Väestörekisterikeskus
Befolkningsregistercentralen

Varmennepolitiikka

Väestörekisterikeskuksen kansalaisvarmennetta varten

OID: 1.2.246.517.1.10.22

SERTIFIOITU inspecta ORGANISAATIO
ISO 9001

SERTIFIOITU inspecta ORGANISAATIO
ISO/IEC 27001

Sisällysluettelo

Esipuhe

Tämä asiakirja perustuu tekniseen määritykseen, jonka on laatinut sähköisiä allekirjoituksia ja järjestelmiä käsittelevä ETSIn tekninen komitea (ETSI Technical Committee Electronic Signatures and Infrastructures (ESI)).

Johdanto

Sähköinen asiointi edellyttää sähköisen tiedon lähteen tunnistamista asiakirjoihin käsin tehtyyn allekirjoitukseen verrattavalla tavalla. Tämä voidaan yleensä toteuttaa käyttämällä sähköisiä allekirjoituksia. Varmennepalveluiden tarjoajat, joita yleisesti kutsutaan varmentajiksi, tuottavat sähköisten allekirjoitusten tekemiseen tarkoitettuja varmenteita.

Sähköisten allekirjoitusten käyttäjät voivat luottaa sähköisten allekirjoitusten aitouteen, jos varmentajalla on käytössään asianmukaiset menettelyt ja suojautumiskeinot, joilla minimoidaan julkisiin salausavainten järjestelmiin liittyvät toiminnalliset ja taloudelliset riskit.

Sähköisiä allekirjoituksia koskevista yhteisön puitteista annetussa Euroopan parlamentin ja neuvoston direktiivissä 1999/39/EY (jäljempänä ”direktiivi”) yksilöidään laatuvarmenteeseen perustuvan sähköisen allekirjoituksen erityiset vaatimukset. Direktiivin liitteessä I määritellään laatuvarmenteita koskevat vaatimukset. Direktiivin liitteessä II määritellään laatuvarmenteita myöntävien varmennepalveluiden tarjoajia koskevat vaatimukset (eli laatuvarmenteita myöntäviä varmentajia koskevat vaatimukset). Tässä asiakirjassa määritellään menettelytapavaatimukset, jotka koskevat direktiivin mukaisesti laatuvarmenteita myöntävien varmentajien toimintaa ja hallintokäytäntöjä. Tässä asiakirjassa esitetyissä menettelytapavaatimuksissa turvallisen allekirjoituksen luomisvälineen käyttö, josta esitetään vaatimuksia direktiivin liitteessä III, on valinnainen osio.

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

Tätä varmennepolitiikkaa sovelletaan Väestörekisterikeskuksen kansalaisvarmenteeseen, joka myönnetään väestötietojärjestelmään rekisteröidyille Suomen kansalaisille ja Suomessa pysyvästi asuville ulkomaalaisille.

Kansalaisvarmenne koostuu varmenneparista, jolla on kaksi eri käyttötarkoitusta: todentamis- ja salausvarmenne ja allekirjoitusvarmenne, joka on vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain mukainen laatuvarmenne.

1. Soveltamisala

Tässä asiakirjassa määritellään menettelytapavaatimukset, jotka koskevat laatuvarmenteita myöntäviä varmentajia. Menettelytapavaatimuksia asetetaan laatuvarmenteita myöntävien varmentajien toiminnalle ja hallintakäytännölle, jotta tilaajat, varmentajan varmentamat allekirjoittajat sekä varmenteeseen luottavat osapuolet voisivat luottaa siihen, että varmenteella voidaan vahvistaa sähköisiä allekirjoituksia.

Väestörekisterikeskuksen tarjoaman vahvan sähköisen tunnistamisen välineen tarjoaminen tapahtuu samassa tuotantoympäristössä, samanlaisin teknisin ja toiminnallisin ratkaisuin ja siihen sovelletaan samoja menettelytapoja noudattaen kuin Väestörekisterikeskuksen myöntämän laatuvarmenteen tarjoamiseen.

Menettelytapavaatimuksissa:

a) määritellään kaksi yleisölle myönnettäviä laatuvarmenteita koskevaa, läheisesti toisiinsa liittyvää laatuvarmennepolitiikkaa, joista toinen edellyttää turvallisen allekirjoituksen luomisvälineen käyttöä

b) esitetään määrittelypuitteet sellaisia laatuvarmennepolitiikkoja varten, joilla parannetaan edellä mainittuja varmennemenettelytapoja tai jotka koskevat muille kuin yleisöksi katsottaville käyttäjäryhmille myönnettäviä laatuvarmenteita.

Varmentajaa koskevat menettelytapavaatimukset sisältävät vaatimuksia rekisteröintipalvelujen tarjoamisesta, varmenteiden luomisesta, varmenteiden jakelusta, varmenteiden peruuttamisen hallinnasta, sulkutilasta ja tarvittaessa allekirjoituksen luomisvälineen tarjoamisesta. Muut varmennepalvelujen tarjoajan toiminnot, kuten aikaleimat, attribuuttivarmenteet ja luottamuksellisuutta tukevat palvelut, eivät kuulu tämän asiakirjan soveltamisalaan. Tässä asiakirjassa ei esitetä vaatimuksia varmentajan varmenteille, ei myöskään varmennehierarkioiden tai ristiinvarmentamisen suhteen. Nämä menettelytapavaatimukset on rajattu koskemaan sähköisten allekirjoitusten yhteydessä käytettävien avainten varmentamista.

Nämä menettelytapavaatimukset on erityisesti kohdistettu yleisölle myönnettäviin laatuvarmenteisiin, joita käytetään tukemaan sähköisiä laatuallekirjoituksia (sellaisia sähköisiä allekirjoituksia, jotka oikeusvaikutuksiltaan vastaavat käsintehtyjä allekirjoituksia sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun EU-direktiivin 5 artiklan 1 kohdan mukaisesti). Erityisesti käsitellään vaatimuksia, jotka koskevat direktiivin liitteiden I ja II mukaisesti laatuvarmenteita myöntäviä varmentajia. Liitteen III mukaisen turvallisen allekirjoituksen luomisvälineen käyttö, joka on 5 artiklan 1 kohdan mukaisesti sähköisiä allekirjoituksia koskeva vaatimus, on tässä asiakirjassa esitetyissä menettelytapavaatimuksissa valinnainen osio.

Näiden menettelytapavaatimusten mukaisesti myönnettyjä varmenteita voidaan käyttää henkilön todentamisessa, kun henkilö toimii omasta puolestaan tai edustamansa luonnollisen henkilön, oikeushenkilön tai yhteisön puolesta.

Nämä menettelytapavaatimukset koskevat julkisen avaimen salauksen käyttöä sähköisten allekirjoitusten vahvistamisessa.

Asiantuntevat riippumattomat elimet voivat käyttää tätä asiakirjaa perustana arvioidessaan, täyttääkö varmentaja laatuvarmenteiden myöntämistä koskevat vaatimukset.

Varmenteenhaltijoita ja varmenteeseen luottavia osapuolia suositellaan lukemaan varmentajan varmennuskäytännöstä tarkempia lisätietoja siitä, kuinka kyseinen varmentaja toteuttaa tiettyä varmennepolitiikkaansa.

Tässä asiakirjassa ei kuitenkaan tarkenneta, kuinka riippumattomat osapuolet voivat arvioida tässä yksilöityjä vaatimuksia, esimerkiksi ei määritetä vaatimuksia riippumattomien arvioijien saataville annettavan tiedon tai riippumattomien arvioijien suhteen.

Vaatimustenmukaisuuden arviointi on yksityiskohtaisesti kuvattu CEN-työryhmän määrityksessä CWA 14172 "EESSI Conformity Assessment Guidance".

2. Viiteluettelo

Tässä asiakirjassa viitataan seuraavissa asiakirjoissa esitettyihin säännöksiin ja määrityksiin, jotka ovat sitovia tässä asiakirjassa kuvattuihin toimintoihin liittyen.

- Käytetyt viittaukset liittyen julkaisupäivään ja laitoksen tai version numeroihin ovat täsmällisiä tai yleisluontoisia.
- Täsmällisten viittausten osalta lähteen myöhempiä tarkistuksia ei sovelleta.
- Yleisluontoisten viittausten osalta sovelletaan lähteen viimeisintä versiota.

Tähän asiakirjaan liittyvää aineistoa on saatavilla muun muassa osoitteessa http://docbox.etsi.org/Reference. ETSI ei takaa linkin toimivuutta pitkällä aikavälillä.

[1] Euroopan parlamentin ja neuvoston direktiivi 1999/93/EY, annettu 13 päivänä joulukuuta 1999, sähköisiä allekirjoituksia koskevista yhteisön puitteista ("direktiivi").

[2] IETF RFC 3647 (2003): "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".Tämä asiakirja kumoaa julkaisun IETF RFC 2527.

[3] ITU-T Recommendation X.509 (2000)4SO/IEC 9594-8 (2001): "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[4] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.

[5] FIPS PUB 140-2 (2001): "Security Requirements For Cryptographic Modules".

[6] ETSI TS 101 862: "Qualified certificate profile".

[7] ISO/IEC 15408 (2005) (osat 1–3): "Information technology - Security techniques - Evaluation criteria for IT security".

[8] CEN Workshop Agreement 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements".

[9] CEN Workshop Agreement 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)".

[10] CEN Workshop Agreement 14167-3: "Security Requirements for Trustworthy

Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)".

[11] CEN Workshop Agreement 14167-4: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP".

[12] Neuvoston direktiivi 93/13/ETY, annettu 5 päivänä huhtikuuta 1993, kuluttajasopimusten kohtuuttomista ehdoista.

[13] ISO/IEC 17799 (2005): "Information technology - Security techniques - Code of practice for information security management".

[14] ETSI TS 102 158: "Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates".

3. Määritelmät ja lyhenteet

3.1. Määritelmät

Tässä asiakirjassa käytetään seuraavia käsitteitä ja määritelmiä:

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

Allekirjoittaja: taho, joka on varmenteessa merkitty varmenteessa annettuun julkiseen avaimeen liittyvän yksityisen avaimen haltijaksi

Allekirjoituksen luomiseen käytettävät tiedot: ainutlaatuinen tietokokonaisuus, esimerkiksi koodit tai yksityiset salausavaimet, joita allekirjoittaja käyttää luodakseen sähköisen allekirjoituksen. Tarkempi kuvaus perustuu sähköisistä allekirjoituksista annetun direktiivin vaatimuksiin.

Kun kyseessä ovat julkisen avaimen salaukseen perustuvat laatuvarmenteet, kuten tämän asiakirjan soveltamisalassa, allekirjoituksen luomiseen käytettävät tiedot sisältävät yksityiset avaimet. Tässä asiakirjassa allekirjoituksen luomiseen käytettävistä tiedoista käytetäänkin käsitettä yksityinen avain.

Allekirjoituksen luomisväline: tarkoituksenmukaisesti määritetty ohjelmisto tai laitteisto, jolla allekirjoituksen luomiseen käytettävät tiedot käsitellään. Tarkempi kuvaus perustuu sähköisistä allekirjoituksista annetun direktiivin vaatimuksiin.

Allekirjoituksen todentamiseen käytettävät tiedot: tietokokonaisuus, esimerkiksi koodit tai julkiset salausavaimet, joita käytetään sähköisen allekirjoituksen todentamiseen. Tarkempi kuvaus perustuu sähköisistä allekirjoituksista annetun direktiivin vaatimuksiin.

Kun kyseessä ovat julkisen avaimen salaukseen perustuvat laatuvarmenteet, kuten tämän asiakirjan soveltamisalassa, allekirjoituksen todentamiseen käytettävät tiedot sisältävät julkiset avaimet. Tässä asiakirjassa allekirjoituksen todentamiseen käytettävistä tiedoista käytetäänkin käsitettä julkinen avain.

Attribuutti: tahoon liitetty tieto, joka määrittelee tahon ominaisuuden, kuten ryhmän jäsenyyden tai roolin, tai muu kyseiseen tahoon liittyvä tieto

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.

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

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

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

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

Kansalaisvarmenne: Väestörekisterikeskuksen luonnolliselle henkilölle myöntämä tässä asiakirjassa tarkemmin määritelty varmennepari, joka laatuvarmenne, jonka tietosisältö on määritelty laissa väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009).

Kehittynyt sähköinen allekirjoitus: sähköinen allekirjoitus, joka täyttää seuraavat vaatimukset: se liittyy yksiselitteisesti

- **a)** sen allekirjoittajaan
- **b)** sillä voidaan yksilöidä allekirjoittaja
- **c)** se on luotu keinoilla, jotka allekirjoittaja voi pitää yksinomaisessa valvonnassaan,
- **d)** se on liitetty sen kohteena olevaan tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita, kuten sähköisistä allekirjoituksista annetussa direktiivin 1999/93/EY liitteessä I.

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

Laatuvarmenne: varmenne, joka täyttää sähköisistä allekirjoituksista annetun direktiivin 1999/93/EY liitteessä I säädetyt vaatimukset ja jonka on myöntänyt direktiivin liitteessä II säädetyt vaatimukset täyttävä varmentaja. Laatuvarmenteen tietosisältö on määritelty vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa.

Laatuvarmennepolitiikka: varmennepolitiikka, johon sisältyy sähköisistä allekirjoituksista annetun direktiivin 1999/93/EY liitteissä I ja II säädetyt vaatimukset

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

Maksukortti: Luotto-, yhdistelmä-, raha- ja maksuaikakortin yleisnimitys.

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

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

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

PUK-koodi: Lukkiutuneen PIN-tunnuksen vapauttamisessa tarvittava koodi.

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

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

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

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

sähköinen allekirjoitus: sähköisessä muodossa oleva tieto, joka on liitetty tai loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään kyseisen muun tiedon todentamismenetelmänä ja joka on tarkemmin määritelty sähköisistä allekirjoituksista annetun direktiivissä.

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

Sähköinen laatuallekirjoitus: kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteeseen ja joka on tehty turvallisella allekirjoituksen luomisvälineellä sähköisistä allekirjoituksista annetussa direktiivissä 1999/93/EY olevan 5 artiklan 1 kohdan mukaisesti

Turvallinen allekirjoituksen luomisväline: allekirjoituksen luomisväline, joka täyttää sähköisistä allekirjoituksista annetun direktiivin 1999/93/EY liitteessä III säädetyt vaatimukset

Varmenne: sisältää käyttäjän julkisen avaimen sekä muita tietoja, joiden väärentäminen on estetty salakirjoittamalla ne varmenteen myöntäneen varmentajan yksityisellä avaimella. Tarkempi kuvaus perustuu ITU-T:n suositukseen X.509.

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

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

Varmennekuvaus: Asiakirja sisältää varmennepolitiikan ja varmennuskäytännön keskeiset kohdat.

Varmennepalvelujen tarjoaja: yhteisö, oikeushenkilö tai luonnollinen henkilö, joka myöntää varmenteita tai tarjoaa muita sähköisiin allekirjoituksiin liittyviä palveluja ja joka on tarkemmin määritelty sähköisistä allekirjoituksista annetussa direktiivissä.

Tässä asiakirjassa käsitellään varmennepalvelujen tarjoajia, jotka myöntävät laatuvarmenteita (tai tarjoavat laatuvarmenteiden myöntämisen osapalveluja – katso kohta 4.1). Tässä asiakirjassa ei käsitellä varmennepalvelujen tarjoajan muuntyyppisiä toimintoja, kuten aikaleimausta ja vara-avainjärjestelmiä.

Varmennepolitiikka: nimetty säännöstö, joissa osoitetaan tietyn varmenteen soveltuvuus tietylle yhteisölle ja/tai sovellusluokka, jota koskee yhteiset turvallisuusvaatimukset. Tarkempi kuvaus perustuu ITU-T:n suositukseen X.509.

Lisätietoja varmennepolitiikkojen ja varmennuskäytännön keskinäisestä suhteesta annetaan kohdassa 4.3. Väestörekisterikeskuksen julkaisemat varmennepolitiikat ovat julkisesti saatavilla. Jokaisella varmennepolitiikalla on yksilöivä tunnuksensa.

Varmennerekisteri: Vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain mukainen rekisteri, jota laatuvarmenteita yleisölle tarjoavan varmentajan on velvollisuus pitää. Tiedot on säilytettävä vähintään 10 vuoden ajan varmenteen voimassaolon päättymisestä.

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

Varmennuskäytännön yksilöivä tunnus on osa varmenteen tietosisältöä.

Varmennuskäytäntö: lausunto toimintatavoista, joita varmentaja noudattaa varmenteiden myöntämisessä, hallinnoimisessa, peruuttamisessa ja uusimisessa sekä varmenteiden avainparin vaihtamisessa. Jokaisella varmennuskäytännöllä on oma yksilöivä tunnuksensa.

Varmentaja: Varmenteita myöntävä organisaatio, joka vastaa varmenteiden tuottamisesta sekä laatii toimintaansa kuvaavan varmennepolitiikan sekä varmennuskäytännön. Varmentajan toimintaan luottaa yksi tai useampi taho.Varmentaja on varmenteita myöntävä varmennepalvelujen tarjoaja. Tarkempi kuvaus perustuu ITU-T:n suositukseen X.509.Varmentajan käsitettä selvennetään lisää kohdassa 4.2.

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

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

Varmenteen hakija: Henkilö, joka hakee kansalaisvarmennetta ja joka tunnistetaan hakemisen yhteydessä luotettavasti.

Varmenteen haltija: Henkilö, jonka henkilöllisyys ja julkinen avain on varmennettu varmentajan sähköisellä allekirjoituksella, ja jonka hallussa varmenteeseen liittyvät yksityiset avaimet ovat.

Varmenteenhakija/haltija: Varmennetta hakeva luonnollinen henkilö, joka tunnistetaan henkilökohtaisella tavalla ja joka vastaanottaessaan varmenteen on varmenteen haltija.

Varmenteen haltijan allekirjoitusvarmenne: Varmenteella olevalla julkisella avaimella todennetaan sitä vastaavalla yksityisellä avaimella eli allekirjoitusavaimella varmenteen haltijan tekemä sähköinen allekirjoitus. Allekirjoituksen tekemiseen tarvitaan allekirjoitustunnusluku (PIN 2).

Varmenteen haltijan todentamis- ja salausvarmenne: Varmennetta käytetään henkilön sähköiseen tunnistamiseen ja tiedon salaukseen. Varmenteen haltija käyttää yksityistä todentamis- ja salausavaintaan sähköiseen tunnistautumiseen ja salatun tiedon tai viestin salauksen purkuun. Avaimen käyttämiseen tarvitaan perustunnusluku (PIN 1).

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

Varmenteeseen luottava osapuoli: varmenteen vastaanottaja, joka toimii luottaen kyseiseen varmenteeseen ja/tai digitaalisiin allekirjoituksiin, jotka on todennettu kyseisellä varmenteella. Tarkempi kuvaus perustuu RFC 3647-määritykseen.

Varmenteiden sulkulista: allekirjoitettu varmenneluettelo, jonka sisältämiä varmenteita niiden myöntäjät eivät enää katso voimassa oleviksi. Tarkempi kuvaus perustuu ITU-T:n suositukseen X.509.

Yksityinen avain: Julkisen avaimen menetelmässä epäsymmetrisessä salauksessa käytettävän avainparin yksityinen osa. Varmenteen haltijan yksityiset avaimet on talletettu mikrosirulle niiden suojaamiseksi oikeudettomalta käytöltä.

3.2. Lyhenteet

ISO 27001	ISO IEC 27001
CA	Certification Authority, varmentaja
CSP	Certification Service Provider: varmennepalvelujen tarjoaja
CP	Certificate Policy, varmennepolitiikka
CPS	Certification Practise Statement, varmennuskäytäntö
CRL	Certificate Revocation List, varmenteiden sulkulista
FINEID	Finnish Electronic Identification
HSM	Hardware Security Module, turvamoduuli
HST	Henkilön sähköinen tunnistaminen
HTTP	Hypertext Transfer Protocol
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol, suorakäyttöinen varmenteen tilan palauttava palvelu
OID	Object Identifier, yksilöivä tunnus
PDS	PKI Disclosure Statement, varmennekuvaus
PIN	Personal Identification Number, PIN-tunnus
PKI	Public Key Infrastructure, julkisen avaimen järjestelmä
PUK	PIN Unblocking Key, PUK-koodi
QCP	Qualified Certificate Policy: laatuvarmennepolitiikka

RSA	Rivest, Shamir, Adleman, RSA-tunniste, eräs julkisen avaimen algoritmi, epäsymmetrinen algoritmi
SATU	Sähköinen asiointitunnus
SIM	Subscriber Identity Module
SSCD	Secure Signature Creation Device: turvallinen allekirjoituksen luomisväline
VRK	Väestörekisterikeskus

4. Yleiskäsitteet

4.1. Varmentaja

Varmentaja luo ja myöntää varmenteita, jonka toimintaan varmennepalvelujen käyttäjät, eli varmenteen hakijat ja varmenteeseen luottavat osapuolet luottavat. Varmentaja on kokonaisvastuussa kohdassa 4.2 määriteltyjen varmennepalvelujen tarjoamisesta. Varmentaja on yksilöity varmenteessa varmenteen myöntäjäksi. Laatuvarmenteet allekirjoitetaan sen yksityisellä avaimella.

Varmentaja voi käyttää varmennepalvelussaan muita osapuolia, jotka tarjoavat palvelun osia. Varmentaja vastaa kuitenkin aina koko tuottamansa palvelun osalta ja varmistaa sen, 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 sekä vastuu yleisölle myönnettävien varmenteiden myöntämisestä sähköisistä allekirjoituksista annetun direktiivin mukaisesti.

Varmentaja on sähköisistä allekirjoituksista annetun direktiivin mukainen varmennepalvelujen tarjoaja, joka myöntää varmenteita.

Väestörekisterikeskus (VRK) toimii valtiovarainministeriön hallinnonalalla. VRK on henkilörekisteriä ylläpitävä viranomainen, jonka väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain (661/2009) mukainen tehtävä on tuottaa varmennettuja sähköisen asioinnin palveluita. Väestörekisterikeskus toimii myös terveydenhuollon lakisääteisenä varmentajana 1.12.2010 alkaen (laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007), laki sähköisestä lääkemääräyksestä (61/2007) sekä laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009); HE 155/2010 vp). Väestörekisterikeskuksen Varmennepalvelut-yksikkö vastaa viraston varmennetoiminnasta. VRK on tarjonnut varmennepohjaisia allekirjoitus- ja tunnistusvälineitä vuodesta 1999 lähtien ja toiminut laatuvarmentajana 31.3.2003 lukien.

VRK:n varmennetietojärjestelmä ja varmennepalvelut perustuvat julkisen avaimen järjestelmään (Public Key Infrastructure eli PKI). VRK:n varmenneinfrastruktuuri muodostuu varmennejärjestelmästä, kortteihin sisältyvien varmennetietojen toimittajasta, sulkulistasta, neuvontapalvelusta ja hakemistopalvelusta. VRK:n toimintoja varmentajana ovat varmenne-, hakemisto- ja sulkupalveluiden tuottaminen, rekisteröinti sekä varmenteen sisältävän kortin valmistus ja yksilöinti. VRK vastaa koko varmennejärjestelmän toimivuudesta, myös käyttämiensä rekisteröijien ja teknisten toimittajien osalta. VRK:n Varmennepalvelut-yksikkö ylläpitää varmenteitaan koskevia varmennepolitiikka-, varmennuskäytäntö- ja varmennekuvausasiakirjoja, jotka ovat saatavilla sähköisesti osoitteessa http://www.fineid.fi.

EU:n sähköisen allekirjoituksen direktiivi tuli voimaan joulukuussa 1999. Direktiivi on implementoitu Suomen lainsäädäntöön lailla sähköisistä allekirjoituksista (14/2003). Laki sähköi-

sistä allekirjoituksista on kumottu lailla vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009). Lailla säädetään vahvan sähköisen tunnistamisen palvelujen tarjoamisesta sekä sähköisestä allekirjoituksesta ja niiden oikeusvaikutuksista. Henkilökortista on säädetty henkilökorttilaissa (829/1999) ja Väestörekisterikeskuksen myöntämistä varmenteista on säädetty väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetussa laissa (661/2009).

VRK tuottaa tietoturvallisuuden tasoltaan korkealaatuisia sähköisen allekirjoituksen ja tunnistamisen varmenteita ja niihin liittyviä palveluja julkiselle ja yksityiselle sektorille. Varmenteen avulla varmennetaan varmenteen haltijan henkilöllisyys sekä varmenteeseen sisältyvien tietojen oikeellisuus, eheys ja alkuperäisyys. Laatuvarmenteella tehty sähköinen allekirjoitus sekä vahvan sähköisten tunnistamisen välineen avulla tehty henkilön vahva sähköinen tunnistaminen antavat kansalaisille mahdollisuuden turvalliseen, ajasta ja paikasta riippumattomaan ja joustavaan verkkoasiointiin. Laatuvarmenteen ja vahvan sähköisen tunnistuspalvelun tarjoajia valvoo Suomessa Viestintävirasto.

Tämän kansalaisvarmenteen myöntämistä kuvaavan varmennepolitiikan on rekisteröinyt Väestörekisterikeskus.

Tämä varmennepolitiikka kuvaa sähköisistä allekirjoituksista annettuun direktiiviin perustuvan, vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain mukaisen sähköisen allekirjoituksen laatuvarmenteen myöntämiseen, tuottamiseen ja vastuun jakoon liittyviä yksityiskohtaisia vaatimuksia.

Tämä asiakirja kuvaa myös kansalaisvarmenteeseen sisältyvän, vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain mukaisen vahvan sähköisen tunnistamisen välineenä tarjottavan tunnistusvarmenteen myöntämiseen, tuottamiseen ja tietojen tallentamiseen liittyviä ratkaisuja ja menettelytapoja laatuvarmenteen tuotantoympäristön vaatimuksia noudattaen.

Kansalaisvarmenne koostuu varmenneparista, jolla on kaksi toisistaan poikkeavaa käyttötarkoitusta. Todentamis- ja salausvarmenne täyttää vahvan sähköisen tunnistamisvälineen vaatimukset. Yksinomaan allekirjoituksen toteuttamiseen tarkoitettu allekirjoitusvarmenne täyttää laatuvarmenteen vaatimukset. Varmenteen hakijan henkilöllisyyden oikeellisuuden takaa Väestörekisterikeskus

4.2. Varmennepalvelut

Varmenne on sähköinen todistus, joka liittää allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistaa varmenteen haltijan henkilöllisyyden. Varmenteen tiedot on sähköisesti allekirjoitettu varmentajan yksityisellä avaimella. Tämän varmennepolitiikan mukainen varmenne perustuu julkisen avaimen järjestelmään ja menetelmiin. Tämän varmennepolitiikan mukaisten varmenteiden tietosisältö on määritelty väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetussa laissa (661/2009).

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

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

Kansalaisvarmenne voidaan myöntää ja tallettaa erilaisille viranomaisen myöntämille teknisille alustoille eli mikrosiruille kuten henkilökortille. Tämä varmennepolitiikka on yhteinen kuvaus näillä eri teknisillä alustoilla oleville kansalaisvarmenteille.

Väestörekisterikeskuksen varmennepolitiikalla ja varmennuskäytännöllä on molemmilla yksilöivä tunnuksensa (OID).

Väestörekisterikeskuksen laatuvarmenteiden myöntäminen on tässä asiakirjassa jaoteltu vaatimusten luokittelusyistä seuraaviin osapalveluihin:

Rekisteröintipalvelu: Rekisteröintipalvelussa todennetaan allekirjoittajan henkilöllisyys ja mahdolliset häneen liittyvät erityiset attribuutit, jotka välitetään varmenteiden luomispalveluun.

Rekisteröintipalvelu sisältää toimintana myös asiakkaan itsensä tai jonkin muun kuin varmentajan generoiman avaimen toimittamisen. Väestörekisterikeskuksen rekisteröintipalvelussa ei käsitellä muita kuin sen itsensä tuottamat avainparit.

Kansalaisvarmenteen rekisteröinti tapahtuu noudattaen lain väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista mukaista menettelytapaa. Tarkempi menettelytapa kuvataan kyseessä olevaa teknistä alustaa kuvaavassa varmennuskäytännössä.

Varmenteiden luomispalvelu: Varmenteiden luomispalvelussa luodaan ja allekirjoitetaan varmenteet, jotka perustuvat rekisteröintipalvelussa todennettuun henkilöllisyyteen ja muihin attribuutteihin.

Jakelupalvelu: Jakelupalvelun kautta varmenteet jaetaan allekirjoittajille sekä asetetaan varmenteeseen luottavien osapuolten saataville, jos allekirjoittajalta saadaan siihen lupa. Lisäksi palvelussa asetetaan varmentajan käyttöehdot sekä kaikki julkaistut varmennepolitiikkoja ja varmennuskäytäntöä koskevat tiedot tilaajien ja varmenteeseen luottavien osapuolten saataville. Väestörekisterikeskus toimittaa tiedot julkiseen hakemistoon. Hakemistopalvelu on julkinen Internet-palvelu, josta on saatavilla kaikki varmentajan myöntämät kansalaisvarmenteet sekä varmentajan varmenteet sekä sulkulista. Hakemistopalvelu on saatavissa osoitteesta ldap://ldap.fineid.fi.

Peruutustenhallintapalvelu: Peruutustenhallintapalvelu sulkee varmenteet, jotka varmenteen haltija haluaa suljettavaksi ennen varmenteen voimassaoloajan päättymistä.

- Peruutusten hallintapalvelussa käsitellään peruuttamispyynnöt ja -ilmoitukset, ja määritetään tarvittavat toimet käsittelyn perusteella. Palvelun tulokset jaetaan sulkulistan välityksellä.

Sulkutilasta tiedottava palvelu:

- Sulkutilasta tiedottavan palvelun kautta annetaan varmenteiden sulkutilatietoja varmenteeseen luottaville osapuolille. Palvelussa voidaan käyttää varmenteiden sulkulistoja tai reaaliaikaista yksittäisten tilatietojen välittämistä. Väestörekisterikeskus ilmoittaa tiedot sulkupalveluun varmenteeseen luottavien osapuolten saataville. Tilatietoja päivitetään tietyin väliajoin, joka on yksityiskohtaisesti kuvattu varmennuskäytäntöasiakirjassa.

Allekirjoituksen luomisvälineen tarjoaminen allekirjoittajalle:

- Allekirjoituksen lu omisväline valmistetaan ja toimitetaan allekirjoittajille. Toimikortin tai mikrosirun valmistaja ja yksilöijä toimii varmenteen, siihen liittyvien avainparien ja aktivointitietojen osalta varmentajan toimeksiannosta ja vastuulla ja yhteistyösopimuksen mukaisesti. Toimikortit ja mikrosirut yksilöidään rekisteröijän toimittamien tietojen mukaisesti.

  Käytetyn palvelujaottelun ainoa tarkoitus on selventää menettelytapavaatimuksia. Tässä kuvauksessa ei rajoiteta varmentajan palvelutoteutuksen jaottelua.

Varmenteeseen luottava osapuoli

- Varmenteeseen luottava osapuoli on henkilö tai organisaatio, joka luottaa varmenteen tietoihin ja joka käyttää varmennetta todentamiseen, tiedon salaukseen ja sähköiseen allekirjoitukseen. Varmenteeseen luottavan osapuolen on tarkastettava, että käytettävä varmenne on voimassa ja että varmenne ei ole sulkulistalla.

4.3. Varmennepolitiikka ja varmennuskäytäntö

Tässä kohdassa kuvataan varmennepolitiikan ja varmennuskäytännön välistä suhdetta. Varmennepolitiikan muotoa tai varmennuskäytännön erittelyjä koskevia rajoituksia ei sovelletan tässä luvussa.

4.3.1. Tarkoitus

Varmennepolitiikka, jonka tunnus ilmoitetaan varmenteessa, kertoo yleisellä tasolla varmennustoiminnan pääperiaatteet. Varmennuskäytännössä kerrotaan varmennetoiminnan, erityisesti luomisen ja ylläpitämisen osalta vaadittavat yksityiskohtaiset toteuttamiseen liittyvät käytännöt ja menetelmät sen osalta, kuinka varmennepolitiikassa esitetyt vaatimukset täytetään.

Tässä asiakirjassa määritetään varmennepolitiikka, joilla täytetään laatuvarmenteita koskevat, sähköisistä allekirjoituksista annetun direktiivin liitteissä I ja II säädetyn mukaiset vaatimukset. Varmentajana toimiva Väestörekisterikeskus määrittää varmennuskäytännöissään, kuinka nämä vaatimukset täytetään.

Väestörekisterikeskus noudattaa tätä varmennepolitiikkaa myöntäessään kansalaisvarmennteen. Varmenteen haltijoiden ja varmenteeseen luottavien osapuolien tulee toimia tämän varmennepolitiikan mukaisesti.

Tämän varmennepolitiikan mukaista kansalaisvarmennetta voidaan käyttää henkilön vahvaan sähköiseen tunnistamiseen, tiedon salaukseen ja sähköiseen allekirjoitukseen. Kansalaisvarmennetta voidaan käyttää käyttötarkoituksensa mukaisesti rajoituksitta sekä hallinnollisissa että yksityisten organisaatioiden 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.

Varmentajana toimiva Väestörekisterikeskus vaihtaa varmennepolitiikkaa koskevan yksilöivän tunnuksen, jos se muuttaa varmennepolitiikkaansa sovellettavuuden osalta.

4.3.2. Yksityiskohtaisuus

Varmennepolitiikka kuvaa varmentajan toiminnan yleiset vaatimukset. Varmennuskäytännössä kuvataan varmennepolitiikkaa yksityiskohtaisemmin menettelytavat, joita varmentaja toteuttaa varmenteiden myöntämisessä ja muussa hallinnoinnissa. Varmennuskäytännössä määritellään, kuinka varmentaja täyttää varmennepolitiikassa määritetyt tekniset sekä organisaatioon ja menettelyihin liittyvät vaatimukset.

Varmentajana toimiva Väestörekisterikeskus on laatinut sisäisten toimintojensa sekä ulkoistettujen toimintojensa ohjaamista varten asiakirjoja, jotka eivät ole julkisia.

Tämän varmennepolitiikan on rekisteröinyt Väestörekisterikeskus. Väestörekisterikeskus on julkista luottamusta nauttivaa valtakunnallista henkilörekisteriä ylläpitävä viranomainen, jonka väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain (661/2009) mukainen tehtävä on tuottaa varmennettuja sähköisen asioinnin palveluita.

4.3.3. Lähestymistapa

Varmennepolitiikka- ja varmennuskäytäntöasiakirjat on laadittu erilaisia käyttötarkoituksia varten. Varmennepolitiikka on yleiskuvaus varmentajan toiminnasta. Varmennuskäytäntö kuvaa varmentajan toiminnan yksityiskohdat organisaatiorakenteen, toimintatapojen, toimitilojen ja tietoteknisen ympäristön mukaisesti.

4.3.4. Muut varmentajan julkaisemat asiakirjat

Varmennepolitiikan ja varmennuskäytännön lisäksi varmentaja voi julkaista muita varmennetoimintaa ohjaavia asiakirjoja. Tällaisia asiakirjoja ovat muun muassa käyttöohjeet ja varmennetoiminnan yleisesitykset kuluttajia, asiakasorganisaatioita ja palvelunrakentajien tarpeita varten.

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

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

Varmennekuvaus on varmentajan käyttöehtojen osa, joka liittyy julkisen avaimen järjestelmän toimintaan. Varmentajana toimiva Väestörekisterikeskus julkaisee varmennekuvauksen sekä varmenteen hakijan että varmenteeseen luottavien osapuolien saataville.

4.4. Varmenteen hakija

Varmenteen hakija voi hakea varmennetta omissa nimissään tapahtuvaa käyttöä varten tai mahdollisesti yhteisön jäsenenä allekirjoittaessaan asiakirjoja yhteisön nimissä. Tämä ero on kuvattu tässä asiakirjassa silloin, kun sen erotteleminen on välttämätöntä. Varmennetta haettaessa kuitenkin tunnistetaan aina yksityinen henkilö henkilökohtaisella tavalla.

Kansalaisvarmenteen hakija on aina henkilökohtaisella tavalla tunnistettu yksityishenkilö.

5. Johdanto laatuvarmennepolitiikkoihin

5.1. Yleistä

Varmennepolitiikalla tarkoitetaan periaatteita, jotka osoittavat tietyn varmenteen soveltuvuuden tietylle yhteisölle. Varmennepolitiikassa on kuvattu myös yhteisesti sovellettavat turvallisuusvaatimukset.

Tässä asiakirjassa menettelytapavaatimukset määritellään varmennepolitiikkojen mukaan. Nämä varmennepolitiikat koskevat sähköisistä allekirjoituksista annetun direktiivin määrittelyjen mukaisia laatuvarmenteita, minkä vuoksi näitä asiakirjoja kutsutaan laatuvarmennepolitiikoiksi.

Tämän asiakirjan mukaisesti myönnetyt varmenteet sisältävät varmennepolitiikan OID-yksilöintitunnuksen, jonka avulla varmenteeseen luottavat osapuolet voivat määrittää varmenteen käyttökelpoisuuden ja luotettavuuden tiettyyn käyttötarkoitukseen. Tässä asiakirjassa määritetään kaksi laatuvarmennepolitiikkaa:

1) yleisölle myönnettäviä laatuvarmenteita koskeva laatuvarmennepolitiikka, jossa edellytetään turvallisten allekirjoituksen luomisvälineiden käyttöä

Tässä asiakirjassa yleisö-käsitteen tulkinta määräytyy tilanteeseen sovellettavan kansallisen lainsäädännön mukaan. Varmentaja voidaan katsoa yleisölle varmenteita myöntäväksi, jos kyseisten varmenteiden käyttöä ei ole rajoitettu osanottajien välisin vapaaehtoisin yksityisoikeudellisin sopimuksin.

2) yleisölle myönnettäviä laatuvarmenteita koskeva laatuvarmennepolitiikka.

Kohdassa 8 esitetään määrittelyn edellytykset muille laatuvarmennepolitiikoille, joilla tehostetaan tai rajoitetaan edellä mainittuja politiikkoja ja jotka mahdollisesti koskevat muille kuin yleisölle myönnettäviä laatuvarmenteita.

Tässä asiakirjassa käytettävät periaatteet on määritelty julkaisuissa RFC 3647 ja ANSI X9.79. Tässä asiakirjassa pyritään mahdollisimman suureen yhdenmukaisuuteen edellä mainittujen asiakirjojen periaatteiden ja vaatimusten kanssa.

Väestörekisterikeskus 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.

Tämän varmennepolitiikan nimi on Varmennepolitiikka Väestörekisterikeskuksen kansalaisvarmennetta varten, jonka OID on 1.2.246.517.1.10.22.

Tämä varmennepolitiikka viittaa varmentajan varmennepolitiikkaan, jonka OID on 1.2.246.517.1.10.1.

Väestörekisterikeskus noudattaa kansalaisvarmenteita myöntäessään yleisölle myönnettäviä laatuvarmenteita koskevaa laatuvarmennepolitiikkaa kohdan 5.2. b) QCP public mukaisesti OID: 0.4.0.1456.1.2

Sekä varmennepolitiikka että varmennuskäytäntö ovat saatavilla osoitteesta http://www.fineid.fi.

Tämän varmennepolitiikan on rekisteröinyt Väestörekisterikeskus. Se on henkilörekisteriä ylläpitävä viranomainen, jonka väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain (661/2009) mukainen tehtävä on tuottaa muiden tehtäviensä lisäksi varmennettuja sähköisen asioinnin palveluita. Väestörekisterikeskus vastaa tämän varmennepolitiikan hallinnoinnista ja päivityksistä.

Tätä varmennepolitiikkaa koskevat kysymykset lähetetään seuraavaan osoitteeseen:

Väestörekisterikeskus
PL 123 (Lintulahdenkuja 4)
00531 Helsinki
Y-tunnus: 0245437-2

vaestorekisterikeskus@vrk.fi
Puh. +358 295 535 001
Fax. +358 9 876 4369

Varmennepolitiikkaan liittyviin kysymyksiin sekä näihin asiakirjoihin liittyvästä viestinnästä vastaa Väestörekisterikeskuksen varmennehallinto-vastuualue.

Väestörekisterikeskus (VRK) Varmennepalvelut
PL 123
00531 Helsinki
www.fineid.fi

Väestörekisterikeskus omistaa kaikki kansalaisvarmenteisiin ja dokumentaatioon liittyvät tiedot teknisten toimitussopimusten mukaisesti. Väestörekisterikeskus omistaa täydet omistus- ja käyttöoikeudet tähän varmennepolitiikkaan.

5.2. Yksilöintitunnukset

Tässä asiakirjassa määriteltyjen laatuvarmennepolitiikkojen OID-yksilöintitunnukset ovat seuraavat:

a) **QCP public** + **SSCD.** Yleisölle myönnettäviä laatuvarmenteita koskeva laatuvarmennepolitiikka, joka edellyttää turvallisen allekirjoituksen luomisvälineen käyttöä.

itu-t(O) identified-organization(4) etsi(O) qualified-certificate-policies(1456) policy-identifiers(1) qcp-public-with-sscd (1)

b) **QCP public.** Yleisölle myönnettäviä laatuvarmenteita koskeva laatuvarmennepolitiikka.

itu-t(O) identified-organization(4) etsi(O) qualified-certificate-policies(1456) policy-identifiers(1) qcp-public (2)

Sisällyttämällä varmenteeseen jommankumman näistä OID-yksilöintitunnuksista varmentaja ilmaisee noudattavansa kyseistä laatuvarmennepolitiikkaa.

Väestörekisterikeskus noudattaa kansalaisvarmenteita myöntäessään yleisölle myönnettäviä laatuvarmenteita koskevaa laatuvarmennepolitiikkaa kohdan b) QCP public mukaisesti OID: 0.4.0.1456.1.2

Tämän varmennepolitiikan mukaisesti myönnetty allekirjoitusvarmenne täyttää Euroopan parlamentin ja neuvoston sähköisen allekirjoituksen direktiivin (1999/93/EC) laatuvarmenteelle asettamat vaatimukset.

Vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa (617/2009) on säädetty laatuvarmenteella tehdyistä sähköisistä allekirjoituksista. Sähköisestä henkilökortista on säädetty henkilökorttilaissa (829/1999) ja Väestörekisterikeskuksen myöntämistä varmenteista on säädetty väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetussa laissa (661/2009).

Tämä varmennepolitiikka astuu voimaan 7.3.2016. Varmennepolitiikan muutosmenettely ja julkaiseminen on kuvattu tämän asiakirjan kohdassa 8.5.

Julkaisun TS 101 862 -kohdassa 5.3 edellytetään, että julkaisun TS 101 862 - kohdan 5.2.1 mukainen lause esi4-qcStatement-1

- OLISI SISÄLLYTETTÄVÄ laatuvarmennelauseen laajennukseen silloin, kun laatuvarmenne on julkaisun TS 101 862 [6] mukainen ja myönnetty viimeistään 30.6.2005
- ON SISÄLLYTETTÄVÄ laatuvarmennelauseen laajennukseen silloin, kun laatuvarmenne on julkaisun TS 101 862 mukainen ja myönnetty 30.6.2005 jälkeen.

Varmentaja sisällyttää noudattamiensa laatuvarmennepolitiikkojen OID-yksilöintitunnukset myös varmenteen hakijoiden ja varmenteeseen luottavien osapuolten saataville asetettaviin käyttöehtoihin ja tällä tavoin ilmaisee noudattavansa kyseistä laatuvarmennepolitiikkaa.

5.3. Käyttäjäyhteisö ja sovellettavuus

5.3.1. QCP public + SSCD -laatuvarmennepolitiikka

QCP public + SSCD -laatuvarmennepolitiikka koskee varmenteita,

a) jotka täyttävät sähköisistä allekirjoituksista annetun direktiivin liitteessä I säädetyt vaatimukset
b) jotka myöntävä varmentaja täyttää sähköisistä allekirjoituksista annetun direktiivin liitteessä II säädetyt vaatimukset
c) joita saa käyttää vain sähköisistä allekirjoituksista annetun direktiivin liitteen III vaatimukset täyttävillä turvallisilla allekirjoituksen luomisvälineillä
d) joita myönnetään yleisölle.

Tämän laatuvarmennepolitiikan mukaisesti myönnettäviä laatuvarmenteita voi käyttää sellaisten sähköisten allekirjoitusten vahvistamisessa, jotka "täyttävät sähköisessä muodossa olevan tiedon osalta allekirjoitukselle asetettavat edellytykset samalla tavoin kuin käsin kirjoitettu allekirjoitus täyttää kyseiset vaatimukset paperilla olevan tiedon osalta", kuten sähköisistä allekirjoituksista annetun direktiivin 5.1 artiklassa säädetään.

5.3.2. QCP public -laatuvarmennepolitiikka

QCP public -laatuvarmennepolitiikka koskee varmenteita,

a) jotka täyttävät sähköisistä allekirjoituksista annetun direktiivin liitteessä I säädetyt vaatimukset
b) jotka myöntävä varmentaja täyttää sähköisistä allekirjoituksista annetun direktiivin liitteessä II säädetyt vaatimukset
c) joita myönnetään yleisölle.

Tämän laatuvarmennepolitiikan mukaisesti myönnettäviä laatuvarmenteita voi käyttää sellaisten sähköisten allekirjoitusten vahvistamisessa, joilta "ei evätä oikeudellista vaikutusta ja hyväksyttävyyttä todisteena oikeudellisissa menettelyissä", kuten sähköisistä allekirjoituksista annetun direktiivin 5.2 artiklassa säädetään.

5.4. Vaatimustenmukaisuus

5.4.1. Yleistä

Varmentajalla on oikeus käyttää edellä kohdassa 5.2 mainittua laatuvarmennepolitiikan yksilöintitunnusta vain,

a) jos varmentaja ilmaisee noudattavansa yksilöityä laatuvarmennepolitiikkaa ja asettaa pyynnöstä tilaajan ja varmenteeseen luottavien osapuolten saataville todisteita vaatimustenmukaisuudesta tai

b) jos pätevä ja riippumaton osapuoli on hiljattain arvioinut yksilöidyn laatuvarmennepolitiikan vaatimusten noudattamisen nykytilaa varmentajalla. Arviointitulokset on asetettava pyynnöstä tilaajien ja varmenteeseen luottavien osapuolten saataville. Tämä vaatimustenmukaisuuden arviointi on kuvattu CEN-työryhmän asiakirjassa CWA 14172 "EESSI Conformity Assessment Guidance".

c) jos myöhemmin osoitetaan, että varmentaja on laiminlyönyt varmennepolitiikan noudattamisen ja että tämä vaikuttaa merkittävästi sen kykyyn täyttää sähköisistä allekirjoituksista annetun direktiivissä määritellyt laatuvarmenteita koskevat vaatimukset, varmentajan on lopetettava kohdan 5.2 mukaisten yksilöintitunnusten sisältävien varmenteiden myöntäminen, kunnes se on osoittanut vaatimustenmukaisuutensa tai kunnes sen on arvioitu noudattavan kyseisen laatuvarmennepolitiikan vaatimuksia; muussa tapauksessa varmentajan on ryhdyttävä kohtuullisen ajan kuluessa toimenpiteisiin vaatimustenmukaisuutta koskevan laiminlyönnin korjaamiseksi.

   Vaatimustenmukaisuuden osoittamiseen vaadittavat keinot voivat vaihdella varmentajan sijoittautumisvaltion lainsäädännön mukaan. Varmentajan vaatimustenmukaisuus tarkistetaan säännöllisesti sekä aina, kun varmentajan toimintaa muutetaan merkittävästi.

5.4.2. QCP Public + SSCD -laatuvarmennepolitiikka

Vaatimusten mukaisen varmentajan on osoitettava, että

a) se täyttää sille kohdassa 6.1 määritellyt vaatimukset

b) se on ottanut käyttöön hallintakeinot, jotka täyttävät kaikki kohdassa 7 esitetyt vaatimukset.

5.4.3. QCP Public -laatuvarmennepolitiikka

Vaatimusten mukaisen varmentajan on osoitettava, että

a) se täyttää sille kohdassa 6.1 määritellyt vaatimukset

b) se on ottanut käyttöön hallintakeinot, jotka täyttävät kohdassa 7 esitetyt vaatimukset, lukuun ottamatta kohdassa 7.2.9 esitettyjä vaatimuksia sekä kohdan 6.2 alakohdissa e) ja f) määriteltyä varmenteen hakijan velvollisuutta.

6. Velvollisuudet ja vastuu sekä vastuunrajoitukset

Tämän kohdan vaatimuksia sovelletaan kumpaankin kohdassa 5 yksilöityyn laatuvarmennepolitiikkaan eli QCP public- ja QCP public +SSCD –laatuvarmennepolitiikkaan, ellei muuta mainita.

6.1. Varmentajan velvollisuudet

Varmentaja varmistaa, että kaikki varmentajalle kohdassa 7 asetetut, valittua laatuvarmennepolitiikkaa koskevat vaatimukset toteutetaan (katso kohdat 5.4.2, 5.4.3 ja 8.4).

Varmentaja on vastuussa laatuvarmennepolitiikassa määrättyjen menettelyjen noudattamisesta, vaikka varmentajan toimintaa toteutettaisiin toimeksiantosopimuksin.

Varmentaja tarjoaa kaikki varmennepalvelu osa-alueet varmennuskäytännössään mainitun mukaisesti.

Varmentajan velvollisuudet

Väestörekisterikeskuksella on lakiin perustuva 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 tai henkilöiden, kuten rekisteröijien ja kortinvalmistajien tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta.

Varmentaja laatii ja ylläpitää varmennepolitiikkaa, joka kuvaa kansalaisvarmenteen myöntämisessä, ylläpidossa ja hallinnoinnissa käytettävät menettelytavat, käyttöehdot, vastuiden jaot ja muut kansalaisvarmenteen käyttöön liittyvät näkökulmat yleisellä tasolla.

Varmentaja laatii ja ylläpitää varmennuskäytäntöjä, jotka kuvaavat, miten varmentaja soveltaa varmennepolitiikkaa.

Varmentaja noudattaa varmennepolitiikkaa ja varmennuskäytäntöä.

Varmentaja julkaisee varmennepolitiikan ja varmennuskäytännön yleisesti saataville.

Varmentaja pitää palveluksessaan riittävästi henkilökuntaa, jolla on varmennepalvelujen tuottamisen edellyttämä asiantuntemus, kokemus ja pätevyys.

Varmentaja käyttää luotettavia järjestelmiä ja tuotteita, jotka on suojattu oikeudettomalta käytöltä.

Varmentaja pitää yleisesti saatavilla kansalaisvarmennetta ja varmennetoimintaa koskevat tiedot, joiden perusteella varmentajan toiminta ja luotettavuus voidaan arvioida.

Varmentaja turvaa allekirjoituksen luomistietojen luottamuksellisuuden.

Varmentaja ei tallenna tai jäljennä allekirjoittajalle luovutettuja allekirjoituksen luomistietoja.

Rekisteröijää koskevat velvollisuudet

Rekisteröijä toimii varmentajan vastuulla ja lukuun sekä noudattaa varmentajan kanssa sovittuja rekisteröintiin liittyviä menettelytapoja.

Rekisteröijä noudattaa rekisteröinnin yhteydessä varmennepolitiikkaa ja varmennuskäytäntöä.

Rekisteröijä tunnistaa varmenteen hakijan henkilökohtaisesti ja luotettavasti varmennuskäytännössä kuvatulla tavalla siten, että hakijan henkilöllisyys ja muut varmenteen myöntämisessä tarpeelliset hakijan henkilöön liittyvät tiedot tulevat huolellisesti tarkastetuiksi.

Rekisteröijä huolehtii henkilötietojen huolellisesta käsittelystä ja luottamuksellisuudesta.

Rekisteröijä antaa varmenteen hakijalle tiedot varmenteen käyttöehdoista.

6.2. Varmenteen hakijan velvollisuudet

Varmentaja velvoittaa sopimuksella (katso kohdan 7.3.1 alakohta i) varmenteenhakijaa noudattamaan kaikkia seuraavassa mainittavia velvollisuuksia. Jos allekirjoittaja ja varmenteen hakija ovat eri tahoja, tilaajan on saatettava allekirjoittajan tietoon kaikki allekirjoittajaan sovellettavat velvollisuudet seuraavan luettelon mukaisesti:

a) Varmentajalle on annettava oikeat ja täydelliset tiedot laatuvarmennepolitiikan vaatimusten mukaisesti, etenkin rekisteröinnin yhteydessä.

b) Avainparia saa käyttää vain sähköisiin allekirjoituksiin ja mahdollisten muiden tilaajalle ilmoitettujen rajoitusten mukaisesti (katso kohta 7.3.4).

c) Varmenteen haltijan on toiminnassaan noudatettava erityistä huolellisuutta, jotta allekirjoittajan yksityistä avainta ei käytetä luvattomasti.

d) Jos varmenteenhakija luo allekirjoittajan avaimet:

   i) allekirjoittajan avaimet on luotava käyttämällä algoritmia, jonka on todettu soveltuvan sähköisiin laatuallekirjoituksiin

   ii) avainpituutena ja algoritmina on käytettävä yhdistelmää, jonka on todettu soveltuvan sähköisiin laatuallekirjoituksiin varmenteen voimassaolon ajan

   Algoritmeja ja niiden parametreja koskevat määritykset ja ohjeet on julkaistu asiakirjassa TS 102 176-1.

   iii) allekirjoittajan yksityinen avain voidaan pitää yksinomaan allekirjoittajan valvonnassa.

e) Jos varmennepolitiikassa edellytetään turvallisen allekirjoituksen luomisvälineen käyttöä (eli käytössä on QCP public + SSCD -laatuvarmennepolitiikka), varmennetta saa käyttää vain tällaisella välineellä luotujen sähköisten allekirjoitusten yhteydessä.

   Edellä kuvattu vaatimus ei koske QCP public -laatuvarmennepolitiikkaa.

f) Jos varmentaja on myöntänyt varmenteen QCP public + SSCD -laatuvarmennepolitiikan mukaisesti ja allekirjoittajan avaimet luodaan tilaajan tai allekirjoittajan valvonnassa, allekirjoittajan avaimet on luotava allekirjoittamiseen käytettävällä turvallisella allekirjoituksen luomisvälineellä.

   Edellä oleva vaatimus ei koske QCP public -laatuvarmennepolitiikkaa.

g) Varmentajalle on ilmoitettava ilman aiheetonta viivästystä, mikäli ennen varmenteessa ilmoitetun voimassaolon päättymistä tapahtuu jokin seuraavista:

   - allekirjoittajan yksityinen avain on kadonnut tai sen käyttö on mahdotonta (esimerkiksi siksi, että avaimen käyttöön tarvittava PIN-koodi on unohtunut), yksityinen avain on varastettu, se on mahdollisesti joutunut vääriin käsiin tai

- allekirjoittajan yksityisen avaimen käyttö ei ole enää hallittavissa, koska aktivointitiedot (esimerkiksi PIN-koodi) ovat joutuneet vääriin käsiin tai muista syistä, ja/tai

iii) varmenteen sisältö on tilaajalle tai allekirjoittajalle ilmoitettuun nähden virheellinen tai sitä on muutettu.

h) Jos allekirjoittajan yksityinen avain on joutunut vääriin käsiin, se peruutetaan välittömästi ja lopullisesti.

Jos tietoon tulee, että allekirjoittajan varmenteen myöntäneen varmentajan toiminta on vaarantunut, on varmistettava, että allekirjoittaja ei käytä varmennetta.

Väestörekisterikeskuksen myöntämän kansalaisvarmenteen käyttötarkoitus on määritelty kunkin varmennetyypin varmennepolitiikassa, varmennuskäytännössä sekä varmenteen haltijan käyttöohjeissa. Varmennetta saa käyttää vain sen käyttötarkoituksen mukaisesti sähköiseen allekirjoitukseen, todentamiseen tai tiedon salaamiseen

Kansalaisvarmenteen haltija vastaa siitä, että kansalaisvarmennetta haettaessa ilmoitetut tiedot ovat oikeita.

Kansalaisvarmenteen haltija on vastuussa kansalaisvarmenteen käytöstä, kansalaisvarmenteella tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista. Allekirjoitusvarmenteen osalta noudatetaan, mitä sähköisistä allekirjoituksista annetussa direktiivissä ja laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista on määrätty.

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

Kansalaisvarmennetta käsitellään ja suojataan noudattaen samaa huolellisuutta kuin muita vastaavia mikrosiruja, kortteja tai asiakirjoja, kuten esimerkiksi luottokortteja, ajokorttia ja passia. Henkilökohtaiset PIN-tunnukset on säilytettävä fyysisesti eri paikassa kuin kansalaisvarmenteen ja yksityiset avaimet sisältävä mikrosiru.

Mikrosirun ja kortin häviämisestä tai väärinkäytön mahdollisuudesta on ilmoitettava viipymättä varmentajalle soittamalla maksuttomaan sulkupalveluun +358 800 162 622.

6.3. Tiedottaminen varmenteeseen luottaville osapuolille

Varmenteeseen luottavien osapuolten saataville asetetuissa ohjeissa (katso kohta 7.3.4) on ilmoitettava, että varmenteeseen luottaminen perustellulla tavalla edellyttää, että osapuoli

a) todentaa varmenteeseen luottavalle osapuolelle osoitetun ajantasaisen sulkutilatiedon (katso kohta 7.3.4) avulla, onko varmenne voimassa tai onko se asetettu keskeytystilaan tai peruutettu. Varmentajan käytännöistä ja sulkutilatietojen jakelutavasta riippuen sulkutilatietojen jakelussa voi esiintyä viivettä, joka on enintään yksi (1) päivä.

b) ottaa huomioon mahdolliset varmenteen käytön rajoitukset, jotka tiedotetaan varmenteeseen luottavalle osapuolelle varmenteessa tai kohdan 7.3.4 mukaises-

ti toimitetuissa ehdoissa

c) noudattaa sopimuksissa tai muualla määrättyjä ehtoja

Sähköisistä allekirjoituksista annetun direktiivin 6 artiklaan perustuvaa, yleisölle laatuvarmenteita myöntävän varmentajan vastuuta sovelletaan osapuoliin, jotka "perustellulla tavalla tukeutuvat" varmenteeseen.

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

Varmenteeseen luottavan osapuolen velvollisuus on varmistaa, että varmennetta käytetään sen käyttötarkoituksen mukaisesti. Allekirjoitusvarmenteen käyttötarkoitus on sähköinen allekirjoitus. Todentamis- ja salausvarmenteen käyttötarkoitus on henkilön todentaminen ja tiedon salaus.

Varmenteeseen luottavan osapuolen on noudatettava varmennepolitiikkaa ja varmennuskäytäntöä.

Kansalaisvarmenteeseen luottava osapuoli voi vilpittömässä mielessä luottaa kansalaisvarmenteeseen, kun hän on tarkistanut, että **kansalaisvarmenne on voimassa ja että se ei ole sulkulistalla**. Kansalaisvarmenteeseen luottavalla osapuolella on velvollisuus tarkistaa varmenteet sulkulistalta. Kansalaisvarmenteen voimassaolon luotettavuuden varmistamiseksi kansalaisvarmenteeseen luottavan osapuolen on noudatettava alla esitettyjä sulkulistan tarkistustoimia.

Jos kansalaisvarmenteeseen luottava osapuoli kopioi sulkulistan hakemistosta, sen on varmistettava sulkulistan aitous tarkistamalla sulkulistan varmentajan sähköinen allekirjoitus. Lisäksi on tarkistettava sulkulistan voimassaoloaika.

Mikäli uusinta sulkulistaa ei voida saada hakemistosta laitteiston tai hakemistopalvelun toimintahäiriön vuoksi, kansalaisvarmennetta ei pidä hyväksyä, mikäli viimeisen saadun sulkulistan voimassaoloaika on päättynyt. Kaikki kansalaisvarmenteen hyväksymiset tämän voimassaoloajan jälkeen tapahtuvat kansalaisvarmenteeseen luottavan osapuolen omalla riskillä.

6.4. Vastuu

Yleisölle laatuvarmenteita myöntäviä varmentajia koskee sähköisistä allekirjoituksista annetun direktiivin 6 artiklassa ja laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista säädetyn mukainen vastuu. Vahvan sähköisen tunnistamisvälineen tai –palvelun tarjoavia palveluntarjoajia koskee laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista säädetyn mukainen vastuu.

Varmentajan vastuut

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

Väestörekisterikeskus vastaa siitä, että kansalaisvarmenne on luotu noudattaen väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetussa laissa, laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista, laissa sähköisestä asioinnista viranomaistoiminnassa ja varmennepolitiikassa sekä varmennuskäytännössä

esitettyjä menettelyjä ja varmenteen hakijan antamien tietojen mukaisesti. Väestörekisterikeskus vastaa ainoastaan niistä tiedoista, jotka se on tallettanut kansalaisvarmenteeseen.

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

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

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

Rekisteröijän vastuut

Kansalaisvarmenteen rekisteröijänä toimii rekisteröintipiste, joka rekisteröi varmenteen hakijan varmentajana toimivan Väestörekisterikeskuksen lukuun ja vastuulla. Rekisteröinnin osalta noudatetaan väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain ja vahvasta sähköisestä tunnistamisesta ja sähköisen allekirjoituslain vaatimuksia sekä henkilökorttilain vaatimuksia silloin, kun kansalaisvarmenne on henkilökortilla.

Kansalaisvarmenteen haltijan vastuut

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

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

Mikrosirun sisältävän kortin jättäminen lukijalaitteeseen saattaa mahdollistaa kansalaisvarmenteen väärinkäytön. Lopettaessaan pääteistunnon tai jättäessään päätelaitteen valvomatta kansalaisvarmenteen haltijan vastuulla on poistaa kansalaisvarmenteen sisältävä mikrosiru lukijalaitteesta ja sulkea käytetyt sovellukset asianmukaisesti tai muuten katkaistava kansalaisvarmenteen käyttämiseksi tarvittava tekninen yhteys.

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

Kansalaisvarmenteeseen luottavan osapuolen vastuut

Kansalaisvarmenteeseen luottava osapuoli ei voi luottaa siihen ja sähköisen allekirjoituksen oikeellisuuteen vilpittömässä mielessä, mikäli kansalaisvarmenteen voimassaoloa ei ole tarkastettu sulkulistalta. Kansalaisvarmenteen hyväksyminen mainitussa tapauksessa vapauttaa Väestörekisterikeskuksen vastuusta. Kansalaisvarmenteeseen luottavan osapuolen on tarkistettava, että myönnetty varmenne vastaa käyttötarkoitustaan siinä oikeustoimessa, jossa sitä on käytetty.

Vastuiden rajoitukset

Väestörekisterikeskus ei vastaa PIN-tunnusten, PUK-koodin ja kansalaisvarmenteen haltijan yksityisten avainten paljastumisen seurauksena syntyvistä vahingoista, ellei paljastuminen välittömästi johdu Väestörekisterikeskuksen välittömästä toiminnasta.

Väestörekisterikeskus vastaa kansalaisvarmenteen haltijalle ja kansalaisvarmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Väestörekisterikeskuksen välittömästä toiminnasta.

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

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

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

Varmentajalla on oikeus kehittää edelleen varmennepalvelua. Kansalaisvarmenteen haltijan tai kansalaisvarmenteeseen luottavan osapuolen on vastattava tämän vuoksi aiheutuvista omista kustannuksistaan eikä varmentaja ole velvollinen korvaamaan kansalaisvarmenteen haltijalle tai kansalaisvarmenteeseen luottavalle osapuolelle tällaisesta varmentajan kehittämistyöstä aiheutuvista kustannuksista.

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

Muut osapuolet

Kansalaisvarmenteeseen luottava osapuoli voi luottaa kansalaisvarmenteen ja sähköisen allekirjoituksen oikeellisuuteen, jos hän on tarkastanut, ettei kansalaisvarmennetta ole asetettu sulkulistalle eikä varmenteen voimassaoloaika ole päättynyt eikä hänellä ole muita syitä perustellusti epäillä varmenteen käytön oikeellisuutta.

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

Varmennepalveluiden tuottamiseen liittyvä Väestörekisterikeskuksen vahingonkorvausvastuu määräytyy varmenteen hakijan kanssa tehdyn palvelusopimuksen ja vahingonkorvauslain (412/1974) säännösten mukaisesti. Väestörekisterikeskusta koskevat myös vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain ja sähköisestä asioinnista viranomaistoiminnasta annetun lain mukaiset varmentajan vastuut.

Väestörekisterikeskus vastaa kansalaisvarmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Väestörekisterikeskuksen toiminnasta.

7. Varmentajan toimintaa koskevat vaatimukset

Tätä kohtaa sovelletaan kumpaankin kohdassa 5 yksilöityyn laatuvarmennepolitiikkaan eli QCP public- ja QCP public + SSCD -laatuvarmennepolitiikkaan, ellei muuta mainita.

Varmentajan toteuttaa seuraavat vaatimukset täyttävät hallintakeinot.

Tämä asiakirja koskee laatuvarmenteita myöntävänä varmentajana toimivaa Väestörekisterikeskusta. Tässä asiakirjassa kuvatun palvelun toteuttamiseen sisältyy rekisteröintipalvelujen tarjoaminen, varmenteiden luominen, varmenteiden jakelu, varmenteiden peruuttamisen hallinta ja sulkutilasta tiedottaminen (kohta 4.2). Jos vaatimus liittyy varmentajan tiettyyn palvelualueeseen, se kuvataan vastaavien alaotsikoiden alla. Mikäli seuraavassa ei yksilöidä 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. Kunkin hallintatavoitteen jälkeen annetaan viite sähköisistä allekirjoituksista annetussa direktiivissä asiasta esitettyyn vaatimukseen.

7.1. Varmennuskäytäntö

Varmentaja varmistaa, että se osoittaa varmennepalvelujen tarjoamisen edellyttämän luotettavuuden, joka on kuvattu sähköisistä allekirjoituksista annetun direktiivin liitteen II kohdassa (a).

Erityisesti:

a) Varmentaja laatii julkilausuma käytännöistä ja menettelyistä, joita käytetään laatuvarmennepolitiikassa yksilöityjen vaatimusten täyttämiseksi. Tässä varmennepolitiikassa ei aseteta varmennuskäytännön rakenteelle mitään vaatimuksia.

b) Varmentajan varmennuskäytännössä yksilöidään varmentajan palvelujen tukena käytettävien kaikkien ulkoisten organisaatioiden velvollisuudet, myös sovellettavat toimintapolitiikat ja -käytännöt.

c) Varmentaja asettaa varmenteen hakijoiden ja varmenteeseen luottavien osapuolten saataville varmennuskäytäntö sekä muu aineisto, jota laatuvarmennepolitiikan vaatimustenmukaisuuden arviointi edellyttää.

Varmentajan ei ole julkaistava toimintansa kaikkia yksityiskohtia.

d) Varmentaja antaa tiedoksi kaikille tilaajille ja mahdollisille varmenteeseen luottaville osapuolille varmenteen käyttöä koskevat ehdot kohdan 7.3.4 mukaisesti.

e) Varmentajalla on organisaatiossaan johtava taho, jolla on varmennuskäytännön hyväksymisessä lopullinen toimivalta ja vastuu.

f) Varmentajan johdon vastuulla on varmistaa, että tässä asiakirjassa määriteltyjen sovellettavien vaatimusten saavuttamiseksi laadittuja varmennuskäytäntöjä toteutetaan asianmukaisesti.

g) Varmentaja määrittelee varmennuskäytäntöjen tarkistusprosessin, joka sisältää varmennuskäytännön ylläpitovastuut.

h) Varmentaja antaa asianmukaisesti ilmoituksen muutoksista, joita se aikoo tehdä varmennuskäytäntöönsä, ja sen on edellä olevan kohdan e mukaisen hyväksynnän mukaisesti asetettava tarkistettu varmennuskäytäntö saataville edellä olevan kohdan c mukaisesti.

i) Varmentaja dokumentoi allekirjoittamisessa käytettävät algoritmit ja parametrit.

Tässä asiakirjassa kuvattuihin toimenpiteisiin liittyvä yksityiskohtainen menettely on kuvattu jokaista varmennetyyppiä ja tallennusalustaa koskevassa varmennuskäytännössä.

7.2. Julkisen avaimen järjestelmässä käytettävien avainten elinkaaren hallinta

7.2.1. Varmentajan avaimen luominen

Varmenteiden luominen

Varmentaja varmistaa, että varmentajan avaimet luodaan turvallisissa olosuhteissa, jotka on kuvattu sähköisistä allekirjoituksista annetun direktiivin II liitteen kohdissa f ja g.

Erityisesti:

a) Varmentajan avaimet luodaan fyysisesti turvallisessa ympäristössä (kohta 7.4.4) ja luomisen toteuttaa luotetuissa rooleissa toimiva henkilöstö (kohta 7.4.3) vähintään kahdelle eri henkilölle hajautetussa valvonnassa. Tähän tehtävään valtuutetun henkilöstön määrä pidetään mahdollisimman pienenä ja varmentajan käytäntöjen mukaisena.

b) Varmentajan avaimet luodaan välineellä, joka

- täyttää julkaisussa FIPS 140-2 yksilöidyt vaatimukset vähintään tasolla 3 tai
- täyttää jossakin seuraavista CEN-työryhmän sopimuksista (CWA) yksilöidyt vaatimukset: CEN Workshop Agreement 14167-2, CWA 14167-3 tai CWA 14167-4, tai
- on luotettava järjestelmä, jonka arvioinnin vakuuttavuustasoksi on luokiteltu ISO/IEC 15408 -standardin mukaisesti vähintään EAL 4 tai joka täyttää vastaavat turvallisuusehdot. Järjestelmän oman turvatavoitteen tai suojaprofiilin on oltava tämän asiakirjan vaatimusten mukainen, perustuttava riskianalyysiin ja sisällettävä sekä fyysiset että muut kuin tekniset turvatoimet.

Kohdan 7.2.2 alakohtien b–e sääntöjä sovelletaan avainten luomiseen myös silloin, kun se toteutetaan erillisessä järjestelmässä.

c) Varmentajan avainten luomisessa käytetään algoritmia, jonka on todettu soveltuvan laatuvarmenteisiin.

d) Varmentajan allekirjoitusavaimen avainpituuden ja algoritmin yhdistelmäksi valitaan

yhdistelmä, jonka on todettu soveltuvan sellaisiin laatuvarmenteisiin, joita varmentaja myöntää.

Algoritmeja ja niiden parametreja koskevat määritykset on julkaistu asiakirjassa TS 102 176-1.

Varmentaja luo tarkoituksenmukaisen ajan ennen varmentajan allekirjoitusavaimen voimassaolon päättymistä (esimerkiksi varmentajan varmenteessa ilmoitettuna ajankohtana) uuden avainparin varmenteen allekirjoittamiseen ja tekee kaikki tarpeelliset toimet, ettei kyseiseen varmentajan avaimeen mahdollisesti luottavien yhteisöjen toimintaan aiheutuisi häiriöitä. Uusi varmentajan avain luodaan ja sen jakelu on toteutetaan näiden menettelytapojen mukaisesti.

Nämä toimet tehdään riittävän ajoissa, jotta kaikki varmentajaan jossakin suhteessa toimivat osapuolet (allekirjoittajat, varmenteen hakijat, varmenteeseen luottavat osapuolet, ylemmällä tasolla toimivat varmentajat) saavat ajoissa tiedon varmentajan avainparin vaihtamisesta ja jotta ne voivat toteuttaa toiminnan häiriöttömän jatkumisen kannalta tarvittavat toimet. Tämä ei koske varmentajaa, joka lopettaa toimintansa ennen sen oman varmentajan varmenteen viimeistä voimassaolopäivää.

7.2.2. Varmentajan avaimen tallennus, varmuuskopiointi, ja palauttaminen

Varmenteiden luominen

Varmentaja varmistaa, että varmentajan yksityisten avainten luottamuksellisuus ja eheys säilyvät sähköisistä allekirjoituksista annetun direktiivin II liitteen kohtien f ja g mukaisesti.

Erityisesti:

a) varmentajan yksityistä allekirjoitusavainta säilytetään ja käytetään turvallisella salausvälineellä, joka
   - täyttää julkaisussa FIPS 140-2 yksilöidyt vaatimukset vähintään tasolla 3 tai
   - täyttää jossakin seuraavista CEN-työryhmän sopimuksista (CWA) yksilöidyt vaatimukset: CEN Workshop Agreement 14167-2, CWA 14167-3 tai CWA 14167-4, tai
   - on luotettava järjestelmä, jonka arvioinnin vakuuttavuustasoksi on luokiteltu ISO/IEC 15408 -standardin mukaisesti vähintään EAL 4 tai joka täyttää vastaavat turvallisuusehdot. Järjestelmän oman turvatavoitteen tai suojaprofiilin on oltava tämän asiakirjan vaatimusten mukainen, perustuttava riskianalyysiin ja sisällettävä sekä fyysiset että muut kuin tekniset turvatoimet.

b) Turvallisen salausvälineen ulkopuolella (kohta a) varmentajan yksityinen allekirjoitusavain suojataan turvallisen salausvälineen suojaustasoa vastaavasti.

c) Varmentajan yksityisen allekirjoitusavaimen varmuuskopioinnin, tallentamisen ja palauttamisen saa tehdä ainoastaan luotetuissa rooleissa toimiva henkilöstö, joka käyttää vähintään kahdelle eri henkilölle hajautettua valvontaa. Nämä toimet tehdään fyysisesti turvallisessa ympäristössä (kohta 7.4.4). Tähän tehtävään valtuutetun henkilöstön määrä pidetään mahdollisimman pienenä ja varmentajan käytäntöjen

mukaisena.

d) Varmentajan yksityisten allekirjoitusavainten varmuuskopioiden osalta käytetään samoja tai tiukempia turvallisuuden hallintakeinoja kuin nykykäytössä olevien avainten osalta.

e) Kun avaimet tallennetaan avainten käsittelyyn varattuun laitteistoyksikköön, pääsynvalvontakeinoilla varmistetaan, ettei avaimiin ole pääsyä laitteistoyksikön ulkopuolelta.

Väestörekisterikeskus luo yksityiset allekirjoitusavaimensa ja yksityisiä allekirjoitusavaimiaan vastaavat julkiset avaimet.

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

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

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

Väestörekisterikeskuksen kansalaisvarmenteessa olevista yksityisistä avaimista ei luoda kopiota.

7.2.3. Varmentajan julkisen avaimen jakelu

Varmenteiden luominen ja jakelu

Varmentaja varmistaa, että allekirjoituksen todentamiseen käytettävän varmentajan (julkisen) avaimen sekä siihen liittyvien parametrien eheys ja aitous säilyvät varmenteeseen luottaville osapuolille jakelun aikana sähköisistä allekirjoituksista annetun direktiivin II liitteen kohtien f ja g mukaisesti.

Erityisesti:

a) Allekirjoitusten todentamiseen käytettävät varmentajan (julkiset) avaimet asetetaan varmenteeseen luottavien osapuolten saataville siten, että varmistetaan varmentajan julkisen avaimen eheys ja todennetaan avaimen aitous.

   Varmentajan julkisia avaimia voidaan jakaa varmentajan itse allekirjoittamissa varmenteissa, kun mukana on vakuutus siitä, että avain todentaa varmentajan, tai niitä voidaan jakaa toisen varmentajan myöntämissä varmenteissa. Itse allekirjoitetusta varmenteesta ei voida tietää, tuleeko se varmentajalta. Tällöin kyseisen varmenteen oikeellisuuden varmistamiseen tarvitaan lisätoimia, kuten varmenteen sormenjäljen vertaamista luotettavasta lähteestä toimitettuun tietoon.

   Kansalaisvarmenteen luomisen yhteydessä mikrosirun julkisia avaimia käyttäen suoritetaan varmenteen luontipyyntö, jossa varmenteen hakijan rekisteröintitiedot yhdistetään kyseessä olevaan julkiseen avaimeen.

   Kansalaisvarmentajan julkinen avain on osa varmentajan varmennetta. Kansalaisvarmenne sisältää varmenteen haltijan julkisen avaimen.

Varmentajan varmenne on saatavilla julkisessa hakemistossa. Jos kansalaisvarmenne sijaitsee toimikortilla, varmentajan varmenne sijoitetaan myös toimikortin mikrosirulle.

Varmentajan varmenne sisältää varmentajan julkisen avaimen. Varmentajan varmenne talletetaan julkiseen hakemistoon. Varmenteen haltijan varmenne talletetaan niin ikään julkiseen hakemistoon. Varmentajan varmenne on saatavilla varmentajan julkisesta hakemistosta sekä varmentajan www-sivuilta.

Varmentaja arkistoi kaikki varmentamansa julkiset avaimet.

7.2.4. Vara-avainjärjestelmä

Allekirjoittajan yksityisiä allekirjoitusavaimia ei säilytetä tavalla, joka mahdollistaa salauksen purun ja varmuuskopioinnin, jolloin valtuutetut tahot voisivat tietyissä tilanteissa purkaa salauksen hyödyntämällä yhden tai useamman osapuolen antamia tietoja (yleisesti tätä kutsutaan vara-avainjärjestelmäksi) sähköisistä allekirjoituksista annetun direktiivin II liitteen kohdan j mukaisesti.

Väestörekisterikeskuksen kansalaisvarmenteessa olevista yksityisistä avaimista ei luoda kopiota.

7.2.5. Varmentajan avaimen käyttö

Varmentajan vastaa siitä, että varmentajan yksityisiä allekirjoitusavaimia käytetään ainoastaan käyttötarkoituksensa mukaisesti. Erityisesti:

Varmenteiden luominen

a) Varmenteiden luomiseen käytettäviä, kohdassa 7.3.3 mainitun mukaisia varmentajan allekirjoitusavaimia voi käyttää myös muuntyyppisten varmenteiden ja sulkutilatietojen allekirjoittamiseen, kunhan noudatetaan kohtien 7.2.1–7.2.3, 7.2.5–7.2.7 ja 7.4 mukaisia varmentajan toimintaympäristöä koskevia toimintavaatimuksia.

b) Varmenteen allekirjoitusavaimia saa käyttää vain fyysisesti turvallisissa tiloissa.

Varmentajan varmenne:

Käyttötarkoitus: Varmenteiden ja sulkulistojen allekirjoitus. Tekninen kuvaus on FINEID S2 -määrityksissä.

7.2.6. Varmentajan avaimen elinkaaren päättyminen

Varmentajan varmistaa, ettei varmentajan yksityisiä allekirjoitusavaimia käytetä niiden elinkaaren päättymisen jälkeen sähköisistä allekirjoituksista annetun direktiivin II liitteen kohtien f ja g mukaisesti.

Erityisesti:

Varmenteiden luominen

a) Kaikki varmentajan yksityisten allekirjoitusavainten kopiot tuhotaan tai tehdään käyttökelvottomiksi.

7.2.7. Varmenteiden allekirjoittamisessa käytettävän salauslaitteiston elinkaaren hallinta

Varmentaja varmistaa salauslaitteiston turvallisuuden koko sen elinkaaren ajan jälkeen sähköisistä allekirjoituksista annetun direktiivin II liitteen f -kohdan mukaisesti.

Varmenteiden luominen

Erityisesti varmentaja varmistaa, että

a) varmenteita ja sulkutilatietoja allekirjoittavaan salauslaitteistoon ei päästä kajoamaan kuljetuksen aikana

b) varmenteita ja sulkutilatietoja allekirjoittavaan salauslaitteistoon ei päästä kajoamaan säilytyksen aikana
c) varmentajan allekirjoitusavainten asennus, aktivointi, varmuuskopiointi ja palauttaminen salauslaitteistossa edellyttävät aina vähintään kahden luotetun työntekijän yhtäaikaista valvontaa

d) varmenteita ja sulkutilatietoja allekirjoittava salauslaitteisto toimii asianmukaisesti

e) varmentajan salauslaitteistoon tallennetut varmentajan yksityiset allekirjoitusavaimet tuhotaan, kun väline poistetaan käytöstä.

7.2.8. Varmentajan tarjoamat allekirjoittajan avaimen hallintapalvelut

Varmentaja varmistaa, että kaikki sen luomat allekirjoittajan avaimet luodaan turvallisesti ja että allekirjoittajan yksityisen avaimen luottamuksellisuus on turvattu sähköisistä allekirjoituksista annetun direktiivin II liitteen kohtien f ja j mukaisesti.

Varmenteiden luominen

Jos varmentaja luo allekirjoittajan avaimet,

varmentajan luomat allekirjoittajan avaimet on luotava käyttämällä sellaista algoritmia, jonka on todettu soveltuvan sähköisiin laatuallekirjoituksiin varmenteen voimassaolon ajan

varmentajan luomien allekirjoittajan avainten avainpituuden sekä avainten yhteydessä käytettävän julkisen avaimen algoritmin on oltava todetusti sähköisiin laatuallekirjoituksiin soveltuvia varmenteen voimassaolon ajan

Algoritmeja ja niiden parametreja koskevat ohjeet on julkaistu asiakirjassa TS 102 176-1.

c) varmentajan luomat allekirjoittajan avaimet luodaan ja tallennetaan turvallisesti ennen kuin ne toimitetaan allekirjoittajalle
d) allekirjoittajan yksityinen avain toimitetaan allekirjoittajalle tarvittaessa tilaajan kautta siten, että avaimen luottamuksellisuus ja eheys eivät vaarannu ja jotta allekirjoittajalle toimittamisen jälkeen yksityinen avain voi säilyä allekirjoittajan yksinomaisessa hallinnassa

e) allekirjoittajalle toimittamisen jälkeen kaikki varmentajan hallussa mahdollisesti olevat allekirjoittajan yksityisen avaimen kopiot on tuhottava.

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

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

Varmenteen tietosisällössä käyttötarkoituksen määräävä kenttä määrittelee varmenteisiin liittyvän avaimen käyttötarkoituksen. Avaimen käyttö rajataan käytettäväksi vain ilmoitettuun käyttötarkoitukseensa.

Varmentajan varmenne:

Käyttötarkoitus: Varmenteiden ja sulkulistojen allekirjoitus. Tekninen kuvaus on FINEID S2 -määrityksissä.

Varmenteen haltijan todentamis- ja salausvarmenne:

Käyttötarkoitus: Sähköisen henkilöllisyyden todentaminen tai tiedon salaus.

Varmenteen haltijan allekirjoitusvarmenne:

Käyttötarkoitus: Sähköinen allekirjoitus

7.2.9. Turvallisen allekirjoituksen luomisvälineen valmistaminen

Tätä kohtaa ei sovelleta QCP public -laatuvarmennepolitiikkaan.

Jos varmentaja myöntää turvallisia allekirjoituksen luomisvälineitä (SSCD), varmentajan on varmistettava sen turvallinen toteuttaminen sähköisistä allekirjoituksista annetun direktiivin III liitteen mukaisesti.

Välineen tarjoaminen allekirjoittajalle

Erityisesti jos varmentaja myöntää turvallisen allekirjoituksen luomisvälineen,

a) palveluntarjoajan on valvottava turvallisesti kyseisen turvallisen allekirjoituksen luomisvälineen valmistamista
b) turvallinen allekirjoituksen luomisväline on tallennettava ja jaeltava turvallisesti
c) turvallisen allekirjoituksen luomisvälineen käytöstä poistamista ja uudelleen käyttöön ottamista on valvottava turvallisesti
d) jos turvalliseen allekirjoitusvälineeseen liittyy käyttäjän aktivointitietoja (esimerkiksi PIN-koodi), aktivointitiedot on laadittava turvallisesti ja jaeltava turvallisesta allekirjoituksen luomisvälineestä erillisenä.

Erillisyys voidaan saada aikaan varmistamalla, että aktivointitietojen jakelu ja turvallisen allekirjoituksen luomisvälineen toimittaminen tapahtuvat eri aikoina tai eri reittejä.

Turvallisen allekirjoituksen luomisvälineen valmistamista koskevat edellä luetellut vaatimukset voidaan täyttää esimerkiksi käyttämällä soveltuvaa suojausprofiilia, joka on määritelty ISO/IEC 15408 -standardin mukaisesti tai vastaavasti.

7.3. Julkisen avaimen järjestelmässä käytettävien varmenteiden elinkaaren hallinta

7.3.1. Allekirjoittajan rekisteröinti

Varmentaja varmistaa, että allekirjoittajat tunnistetaan ja todennetaan asianmukaisesti ja että allekirjoittajan varmennepyynnöt ovat virheettömiä, paikkansapitäviä ja jotka perustuvat asianmukaiseen valtuutukseen sähköisistä allekirjoituksista annetun direktiivin II liitteen d-kohdan mukaisesti.

Erityisesti:

Rekisteröinti

Rekisteröinnissä allekirjoittaja tunnistetaan henkilöksi, johon liittyy tiettyjä attribuutteja. Attribuutit ovat erityismääreitä, jotka voivat ilmaista esimerkiksi henkilöön liittyvän organisaation tai roolin.

a) Ennen kuin varmentaja muodostaa sopimussuhteeseen tilaajan kanssa, varmentajan on ilmoitettava tilaajalle varmenteen käytön ehdoista ja vaatimuksista kohdan 7.3.4 mukaisesti, joka on kuvattu sähköisistä allekirjoituksista annetun direktiivin II liitteen kohdassa k.

b) Varmentaja ilmoitettaa nämä tiedot muuttamattomana viestinä ja ymmärrettävällä kielellä. Tiedot voidaan välittää sähköisesti.

c) Palveluntarjoaja toteaa rekisteröinnin yhteydessä tarkoituksenmukaisin keinoin kansallisen lainsäädännön mukaisesti sen henkilön henkilöllisyys, ja tarvittaessa tietyt attribuutit, jolle laatuvarmenne myönnetään. Henkilöllisyys tarkistetaan vertaamalla suoraan fyysiseen henkilöön tai on turvauduttava välillisesti tehtyyn tarkistukseen, jonka tarkistuskeinoilla henkilöllisyys on voitu varmistaa vastaavasti kuin fyysisen läsnäolon perusteella (katso huomautus 3). Henkilöllisyyttä osoittavat asiakirjat voidaan toimittaa paperisina tai sähköisinä asiakirjoina.

   Attribuuttivarmenteet eivät kuulu tämän asiakirjan soveltamisalan piiriin, koska ne eivät sisällä julkisia allekirjoitusavaimia.

d) Jos allekirjoittaja on henkilö, seuraavat henkilötiedot on esitettävä on esitettävä:

   - koko nimi (sukunimi ja etunimet sovellettavan lainsäädännön ja kansallisten tunnistuskäytäntöjen mukaisesti)
   - syntymäaika ja -paikka, kansallinen henkilötunnus henkilötunnus, tai muita attribuutteja, joilla voidaan mahdollisimman pitkälle erottaa henkilö muista samannimisistä henkilöistä.

Varmentaja on vastuussa siitä, että kaikki varmenteen sisältämät tiedot ovat oikeita.

e) Jos allekirjoittaja on henkilö, joka tunnistetaan oikeushenkilön tai muun organisaatioyksikön yhteydessä, seuraavista tiedoista on esitettävä selvitys:

- allekirjoittajan koko nimi (sukunimi ja etunimet)
- allekirjoittajan syntymäaika ja -paikka, kansallisesti tunnustettu henkilötunnus, tai muita attribuutteja, joilla voidaan mahdollisimman pitkälle erottaa henkilö muista samannimisistä henkilöistä
- asiaan liittyvän oikeushenkilön tai muun organisaatioyksikön koko nimi ja oikeusasema
- asiaan liittyvää oikeushenkilöä tai muuta organisaatioyksikköä koskevat olennaiset nykyiset rekisteröintitiedot (esimerkiksi yrityksen rekisteröinti)
- selvitys siitä, että allekirjoittaja liittyy oikeushenkilöön tai muuhun organisaatioyksikköön.

f) Varmentaja säilyttää kaikki allekirjoittajan henkilöllisyyden todentamisessa käytetyt tiedot ja mahdollisesti asiaa koskevat tietyt attribuutit, kuten todentamisessa käytettyjen asiakirjojen viitenumerot, sekä niiden mahdolliset voimassaolorajoitukset.

Jos muu taho kuin allekirjoittaja tilaa varmentajan palvelut (eli tilaaja ja allekirjoittaja ovat eri osapuolia – katso kohta 4.4), on esitettävä todisteet siitä, että tilaaja on valtuutettu toimimaan allekirjoittajan puolesta määritellyn mukaisesti (esimerkiksi valtuutettu toimimaan kaikkien yksilöidyn organisaation jäsenten puolesta).

h) Tilaajan on esitettävä käyntiosoite tai muita attribuutteja, joilla kuvataan, miten tilaajaan saa yhteyden.

i) Varmentaja säilyttää tilaajan kanssa allekirjoitetun sopimuksen, joka sisältää

- tilaajan velvollisuuksien hyväksymisen (kohta 6.2)
- varmentajan niin edellyttäessä suostumuksen turvallisen allekirjoituksen luomisvälineen käyttämiseen

  Edellä olevaa kohtaa ei sovelleta QCP Public -laatuvarmennepolitiikkaan.

- suostumuksen siihen, että varmentaja säilyttää tiedot, joita on käytetty rekisteröinnissä (katso kohdan 7.4.11 alakohdat h, i ja j), välineen toimittamisessa allekirjoittajalle (kohdan 7.4.11 alakohdat m ja n), varmenteen mahdollisessa myöhemmässä peruuttamisessa (kohdan 7.4.11 alakohta o) sekä varmenteeseen sisältyvät tiedot henkilön henkilöllisyydestä ja häneen liittyvistä tietyistä attribuuteista, ja että kyseiset tiedot saa välittää kolmansille osapuolille kyseessä olevan varmennepolitiikan mukaisin ehdoin, mikäli varmentaja lopettaa palvelunsa
- tiedon siitä, edellyttääkö tilaaja varmenteen julkaisemista ja millaisin ehdoin, sekä suostuuko allekirjoittaja siihen

- vakuutuksen siitä, että varmenteen sisältämät tiedot ovat virheettömät.

Tilaaja ja allekirjoittaja voivat hyväksyä tämän sopimuksen eri kohtia rekisteröinnin eri vaiheiden aikana. Esimerkiksi sen hyväksyntä, ovatko varmenteen sisältämät tiedot virheettömät, voidaan antaa muiden hyväksyntää edellyttävien kohtien jälkeen.

Tämän sopimuksen muodostamiseen voi osallistua muita osapuolia (esimerkiksi asiaan liittyvä oikeushenkilö). Tämä sopimus voi olla sähköisessä muodossa.

Edellä yksilöidyt tiedot on säilytettävä tilaajalle ilmoitettua vastaavan ajan (katso edellä olevat kohdat a ja b) sekä varmennuksesta oikeudellisissa menettelyissä edellytettävien todisteiden esittämistä varten sovellettavan lainsäädännön mukaisesti.

Kun määritellään "sovellettavaa lainsäädäntöä", on otettava huomioon seuraavat seikat:

i) Varmentajan sijoittautumisvaltion lainsäädäntö on aina otettava huomioon.

ii) Jos allekirjoittajat ovat rekisteröityneet muussa kuin varmentajan sijoittautumisvaltiossa sijaitsevan rekisteröijän kautta, kyseisen rekisteröijän on noudatettava myös oman valtionsa säädöksiä ja määräyksiä.

iii) Jos lisäksi jotkin tilaajat sijaitsevat toisessa valtiossa, on otettava huomioon myös tällaisia tilaajia koskevat sopimuksiin ja lainsäädäntöön perustuvat vaatimukset.

k) Jos varmentaja ei luo allekirjoittajan avainparia, varmennepyyntöprosessissa on varmistettava, että allekirjoittajan hallussa on varmentamisen yhteydessä esitettävään julkiseen avaimeen liittyvä yksityinen avain.

1) Jos varmentaja ei luo allekirjoittajan avainparia ja varmennepolitiikka edellyttää turvallisen allekirjoituksen luomisvälineen käyttöä, (QCP public + SSCD - laatuvarmennepolitiikka), varmennepyyntöprosessissa on varmistettava, että varmennettava julkinen avain on peräisin avainparista, joka on tosiasiallisesti luotu turvallisella allekirjoituksen luomisvälineellä.

Kansalaisvarmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa ja yleisissä käyttöehdoissa, jotka muodostavat varmenteen hakijan kanssa tehtävän sopimuksen. Hakemusasiakirjassa on tiedot kummankin osapuolen oikeuksista ja velvollisuuksista.

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

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

Kun varmentaja myöntää kansalaisvarmenteen, se samalla hyväksyy varmennehakemuksen.

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

Kansalaisvarmenteella olevat tiedot määrittelevät kansalaisvarmenteen haltijan yksikäsitteisesti. Varmentaja selvittää tarvittaessa varmenteen hakijan virallisen henkilöllisyyden.

Kansalaisvarmenteeseen liittyvät, mikrosirulla tai muussa turvallisessa ympäristössä luodut yksityiset avaimet toimitetaan kansalaisvarmenteen hakijalle luovutuksen yhteydessä.

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

Kansalaisvarmenne voidaan noutaa henkilökohtaisesti rekisteritoimipisteestä.

Kansalaisvarmenteen haltijan vastuulla on estää hänelle kuuluvien yksityisten avaintensa ja niihin liittyvien PIN-tunnusten käyttäminen käyttöehtojen vastaisella tavalla huolehtimalla niistä käyttöehdoissa mainitulla tavalla.

Väestörekisterikeskuksen kansalaisvarmenteen haltijan avainpari luodaan turvatiloissa. Julkista avainta käytetään varmenteen luomiseen ja yksityinen avain säilytetään luku- ja kirjoitussuojattuna mikrosirulla.

Kortinvalmistaja luo avainten käytön mahdollistavat aktivointitiedot eli PIN-tunnukset.

PIN-tunnukset on suojattu niin, ettei niitä voi lukea tai kopioida kortilta. Varmenteen haltijan vastuulla on suojata avaintensa käyttö huolehtimalla mikrosirustaan tai kortistaan ja tunnusluvuistaan käyttöehdoissa mainitulla tavalla.

Kansalaisvarmenteen käyttämiseksi tarvittavia PIN-tunnuksia ja PUK-koodeja käsitellään turvallisuuden takaamiseksi siten, etteivät ne ole yhtä aikaa samassa paikassa ennen toimitusta ja toimituksessa varmenteen hakijalle.

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

Kansalaisvarmenteen haltijalle selvitetään, että hänellä on mahdollisuus vaihtaa alkuperäiset PIN-tunnukset uusiksi tunnuksiksi. PIN-tunnusten vaihto-ohjelma on maksutta kortinhaltijan saatavissa osoitteessa http://www.fineid.fi.

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

7.3.2. Varmenteen uusiminen, sen avainparin vaihtaminen ja varmenteen päivittäminen

Varmentaja varmistaa, että jo aikaisemmin rekisteröityneelle allekirjoittajalle myönnettäviä varmenteita koskevat pyynnöt ovat täydelliset, paikkansapitävät ja asianmukaisesti valtuutetut. Näihin sisältyvät varmenteen uusiminen, peruuttamisen jälkeen tai ennen voimassaolon päättymistä tehtävä avainparin vaihtaminen, sekä allekirjoittajan attribuuttien muuttumisesta johtuva päivittäminen sähköisistä allekirjoituksista annetun direktiivin II liitteen kohdan g mukaisesti.

Mikäli varmentaja tarjoaa varmenteen uusimispalvelua, tilaaja voi pyytää uusimista esimerkiksi silloin, jos varmennetta varten varmentajalle esitetyt oleelliset attribuutit ovat muuttuneet tai jos varmenteen käyttöaika on päättymässä.

Erityisesti:

Rekisteröinti

a) Varmentaja tarkistaa uusittavan varmenteen olemassaolon ja voimassaolon ja että allekirjoittajan henkilöllisyyden ja häneen liittyvien attribuuttien todentamisessa käytetty tieto on edelleen voimassa.
b) Mikäli varmentajan käyttöehtoihin on tehty muutoksia, niistä ilmoitetaan tilaajalle ja sovittava kohdan 7.3.1 alakohtien a, b ja i mukaisesti.
c) Mikäli varmennettuja nimiä tai attribuutteja on muutettu tai mikäli aiempi varmenne on peruutettu, rekisteröintitiedot todennetaan ja tallennettaan ja tilaaja hyväksyy ne kohdan 7.3.1 alakohtien c–g mukaisesti.
d) Varmentaja myöntää uuden varmenteen käyttämällä allekirjoittajan aiempaa varmennettua julkista avainta vain, jos sen salausturvallisuus on uuden varmenteen voimassaolon ajan edelleen riittävä ja jos merkkejä ei ole allekirjoittajan yksityisen avaimen joutumisesta vääriin käsiin.

Kansalaisvarmenteella olevia julkisia avaimia ja sirulla olevia yksityisiä avaimia ei voi uusia. Uusien avainparien muodostaminen edellyttää uuden kansalaisvarmenteen hakemista. Tällöin noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa. Menettelytavat on kuvattu yksityiskohtaisesti varmennuskäytäntö-asiakirjassa.

7.3.3. Varmenteiden luominen

Varmentaja varmistaa, että se myöntää varmenteita turvallisesti niiden aitouden säilyttämiseksi sähköisistä allekirjoituksista annetun direktiivin II liitteen kohdan g mukaisesti. Erityisesti:

Varmenteiden luominen

a) Varmenteet luodaan ja myönnetään sähköisistä allekirjoituksista annetun direktiivin I liitteen mukaisesti. Laatuvarmenteessa on oltava
   - osoitus siitä, että varmenne on myönnetty laatuvarmenteena
   - tiedot varmentajasta [varmennepalvelujen tarjoajasta] ja valtiosta, johon se on sijoittautunut
   - allekirjoittajan nimi tai salanimi, jonka osalta on mainittava kyseessä olevan salanimi
   - mahdollisuus lisätä allekirjoittajaan liittyvä asiaankuuluva attribuutti, riippuen varmenteen aiotusta käyttötarkoituksesta
   - allekirjoituksen todentamiseen käytettävät tiedot, jotka vastaavat allekirjoittajan valvonnassa olevia allekirjoituksen luomiseen käytettäviä tietoja;
   - tieto varmenteen voimassaoloajan alkamis- ja päättymisajankohdasta
   - varmenteen tunnuskoodi
   - varmenteen myöntävän varmennepalvelujen tarjoajan kehittynyt sähköinen allekirjoitus

- mahdolliset varmenteen käyttörajoitukset, ja
- mahdolliset arvomääräiset rajoitukset toimille, joihin varmennetta voidaan käyttää.

Julkaisussa TS 101 862 sisältää vakiomuotoinen laatuvarmenteiden määrityksen, joka täyttää sähköisistä allekirjoituksista annetun direktiivin liitteen I vaatimukset.

b) Varmentajan on toteutettava toimenpiteet varmenteiden väärentämisen ehkäisemiseksi ja, silloin kun varmentaja luo allekirjoituksen luomiseen käytettävät tiedot, taattava luottamuksellisuus kyseisiä tietoja luotaessa sähköisistä allekirjoituksista annetun direktiivin liitteen II kohdan g mukaisesti.

c) Varmenteen myöntämismenettely liittyy turvallisesti siihen liittyvään rekisteröintiin, varmenteen uusimiseen tai varmenteen avainparin vaihtamiseen, mukaan luettuna mahdollinen allekirjoittajan luoman julkisen avaimen tarjoaminen.

d) Jos varmentaja luo allekirjoittajan avaimen,
   - varmenteen myöntämismenettelyn on liityttävä turvallisesti varmentajan suorittamaan avainparin luomiseen
   - yksityinen avain (tai turvallinen allekirjoituksen luomisväline, (kohta 7.2.9) on välitettävä rekisteröidylle allekirjoittajalle turvallisesti.

e) Varmentaja varmistaa, että allekirjoittajalle osoitettu yksilöivä nimi asiointitunnuksineen säilyy ajan kuluessa ainutlaatuisena varmentajan toimialueella. Myönnetyssä varmenteessa käytettyä yksilöityä nimeä asiointitunnuksineen ei koskaan varmentajan elinkaaren aikana anneta toiselle yhteisölle.

f) Rekisteröintitietojen luottamuksellisuus ja eheys suojataa erityisesti, kun tietoja vaihdetaan tilaajan, allekirjoittajan tai varmentajan järjestelmän hajautettujen osien välillä.

Tietosuojavaatimukset on kuvattu kohdassa 7.4.10.

g) Varmentajan on todennettava, että rekisteröintitietoja vaihdetaan sellaisten tunnustettujen rekisteröintipalvelujen tarjoajien kanssa, joiden henkilöllisyys on todennettu, mikäli käytetään ulkoisia rekisteröintipalvelujen tarjoajia.

Kansalaisvarmenteen haltijoiden yksityiset avaimet luodaan turvallisesti laatuvarmenteen vaatimukset täyttävällä tavalla. Varmenteen haltijan itsensä luomia avainpareja ei hyväksytä. Yksityisistä avaimista ei tehdä kopioita niiden luontivaiheessa, eivätkä ne ole siirrettävissä tai kopioitavissa mikrosirulta. Varmentajalla ja kortinvalmistajalla ei ole pääsyä varmenteen haltijoiden yksityisiin avaimiin.

Avainten luontivaiheessa avaimia ei ole vielä kohdistettu kenellekään henkilölle.

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

Varmenteen haltijan yksityisistä avaimista ei ole kopioita.

Varmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa.

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

7.3.4. Käyttöehtojen jakelu

Varmentaja varmistaa, että käyttöehdot ja ohjeet asetetaan tilaajien ja varmenteeseen luottavien osapuolten saataville sähköisistä allekirjoituksista annetun direktiivin liitteen I kohta k:n mukaisesti.

Erityisesti:

a) Varmentaja asettaa tilaajien ja varmenteeseen luottavien osapuolten saataville varmenteen käyttöä koskevat ehdot, myös sähköisistä allekirjoituksista annetun direktiivin liitteen I kohta k:n mukaisesti.
   - laatuvarmennepolitiikkaa sovellettaessa ilmoitetaan selkeästi, koskeeko politiikka yleisölle myönnettäviä varmenteita ja edellytetäänkö siinä turvallisen allekirjoituksen luomisvälineen käyttöä
   - mahdolliset varmenteen käyttöä koskevat rajoitukset
   - kohdassa 6.2. määritellyn mukaiset tilaajan velvollisuudet, myös edellytetäänkö varmennepolitiikassa **turvallisen allekirjoituksen luomisvälineen** käyttöä
   - tiedot siitä, kuinka varmenne todennetaan, myös vaatimukset tarkistaa varmenteen sulkutila, jotta varmenteeseen luottavan osapuolen voidaan katsoa "luottavan vilpittömässä mielessä" varmenteeseen (kohta 6.3)
   - vastuunrajoitukset, mukaan luettuina käyttötarkoitukset, joiden osalta varmentaja hyväksyy (tai ei hyväksy) olevansa vastuussa
   - rekisteröintitietojen säilytysaika (kohta 7.3.1)
   - varmentajan tapahtumalokien säilytysaika (kohta 7.4.11)
   - valitus- ja riitojenratkaisumenettelyt
   - sovellettava oikeusjärjestelmä ja
   - onko varmentaja todistettu yksilöidyn laatuvarmennepolitiikan vaatimusten mukaiseksi ja millä arviointijärjestelmällä tämä on todettu.

   b) Edellä kohdassa a yksilöityjen tietojen ovat saatavilla muuttamattomassa muodossa tiedon eheänä säilyttävän viestintämuodon kautta selvästi ymmärrettävällä kielellä. Tiedot voidaan välittää sähköisesti.

Tämän varmennepolitiikan mukaisesti myönnetty allekirjoitusvarmenne täyttää Euroopan parlamentin ja neuvoston sähköisen allekirjoituksen direktiivin (1999/93/EC) laatuvarmenteelle asettamat vaatimukset.

Tiedot voidaan toimittaa tilaajan tai varmenteeseen luottavan osapuolen sopimuksen osana. Käyttöehdot voidaan sisällyttää varmennuskäytäntöön niin, että lukijan on ne helppo havaita ja tunnistaa.

Yleisölle myönnettäviä varmenteita koskevien sopimusehtojen osalta otetaan huomioon kuluttajalainsäädännön vaatimukset, myös kuluttajasopimusten kohtuuttomista ehdoista annettu direktiivi 93/13/ETY

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

Kansalaisvarmennetta haetaan sen mukaisesti kuin varmennuskäytännössä on kuvattu.

Sähköisen henkilökortin hankintahinta määräytyy kulloinkin voimassa olevan valtiovarainministeriön asetuksen Väestörekisterikeskuksen suoritteista mukaisesti.

Muilla mikrosiruilla olevat kansalaisvarmenteet on hinnoiteltu voimassaolevan Väestörekisterikeskuksen liiketaloudellisia suoritteita koskevan hinnaston mukaisesti.

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

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

Neuvontapalvelun käytöstä peritään erillinen maksu voimassaolevan hinnaston mukaisesti.

Jos palveluntarjoaja haluaa järjestää tietohuoltopalvelun kansalaisvarmenteiden yksilöivän tunnisteen ja oman taustajärjestelmänsä tunnistetietojen tai muiden päivitystietojen välillä, palveluntarjoaja voi hakea tietopalveluun tietojenluovutuslupaa Väestörekisterikeskukselta. Tämä palvelu hinnoitellaan voimassa olevan maksuperustelain ja valtiovarainministeriön asetuksen rekisterihallinnon suoritteista mukaisesti.

Kansalaisvarmenteen käyttöön liittyvät ohjeet ja käyttöehdot annetaan varmenteen hakijoiden tutkittaviksi ennen varmennetta koskevan sopimuksen ja myöntämispäätöksen tekemistä sekä rekisteröintipisteessä että Väestörekisterikeskuksen verkkosivuilla.

7.3.5. Varmenteiden jakelu

Varmentaja varmistaa, että varmenteet asetetaan tarvittavalla tavalla tilaajien, allekirjoittajien ja varmenteeseen luottavien osapuolten saataville sähköisistä allekirjoituksista annetun direktiivin liitteen II kohta l:n mukaisesti.

Erityisesti:

Jakelu

a) Luomisen jälkeen valmiin ja paikkansapitävän varmenteen on sen tilaajan tai allekirjoittajan saatavilla, jolle varmenne myönnetään.

b) Varmenteita koskevia hakuja on mahdollista tehdä vain silloin, kun varmenteen allekir joittajalta on saatu lupa.

c) Varmentaja asettaa varmenteeseen luottavien osapuolten saataville varmenteen käyttöä koskevat ehdot (kohta 7.3.4).

d) Varmentaja ilmeisee selkeästi, mitä käyttöehtoja tiettyyn varmenteeseen sovelletaan.

e) Edellä kohdissa b ja c yksilöidyt tiedot ovat saatavilla vuorokauden ympäri viikon jokai-

sena päivänä. Järjestelmän toimintahäiriön, palvelun tai muiden tekijöiden osalta, jotka eivät ole varmentajan hallinnassa, varmentaja varmistaa, ettei kyseinen tiedotuspalvelu ole poissa käytöstä varmennuskäytännössä ilmoitettua enimmäisaikaa kauemmin.

f) Edellä kohdissa b ja c yksilöidyt tiedot ovat julkisesti ja kansainvälisesti saatavilla.

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

Varmentaja julkaisee kaikki kansalaisvarmenteet ja sulkulistat maksuttomassa, yleisesti saatavilla olevassa julkisessa hakemistossa. Varmentaja julkaisee varmennepolitiikan, varmennuskäytännöt, varmennekuvauksen (PDS) sekä muut julkiset varmennepalvelujen tuottamiseen liittyvät dokumentit www-sivuillaan.

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

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

7.3.6. Varmenteen peruuttaminen ja asettaminen keskeytystilaan

Varmentaja varmistaa, että varmenteet peruutetaan oikea-aikaisesti valtuutettujen ja vahvistettujen varmenteiden peruutuspyyntöjen perusteella sähköisistä allekirjoituksista annetun direktiivin liitteen II kohta b:n mukaisesti.

Erityisesti:

Peruutusten hallinta

a) Varmentajan on varmennuskäytännön (kohta 7.1) osana dokumentoitava varmenteiden peruuttamismenettelyt, mukaan luettuina tiedot seuraavista:

- kuka saa lähettää peruuttamispyyntöjä ja -ilmoituksia
- kuinka ne on toimitettava
- peruuttamisilmoitusten ja -pyyntöjen myöhempää vahvistusta koskevat mahdolliset vaatimukset

  Vahvistusta voidaan esimerkiksi vaatia tilaajalta, jos kolmas osapuoli ilmoittaa tietosuojan vaarantumisesta:
- voidaanko varmenteita asettaa keskeytystilaan ja mistä syystä
- käytettävä sulkutilatietojen jakelumenetelmä
- enimmäisviive, joka kuluu peruuttamispyynnön tai -ilmoituksen vastaanottamisesta

siihen, kunnes kaikkien varmenteeseen luottavien osapuolten saatavilla olevat sulkutilatiedot on muutettu; suurin sallittu viive on 1 vuorokausi.

b) Peruuttamispyynnöt ja -ilmoitukset (jotka koskevat esimerkiksi allekirjoittajan yksityisen avaimen joutumista vääriin käsiin, allekirjoittajan kuolemaa, odottamatonta tilaajan tai allekirjoittajan sopimuksen tai yritystoiminnan päättymistä, sopimusvelvoitteiden rikkomista) on käsiteltävä vastaanotettaessa.

- Peruuttamiseen liittyvät pyynnöt ja ilmoitukset on todennettava ja tarkistettava, että ne ovat peräisin valtuutetusta lähteestä. Nämä ilmoitukset ja pyynnöt vahvistetaan varmentajan käytännöissä edellytettävällä tavalla.
- Peruutuksen vahvistamisen ollessa kesken varmenne voidaan asettaa keskeytystilaan. Varmentajan on varmistettava, ettei varmenne jää keskeytystilaan kauemmaksi kuin sulkutilan vahvistaminen edellyttää.

Varmenteen keskeytystilan tukeminen on valinnaista.

c) Peruutetun tai keskeytystilaan asetetun varmenteen allekirjoittajalle ja tapauksen mukaan tilaajalle on tiedotettava varmenteen tilan muutoksesta.

d) Kun varmenne on lopullisesti peruutettu (eli ei keskeytetty), sitä ei saa enää ottaa uudelleen käyttöön.

Varmenteiden sulkulistoja (CRL-listoja) ja niiden muunnelmia (esimerkiksi delta-CRL-listoja, jotka sisältävät vain edelliseen listaan nähden muuttuneet tiedot) käytettäessä ne on julkaistava vähintään päivittäin ja

- jokaisessa sulkulistassa on ilmoitettava seuraavan sulkulistan julkaisuajankohta
- uusi sulkulista voidaan julkaista ennen seuraavan sulkulistan ilmoitettua julkaisuajankohtaa
- varmentajan tai varmentajan määrittämän yhteisön on allekirjoitettava sulkulista.

Mahdollisimman suuren yhteensopivuuden kannalta on suositeltavaa, että varmenteiden sulkulistat julkaistaan ISO/IEC 9594-8 -standardin mukaisesti.

e) Peruutusten hallintapalvelujen on oltava saatavilla vuorokauden ympäri viikon jokaisena päivänä. Järjestelmän toimintahäiriön, palvelun tai muiden tekijöiden osalta, jotka eivät ole varmentajan hallinnassa, varmentajan on pyrittävä parhaansa mukaan varmistamaan, ettei kyseinen palvelu ole poissa käytöstä varmennuskäytännössä ilmoitettua enimmäisaikaa kauemmin.

Sulkutila

f) Sulkutilatietojen on oltava saatavilla vuorokauden ympäri viikon jokaisena päivänä. Järjestelmän toimintahäiriön, palvelun tai muiden tekijöiden osalta, jotka eivät ole varmentajan hallinnassa, varmentajan on pyrittävä parhaansa mukaan varmistamaan, ettei kyseinen tiedotuspalvelu ole poissa käytöstä varmennuskäytännössä ilmoitettua enimmäisaikaa kauemmin.

Sulkutilatietoja voidaan antaa esimerkiksi käyttämällä reaaliaikaista varmenteen tilapalvelua tai sulkulistan jakelua tietyssä tallennuspaikassa.

g) Tilatietojen eheys ja aitous on turvattava.

h) Sulkutilatietojen on oltava julkisesti ja kansainvälisesti saatavilla.

i) Sulkutilatietojen on sisällettävä varmenteiden tilatiedot vähintään varmenteen voimassaolon päättymiseen asti.

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

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

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

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

Varmenteen haltijan vastuulla on suojata yksityisten avaintensa käyttö huolehtimalla mikrosirustaan tai kortistaan ja tunnusluvuistaan käyttöehdoissa mainitulla tavalla. Varmenteen haltijan on ilmoitettava varmenteet välittömästi sulkulistalle, mikäli hän epäilee, että sopimusehtojen vastainen käyttö on tullut mahdolliseksi.

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

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

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

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

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

Varmenteen sulkemisen perusteet, ajankohta ja suorittajan tiedot talletetaan.

Kansalaisvarmenteen sulkupyyntö voidaan tehdä seuraavilla tavoilla:

a) Puhelinsoitolla sulkupalveluun

b) Käymällä rekisteröijän luona

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

Varmenteen sulkeminen ja sen vaikutukset on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Varmenteiden sulkeminen Väestörekisterikeskuksen pyynnöstä

Väestörekisterikeskus sulkee varmenteet aina silloin, kun se on saanut tiedon varmenteen haltijan kuolemasta. Väestörekisterikeskus tekee sulkemista koskevan ilmoituksen kuolleen varmenteen haltijan oikeudenomistajille.

Väestörekisterikeskus sulkee myöntämänsä varmenteet, mikäli varmenteiden tietosisällössä havaitaan virhe.

Väestörekisterikeskus voi sulkea käyttämällään yksityisellä avaimellaan allekirjoitetut varmenteet, mikäli on syytä epäillä Väestörekisterikeskuksen yksityisten avainten paljastuneen tai joutuneen vääriin käsiin.

Kaikki paljastuneella avaimella myönnetyt ja voimassa olevat varmenteet on suljettava yhdellä tai useammalla sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeisen suljetun varmenteen 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 kortinhaltijoille ja Viestintävirastolle asianmukaisella tavalla.

Väestörekisterikeskus voi sulkea varmenteen erityisestä syystä.

Varmenteen sulkeminen toteutetaan välittömästi sulkupyynnön yhteydessä.

Sulkulistan julkaisutiheys

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

Sulkulista sisältää seuraavan sulkulistan julkaisuajankohdan.

Uusi sulkulista julkaistaan viimeistään voimassaolevan sulkulistan voimassaolon päättymisajankohtaan mennessä.

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

Varmentaja ei toistaiseksi tarjoa suorakäyttöistä varmenteen tilan tarkistuspalvelua eli OCSP-palvelua. Varmentaja julkaisee suljetuista varmenteista sulkulistan.

Avainparin uusiminen varmenteen sulkulistalle asettamisen jälkeen

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

Kansalaisvarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

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

7.4. Varmentajan johtamis- ja toimintakäytännöt

7.4.1. Turvallisuuden hallinta

Varmentaja varmistaa, että se noudattaa asianmukaisia ja tunnustettujen standardien mukaisia hallinnollisia ja liikkeenjohdollisia menettelytapoja sähköisistä allekirjoituksista annetun direktiivin II liitteen kohdan e mukaisesti.

Erityisesti:

Varmentaja yleisesti

a) Varmentaja toteuttaa riskinarvioinnin, jossa arvioidaan liiketoimintariskit ja määritetään tarvittavat turvallisuusvaatimukset ja toimintatavat. Riskianalyysi katselmoidaan säännöllisesti ja sitä tarkistetaan tarvittaessa.

b) Varmentaja on vastuussa kaikista varmennepalvelujen tarjoamisen näkökohdista, vaikka osa toiminnoista olisikin ulkoistettu alihankkijoille. Varmentajan on selkeästi määriteltävä kolmansien osapuolien vastuut ja sen on tarkoituksenmukaisin järjestelyin varmistettava, että kolmannet osapuolet sitoutuvat toteuttamaan varmentajan edellyttämiä hallintakeinoja. Varmentaja on vastuussa kaikkia osapuolia koskevien käytäntöjen julkistamisesta.

c) Varmentajan johto antaa tietoturvaa koskevat linjaukset tarkoituksenmukaisen korkean tason ohjausryhmän kautta. Ohjausryhmä vastaa varmentajan tietoturvapolitiikasta sekä sen tiedottamisesta kaikille työntekijöille, joita tietoturvapolitiikka koskee.

d) Varmentajalla on laadun ja tietoturvallisuuden hallintajärjestelmä tai -järjestelmiä, jotka ovat tarjottavien varmennepalvelujen kannalta tarkoituksenmukaisia.

e) Varmentajan sisäisen turvallisuuden hallinnan kannalta välttämätöntä tietoturvajärjestelmää ylläpidetään jatkuvasti. Varmentajan ohjausryhmä hyväksyy kaikki turvallisuustasoon vaikuttavat muutokset.

Tietoturvallisuuden hallintaa koskevia lisäohjeita esimerkiksi tietoturvajärjestelmästä, tietoturvaryhmästä ja tietoturvapolitiikoista annetaan ISO/IEC 17799 -standardissa. Lähdekirjallisuudessa mainitaan myös muita ohjeistavia asiakirjoja.

f) Turvallisuuden hallintakeinot ja menettelytavat, jotka koskevat varmennepalvelujen tarjoamiseen käytettäviä varmentajan toimitiloja, järjestelmiä ja tietovarantoja, on dokumentoitava ja niitä on noudatettava ja ylläpidettävä.

Kyseisissä asiakirjoissa (järjestelmän tietoturvakuvauksissa) yksilöidään kaikki tarjottaviin palveluihin liittyvät asiaankuuluvat kohteet ja mahdolliset uhat sekä suojauskeinot, joilla pyritään välttämään kyseisten uhkien toteutuminen tai rajoittamaan toteutumisen vaikutuksia. Asiakirjoissa kuvataan ne säännöt, ohjeet ja menettelyt, joilla yksilöidyt palvelut ja niiden turvataso toteutetaan, sekä määritellä menettelytavat tietoturvaloukkausten ja hätätilanteiden yhteydessä.

Varmistaja varmistaa tietoturvallisuuden säilymisen, mikäli varmentaja hankkii palveluita toiselta organisaatiolta tai yhteisöltä.

7.4.2. Varantojen luokittelu ja hallinta

Varmentaja varmistaa, että sen tietovarantojen ja tietojen suojaustaso on tarkoituksenmukainen sähköisistä allekirjoituksista annetun direktiivin II liitteen kohdan e mukaisesti.

Erityisesti:

Varmentaja yleisesti

a) Varmentaja pitää kirjaa kaikista sen tietovarannoista ja määrittelee niille suojausluokan riskianalyysin mukaisesti.

Väestörekisterikeskuksen julkaisemat tiedot ovat saatavilla varmentajan www-sivuilla. Varmennejärjestelmän salaiset 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 henkilötietolain mukaisen rekisteriselosteen henkilötietojen käsittelyn osalta.

Varmennejärjestelmän tiedot ovat salaisia, elleivät ne perustu henkilötietolain, viranomaisten julkisuudesta annetun lain, väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain (661/2009) tai vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain säännöksiin tietojen luovuttamisesta tai varmennepolitiikassa tai varmennuskäytännössä määriteltyihin tarkoituksiin.

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

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

Viranomaisille luovutettavat tiedot määritellään voimassaolevan lainsäädännön mukaisesti.

Varmennejärjestelmän tietoja ei luovuteta kuin edellä tässä asiakirjassa mainittuihin tarkoituksiin.

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

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

Väestörekisterikeskus noudattaa henkilötietojen käsittelyssä henkilötietolakia sekä erityislainsäädäntöä. Väestörekisterikeskus on valmistellut käytännesäännöt sekä tietojen luovuttamisesta että varmennetoiminnan yhteydessä tapahtuvasta henkilötietojen käsittelystä. Henkilötietojen käsittelyssä noudatetaan erityistä huolellisuutta.

Väestörekisterikeskuksen tuottamat varmennepalvelut ovat sellaisen taloushallinnollisen järjestelmän ja valvonnan piirissä kuin on erikseen säädetty. Varmentajan taloushallinnon toteuttaminen on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Yksityiskohtaiset vaatimukset on kuvattu ISO/IEC 17799 -standardissa.

7.4.3. Henkilöstö ja tietoturva

Varmentaja varmistaa, että henkilöstö ja rekrytointikäytännöt edistävät ja tukevat varmentajan toiminnan luotettavuutta sähköisistä allekirjoituksista annetun direktiivin II liitteen kohdan e mukaisesti.

Erityisesti:

Varmentaja yleisesti

a) Varmentajan on pidettävä palveluksessaan riittävä määrä henkilökuntaa, jolla on tarjottujen palvelujen ja työtehtävän edellyttämä asiantuntemus, kokemus ja pätevyys.

   On suositeltavaa, että varmentajan henkilökunnalta edellytettävät "asiantuntemus, kokemus ja pätevyys" perustuvat viralliseen tutkintoon viralliseen ja henkilön saamiin suosituksiin tai käytännön kokemukseen tai näiden yhdistelmään.

b) Varmentajan varmennepolitiikkoja tai menettelyjä rikkovalle työntekijälle seuraa asian mukaisia sanktioita.

c) Varmentajan tietoturvapolitiikassa yksilöidyt turvallisuuteen liittyvät roolit ja vastuut on kirjattava tehtäväkuvauksiin. Luotetut roolit, joista varmentajan toiminnan turvallisuus riippuu, on määriteltävä selkeästi.

d) Varmentajan henkilöstön määräaikaiset ja pysyvät tehtäväkuvaukset on määriteltävä tehtävien eriyttämisen ja ainoastaan tehtävässä tarpeellisten käyttöoikeuksien näkökulmasta. Kuvauksissa on määriteltävä toimen arkaluonteisuuden aste siihen liittyvien tehtävien, käyttöoikeuksien, taustatietojen selvittämisen sekä työntekijän kouluttamisen ja tietojen näkökulmasta. Tarvittaessa kuvauksissa on eroteltava yleiset toiminnot ja varmentajakohtaiset toiminnot.

   Työkuvausten on suositeltavaa sisältää taitoja ja kokemusta koskevat vaatimukset.

e) Henkilöstön on toteutettava varmentajan tietoturvallisuuden hallintamenettelyjen mukaisia hallinnollisia ja liikkeenjohdollisia menettelytapoja (kohta 7.4.1).

Rekisteröinti, varmenteiden luominen, välineen tarjoaminen allekirjoittajalle, varmenteiden peruuttamisen hallinta

f) Johtotehtävissä on henkilöitä, joilla on johtotehtävissä toimimiseen riittävä sähköisten allekirjoitusten tekniikoihin liittyvä kokemus tai koulutus, jotka ovat perillä turvallisuudesta vastuussa olevaa henkilöstöä koskevista turvatoimista ja joilla on kokemusta tietoturvasta ja riskinarvioinnista.

g) Niillä varmentajan henkilökunnan jäsenillä, jotka toimivat luotetuissa rooleissa, ei saa

olla eturistiriitoja, jotka saattavat vaarantaa varmentajan toiminnan puolueettomuuden.

h) Vastuullisia henkilöitä ovat seuraavat:
- Turvallisuuspäällikkö: Kokonaisvastuu turvallisuuskäytäntöjen toteuttamisen hallinnasta. Lisäksi hän hyväksyy varmenteiden luomisen, peruuttamisen ja niiden asettamisen keskeytystilaan.
- Järjestelmänvalvoja: Lupa asentaa varmentajan luotettavia järjestelmiä, joita käytetään rekisteröinnissä, varmenteiden luomisessa, välineen tarjoamisessa allekirjoittajalle ja varmenteiden peruuttamisen hallinnassa, ja määrittää niihin asetuksia ja ylläpitää niitä.
- Järjestelmäoperaattori: Vastuussa varmentajan luotettavien järjestelmien päivittäisestä toiminnasta. Valtuutus suorittaa järjestelmän varmuuskopiointi ja palautus.
- Järjestelmän auditoija: Valtuutus tarkastella varmentajan luotettavien järjestelmien arkistoja ja auditointilokeja.

i) Turvallisuudesta vastaava ylempi johto nimittää viralliset vastuuhenkilöt.

j) Varmentaja ei saa nimittää vastuuhenkilöiksi tai johtoon sellaista henkilöä, jonka tiedetään tehneen vakavan rikoksen tai muunlaisen työtehtävään soveltumiseen vaikuttavan rikkomuksen. Henkilöstöllä ei saa olla pääsyä ydintoimintoihin ennen kuin kaikki tarvittavat tarkistukset on tehty.

Väestörekisterikeskus toimii varmentajana, joka vastaa varmennetoiminnasta. Teknisten palveluiden toimittajien valinta perustuu julkisiin hankintoihin liittyvään kilpailutusmenettelyyn ja ne toimivat Väestörekisterikeskuksen vastuulla ja lukuun.

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

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

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

Turvallisuusselvitysmenettely on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Väestörekisterikeskuksen henkilökunnan koulutus suunnitellaan ja toteutetaan siten, että tehtävän hoitaminen parhaalla mahdollisella tavalla on mahdollista. Väestörekisterikeskuksessa on koulutussuunnitelma, jonka toteuttamisesta vastaa Väestörekisterikeskuksen hallinto ja johdon tuki -yksikkö.

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

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

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

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.

Henkilökunnalla on aina käytössään Väestörekisterikeskuksen laatu- ja turvallisuusasiakirjat.

7.4.4. Fyysinen ja ympäristön turvallisuus

Varmentajan on varmistettava, että fyysistä pääsyä kriittisiin palveluihin valvotaan ja että varantoja koskevat fyysiset riskit minimoidaan sähköisistä allekirjoituksista annetun direktiivin 1999/93/EY II kohdan f mukaisesti.

Erityisesti:

Varmentaja yleisesti

a) Vain asianmukaisesti valtuutetuille henkilöille on sallitaan fyysinen pääsy toimitiloihin, jotka liittyvät varmenteiden luomiseen, välineen laatimiseen allekirjoittajalle ja varmenteiden peruuttamisen hallintapalveluihin.

b) Käytössä ovat hallintakeinot, joilla pyritään välttämään varantojen menetykset, vahingot ja vaarantuminen sekä liiketoiminnan keskeytyminen.

c) Käytössä ovat hallintakeinot, joilla pyritään välttämään tiedon ja tiedonkäsittelytilojen vaarantuminen ja niitä koskevat varkaudet.

Varmenteiden luominen, välineen tarjoaminen allekirjoittajalle, valmistaminen ja varmenteiden peruuttamisen hallinta

d) Varmenteiden luomisessa, välineen valmistamisessa allekirjoittajalle (katso kohta 7.2.9) ja varmenteiden peruuttamisen hallinnassa käytettävien toimitilojen ympäristö suojataan niin, että estetään luvaton pääsy järjestelmiin tai tietoon ja palvelujen vaarantuminen.

e) Tälle fyysisesti turvalliselle alueelle saapuvia henkilöitä ei jätetä merkittäväksi ajaksi ilman valtuutetun henkilön valvontaa.

f) Fyysinen suojaus saadaan aikaan muodostamalla selkeästi määritellyt turvallisuusrajat (fyysiset esteet) varmenteiden luomisen, allekirjoittajalle toimitettavan välineen valmistamisen (katso kohta 7.2.9) ja varmenteiden peruuttamisen hallintapalvelujen ympärille. Muiden organisaatioiden kanssa mahdollisesti yhteiskäytössä olevien tilat sijaitsevat näiden rajojen ulkopuolella.

g) Käytössä on fyysisen ja ympäristön turvallisuuden hallintakeinoja, joilla suojataan järjestelmäresurssien sijaintitiloja, järjestelmäresursseja ja niiden käyttöä tukevia toimitiloja. Varmentajan fyysistä ja ympäristön turvallisuutta koskevissa menettelytapaohjeissa käsitelläänvarmenteiden luomiseen, allekirjoittajalle toimitettavan välineen valmistamiseen (katso kohta 7.2.9) ja varmenteiden peruutusten hallintapalveluihin liitty-

vien järjestelmien osalta esimerkiksi fyysisen pääsyn valvontaa, luonnonmullistuksilta suojaamista, paloturvallisuustekijöitä, kunnallisteknisten verkostojen häiriöitä (esimerkiksi sähkö, teleliikenne), rakenteiden pettämistä, putkistovuotoja, varkaus- ja murtovarkaussuojausta sekä hätätilanteesta toipumista.

h) Käytössä on hallintakeinoja, joilla suojataan varmentajan palveluihin liittyvien laitteiden, tietojen, tietovälineiden ja ohjelmistojen luvaton vienti pois paikalta.

Fyysisen turvallisuuden ja ympäristön turvallisuuden järjestämisestä on asetettu vaatimuksia ISO/IEC 17799 -standardissa.

Samalla turvallisella alueella voidaan suorittaa muitakin toimintoja, jos ainoastaan valtuutella henkilöllä on pääsy sinne.

Väestörekisterikeskukselle on myönnetty tietoturvasertifikaatti, joka varmentaa, että VRK:n tietoturvallisuus täyttää standardin ISO/IEC 27001 vaatimukset. Väestörekisterikeskus käyttää teknisiä palvelutoimittajia varmennepalvelun tietoteknisten tehtävien hoitamiseen. VRK vastaa varmentajana varmennetuotannon turvallisuudesta ja toiminnasta asianmukaisella tavalla sen kaikilla osa-alueilla.

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.

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.

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

Toiminnan kannalta kriittisten laitteiden varaosien saanti ja huolto on varmistettu.

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

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

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

Järjestelmän käyttämiseen vaaditaan yhden tehtävään oikeutetun henkilön läsnäolo.

Kansalaisvarmenteen rekisteröiminen ja hakijan tunnistaminen vaatii yhden henkilön läsnäolon.

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

7.4.5. Toiminnan hallinta

Varmentajan on varmistettava, että varmentajan järjestelmät ovat turvalliset ja että niitä käytetään asianmukaisesti toimintahäiriöriskit minimoiden sähköisistä allekirjoituksista annetun direktiivin liitteen II kohdan e mukaisesti.

Erityisesti:

Varmentaja yleisesti

a) Varmentajan järjestelmien ja tietojen eheyttä suojataan viruksilta sekä haitallisilta ja luvattomilta ohjelmistoilta.

b) Tietoturvaloukkausten ja toimintahäiriöiden vahingot minimoidaan käyttämällä tapahtumailmoituksia ja niihin reagoimista koskevia menettelyjä.

c) Varmentajalla käytettäviä tietovälineitä käsitellään turvallisesti, jotta voidaan välttää tietovälineiden vahingot, varkaudet ja luvaton käyttö.

   Jokaisen johtotehtävissä toimivan henkilökunnan jäsenen vastuulla on suunnitella ja toteuttaa tehokkaasti varmennepolitiikkaa sekä siihen liittyviä käytäntöjä varmennuskäytännössä kirjatun mukaisesti.

d) Tietovälineiden hallintamenettelyillä turvataan, etteivät tietovälineet vanhene tai heikkene tietojen vaadittuna säilytysaikana.

e) Kaikkia varmennepalvelujen tarjoamiseen vaikuttavia luotettuja ja hallinnollisia rooleja varten luodaan menettelyt ja niitä toteutetaan.

Tietovälineiden käsittely ja turvallisuus

f) Kaikkia tietovälineitä käsitellään turvallisesti tietojen luokittelujärjestelmän vaatimusten mukaisesti (katso kohta 7.4.2). Luottamuksellista tietoa sisältävät tietovälineet hävitetään turvallisesti, kun niitä ei enää tarvita.

Järjestelmäsuunnittelu

g) Suorituskykyvaatimuksia seurataan ja tulevista suorituskykyvaatimuksista tehdään arvioita, jotta voidaan varmistaa riittävän suoritustehon ja tallennustilan saatavuus.

Tapahtumailmoitukset ja niihin reagointi

h) Varmentaja toimii oikea-aikaisesti ja koordinoidusti, jotta tietoturvaloukkauksiin voidaan reagoida ripeästi ja jotta niiden vaikutuksia voidaan rajoittaa. Kaikista tietoturvaloukkauksista ilmoitetaan mahdollisimman pian tapahtuman jälkeen.

i) Kohdan 7.4.11 vaatimukset täyttävät auditointiprosessit aloitetaan järjestelmän käyttöönoton yhteydessä ja niitä jatketaan järjestelmän käytöstä poistamiseen asti.

j) Auditointilokeja seurataan ja tarkistetaan säännöllisesti, jotta haitallisista toimista voidaan havaita näyttöä.

Varmenteiden luominen, peruutusten hallinta

Toiminnassa noudatettavat menettelytavat ja vastuualueet

k) Varmentajan turvatoiminta on erotettava tavanomaisesta toiminnasta.

Varmentajan turvatoiminnan vastuualueita ovat

- toimintatavat ja vastuualueet
- turvallisten järjestelmien suunnittelu ja hyväksyminen
- haittaohjelmilta suojautuminen
- aputoimet
- verkonhallinta
- aktiivinen auditointipäiväkirjojen seuranta, tapahtumien analysointi ja seuranta
- tietovälineiden käsittely ja turvallisuus
- tietojen ja ohjelmistojen vaihto.

Väestörekisterikeskus käyttää varmennetuotannon rekisteröinti- ja tietoteknisiin tehtäviin teknisiä palvelutoimittajia. Väestörekisterikeskus toimii varmentajana, joka vastaa varmennetoiminnasta.

Varmentajan tehtävät on jaettu tehtävänmukaisiin vastuualueisiin, jotka on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Varmentajan turvallisuudesta vastaava taho johtaa näitä vastuualueita, mutta käytännön toiminnassa käyttöhenkilökunta toteuttaa niitä valvonnan alaisena turvallisuutta koskevan asianmukaisen menettelytapaohjeen sekä roolit ja vastuualueet määrittävien asiakirjojen mukaisesti.

Väestörekisterikeskus tarkastaa teknisten toimittajiensa toimitilat, laitteet ja toiminnan tarkoituksenmukaisella tavalla.

Väestörekisterikeskuksen tietoturvatarkastuksen tekee Väestörekisterikeskuksen tietoturvapäällikkö tai ulkopuolinen tarkastaja, joka on erikoistunut varmennepalveluihin liittyvien teknisten toimittajien auditointiin.

Väestörekisterikeskukselle on myönnetty tietoturvasertifikaatti, joka varmentaa, että VRK:n tietoturvallisuus täyttää standardin ISO/IEC 27001 vaatimukset.

Tarkastuksen kohteet määräytyvät laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista tai Väestörekisterikeskuksen suorittaessa tarkastusta tietoturvastandardin ISO/IEC 27001, Väestörekisterikeskuksen tietoturvapolitiikan tai teknisten toimitussopimusten mukaisesti.

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

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

Tarkastuksissa otetaan huomioon hallinnollisen tietoturvallisuuden lisäksi palveluntoimittajat.

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

Tarkastuksen tuloksesta tiedotetaan lain, tietoturvastandardin ISO/IEC 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.

Väestörekisterikeskus tiedottaa tarkastuksen tuloksista Viestintävirastolle vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain sekä Viestintäviraston määräysten ja suositusten mukaisesti.

Laatuvarmentajia valvova Viestintävirasto voi tarkastaa varmentajan toiminnan laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista säädetyin edellytyksin.

Tarkastus kattaa Viestintäviraston antamat määräykset varmentajan toiminnan tietoturvallisuudesta.

7.4.6. Järjestelmiin pääsyn hallinta

Varmentaja varmistaa, että vain asianmukaisesti valtuutetuilla henkilöillä on pääsy varmentajan järjestelmään sähköisistä allekirjoituksista annetun direktiivin liitteen II kohdan f mukaisesti.

Erityisesti:

Varmentaja yleisesti

a) Hallintakeinoja (esimerkiksi palomuureja) on toteutettava, jotta varmentajan sisäisiä verkkotoimialueita voidaan suojata kolmansien osapuolten käytettävissä olevilta ulkoisilta verkkotoimialueilta.

   Palomuurien määrityksissä suositellaan estettäväksi protokollat ja käyttöoikeudet, joita varmentajan toiminta ei edellytä.

b) Luottamuksellinen tieto on suojattava luvattomalta käytöltä tai muokkaamiselta. Luottamuksellinen tieto on suojattava (esimerkiksi salauksella ja eheyden turvaavalla menetelmällä), kun sitä vaihdetaan verkoissa, jotka eivät ole turvallisia.

Rekisteröintitiedot ovat luottamuksellisia tietoja.

c) Varmentajan varmistaa järjestelmän turvallisuuden ylläpitämiseksi tehokkaan käyttäjien (näitä ovat järjestelmän operaattorit ja valvojat sekä kaikki käyttäjät, joille on annettu suorat käyttöoikeudet järjestelmään) käyttöoikeuksien hallinnan, joka sisältää käyttäjätilin hallinnan, auditoinnin sekä oikea-aikaisen käyttöoikeuksien muokkaamisen tai poistamisen.

d) Varmentaja varmistaa, että pääsyä tietoon ja sovellusten järjestelmätoimintoihin rajoitetaan pääsynvalvontaa koskevien menettelytapaohjeiden mukaisesti. Se myös varmistaa, että varmentajan järjestelmässä on riittävästi tietokoneiden turvallisuuden hallintakeinoja, joilla varmentajan käytännöissä määritellyt luotetut roolit voidaan eriyttää ja voidaan eriyttää turvallisuutta valvova rooli operatiivisista toiminnoista. Etenkin järjestelmäapuohjelmien käyttöä rajoitetaan ja valvotaan tiukasti. Käyttöoikeuksia rajoitetaan siten, että käyttäjälle annetaan oikeudet vain sellaisten resurssien käyttöön, joita tarvitaan hänelle osoitetussa roolissa tai rooleissa.

e) Varmentajan henkilöstön jäsenet tunnistetaan ja todennetaan, ennen kuin he käyttävät varmenteiden hallintaan liittyviä kriittisiä sovelluksia.

f) Varmentajan henkilöstön jäsenet asetetaan vastuuseen omista toimistaan, esimerkiksi tapahtumalokien säilyttämisen avulla (katso kohta 7.4.11).

g) Luottamuksellinen tieto suojataan siten, ettei se paljastu sen vuoksi, että luvattomat käyttäjät pääsevät käyttämään uudelleen tallennuskohteita.

   Rekisteröintitiedot ovat luottamuksellisia tietoja.

Varmenteiden luominen

h) Varmentaja varmistaa, että paikallisverkon osat (esimerkiksi reitittimet) pidetään fyysisesti turvallisessa ympäristössä ja että säännöllisissä auditoinneissa varmistetaan, että osien kokoonpanot ovat varmentajan määrittämien vaatimusten mukaisia.

i) Varmentajalla on jatkuvakäyttöinen valvonta- ja hälytysvälineistö, jolla varmentaja voi oikea-aikaisesti havaita luvattomat ja/tai sääntöjenvastaiset yritykset käyttää sen resursseja sekä kirjata tällaiset yritykset ja reagoida niihin.

   Tällainen järjestelmä voi olla esimerkiksi tunkeutumisen havaitsemisjärjestelmä, käyttöoikeuksien valvonta ja hälytysvälineistö.

Jakelu

j) Jakelusovelluksessa on pakotettu käytönvalvonta silloin, kun yritetään lisätä tai poistaa varmenteita tai muokata muita asiaan liittyviä tietoja.

Peruutusten hallinta

k) Varmentajalla on jatkuvakäyttöinen valvonta- ja hälytysvälineistö, jolla varmentaja voi oikea-aikaisesti havaita luvattomat ja/tai sääntöjenvastaiset yritykset käyttää sen resursseja sekä kirjata tällaiset yritykset ja reagoida niihin.

   Tällainen järjestelmä voi olla esimerkiksi tunkeutumisen havaitsemisjärjestelmä, käyttöoikeuksien valvonta ja hälytysvälineistö.

Sulkutila

1) Sulkutilasovelluksessa on pakotettu käytönvalvonta silloin, kun sulkutilatietoja yritetään muokata.

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

   Varmennejärjestelmän laitteistoina käytetään vain käyttötarkoitukseensa sopivia laitteistoja.

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

   Väestörekisterikeskuksen tietoturvallisuutta hallitaan Väestörekisterikeskuksen tietoturvapolitiikan ja standardin ISO/IEC 27001 mukaisesti.

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

7.4.7. Luotettavien järjestelmien käyttöönotto ja ylläpito

Varmentaja käyttää luotettavia järjestelmiä ja tuotteita, jotka on suojattu muutostöiltä sähköisistä allekirjoituksista annetun direktiivin liitteen II f-kohdan mukaisesti.

Luotettavia järjestelmiä koskevien vaatimusten täyttäminen voidaan varmistaa esimerkiksi käyttämällä julkaisun CWA 14167-1 mukaisia järjestelmiä tai soveltuvaa suojausprofiilia (tai -profiileja), joka on määritelty ISO/IEC 15408 -standardin mukaisesti.

Varmentajan palveluja koskevassa riskianalyysissä (katso kohta 7.4.1) on suositeltavaa yksilöidä varmentajan kriittiset palvelut, joissa edellytetään luotettavia järjestelmiä, sekä vaadittava varmuustaso.

Erityisesti:

Varmentaja yleisesti

a) Kaikissa varmentajan toteuttamissa tai teettämissä järjestelmien kehityshankkeissa on tehtävä suunnittelu- ja vaatimusmäärittelyvaiheessa turvallisuusvaatimusten analysointi, jotta voidaan varmistaa, että tietotekniset järjestelmät rakennetaan turvallisiksi.

b) Kaikkien käytettävien ohjelmistojen versioita, muutoksia ja korjauspäivityksiä varten on oltava valvontamenettelyt.

7.4.8. Liiketoiminnan jatkuvuuden hallinta ja häiriötilojen käsittely

Varmentaja varmistaa hätätilanteen sattuessa, esimerkiksi varmentajan yksityisen allekirjoitusavaimen vaarantumistilanteessa, että toiminta palautetaan mahdollisimman pian sähköisistä allekirjoituksista annetun direktiivin liitteen II a kohdan mukaisesti.

Erityisesti:

Varmentaja yleisesti

a) Varmentaja määrittelee hätätilanteen sattuessa toteutettava jatkuvuussuunnitelma ja

ylläpidettävä sitä.

Varmentajan järjestelmien varmuuskopiointi ja palautus

b) Varmentajan toimintojen palauttamisessa tarvittavat varmentajan järjestelmätiedoista otetaan varmuuskopiot ja niitä säilytetään turvallisessa ja asianmukaisessa paikassa, jotta varmentaja voi nopeasti palauttaa toimintansa häiriö- tai hätätilanteessa.

ISO/IEC 17799 -standardin kohdan 8.4.1 mukaisesti liiketoiminnan olennaiset tiedot ja ohjelmtot on varmuuskopioitava säännöllisesti. Käytössä on oltava tarkoituksenmukainen varmuuskopiointivälineistö, jolla varmistetaan, että kaikki liiketoiminnan kannalta olennaiset tiedot ja ohjelmistot voidaan palauttaa hätätilanteen tai tietovälineen toimintahäiriön jälkeen. Yksittäisten järjestelmien varmuuskopiointijärjestelyt on testattava säännöllisesti, jotta voidaan varmistaa niiden täyttävän liiketoiminnan jatkuvuussuunnitelman vaatimukset.

c) Varmuuskopiointi- ja palautustoiminnot suorittavat asiaankuuluvissa, kohdassa 7.4.3 määritellyissä luotetuissa rooleissa toimivat henkilöt.

Riskianalyysin määrittelyn mukaisesti saman henkilömäärän on oltava toimenpiteen suorituksen aikana läsnä kuin saman toiminnan muiden osa-alueiden suorittamisen aikana.

Varmentajan avaimen vaarantuminen

d) Varmentajan liiketoiminnan jatkuvuussuunnitelmassa (tai hätätilanteesta palautumissuunnitelmassa) on pidettävä hätätilanteena varmentajan yksityisen allekirjoitusavaimen vaarantumista tai epäiltyä vaarantumista.

Varmenteen tilatiedot

e) Avaimen vaarantumistilanteessa varmentajan on ryhdyttävä vähintään seuraaviin toimiin:
   - Ilmoitettava vaarantumisesta seuraaville: kaikille sellaisille tilaajille ja muille tahoille, esimerkiksi varmenteeseen luottaville osapuolille ja varmentajille, joiden kanssa varmentaja on sopimussuhteessa tai muunlaisessa vakiintuneessa suhteessa. Lisäksi tämä tieto on saatettava muiden varmenteeseen luottavien osapuolten saataville.
   - Ilmoitettava, että varmenteet ja sulkulistat joiden myöntämisessä tai julkaisussa on käytetty kyseistä varmentajan avainta, eivät ehkä ole enää voimassa.

   Jos varmentaja saa tietoonsa, että jonkin toisen varmentajan avain on vaarantunut, on suositeltavaa peruuttaa kyseisen toisen varmentajan mahdollisesti myöntämät varmentajan varmenteet.

Algoritmin vaarantuminen

f) Jos jokin varmentajan tai sen tilaajien käyttämistä algoritmeista tai niihin liittyvistä parametreista osoittautuu riittämättömäksi sen jäljellä olevaa suunniteltua käyttöä varten, varmentajan on toimittava seuraavasti:

- Asiasta on tiedotettava kaikille sellaisille tilaajille ja varmenteeseen luottaville osapuolille, joiden kanssa varmentaja on sopimussuhteessa tai muunlaisessa vakiintuneessa suhteessa. Lisäksi tieto on saatettava muiden varmenteeseen luottavien osapuolten saataville.

- Sen on peruutettava kaikki varmenteet, joita asia koskee.

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

Väestörekisterikeskuksella on poikkeusoloja koskeva jatkuvuus- ja valmiussuunnitelma, joka mahdollistaa Väestörekisterikeskuksen toiminnan jatkuvuuden.

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

7.4.9. Varmentajan toiminnan lakkauttaminen

Varmentaja varmistaa, että sen varmennepolitiikan alaisten palvelujen lakkauttamisesta tilaajille ja varmenteeseen luottaville osapuolille aiheutuvat mahdolliset häiriöt minimoidaan ja että sellaisia tietoja ylläpidetään jatkuvasti, joilla varmentamista koskevia todisteita voidaan esittää oikeudellisissa menettelyissä sähköisistä allekirjoituksista annetun direktiivin II liitteen i kohdan mukaisesti.

Erityisesti:

Varmentaja yleisesti

a) Ennen kuin varmentaja lopettaa palvelunsa, suorittaa vähintään seuraavat toimet:

   - Varmentajan ilmoittaa lopettamisesta seuraaville: kaikille sellaisille tilaajille ja muille tahoille, esimerkiksi varmenteeseen luottaville osapuolille ja varmentajille, joiden kanssa varmentaja on sopimussuhteessa tai muunlaisessa vakiintuneessa suhteessa. Lisäksi tämä tieto saatetaan muiden varmenteeseen luottavien osapuolten saataville.

Varmenteeseen luottavan osapuolen osalta ei edellytetä aikaisempaa suhdetta varmentajaan.

- Varmentaja peruuttaa alihankkijoiltaan kaikki antamansa valtuutukset suorittaa varmentajan puolesta varmenteiden myöntämisprosessiin liittyviä toimintoja.

- Varmentaja toteuttaa tarpeelliset toimet siirtääkseen velvollisuutensa säilyttää rekisteröintitiedot (katso kohta 7.3.1) ja tapahtumalokien arkistot, myös varmenteen tilatiedot, (katso kohta 7.4.11) vaaditun ajan tilaajalle ja varmenteeseen luottaville osapuolille ilmoitetun mukaisesti (katso kohta 7.3.4).

- Varmentaja tuhoaa kohdan 7.2.6 mukaisesti tuhottava yksityiset avaimensa tai pidättäytyy niiden käyttämisestä.

b) Varmentajalla on vähimmäisvaatimusten täyttämisestä aiheutuvat kustannukset kattava järjestely, mikäli se joutuu konkurssiin tai ei muista syistä pysty itse kattamaan kustannuksia, siinä määrin kuin se on sovellettavan konkurssilainsäädännön rajoitusten mukaisesti mahdollista.

c) Varmentajan on käytännöissään ilmoitettava palvelun lakkauttamista koskevat tehdyt varautumistoimet. Näihin kuuluvat
   - ilmoittaminen tahoille, jota asia koskee
   - varmentajan velvollisuuksien siirtäminen muille osapuolille
   - edelleen voimassa olevien myönnettyjen varmenteiden tilatietojen käsittely.

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

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

Ennen varmentajan lakkauttamista suoritetaan vähintäänkin seuraavat toimenpiteet:

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

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

c) Varmentaja varmistaa, että kohdassa 4.6 mainittu saatavuus varmentajan arkistoihin säilyy varmentajan lakkauttamisen jälkeenkin.

d) Varmentaja huolehtii lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 38 § mukaisten tietojen arkistoinnista sekä noudattaa muutoinkin arkistolain säännöksiä tietojen arkistoinnin osalta.

7.4.10. Lainsäädäntöön perustuvien vaatimusten noudattaminen

Varmentajan on varmistettava, että lainsäädäntöön perustuvia vaatimuksia noudatetaan.

Erityisesti:

Varmentaja yleisesti

a) Varmentajan on varmistettava, että se täyttää kaikki sovellettavat lakisääteiset vaatimukset, jotka liittyvät tietojen suojaamiseen menetyksiltä, tuhoamiselta ja väärentämiseltä. Lakisääteisten vaatimusten noudattaminen ja olennaisten liiketoimintojen tukeminen saattaa joidenkin tietojen osalta edellyttää turvallista säilyttämistä (katso kohta 7.4.11).

b) Varmentajan on varmistettava, että kansallisessa lainsäädännössä täytäntöönpannun EU:n tietosuojadirektiivin vaatimuksia noudatetaan.

Näitä menettelytapoja koskevia tietosuojakysymyksiä käsitellään seuraavissa kohdissa:

- Rekisteröinti (myös salanimien käyttö) (katso kohta 7.3.1)
- Tallennettujen tietojen luottamuksellisuus (katso kohdan 7.4.11 alakohta a sekä kohdan 7.3.3 alakohta f)
- Henkilötietoihin pääsyn suojaus (katso kohta 7.4.6)
- Käyttäjän lupa (katso kohdan 7.3.1 alakohta i).

c) Asianmukaisilla teknisillä ja organisaatioon liittyvillä toimilla estetään luvaton tai laiton henkilötietojen käsittely, niiden häviäminen vahingossa tai niiden hävittäminen sekä henkilötietoja koskevat vahingot.

d) Käyttäjien varmentajalle luovuttamat tiedot suojataan täydellisesti, jotta ne eivät joudu kenenkään tietoon ilman käyttäjän lupaa, oikeuden määräystä tai muuta lainvoimaista valtuutusta.

Yleisölle myönnettäviä varmenteita koskevien sopimusehtojen osalta otetaan huomioon kuluttajalainsäädännön vaatimukset, myös kuluttajasopimusten kohtuuttomista ehdoista annettu direktiivi 93/13/ETY

Tämän varmennepolitiikan mukaisesti myönnetty allekirjoitusvarmenne täyttää Euroopan parlamentin ja neuvoston sähköisen allekirjoituksen direktiivin (1999/93/EC) laatuvarmenteelle asettamat vaatimukset.

Vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa (617/2009) on säädetty laatuvarmenteella tehdyistä sähköisistä allekirjoituksista. Sähköisestä henkilökortista on säädetty henkilökorttilaissa (829/1999) ja Väestörekisterikeskuksen myöntämistä varmenteista on säädetty väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetussa laissa (661/2009).

Varmennepalveluiden tuottamiseen liittyvä Väestörekisterikeskuksen vahingonkorvausvastuu määräytyy vahingonkorvauslain (412/1974) säännösten mukaisesti. Väestörekisterikeskusta koskevat myös vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain (617/2009) ja sähköisestä asioinnista viranomaistoiminnassa annetun lain (13/2003) mukaiset vaatimukset.

Sähköisestä asioinnista viranomaistoiminnassa annetun lain mukaan laatuvarmenteella voidaan aina asioida viranomaishallinnossa tarjottavissa sähköisissä palveluissa.

Väestörekisterikeskus noudattaa henkilötietolain (523/1999) mukaista henkilötietojen hyvää tietojenkäsittelytapaa ja viranomaisten toiminnan julkisuudesta annetun lain (621/1999) mukaista hyvää tiedonhallintatapaa. Väestörekisterikeskuksessa tietoturvallisuus turvataan mm. jatkuvalla koulutuksella. Väestörekisterikeskus on myös valmistellut käytännesäännöt sekä tietopalveluille että varmennepalveluille.

Väestörekisterikeskus hankkii rekisteröintiin ja henkilön tunnistamiseen liittyvät tehtävät erillisellä rekisteröintitoimia koskevalla yksityisoikeudellisella sopimuksella. Väestörekisterikeskus voi hankkia palvelun esimerkiksi noudattamalla julkisen hallinnon yhteispalvelusta annetussa laissa (2007/223) noudatettuja säännöksiä.

Väestörekisterikeskuksen asemasta on säädetty rekisterihallintolaissa (166/1996) ja -asetuksessa (248/1996). Laatuvarmentajia valvoo Suomessa Viestintävirasto.

7.4.11. Laatuvarmenteita koskevan tiedon säilyttäminen

Varmentaja varmistaa, että kaikki laatuvarmennetta koskevat tiedot tallennetaan tarkoituksenmukaiseksi ajaksi, erityisesti jotta se voi esittää varmentamista koskevia todisteita oikeudellisissa menettelyissä sähköisistä allekirjoituksista annetun direktiivin II liitteen i kohdan mukaisesti.

Laatuvarmenteita koskevia tallenteita ovat rekisteröintitiedot (katso kohta 7.3.1) ja tiedot varmentajalla sattuneista ympäristöön, avainten hallintaan tai varmenteiden hallintaan liittyvistä merkittävistä tapahtumista.

Erityisesti:

Yleisesti

a) Laatuvarmenteita koskevien nykyisten ja arkistoitujen tallenteiden luottamuksellisuus ja eheys säilytetään.

b) Laatuvarmenteita koskevat tallenteet arkistoidaan julkistettujen liiketoimintatapojen mukaisesti täydellisinä ja luottamuksellisina.

c) Laatuvarmenteita koskevat tallenteet asetetaan tarvittaessa saataville, jotta voidaan esittää varmentamista koskevia todisteita oikeudellisissa menettelyissä. Allekirjoittajalla, ja tietosuojavaatimusten rajoissa myös tilaajalla (katso kohta 7.4.10), on pääsy allekirjoittajan rekisteröintitietoihin ja muihin allekirjoittajaa koskeviin tietoihin.

   Tätä voidaan käyttää esimerkiksi varmenteen ja allekirjoittajan välisen yhteyden varmistamiseen.

d) Varmentajalla sattuneiden ympäristöön, avainten hallintaan tai varmenteiden hallintaan liittyvien merkittävien tapahtumien tarkka ajankohta on kirjattava.

   Varmentaja ilmoittaa käytännöissään tapahtumien ajoittamisessa käytettävän kellon tarkkuus sekä miten kyseinen tarkkuus varmistetaan.

e) Laatuvarmenteita koskevia tallenteita on säilytettävä tarkoituksenmukaisen ajan, jota edellytetään sähköisten allekirjoitusten tueksi vaadittavien oikeudellisten todisteiden esittämiseen sovellettavan lainsäädännön mukaisesti.

   Jos käyttötarkoitukseltaan erilaisia varmenteita koskevat eri säilytysajat, varmenteissa käytetään eri laatuvarmennepolitiikkojen tunnuksia. Jos rekisteröintitietojen ja tapahtumalokitietojen eri osia koskevat eri säilytysajat, tästä ilmoitetaan tilaajalle ja varmenteeseen luottavalle osapuolelle kohtien 7.3.1 ja 7.3.4 mukaisesti.

f) Tapahtumat kirjataan lokiin siten, ettei niitä voi helposti poistaa tai tuhota kyseisiltä tiedoilta vaadittavan säilytysajan kuluessa.

g) Varmentajan dokumentoi sellaiset tapahtumat ja tiedot, jotka on tallennettava lokiin.

Kansalaisvarmenteen 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 10 vuoden ajan varmenteiden voimassaolon päättymisestä.

Varmentajan arkistoimat tiedot on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Arkistotiedot säilytetään varmentajana toimivaa viranomaista koskevien säännösten mukaisesti.

Arkistoitava tieto säilytetään korkean turvatason tiloissa, joissa on pääsynvalvonta.

Varmuuskopiot varastoidaan fyysisesti erilliseen tilaan alkuperäisistä tiedoista.

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

Rekisteröinti

h) Varmentaja varmista, että lokiin kirjataan kaikki rekisteröintiin liittyvät tapahtumat, myös varmenteen uusimista tai sen avainparin vaihtamista koskevat pyynnöt.

i) Varmentaja varmistaa, että kaikki rekisteröintitiedot tallennetaan, vähintään seuraavat:

- rekisteröintiä varten hakijan esittämän asiakirjan tai -kirjojen tyyppi
- tallenne yksilöivistä tunnistamistiedoista, -numeroista tai niiden yhdistelmästä (esimerkiksi hakijan ajokortin numero) tai tarvittaessa tunnistamisasiakirjoista
- paikka, jossa säilytetään kopioita hakemuksista ja tunnistamisasiakirjoista, myös allekirjoitetusta tilaajan sopimuksesta (katso kohdan 7.3.1 alakohta i);
- tarkentavat valinnat tilaajan sopimuksessa (esimerkiksi lupa varmenteen julkaisuun) katso kohdan 7.3.1 alakohta i
- hakemuksen hyväksyvä taho
- tunnistamisasiakirjojen aitouden todentamisessa käytetty menetelmä
- vastaanottavan varmentajan nimi ja/tai tarvittaessa toimittavan rekisteröijän nimi.

j) Varmentajan on varmistettava, että allekirjoittajan tiedot säilyvät luottamuksellisina.

Varmenteiden luominen

k) Varmentaja kirjaa lokiin kaikki varmentajan avainten elinkaareen liittyvät tapahtumat.

l) Varmentaja kirjaa lokiin kaikki varmenteiden elinkaareen liittyvät tapahtumat.

Välineen tarjoaminen allekirjoittajalle

m) Varmentaja kirjaa lokiin kaikki tapahtumat, jotka liittyvät varmentajan hallinnoimien avainten, myös varmentajan mahdollisesti luomien allekirjoittajan avainten, elinkaareen.

n) Varmentaja kirjaa kaikki turvallisen allekirjoituksen luomisvälineen valmistamiseen liittyvät mahdolliset tapahtumat.

Peruutusten hallinta

o) Varmentajan on varmistettava, että kaikki peruuttamiseen liittyvät pyynnöt ja ilmoitukset sekä niitä seuranneet toimenpiteet kirjataan lokiin.

7.5. Organisaatioon liittyvät vaatimukset

Varmentajan on varmistettava, että sen organisaatio on luotettava sähköisistä allekirjoituksista annetun direktiivin II liitteen a kohdan mukaisesti. Erityisesti:

Varmentaja yleisesti

a) Varmentajan toiminnassa noudatettavat politiikat ja menettelyt ovat syrjimättömiä.

b) Varmentaja asettaa palvelunsa kaikkien sellaisten hakijoiden saataville, joiden toiminta kuuluu varmentajan ilmoitetun toiminta-alueen piiriin.

c) Varmentaja on kansallisen lainsäädännön mukainen oikeushenkilö.

d) Varmentaja on tehnyt tarkoituksenmukaiset järjestelyt, joilla katetaan sen toiminnan vastuut.

e) Varmentaja on taloudellisesti riittävän vakaa ja sillä on riittävät resurssit, jotta se voi toimia näiden menettelytapojen mukaisesti.

f) Varmentajalla on käytössään menettelytavat ja käytännöt, joilla ratkaistaan asiakkaiden tai muiden osapuolten tekemät, sähköisten luottamuspalvelujen tarjoamista tai muita asiaankuuluvia asioita koskevat valitukset tai riidat.

g) Varmentajalla on asianmukaisesti dokumentoitu sopimus ja sopimussuhde, mikäli palvelujen tarjoamiseen sisältyy alihankintaa, ulkoistamista tai kolmannen osapuolen kanssa tehtyjä järjestelyjä.

Varmenteiden luominen, peruutusten hallinta

h) Varmenteiden luomiseen ja peruutusten hallintaan liittyvien varmentajan osat ovat palvelujen perustamista, tarjoamista, ylläpitämistä ja keskeyttämistä koskevien päätösten osalta riippumattomia muista organisaatioista; etenkään johtajaan, johtotehtävissä toimivaan henkilöstöön ja luotetuissa rooleissa toimivaan henkilöstöön ei kohdistu kaupallisia, taloudellisia tai muita paineita, jotka saattaisivat heikentää luottamusta tarjottaviin palveluihin.

i) Varmenteiden luomiseen ja peruutusten hallintaan liittyvillä varmentajan osilla on toiminnan puolueettomuuden turvaava dokumentoitu rakenne.

Väestörekisterikeskus on tämän varmennepolitiikan mukainen varmenteen myöntäjä. Väestörekisterikeskuksen asemasta on säädetty rekisterihallintolaissa (166/1996) ja -asetuksessa (248/1996).

Tämän varmennepolitiikan mukaisesti myönnetty allekirjoitusvarmenne täyttää Euroopan parlamentin ja neuvoston sähköisen allekirjoituksen direktiivin (1999/93/EC) laatuvarmenteelle asettamat vaatimukset.

Väestörekisterikeskus noudattaa henkilötietolain (523/1999) mukaista henkilötietojen hyvää tietojenkäsittelytapaa ja viranomaisten toiminnan julkisuudesta annetun lain (621/1999) mukaista hyvää tiedonhallintatapaa. Väestörekisterikeskuksessa tietoturvallisuus turvataan mm. jatkuvalla koulutuksella. Väestörekisterikeskus on myös valmistellut käytännesäännöt sekä tietopalveluille että varmennepalveluille.

Väestörekisterikeskus hankkii rekisteröintiin ja henkilön tunnistamiseen liittyvät tehtävät erillisellä rekisteröintitoimia koskevalla yksityisoikeudellisella sopimuksella. Väestörekisterikeskus voi hankkia palvelun esimerkiksi noudattamalla julkisen hallinnon yhteispalvelusta annetussa laissa (2007/223) noudatettuja säännöksiä.

Väestörekisterikeskus vastaa siitä, että kansalaisvarmenteet on luotu noudattaen väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetussa laissa, laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista, laissa sähköisestä asioinnista viranomaistoiminnassa ja varmennepolitiikassa esitettyjä menettelyjä ja varmenteen hakijan antamien tietojen mukaisesti.

Henkilötietojen käsittely osalta Väestörekisterikeskus noudattaa henkilötietolakia. Väestörekisterikeskus on jatkuvassa yhteistyössä henkilötietojen käsittelyn osalta tietosuojavaltuutetun kanssa.

Valitusten ja riitojen ratkaisussa sekä hallinnollisessa valvonnassa ja lainkäytössä noudatetaan voimassaolevaa lainsäädäntöä. Kansalaisvarmenteen tuotannossa huomioon on otettava erityisesti laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista ja siinä kuvattu valvonta- ja muutoksenhallintamenettely.

Väestörekisterikeskus vastaa kansalaisvarmenteita myöntäessään siitä, että kansalaisvarmenne täyttää tässä kansalaisvarmennetta koskevassa varmennepolitiikassa esitetyt vaatimukset. Mahdolliset erimielisyydet ratkaistaan Suomen oikeusjärjestyksen mukaisesti.

Sähköisen henkilökortin hankintahinta määräytyy kulloinkin voimassa olevan valtiovarainministeriön asetuksen Väestörekisterikeskuksen suoritteista mukaisesti.

Muilla mikrosiruilla olevat kansalaisvarmenteet on hinnoiteltu voimassaolevan Väestörekisterikeskuksen liiketaloudellisia suoritteita koskevan hinnaston mukaisesti.

8. Määrittelypuitteet muita laatuvarmennepolitiikkoja varten

Määritysasiakirjojen hallinta

Tässä kohdassa määritellään laatuvarmenteita myöntävien varmentajien muita varmennepolitiikkoja koskevat yleiset puitteet. Varmentaja voi ilmaista noudattavansa näiden yleisten määrittelypuitteiden vaatimuksia kohdan 8.4 mukaisesti. Vaatimustenmukaisuus edellyttää kohtien 6 ja 7 vaatimusten noudattamista lukuun ottamatta niitä vaatimuksia, joita sovelletaan vain yleisölle varmenteita myöntäviin varmentajiin.

Tätä kohtaa ei sovelleta kumpaankaan kohdassa 5 yksilöityyn laatuvarmennepolitiikkaan, QCP public- ja QCP public + SSCD -laatuvarmennepolitiikkaan.

Väestörekisterikeskuksen kansalaisvarmenteet ovat laatuvarmenteita, minkä vuoksi tätä kohtaa ei sovelleta tämän kansalaisvarmenteen tarjoamiseen liittyen.

8.1. Laatuvarmennepolitiikan hallinta

Varmentaja varmistaa, että sen varmennepolitiikka on ajantasainen. Erityisesti:

a) Varmennepolitiikassa yksilöidään, kumpaan tässä asiakirjassa määriteltyyn laatuvarmennepolitiikkaan se pohjautuu ja mitä mahdollisia muunnelmia siinä sovelle-

taan.

b) Varmentajalla on varmennepolitiikasta vastaava taho, joka vastaa viime kädessä laatuvarmennepolitiikan määrittämisestä ja hyväksymisestä.

c) Liiketoimintavaatimusten arvioimiseksi ja laatuvarmennepolitiikkaan sisällytettävien turvallisuusvaatimusten määrittämiseksi kaikista edellä mainituista osa-alueista laaditaan riskinarviointi.

d) Varmennepolitiikan tai -politiikkojen hyväksymisessä ja muokkaamisessa noudatetaan määriteltyä tarkistusprosessia, joka sisältää laatuvarmennepolitiikan ylläpitovastuut.

e) Tarkistusprosessin tehtävänä on varmistaa, että varmentajan varmennuskäytäntö tukee laatuvarmennepolitiikkoja.

f) Varmentaja asettaa varmentajan tukemat laatuvarmennepolitiikat kaikkien asianomaisten tilaajien ja varmenteeseen luottavien osapuolten saataville.

g) Varmentajan tukemien laatuvarmennepolitiikkojen tarkistukset asetetaan tilaajien ja varmenteeseen luottavien osapuolten saataville.

h) Laatuvarmennepolitiikka sisältää kaikki kohtien 6 ja 7 tai niitä tiukemmat vaatimukset, lukuun ottamatta jäljempänä ilmoitettuja poikkeuksia. Mahdollisissa ristiriitatapauksissa sovelletaan tämän asiakirjan vaatimuksia.

i) Varmennepolitiikalle on hankittu OID-yksilöintitunnus, joka on muodoltaan ITU-T:n suosituksen X.509 mukainen.

Väestörekisterikeskus voi muuttaa määrityksiä lainsäädännöllisten tai toiminnallisten vaatimusten vuoksi. Määritysten muutokset kirjataan varmennepolitiikka- ja varmennuskäytäntöasiakirjoihin tässä kohdassa kuvatulla tavalla.

Väestörekisterikeskus julkaisee varmennepolitiikan ja varmennuskäytännön, jotka ovat saatavilla Internet-sivuilla ja http://www.fineid.fi.

Väestörekisterikeskuksen julkiset varmenteiden tuotantoon liittyvät määritykset ovat saatavilla samoilla Internet-sivuilla.

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

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

Väestörekisterikeskus ilmoittaa muutoksista hyvissä ajoin ennen niiden voimaantuloa sekä Viestintävirastolle että 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 22.2.2016 jälkeen 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 22.2.2016 jälkeen ilmoittamalla niistä 14 päivää aikaisemmin

8.2. Poikkeukset laatuvarmennepolitiikkoihin, jotka koskevat muille kuin yleisölle myönnettäviä laatuvarmenteita

Mikäli varmenteita myönnetään muille kuin yleisölle, kyseistä toimintaa koskevan laatuvarmennepolitiikan ei tarvitse noudattaa seuraavia laatuvarmenteita koskevia menettelytapavaatimuksia:

Varmentajan ei katsota myöntävän laatuvarmenteita yleisölle, jos kyseisten varmenteiden käyttöä on rajoitettu osanottajien välisin vapaaehtoisin yksityisoikeudellisin sopimuksin.

a) vastuu kohdan 6.3 mukaisesti

b) varmenteiden luomispalvelun ja peruuttamisen hallintapalvelun tarjoajien riippumattomuus kohdan 7.5 alakohtien h ja i mukaisesti

c) varmenteiden jakelu julkisesti kohdan 7.3.5 alakohdan f mukaisesti

d) sulkutilatietojen julkinen saatavuus kohdan 7.3.6 alakohdan k mukaisesti.

Väestörekisterikeskuksen kansalaisvarmenteet sisältävät laatuvarmenteen ja vahvan sähköisen tunnistamisen välineen. Tämän vuoksi tätä kohtaa ei sovelleta tämän kansalaisvarmenteen tarjoamiseen liittyen.

8.3. Lisävaatimukset

Tilaajille ja varmenteeseen luottaville osapuolille on ilmoitettava osana kohdan 7.3.4 vaatimusten täyttämistä,

a) mikäli varmennepolitiikka ei koske yleistä käyttöä ja sovelletaanko kohdassa 8.2 mainittuja poikkeuksia

b) mikäli varmennepolitiikka sisältää vaatimuksia turvallisen allekirjoituksen luomisvälineen käytöstä

c) millä tavoin kyseinen politiikka lisää tai tiukentaa tässä asiakirjassa määritellyn laatuvarmennepolitiikan vaatimuksia.

8.4. Vaatimustenmukaisuus

Varmentaja saa ilmaista toimivansa tämän asiakirjan ja sovellettavan laatuvarmennepolitiikan mukaisesti vain,

a) jos varmentaja ilmaisee noudattavansa yksilöityä laatuvarmennepolitiikkaa ja asettaa pyynnöstä tilaajan ja varmenteeseen luottavien osapuolten saataville selvityksen vaa-

timustenmukaisuudesta tai

Selvityksenä voi olla esimerkiksi auditoijan kertomus, jossa vahvistetaan varmentajan noudattavan yksilöidyn laatuvarmennepolitiikan vaatimuksia. Kyseessä voi olla varmentajan organisaation sisäinen auditoija, mutta auditoija ei saa olla hierarkisessa suhteessa varmentajan toimintaa toteuttavaan osastoon.

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

Vaatimustenmukaisuuden arviointia koskee CEN-työryhmän asiakirja 14172 "EESSI Conformity Assessment Guidance".

c) jos myöhemmin osoitetaan, että varmentaja on laiminlyönyt varmennepolitiikan noudattamisen ja että tämä vaikuttaa merkittävästi varmentajan kykyyn täyttää sähköisistä allekirjoituksista annetussa direktiivissä määritellyt laatuvarmenteita koskevat vaatimukset, varmentajan on lopetettava kyseiseen laatuvarmennepolitiikkaan viittaavien varmenteiden myöntäminen, kunnes se on osoittanut vaatimustenmukaisuutensa tai kunnes sen on arvioitu noudattavan kyseisen laatuvarmennepolitiikan vaatimuksia; muussa tapauksessa varmentajan on ryhdyttävä kohtuullisen ajan kuluessa toimenpiteisiin vaatimustenmukaisuutta koskevan laiminlyönnin korjaamiseksi

d) varmentajan vaatimustenmukaisuus on tarkistettava säännöllisesti sekä aina, kun varmentajan toimintaa muutetaan merkittävästi.

Vaatimustenmukaisuuden osoittamiseen vaadittavat menetelmät voivat vaihdella varmentajan sijoittautumisvaltion lainsäädännön mukaan.

Vaatimusten mukainen varmentaja osoittaa, että

a) se täyttää sille kohdassa 6.1 määritellyt vaatimukset

b) se on ottanut käyttöön hallintakeinot, jotka täyttävät kaikki kohdassa 7 esitetyt vaatimukset, lukuun ottamatta seuraavia:

c) kohta 7.2.9, mikäli varmentaja ei edellytä turvallisen allekirjoituksen luomisvälineen käyttöä

d) kohdan 8.2 vaatimukset, mikäli varmentaja ei tarjoa palvelua yleisölle

e) noudattaa kohdan 8.1 vaatimukset täyttävää laatuvarmennepolitiikkaa

f) on ottanut käyttöön hallintakeinot, jotka täyttävät kaikki käytettäviä laatuvarmennepolitiikkoja koskevat lisävaatimukset

g) täyttää kohdassa 8.3 määritellyt lisävaatimukset.

8.5. Versionhallinta

Varmennepolitiikka Väestörekisterikeskuksen kansalaisvarmennetta varten, v.1.1.

Versio	**Päivämäärä**	**Kuvaus / muutokset**
v 1.0	21.11.2013	Hyväksytty versio 1.0.
v 1.1	22.2.2016	Muuttunut sulkulistan voimassaolo 8h