiantuntijat sekä Väestörekisterikeskuksen tehtävään valtuutetut henkilöt.

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

7.4.8 Liiketoiminnan jatkuvuuden hallinta ja häiriötilanteiden käsittely

Väestörekisterikeskuksella on jatkuvuus- ja valmiussuunnitelma, joka mahdollistaa varmennus toiminnan jatkuvuuden.

Varmentajan yksityinen avain on paljastunut tai 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 7.4.9 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 7.3.3 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.

Turvallisuuden vaarantuminen luonnonmullistuksen tai muun katastrofin seurauksena

Väestörekisterikeskuksen turvapolitiikassa on otettu huomioon ulkoisen turvallisuuden vaarantumisen aiheuttamat toimenpiteet. Väestörekisterikeskus on saanut ISO 27001 -tietoturvaseritifikaatin, joka asettaa vaatimukset Väestörekisterikeskuksen toiminnalle myös mahdollisen katastrofin tapahduttua.

7.4.9 Varmentajan toiminnan lakkauttaminen

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

Varmentaja ilmoittaa varmennepalveluiden lakkauttamisesta mahdollisimman pian, kuitenkin vähintään yhtä kuukautta ennen lakkauttamisen ajankohtaa.

Ennen varmentajan lakkauttamista suoritetaan vähintäänkin seuraavat toimenpiteet:

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

b) Varmentaja lakkauttaa kaikki sopimuskumppaniensa valtuudet suorittaa varmenteiden myöntämisprosessiin liittyviä tehtäviä varmentajan puolesta.

c) Varmentaja varmistaa, että saatavuus varmentajan arkistoihin säilyy varmentajan lakkauttamisen jälkeenkin.

7.4.10 Sovellettava lainsäädäntö

Väestörekisterikeskus noudattaa varmennepalvelutoiminnassaan voimassaolevaa Suomen lainsäädäntöä.

Väestörekisterikeskuksen myöntämistä varmenteista on säädetty laissa väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009).

VRK/DiPa 1.2.2018

Varmennepalveluiden tuottamiseen liittyvä Väestörekisterikeskuksen vahingonkorvausvastuu määräytyy voimassaolevien yhteistyösopimusten ja vahingonkorvauslain (412/1974) mukaisesti.

Varmenteita koskevan tiedon säilyttäminen

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

Arkistoinnissa sovelletaan yleislakina arkistolain (831/1994) säännöksiä. Oikeus tietojensaantiin määräytyy viranomaisen toiminnan julkisuudesta annetun lain (621/1999) mukaisesti. Varmenteiden arkistoinnissa osalta sovelletaan lisäksi, mitä sähköisen asioinnin lainsäädännössä on arkistoinnista määrätty. Varmennerekisterin tiedot säilytetään 5 vuoden ajan varmenteiden voimassaolon päättymisestä. Varmentaja arkistoi seuraavat tiedot:

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

b) Myönnetyt palvelinvarmenteet, niiden tietosisältö ja elinkaaren hallintaan liittyvät lisätiedot siitä hetkestä, kun palvelinvarmenteen voimassaoloaika on päättynyt tai siitä kun varmenne on suljettu

c) Varmentajan yksityisen avaimen luomiseen ja uusintaan liittyvät tapahtumat

d) Palvelinvarmenteen sulkupyynnöt

e) Julkiseen hakemistoon talletetut sulkulistat ja muu palvelinvarmenteen sulkemiseen liittyvä tieto

f) Voimassaoleva ja aikaisemmin julkaistut varmennepolitiikat ja niitä vastaavat varmennuskäytännöt

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

h) Tarkastusraportit ja pöytäkirjat käsittäen tietoturvatarkastukset ja järjestelmän auditoinnin.

Arkistotiedot säilytetään laatuvarmentajana toimivaa viranomaista koskevien säännösten mukaisesti.

Arkistojen suojaus

Varmentaja säilyttää palvelinvarmenteen hakemiseen, henkilön tunnistamiseen ja palvelinvarmenteen luovutukseen liittyvät arkistoitavat asiakirjat asianmukaisissa tiloissa.

Arkistoitava tieto säilytetään korkean turvatason tiloissa, joissa on pääsynvalvonta.

Arkistotietojen varmistusmenettelyt

Varmuuskopiot varastoidaan fyysisesti erilliseen tilaan alkuperäisistä tiedoista.

Arkistotietojen hankinta- ja varmistusmenetelmät

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

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

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

7.5 Organisaatioon liittyvät vaatimukset

Väestörekisterikeskus on henkilörekisteriä ylläpitävä viranomainen, jonka väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009) annetun lain mukainen tehtävä on tuottaa muiden tehtäviensä lisäksi varmennetun sähköisen asioinnin palveluita.

Väestörekisterikeskus myöntää varmenteita hakemuksesta. Varmenteen hakijan oikeudet ja velvollisuudet on mainittu Väestörekisterikeskuksen varmennehakemusasiakirjassa ja yleisissä käyttöehdoissa, jotka muodostavat varmenteen hakijan kanssa tehtävän sopimuksen.

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

Väestörekisterikeskuksen tuottamat varmennepalvelut ovat sellaisen taloushallinnollisen järjestelmän ja valvonnan piirissä kuin on erikseen säädetty. Väestörekisterikeskus on valtiovarainministeriön alaisuudessa toimiva virasto. Väestörekisterikeskuksen 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.

Väestörekisterikeskus noudattaa varmennepalvelutoiminnassaan voimassaolevaa Suomen lainsäädäntöä. Väestörekisterikeskus toimii huolellisesti, luotettavasti ja asianmukaisesti. Väestörekisterikeskus pitää yleisesti saatavilla varmenteita ja varmennetoimintaa koskevat tiedot, joiden perusteella varmentajan toiminta ja luotettavuus voidaan arvioida.

Väestörekisterikeskus kiinnittää erityistä huomiota sekä oman henkilökuntansa että teknisten toimittajien ja rekisteröijien luotettavuuteen ja tehtävien suorittamiseen tarvittaviin taitoihin. Väestörekisterikeskuksella on riittävät tekniset taidot ja taloudelliset voimavarat varmennetoiminnan asianmukaiseksi järjestämiseksi sekä mahdollisen vahingonkorvausvastuun kattamiseksi. Väestörekisterikeskuksen henkilökunta toimii tehtävissään virkavastuulla ja Väestörekisterikeskuksen sisäisten ohjeiden mukaisesti. Virkamiehen asemasta on säännelty valtion virkamieslaissa (750/1994).

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

Tämän varmennuskäytännön on rekisteröinyt Väestörekisterikeskus ja sen mukaiset tekijänoikeudet kuuluvat Väestörekisterikeskukselle. Väestörekisterikeskus omistaa kaikki varmenteisiin ja dokumentaatioon liittyvät tiedot teknisten toimitussopimusten mukaisesti. Väestörekisterikeskus omistaa täydet omistus- ja käyttöoikeudet tähän varmennuskäytäntöön. Väestörekisterikeskus vastaa tämän varmennuskäytännön hallinnoinnista ja päivityksistä.

8 . Määrittelypuitteet muita varmennepolitiikka-asiakirjoja varten

Tässä kohdassa määritellään varmenteita myöntävien varmentajien muita varmennepolitiikkoja koskevat yleiset puitteet. Varmentaja voi ilmaista noudattavansa näiden yleisten määrittelypuitteiden vaatimuksia kohdan 8.3 mukaisesti. Yleisesti ottaen vaatimustenmukaisuus edellyttää kohtien 6 ja 7 vaatimusten noudattamista lukuun ottamatta niitä vaatimuksia, joita sovelletaan vain yleisölle varmenteita myöntäviin varmentajiin.

8.1 Määritysasiakirjojen hallinta

Määritysten muuttaminen

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

Julkaiseminen ja tiedottaminen

Varmentaja julkaisee varmennepolitiikan ja varmennuskäytännön, jotka ovat saatavilla internetsivustoilla http://www.fineid.fi/ .

Varmentajan 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.

Varmennuskäytännön muutos- ja hyväksymismenettely

VRK/DiPa 1.2.2018

Väestörekisterikeskus hyväksyy sekä palveluvarmennetta koskevan varmennepolitiikan että varmennuskäytännöt. Asiakirjoja voidaan muuttaa Väestörekisterikeskuksen sisäisin muutosmenettelyin.

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

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

8.2 Lisävaatimukset

Tilaajille ja varmenteeseen luottaville osapuolille tulee kohdassa 7.3.4 määriteltäviä vaatimuksia täytäntöön pantaessa tiedottaa siitä, miten kulloinenkin politiikka lisää tai edelleen rajoittaa varmennepolitiikan vaatimuksia sellaisina kuin ne tässä asiakirjassa määritellään.

8.3 Vaatimustenmukaisuus

Varmentaja saa ilmaista toimivansa tämän varmennuskäytännön mukaisesti vain,

a) jos varmentaja ilmaisee noudattavansa yksilöityä varmennepolitiikkaa ja asettaa pyynnöstä tilaajan ja varmenteeseen luottavien osapuolten saataville todisteita vaatimustenmukaisuudesta tai Todisteena voi olla esimerkiksi auditoijan kertomus, jossa vahvistetaan varmentajan noudattavan yksilöidyn varmennepolitiikan vaatimuksia. Kyseessä voi olla varmentajan organisaation sisäinen auditoija, mutta auditoija ei saa olla hierarkkisessa suhteessa varmentajan toimintaa toteuttavaan osastoon.

b) jos pätevä ja riippumaton osapuoli on hiljattain arvioinut yksilöidyn varmennepolitiikan vaatimusten noudattamisen nykytilaa varmentajalla. Arviointitulokset on asetettava pyynnöstä tilaajien ja varmenteeseen luottavien osapuolten saataville