DIGI- JA VÄESTÖTIETO-VIRASTO

Varmennuskäytännön tiivistelmä

Suomen luottamien ulkomaisten CSCA-varmenteiden luottamusluettelon allekirjoittamista varten

v.1.1

CERTIFIED SFS ORGANIZATION ISO 9001

kiwa ISO/IEC 27001

Sisällysluettelo

1. Johdanto

Tämä dokumentti on Digi- ja väestötietoviraston ja Poliisihallituksen laatima tiivistelmä Varmentajan varmennuskäytännöstä liittyen Suomen sirullisten matkustusasiakirjojen varmennejärjestelmään. Varmennuskäytäntöä sovelletaan Digi- ja väestötietoviraston myöntämään Suomen luottamien ulkomaisten CSCA-varmenteiden luottamusluettelon allekirjoitusvarmenteeseen ”Master List Signer” (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: 1.2.246.517.2.10.5

Varmennuskäytäntö Master List -allekirjoitusvarmennetta varten:

OID: 1.2.246.517.2.10.5.4

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 Digi- ja väestötietovirasto.

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 Digi- ja väestötietovirasto.

2.3 Allekirjoitusvarmenteen haltija

Varmennuskäytännön mukainen Allekirjoitusvarmenne myönnetään Suomen valtiolle, jonka edustaja on Poliisihallitus. 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.

Master List Signer -varmenteita myöntävän viranomaisen yhteystiedot:

Poliisihallitus

Postiosoite

Vuorimiehentie 3

PL 1000 02150 ESPOO

Vaihde 0295 480 181

Sähköposti: CSCA.Finland@govsec.fi

Kirjaamon sähköposti: kirjaamo.poliisihallitus@poliisi.fi

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.

Suomen luottamien ulkomaisten CSCA-varmenteiden luottamusluettelon allekirjoitusvarmenteen käyttötarkoitus on digitaalisen allekirjoituksen todentaminen. Digitaalinen allekirjoitus varmistaa allekirjoitettujen tietojen aitouden ja eheyden, ts. varmistaa tietojen alkuperän ja sen, ettei tietoja ole muutettu luottamusluettelon valmistamisen jälkeen. Varmentajan varmenteella tarkistetaan allekirjoitusvarmenteiden aitous. Varmenteiden tietojen oikeellisuuden takaa Digi- ja väestötietovirasto.

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 140-2 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 kaksi vuotta. 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

Digi- ja väestötietovirasto 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

Digi- ja väestötietoviraston tietoturvallisuutta hallitaan Digi- ja väestötietoviraston tietoturvapolitiikan ja standardin ISO/IEC 27001 mukaisesti. Digi- ja väestötietoviraston tietoturvatarkastuksen tekee Digi- ja väestötietoviraston 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 voimassa olevien 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

Digi- ja väestötietovirastolla on jatkuvuus- ja valmiussuunnitelma, joka mahdollistaa Digi- ja väestötietoviraston 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 jot-

ka 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 päteväksi 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

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

6 Varmenne- ja sulkulistaprofiilit

6.1 Varmenteiden tekniset tiedot

6.1.1 Varmentajan varmenne

Varmentajan varmenteen myöntäjä on CSCA Finland “Finland Country CA 5”. Kyse on ICAO:n suosittaman ns. flat-mallin mukaisesta self signed –varmenteesta. Digi- ja väestötietovirasto tallettaa varmentajan varmenteet avoimeen kansalliseen hakemistoon.

Varmentajan varmenteen avainparin pituus on 512 bittiä, allekirjoitusfunktio on ECC ja merkistössä on käytetty UTF8-koodausta, pois lukien C-kenttä joka on PrintableString.

Issuer:

CN = CSCA Finland

OU = VRK

O = Finland

C = FI

Subject:

CN = CSCA Finland

OU = VRK

O = Finland

C = FI

Voimassaolo = 10 vuotta, 3 kuukautta (3650+92=3742 vuorokautta)

Varmennesarjanumeroavaruus = 10.400.000-

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

6.1.2 Allekirjoitusvarmenne

Suomen luottamien ulkomaisten CSCA-varmenteiden luottamusluettelon allekirjoittava allekirjoitusvarmenne, ts. ” ICAO Compliant Master List Signer”. Digi- ja väestötietovirasto tallettaa Allekirjoitusvarmeet avoimeen kansalliseen hakemistoon.

Allekirjoitusvarmenteen ECC-avainparin pituus on 512 bittiä, allekirjoitusfunktio on BrainpoolP512r1.

Issuer:

CN = CSCA Finland

OU = VRK

O = Finland

C = FI

Subject:

CN = ICAO Compliant Master List Signer

O = Finland

C = FI

CPS-OID = 1.2.246.517.2.10.5.4

CPS-URL = Ei käytössä

Voimassaolo = 2 vuotta (730 vuorokautta)

Varmennesarjanumeroavaruus = 10.400.000-

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

Toissijainen CRL-url = https://pkddownload1.icao.int/CRLs/FIN.crl

6.1.3 Sulkulistaprofiili

Digi- ja väestötietovirasto tallettaa sulkulistat avoimeen kansalliseen hakemistoon. Sulkulistat allekirjoitetaan CA:n avaimilla ja niissä käytetään samaa allekirjoitusalgoritmia kuin ko. CA:n CA-varmenteen allekirjoituksessa.

Issuer:

CN = CSCA Finland

OU = VRK

O = Finland

C = FI

Voimassaolo = 30 vuorokautta

Next Update = 40 vuorokautta

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

7 Versionhallinta

Varmennuskäytännön tiivistelmä Suomen luottamien ulkomaisten CSCA-varmenteiden luottamusluettelon Allekirjoitusvarmenteita varten, v 1.1.

Versio	**Päivämäärä**	**Kuvaus / muutokset**
v 1.0	2.11.2023	Uusi asiakirjaversio 1.0.
v 1.1	1.2.2024	Poliisihallituksen kommentit huomioitu.