Väestörekisterikeskus
Befolkningsregistercentralen

Varmennuskäytännön tiivistelmä

Suomen sirullisten passien allekirjoitusvarmennetta varten

v.2.0

ISO 9001

ISO/IEC 27001

Sisällysluettelo

1. Johdanto

Tämä dokumentti on Väestörekisterikeskuksen ja Poliisihallituksen laatima tiivistelmä Varmentajan varmennuskäytännöstä liittyen Suomen sirullisten passien varmennejärjestelmään. Varmennuskäytäntöä sovelletaan Väestörekisterikeskuksen myöntämään sirullisten passien allekirjoitusvarmenteeseen (jäljempänä Allekirjoitusvarmenne), joka myönnetään passilaissa määritellylle viranomaiselle. Varmennuskäytäntö ei ole julkinen asiakirja, mutta siihen sisältyvät julkiset asiat tuodaan esille tässä tiivistelmässä. Varmennepolitiikka ja varmennuskäytäntö ovat varmentajan laatimat viralliset osapuolten välillä noudatettavat asiakirjat.

Tämä dokumentti viittaa asiakirjoihin:

Varmennepolitiikka Suomen sirullisten matkustusasiakirjojen ja oleskelulupa-asiakirjojen allekirjoitusvarmennetta varten:

OID: 1.2.246.517.3.10.1

Varmennuskäytäntö Suomen sirullisten passien allekirjoitusvarmennetta varten:

OID: 1.2.246.517.3.10.1.1

2. Varmentaja ja varmenteiden sovellusalueet

Varmentaja tuottaa varmennepalvelut varmennepolitiikassa sekä varmennuskäytännössä mainituin ehdoin ja vastaa niiden toimivuudesta Allekirjoitusvarmenteen haltijalle. Varmentaja vastaa koko varmennejärjestelmän toimivuudesta, myös käyttämiensä teknisten toimittajien osalta. Se on henkilörekisteriä ylläpitävä viranomainen, jonka passilain mukainen tehtävä on tuottaa varmennepalveluita Suomen sirullisiin matkustusasiakirjoihin.

2.1 Varmentaja

Varmentajan tehtävänä on:

- Tarjota passilain tarkoittamia varmennepolitiikan ja varmennuskäytännön mukaisia varmenne-, hakemisto, sulku- ja rekisteröintipalveluita.
- Tunnistaa Allekirjoitusvarmenteen hakija.
- Huolehtia varmenteiden tietosisällön virheettömyydestä.
- Huolehtia varmenteiden sulkemisesta ja varmenteiden sulkulistojen julkaisemisesta.
- Noudattaa varmenteen haltijan tietojen käsittelyssä hyvää tietosuojan tasoa sekä hyvää tietojenkäsittelytapaa.

Varmentajana toimii Väestörekisterikeskus.

2.2 Rekisteröijä

Allekirjoitusvarmenteen rekisteröinti tapahtuu noudattaen varmennuskäytännön luvun 3 mukaisia menettelyitä.

- Rekisteröijä toimii Varmentajan toimeksiannosta ja vastuulla.

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

Rekisteröijänä toimii Väestörekisterikeskus.

2.3 Allekirjoitusvarmenteen haltija

Varmennuskäytännön mukainen Allekirjoitusvarmenne myönnetään Suomen valtiolle, jonka edustaja on sisäasiainministeriön poliisiosasto. Allekirjoitusvarmenteen haltijan tulee noudattaa Varmentajan varmennepolitiikkaa ja varmennuskäytäntöä.

2.4 Varmenteeseen luottava osapuoli

Varmenteeseen luottava osapuoli on henkilö tai organisaatio, joka luottaa varmenteen tietoihin ja joka käyttää varmennetta sähköisen allekirjoituksen tarkistamiseen. Varmenteeseen luottavan osapuolen on tarkastettava, että käytettävä varmenne on voimassa, varmenne ei ole sulkulistalla ja että varmenneketju on eheä.

2.5 Hakemistopalvelu

Hakemistopalvelu on julkinen Internet-palvelu, josta on saatavilla kaikki Varmentajan myöntämät ja hakemistossa julkaistavat Varmentajan varmenteet, allekirjoitusvarmenteet sekä sulkulistat. Hakemistopalvelu on saatavissa osoitteesta ldap://ldap.fineid.fi. Edellä mainittuja varmenteita ja sulkulistoja ei julkaista ICAO:n ylläpitämässä hakemistopalvelussa.

Väestörekisterikeskuksen hakemistopalvelussa on kerrottu myös passeja myöntävän viranomaisen yhteystiedot:

- mail: CSCA.Finland@intermin.fi
- street: Kirkkokatu 12
- postalAddress: GOVERNMENT
- postalCode: FI-00023
- postOfficeBox: PO Box 26
- locality: Helsinki
- telephoneNumber: +358 71 878 0171
- facsimileTelephoneNumber: +358 71 878 8555

2.6 Varmenteen käyttäminen

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

Sirullisten passien allekirjoitusvarmenteen käyttötarkoitus on passin sirulle talletettavien tietojen digitaalisen allekirjoituksen todentaminen. Digitaalinen allekirjoitus varmistaa allekirjoitet-

tujen tietojen aitouden ja eheyden, ts. varmistaa tietojen alkuperän ja sen, ettei tietoja ole muutettu passin valmistamisen jälkeen. Varmentajan varmenteella tarkistetaan allekirjoitusvarmenteiden aitous. Varmenteiden tietojen oikeellisuuden takaa Väestörekisterikeskus.

3. Tekniset turvajärjestelyt

Tekniset turvajärjestelyt on kuvattu yksityiskohtaisesti varmennuskäytännössä.

3.1 Avainparin luominen ja tallettaminen

3.1.1 Avainparin luominen

Varmentaja luo yksityisen allekirjoitusavaimensa ja yksityistä allekirjoitusavaintaan vastaavan julkisen avaimen. Varmentajan yksityistä avainta säilytetään turvamoduulissa. Varmentaja huolehtii siitä, että Varmentajan yksityiset avaimet on suojattu paljastumiselta ja luvattomalta käytöltä. Varmentajan yksityisistä avaimista otetaan varmuuskopio kriittisen tietoturvallisuuden edellyttämällä tavalla.

Varmenteen haltijan avainpari luodaan ja säilytetään varmenteen haltijan toimesta FIPS 140-1 luokan 3 mukaisessa turvamoduulissa.

3.1.2 Avainparin uusiminen

Allekirjoitusvarmenteen julkista avainta ei voi uusia. Uuden avainparin muodostaminen edellyttää uutta Allekirjoitusvarmennetta. Allekirjoitusvarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

3.1.3 Avainparin uusiminen Allekirjoitusvarmenteen sulkulistalle asettamisen jälkeen

Allekirjoitusvarmenteen julkista avainta ja sitä vastaavaa yksityistä avainta ei voi uusia. Uuden avainparin muodostaminen edellyttää uutta Allekirjoitusvarmennetta. Allekirjoitusvarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.

3.1.4 Julkisten ja yksityisten avainten voimassaoloaika

Allekirjoitusavaimet ovat voimassa enintään 3 kuukautta. Allekirjoitusvarmenteen voimassaoloaika on viisi vuotta kolme kuukautta. Allekirjoitusvarmenne voidaan sulkea sen voimassaoloaikana. Allekirjoitusvarmennetta voidaan käyttää allekirjoituksen todentamiseen varmenteen vanhenemisen tai sulkemisen jälkeen, jos varmennettu allekirjoitus on luotu ennen varmenteen sulkemista tai vanhenemisaikaa.

3.1.5 Avainten käyttötarkoitukset

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

Sekä Varmentajan varmenne että Allekirjoitusvarmenne poikkeavat joiltakin osin ICAO:n suosituksista.

Varmentajan varmenne:

Käyttötarkoitus: Varmenteiden ja sulkulistojen allekirjoitus.

ICAO:n suositusten vastaisesti Varmentajan varmenteen käyttötarkoituksina ovat myös digitaalinen allekirjoitus ja hyväksyntä.

Varmenteen haltijan allekirjoitusvarmenne:

Käyttötarkoitus: Digitaalinen allekirjoitus

ICAO:n suositusten vastaisesti Allekirjoitusvarmenteessa on sähköpostiosoite Subject Alternative Name -laajennuksessa.

4. Varmennejärjestelmän elinkaaren hallinta

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

4.1 Järjestelmän kehittämiseen liittyvä valvonta

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

4.2 Järjestelmän valvonta

Varmentaja tallettaa järjestelmän valvontaa varten lokitietoa varmennetuotannon tapahtumista, varmennejärjestelmän käyttöoikeuksien hallinnasta, laitekokoonpanosta, varusohjelmista ja sovellusohjelmista muutoksineen, varmistuksista sekä niiden palautuksista. Varmentaja valvoo myös toimintaan liittyviä asiakirjoja.

4.3 Turvallisuuden hallinta

Väestörekisterikeskuksen tietoturvallisuutta hallitaan Väestörekisterikeskuksen tietoturvapolitiikan ja standardin ISO/IEC 27001 mukaisesti. Väestörekisterikeskuksen tietoturvatarkastuksen tekee Väestörekisterikeskuksen tietoturvapäällikkö tai ulkopuolinen tarkastaja, joka on erikoistunut varmennepalveluihin liittyvien teknisten toimittajien auditointiin. Tarkastus tehdään vähintään kerran vuodessa. Havaitut poikkeamat kirjataan tarkastusraporttiin ja niihin reagoidaan lain, tietoturvastandardin ISO/IEC 27001 ja voimassaolevien toimitussopimusten mukaisesti.

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

Sulkupalvelu:

- tietoliikenneturvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus

Varmennetuotanto:

- työnjaot ja kunkin tehtävät – henkilöstöturvallisuus
- fyysinen turvallisuus
- Varmentajan avaimiin liittyvä turvallisuus
- Varmenteiden tuotantojärjestelmä ja varajärjestelmä
- tietoliikenneturvallisuus

Hakemistopalvelu:

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

5. Toiminnan jatkuvuuden hallinta ja poikkeustapausten käsittely

Väestörekisterikeskuksella on jatkuvuus- ja valmiussuunnitelma, joka mahdollistaa Väestörekisterikeskuksen toiminnan jatkuvuuden. Poikkeustapauksiin varautuminen on kuvattu varmennuskäytännössä.

5.1 Varmentajan yksityinen avain paljastunut tai Varmentajan varmenne on suljettu

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

Tällaisessa tapauksessa varmentaja joko lakkauttaa toimintansa varmennuskäytännössä esitetyllä tavalla tai suorittaa seuraavat toimenpiteet:

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

b) Varmentaja luo uuden avaimen varmennuskäytännön luvun 6 mukaisesti.

c) Kaikki paljastuneella avaimella myönnetyt ja voimassa olevat Allekirjoitusvarmenteet suljetaan yhdellä tai useammalla sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeisen suljetun Allekirjoitusvarmenteen voimassaoloaika on päättynyt. Tieto varmenteen viennistä sulkulistalle on julkisesti saatavilla viimeistään kolmen arkivuorokauden kuluttua siitä, kun sulkupyyntö on todettu pätevästi ja hyväksytty.

d) Varmentaja arkistoi tiedot arkistolain vaatimaksi ajaksi sekä noudattaa muutoinkin arkistolain säännöksiä tietojen arkistoinnin osalta.

5.2 Turvallisuuden vaarantuminen luonnonmullistuksen tai muun katastrofin seurauksena

Väestörekisterikeskuksen tietoturvapolitiikassa on otettu huomioon ulkoisen turvallisuuden vaarantumisen aiheuttamat toimenpiteet. Väestörekisterikeskus on saanut ISO/IEC 27001 – tietoturvasertifikaatin, joka asettaa vaatimukset Väestörekisterikeskuksen toiminnalle myös mahdollisen katastrofin tapahduttua. Varmenteiden myöntämisen ja ylläpidon yhteydessä Väestörekisterikeskus noudattaa tietoturvallisuuden noudattamisesta määriteltyjä menettelytapoja.

6 Varmenne- ja sulkulistaprofiilit

6.1 Varmenteiden tekniset tiedot

6.1.1 Varmentajan varmenne

Varmentajan varmenteen myöntäjä on “Finland Country CA 2”. Kyse on ICAO:n suosittaman ns. flat-mallin mukaisesta self signed –varmenteesta. Väestörekisterikeskus tallettaa varmentajan varmenteet avoimeen kansalliseen hakemistoon.

Varmentajan varmenteen avainparin pituus on 4096 bittiä, allekirjoitusfunktio on SHA-256 ja merkistössä on käytetty UTF8-koodausta.

Issuer:

CN = Finland Country CA 2

OU = VRK

O = Suomi Finland

C = FI

Subject:

CN = Finland Country CA 2

OU = VRK

O = Suomi Finland

C = FI

Voimassaolo = 10 vuotta, 3 kuukautta (3650+3+92+1=3744 vuorokautta)

Varmennesarjanumeroavaruus = 10.100.000-

CRL-url = http://proxy.fineid.fi/crl/fccac2.crl

ARL-url = http://proxy.fineid.fi/arl/fccaa2.crl

6.1.2 Allekirjoitusvarmenne

Passit allekirjoittava allekirjoitusvarmenne, ts. ”Document Signer Certificate”. Väestörekisterikeskus tallettaa Allekirjoitusvarmeet avoimeen kansalliseen hakemistoon.

Allekirjoitusvarmenteen avainparin pituus on 2048 bittiä, allekirjoitusfunktio on SHA-256 ja merkistössä on käytetty UTF8-koodausta

Issuer:

CN = Finland Country CA 2

OU = VRK

O = Suomi Finland

C = FI

Subject:

CN = ICAO Compliant Document Signer for Passports

O = Suomi Finland

C = FI

CPS-URL = http://www.fineid.fi/cp-csca2/

Voimassaolo = 5 vuotta, 3 kuukautta (1825+1+92+1=1919 vuorokautta)

Yksityisen avaimen käyttöaika = enintään 3 kuukautta

Varmennesarjanumeroavaruus = 10.100.000-

CRL-url = http://proxy.fineid.fi/crl/fccac2.crl

ARL-url = http://proxy.fineid.fi/arl/fccaa2.crl

6.1.3 Sulkulistaprofiili

Väestörekisterikeskus tallettaa sulkulistat avoimeen kansalliseen hakemistoon. Sulkulistan allekirjoitusfunktio on SHA-256 ja merkistössä on käytetty UTF8-koodausta.

Issuer:

CN = Finland Country CA 2

OU = VRK

O = Suomi Finland

C = FI

Voimassaolo = 30 vuorokautta

Next Update = 40 vuorokautta

Uusi sulkulista julkaistaan viimeistään voimassaolevan sulkulistan voimassaolon päättymisajankohtaan mennessä. Sulkulista sisältää seuraavan sulkulistan julkaisuajankohdan.

7 Versionhallinta

Varmennuskäytännön tiivistelmä Suomen sirullisten passien Allekirjoitusvarmenteita varten, v 2.0.

Versio	**Päivämäärä**	**Kuvaus / muutokset**
v 1.0	17.8.2006	Hyväksytty versio 1.0.
v 2.0	27.5.2011	Hyväksytty versio 2.0.