Varmennepalvelut

11.5.2023

Palvelukuvaus

DVV:n kansalaisvarmenne henkilökortilla tai muulla teknisellä alustalla

11.5.2023

Dokumentinhallinta

Omistaja	
Laatinut	Anita Holkko
Tarkastanut	
Hyväksynyt	

Version hallinta

versionro	mitä tehty	pvm/henkilö
0.5	Luonnos	26.10.2017
1.0	Päivitetty säädösviittaukset. Lisätty maininta sosiaalihuollon varmentajuudesta. Kieliasulliset korjaukset	5.3.2018 Katja Lingonheimo, Anita Holkko
1.1	Päivitetty Väestörekisterikeskuksen muutos Digi- ja väestövirastoksi	19.3.2020 Anita Holkko
1.2	Korjattu kieliasua ja päivitetty linkit. Tarkennettu kohtaan 2.2, kuinka henkilökortin hakuprosessi etenee.	2.3.2023 Annika Gibson
1.3	Päivitetty lukua 6.1 Avainparien luominen algoritmien ja avainpituuksien osalta.	11.5.2023 Tuomo Hakala

Sisällysluettelo

1 Johdanto 4
2 Kansalaisvarmenteen hakeminen ja rekisteröinti 5
2.1 Kansalaisvarmenteen myöntämisen edellytykset 6
2.2 Kansalaisvarmenteen hakeminen 6
2.3 Rekisteröintiprosessi 8
2.4 DVV:n kansalaisvarmenteen tietojen arkistointi 9
3 DVV:n varmenteiden hakemistopalvelu 10
4 Varmenteen sulkeminen 10
5 Neuvontapalvelu 10
6 Kansalaisvarmenteen käyttöön liittyvät turvaratkaisut 10
6.1 Avainparien luominen 10
6.2 PKI-toiminnallisuudet kansalaisvarmenteen varmennealustalla ja aktivointitiedot 11
6.3 Julkisen avaimen, varmennealustatietojen ja varmennetietojen toimittaminen 11
7 Valvonta ja laadunseuranta 11

Digi- ja väestötietoviraston (DVV) kansalaisvarmenne henkilökortilla tai muulla teknisellä alustalla

1 Johdanto

Digi- ja väestötietovirasto (DVV) (31.12.2019 asti Väestörekisterikeskus) tuottaa korkealaatuisia sähköisessä asioinnissa tarvittavia tunnistusratkaisuja yhteiskunnan eri tarpeisiin. DVV (31.12.2019 asti VRK) on toiminut varmentajana vuodesta 1999 tuottaen varmenteita julkiselle ja yksityiselle sektorille sekä vuodesta 2011 lähtien terveydenhuoltosektorille. DVV on toiminut myös sosiaalihuollon lakisääteisenä varmentajana vuodesta 2015 alkaen. DVV:n Varmennetietojärjestelmä ja varmennepalvelut perustuvat julkisen avaimen järjestelmään (Public Key Infrastructure eli PKI).

DVV:n toimintaa sähköisen tunnistuspalvelun tarjoajana ja hyväksyttynä luottamuspalvelun tarjoajana (aikaisemman sääntelyn nojalla laatuvarmentaja) säätelee syyskuussa 2014 voimaan tullut Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (ns. eIDAS-asetus). Direktiivi 1999/93/EY on sisältänyt sähköisiä allekirjoituksia koskevan sääntelyn. eIDAS-asetus on jäsenvaltioissa suoraan sovellettavaa oikeutta ja sitä on sovellettu 1.7.2016 alkaen.

Edellä mainittua EU-sääntelyä täydentää komission täytäntöönpanoasetus (EU) 2015/1502, teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti (ns. varmuustasoasetus). Varmuustasoasetuksen vaatimukset täyttäessään palveluntarjoaja profiloituu Suomessa sähköisten tunnistuspalvelujen osalta korotetun tai korkean varmuustason mukaisena palveluntarjoajana. DVV tarjoaa korkean varmuustason mukaisia sähköisiä tunnistuspalveluja.

Kansallisessa laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) säädetään vahvan sähköisen tunnistamisen palvelujen tarjoamisesta ja sähköisistä luottamuspalveluista, mm. sähköisestä allekirjoituksesta, ja niiden oikeusvaikutuksista. Lakia on muutettu vastaamaan eIDAS-asetuksen vaatimuksia (ent. laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista) ja muutokset ovat tulleet voimaan 1.7.2016 alkaen.

DVV on toiminut laatuvarmentajana 31.3.2003 lukien. Direktiivin 1999/93/EY ja kansallisen lainsäädännön mukaisesti tuotettuja DVV:n laatuvarmenteita pidetään eIDAS-asetuksen mukaisina sähköisten allekirjoitusten hyväksyttyinä varmenteina niiden voimassaolon päättymiseen saakka. DVV:tä varmennepalvelujen tarjoajana pidetään eIDAS-asetuksen mukaisena hyväksyttynä luottamuspalvelun tarjoajana (mm. sähköisten allekirjoitusten hyväksyttyjen varmenteiden tarjoajana) DVV:n osoittaessa valvontaelimenä toimivalle Traficomille täyttävänsä hyväksytyn luottamuspalvelun tarjoajalle asetetut vaatimukset.

Digi- ja väestötietovirasto vastaa varmentajana koko Varmennetietojärjestelmän turvallisuudesta, luotettavuudesta ja toimivuudesta. Varmentaja vastaa kaikista varmennetoiminnan osa-alueista, myös varmentajan apunaan käyttämien alihankkijoiden tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta. Varmentaja vastaa toimeksiantona hankkimistaan palveluista samoin kuin olisi itse tuottanut palvelun.

DVV:n Varmennetietojärjestelmä on korkean turvatason ja hyväksytyn varmenteen vaatimukset sekä poikkeusoloihin varautumisen vaatimukset täyttävä tietojärjestelmäkokonaisuus (kahdennetut järjestelmät hajautettuna eri konesaleihin).

Digi- ja väestötietovirasto luo kansalaiselle sähköisen henkilöllisyyden samoin kuin se antaa henkilötunnuksen. Sähköinen asiointitunnus (SATU) toimii varmenteessa henkilön yksilöivänä tunnistetietona. Se on numeroista ja tarkistusmerkistä muodostettu tietojoukko, jonka avulla yksilöidään Suomen kansalaiset ja kotikuntalain mukaisesti Suomessa vakinaisesti asuvat ulkomaalaiset, jotka on merkitty väestötietojärjestelmään.

Sähköinen asiointitunnus aktivoidaan, kun henkilö hankkii Digi- ja väestötietoviraston kansalaisvarmennetta hyödyntävän varmennekortin, esimerkiksi henkilökortin. Kansalaisvarmenne on sähköinen henkilöllisyys, joka sisältää muun muassa etunimen, sukunimen ja sähköisen asiointitunnuksen.

Varmennetta käytetään tunnistautumiseen sekä sähköpostien ja dokumenttien salaamiseen ja sähköiseen allekirjoitukseen. Sähköisesti allekirjoitettu asiakirja on juridisesti yhtä sitova ja kiistämätön kuin käsin allekirjoitettu. Kansalaisvarmenteen avulla tapahtuva sähköinen asiointi on turvallista.

Varmennetietojärjestelmän palvelut ovat ympärivuorokautisessa valvonta- ja hallintapalvelussa. Varmennetietojärjestelmän CA-järjestelmällä on oma suljettu korkean turvatason tietoliikenneverkko.

2 Kansalaisvarmenteen hakeminen ja rekisteröinti

Kansalaisvarmenteen rekisteröintiprosessi noudattaa voimassaolevaa lainsäädäntöä ja henkilökorttilakia (663/2016).

Hakija voi laittaa henkilökorttihakemuksen vireille poliisin sähköisessä asiointipalvelussa, poliisin lupapalvelupisteessä tai Suomen ulkomaan edustuksessa. Suomen ulkomaan edustuksen muodostavat diplomaattiset edustustot ja konsuliedustustot.

DVV:n kansalaisvarmenne tilataan viranomaisen myöntämälle varmennealustalle (esim. henkilökortti, USB-token). Poliisi tai Suomen ulkomaan edustusto suorittaa kansalaisvarmenteen rekisteröinnin. Rekisteröinnin yhteydessä rekisteröintitietojärjestelmään lisätään kansalaisvarmenteen luomisessa ja hallinnoimisessa tarvittavat tiedot, jotka toimitetaan korttitilauksen yhteydessä korttitehtaalle.

Korttitehtaalla varmennealustan valmistamisen yhteydessä tehdään DVV:n varmennejärjestelmän työasemalla varmenteiden (allekirjoitusvarmenne, tunnistus- ja salausvarmenne) luontipyyntö CA:lle. CA luo pyydetyt varmenteet ja palauttaa ne kortti-

tehtaalle, jossa nämä luodut varmenteet tallennetaan varmennealustalle. Korttitehdas toimittaa päivittäin eräajona DVV:n järjestelmään tiedot luoduista varmenteista sekä henkilön ja varmennealustan yksilöimiseksi tarpeelliset tiedot. Korttitehdas toimittaa aktivointitunnusluvun ja varmennealustan hakijalle normaalin toimitusmenettelynsä mukaisesti.

Poliisin myöntämän henkilökortin osalta tarkemmat hakemiseen liittyvät ohjeet https://poliisi.fi/henkilokortti.

Edustustoverkosta ja henkilökortin hakemisesta ulkomailla saa tarkempia tietoja ulkoministeriöstä https://um.fi/hakeminen-ulkomailla.

2.1 Kansalaisvarmenteen myöntämisen edellytykset

Kansalaisvarmenne voidaan myöntää vain Suomen kansalaiselle sekä ulkomaalaiselle, jolla on kotikuntalaissa tarkoitettu kotikunta Suomessa, jonka tiedot on talletettu väestötietojärjestelmään ja jonka henkilöllisyys on luotettavasti todennettu. Lisäksi edellytetään, että ulkomaalaisella on voimassa oleva oleskelulupa tai oleskelukortti taikka että hänen oleskeluoikeutensa on rekisteröity.

Kansalaisvarmenteen myöntämis- ja rekisteröintiprosessi perustuu väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (VTVPL) 66§:ään. Kansalaisvarmenne voi sijaita henkilökortilla tai muulla viranomaisen myöntämällä teknisellä alustalla (VTVPL 61 §).

Kansalaisvarmenteen myöntää Digi- ja väestötietovirasto. Rekisteröijänä toimii Poliisi.

Ulkomailla oleskelevalle Suomen kansalaiselle rekisteröijänä toimii poliisin sijasta Suomen ulkomaan edustusto.

Poliisi voi myöntää henkilökortin edellä mainitut edellytykset täyttävälle ulkomaalaiselle. Ulkomaalaiselle myönnettyä henkilökorttia ei voi käyttää matkustusasiakirjana.

Matkustusasiakirjaksi kelpaavaa henkilökorttia ei myönnetä, jos hakija on määrätty pakkokeinolaissa tarkoitettuun matkustuskieltoon tai konkurssilaissa tarkoitettuun maastapoistumiskieltoon. Jos tavallista henkilökorttia ei edellä mainituista syistä voida myöntää, hakijalle voidaan myöntää henkilökortti, jolla ei voi matkustaa mutta jota voidaan käyttää sähköisessä asioinnissa.

Digi- ja väestötietovirasto vastaa koko varmennejärjestelmän toiminnasta, myös käyttämistään ulkopuolisista rekisteröijistä.

2.2 Kansalaisvarmenteen hakeminen

a) Verkkoasioinnissa

   Henkilökorttihakemuksen voi tehdä alusta loppuun Poliisin sähköisessä asiointipalvelussa https://asiointi.poliisi.fi/. Poliisin sähköisen asiointipalvelun käyttöä ulkomailta käsin ei ole estetty, mutta sille ei voida taata samaa palvelutasoa kuin Suomen rajojen sisällä.

Hakijan ei tarvitse saapua henkilökohtaisesti viranomaisen luokse henkilökortin hakemisen yhteydessä, jos seuraavat edellytykset täyttyvät:

1. **Hakijalle on myönnetty viimeisen 6 vuoden aikana sellainen passi tai henkilökortti, jota haettaessa hakija on asioinut henkilökohtaisesti myöntöviranomaisen luona ja häneltä on otettu sormenjäljet. Hakijan on lisäksi tullut olla myöntöhetkellä vähintään 12-vuotias**. Aiemman passin tai henkilökortin ei tarvitse olla voimassa. Vaatimus sormenjälkien ottamisesta ei koske haettaessa ulkomaalaisen henkilökorttia, koska kyseinen asiakirja ei sisällä sormenjälkiä.

2. **Hakijan nimi on sama kuin viimeksi myönnetyssä passissa tai henkilökortissa.** Jos nimi on muuttunut edellisen passin tai henkilökortin myöntämisen jälkeen, hakijan täytyy käydä antamassa uusi nimikirjoitusnäyte lupapalvelupisteessä.

3. **Hakemukseen on liitetty riittävän tuore, laatuvaatimukset täyttävä valokuva sähköisessä muodossa**. Jos passi- tai henkilökorttirekisterissä on enintään 6 kuukautta vanha kuva, asiointipalvelu antaa liittää sen hakemukseen. Useimmiten näin ei ole, ja uusi kuva on toimitettava sähköisesti. Lähes kaikki valokuvaamot syöttävät passikuvan poliisin valokuvapalvelimelle. Uutta kuvaa verrataan poliisissa aiempiin kuviin. Jos virkailija ei pysty varmistumaan, että kuvat esittävät samaa henkilöä, hän kutsuu hakijan tunnistettavaksi.

   Jos kaksi ensimmäistä ehtoa eivät täyty, hakemuksen voi edelleen tehdä sähköisesti mutta se käsitellään vasta, kun hakija käy poliisin lupapalvelupisteessä tunnistettavana. Järjestelmä kertoo hakijalle hakemusta tehtäessä, tarvitaanko käynti.

   Alaikäiselle ilman huoltajan suostumusta myönnettävää henkilökorttia on mahdollista hakea verkosta, mutta hakemuksen käsitteleminen edellyttää aina hakijan henkilökohtaista käyntiä poliisiasemalla.

b) Lupapalvelupisteessä

Poliisin lupapalvelupisteestä henkilökorttia haettaessa on oltava mukana:

- Yksi (1) kasvokuva (enintään 6 kuukautta vanha), kuva toimitetaan ensisijaisesti sähköisesti, kuten yllä on esitetty. Poliisilaitoksella asioidessa on kuitenkin mahdollista käyttää tulostettua valokuvaa

- luotettava selvitys henkilöllisyydestä (esimerkiksi passi tai EU-kansalaisen henkilökortti, jolla on matkustusoikeus. jos henkilöllä ei ole edellä mainittuja asiakirjoja, kyseeseen voi tulla myös poliisin myöntämä asiakirja erillisen tunnistuksen perusteella.),

- jos hakija on alle 18-vuotias, huoltajan suostumus (paitsi ns. alaikäisen henkilökortti): huoltaja voi antaa suostumuksen verkossa tai huoltajan suostumus -lomakkeella,

- jos ulkomaalaisella henkilöllä ei ole esittää voimassa olevaa henkilöllisyyttä osoittavaa asiakirjaa, hänen tulee esittää voimassa oleva oleskelulupakortti tai oleskelukortti.

Henkilökortin hakijan antamien henkilötietojen tulee vastata henkilötietoja, jotka on merkitty väestötietojärjestelmään. Lisätietoja väestötietojärjestelmästä osoitteessa https://dvv.fi/vaestotietojarjestelma.

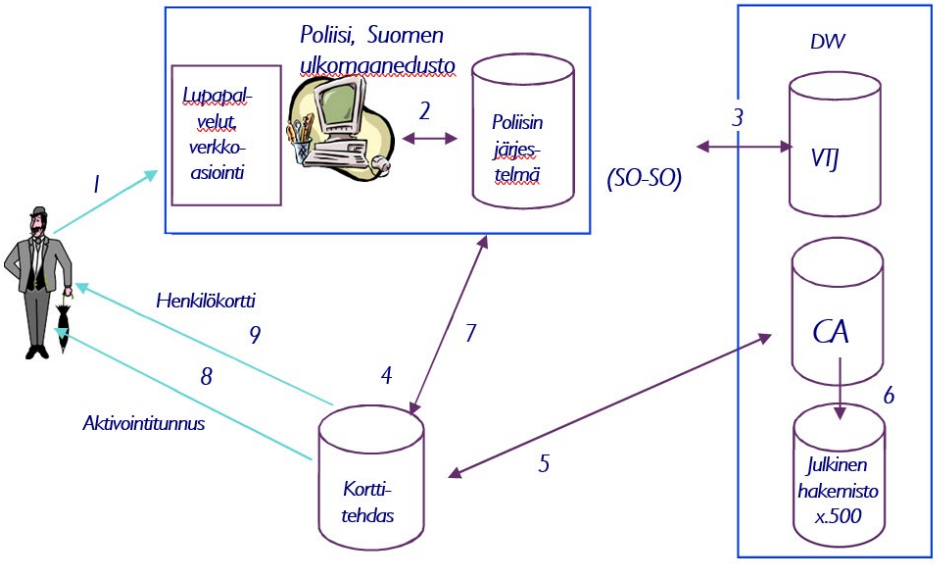
Ulkomaalaisen henkilökortin kansalaisuusmerkintä on aina XXX.

Jos ulkomaalaisen henkilökorttia hakevalla ei ole esittää voimassa olevaa henkilöllisyyttä osoittavaa asiakirjaa, hänen tulee esittää voimassa oleva oleskelulupakortti tai oleskelukortti. Hakemuksen vastaanottava viranomainen saa tällöin ottaa hakijalta sormenjäljet ja verrata niitä oleskelulupakortin tai oleskelukortin tekniseen osaan talletettuihin sormenjälkiin hakijan henkilöllisyyden todentamiseksi. Vertaamista varten otettuja sormenjälkitietoja voidaan käyttää vain vertaamisen ajan, ja ne hävitetään välittömästi vertaamisen jälkeen.

c) Suomen ulkomaan edustoissa

Ulkomailla ollessaan Suomen kansalainen jättää henkilökorttihakemuksen Suomen ulkomaan edustustoon. Edustustoverkosta ja henkilökortin hakemisesta ulkomailla saa tarkempia tietoja ulkoministeriöstä https://um.fi/hakeminen-ulkomailla.

2.3 Rekisteröintiprosessi



Kuva 1 Kansalaisvarmenteen rekisteröinti

1) Hakija voi laittaa henkilökorttihakemuksen vireille poliisin sähköisessä asiointipalvelussa, tai Poliisin lupapalvelupisteessä tai Suomen ulkomaan edustustossa.

2) Asiointipalveluun kirjaudutaan vahvasti tunnistautumalla. Lupapalvelupisteessä rekisteröijä tunnistaa hakijan luotettavasti tämän esittämästä voimassa olevasta Poliisin myöntämästä henkilöllisyyden osoittavasta asiakirjasta (esim. henkilökortista tai passista), tai Maahanmuuttoviraston myöntämästä oleskelulupakortista tai oleskelukortista.

3) Asiointipalvelussa tunnistautumisen yhteydessä järjestelmä tarkistaa henkilön tiedot väestötietojärjestelmästä (VTJ).

   Palvelupisteessä rekisteröijä varmistaa tunnistamisen tiedot syöttämällä hakijan henkilötunnuksen Poliisin tietojärjestelmään, joka hakee rajapinnan kautta VTJ:stä hakijan etunimet, sukunimen sekä sähköisen asiointitunnuksen (SATU).

   Jos VTJ:ssä olevien tietojen ja asiakirjassa olevien tunnistamistietojen välillä on ristiriitoja, pyydetään hakijaa olemaan yhteydessä DVV:hen ennen varmenteen myöntämistä.

4) Tilauksen tiedot välittyvät Poliisin järjestelmän kautta korttitehtaalle.

5) Korttitehdas valmistaa tilatun kortin ja hakee varmenteet DVV:n CA-järjestelmästä.

   Kun kortit on visuaalisesti yksilöity, tehdään erän korteille sertifikaattipyynnöt. Pyynnöt siirretään salasanasuojatulla USB-tikulla erilliseen APM-työasemaan, joka hoitaa sertifikaattien varmentamisen DVV:n varmennepalvelun kanssa. Valmiit varmenteet tallennetaan salasanasuojatulle USB-tikulle, jolla ne siirretään tuotantojärjestelmään.

6) CA julkaisee varmenteet julkiseen hakemistoon.

7) Korttitehdas palauttaa Poliisin järjestelmään kortin tiedot.

8) Kansalaisvarmenteen käyttöönottoon tarvittava aktivointitunnusluku lähetetään asiakkaalle erillisenä lähetyksenä. Aktivointitunnusluku toimitetaan asiakkaalle postitse kahden viikon kuluessa kansalaisvarmennehakemuksen tallentuneeseen osoitteeseen.

9) Kansalaisvarmenteen sisältävä kortti toimitetaan asiakkaalle toimitusprosessin mukaisesti.

Kansalaisvarmenteen käyttöönottoon ja käyttöön liittyvä ohjeistus on julkaistu DVV:n verkkosivuilla dvv.fi/kansalaisvarmenne. Varmentajan toimintaa kuvaavat varmennepolitiikka-asiakirjat ovat saatavilla osoitteessa dvv.fi/cpswww.fineid.fi.

2.4 DVV:n kansalaisvarmenteen tietojen arkistointi

Kansalaisvarmenteen tietojen arkistoinnissa sovelletaan yleislakina arkistolain (831/1994) säännöksiä. Oikeus tietojen saantiin määräytyy viranomaisten toiminnan julkisuudesta annetun lain (621/1999) mukaisesti. Varmennerekisterin tietojen säilyttämisestä on säädetty laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä

luottamuspalveluista (617/2009). Varmennerekisterin tiedot säilytetään 5 vuoden ajan kansalaisvarmenteiden voimassaolon päättymisestä.

3 DVV:n varmenteiden hakemistopalvelu

Hakemistopalvelu on julkinen internetpalvelu, josta on saatavilla kaikki DVV:n myöntämät varmenteet, varmentajan varmenteet sekä sulkulistat. Hakemistopalvelu on saatavissa osoitteesta ldap://ldap.fineid.fi. DVV:n hakemistopalvelu on käytettävissä ympärivuorokautisesti kaikkina vuoden päivinä.

4 Varmenteen sulkeminen

Varmenteen haltijan tulee sulkea henkilökortilla oleva kansalaisvarmenteensa, jos kortti katoaa tai tulee tarpeettomaksi. Varmenne suljetaan soittamalla sulkupalveluun.

Varmenteiden sulkupalvelu on auki ympäri vuorokauden kaikkina viikonpäivinä:

- **Puh. 0800 162 622** (maksuton Suomesta soitettaessa)
- **Ulkomailta soitettaessa +358 800 162 622** (+ paikallisen operaattorin veloitus)

DVV sulkee kansalaisvarmenteen saatuaan tiedon kansalaisvarmenteen haltijan kuolemasta.

5 Neuvontapalvelu

Sirullisen henkilökortin käyttöön ja sähköiseen asiointiin liittyvää neuvontapalvelua on saatavilla maanantaista perjantaihin klo 8 - 21 ja lauantaina klo 9 - 15 numerosta 0600 96160 (pvm/ mpm). Palvelu on suljettu sunnuntaisin ja arkipyhinä. Neuvontapalvelu palvelee suomeksi, ruotsiksi ja englanniksi. Kysymykset voi lähettää myös sähköisesti osoitteessa http://www.kansalaisneuvonta.fi.

6 Kansalaisvarmenteen käyttöön liittyvät turvaratkaisut

6.1 Avainparien luominen

Varmennealustalla on korttivalmistajan generoimana DVV:n varmenteita varten kaksi kappaletta 384-bittistä EC-avainparia sekä yksi 3072-bittinen RSA-avainpari.

Avainparien generointi tapahtuu sirulla (On Board Key Generation), jolloin avainparin yksityistä komponenttia (private key) ei tuoda missään vaiheessa sirun ulkopuolelle.

Avainten luontiympäristöön ja operoinnin turvallisuuteen vaikuttavia tapahtumia valvotaan ja niistä kerätään lokitietoja, joista selviää, kuka on tehnyt, milloin on tehty ja mahdollisuuksien mukaan, mitä on tehty.

6.2 PKI-toiminnallisuudet kansalaisvarmenteen varmennealustalla ja aktivointitiedot

Kansalaisvarmenteen käyttö sähköisessä asioinnissa edellyttää aktivointia aktivointitunnusluvun avulla. Kun kansalaisvarmennetta käytetään ensimmäisen kerran sähköisessä asioinnissa, käynnistetään kansalaisvarmenteen aktivointiprosessi. Tämän prosessin aikana käyttäjältä kysytään aktivointitunnusluku, jonka jälkeen käyttäjä voi aktivoida ja määritellä omat, henkilökohtaiset PIN-tunnuslukunsa.

Aktivoitavia tunnuslukuja on kaksi. Perustunnusluku, jonka avulla käyttäjä kontrolloi kansalaisvarmenteen ylläpitoa ja sähköistä tunnistautumista ja allekirjoitustunnusluku, jonka avulla käyttäjä voi tehdä sähköisen allekirjoituksen. Jos käyttäjä antaa tunnusluvun viisi kertaa väärin, kortti lukittuu eikä tunnusluvun suojaamaa toimintoa voi enää käyttää. Perustunnusluvun lukittuminen estää kaikkien tunnusluvun suojaamien sovellutusten käytön. Allekirjoitustunnusluvun lukittuminen estää sähköisen allekirjoituksen käytön. Lukkiutuneet tunnusluvut vapautetaan aktivointitunnusluvulla.

6.3 Julkisen avaimen, varmennealustatietojen ja varmennetietojen toimittaminen

Korttitehtaan, Poliisin ja DVV:n on varmistettava, että järjestelmien välillä toimitettavat tiedot eivät paljastu asiaankuulumattomille tahoille ja että asiaankuulumattomat tahot eivät pääse muuttamaan tai tuhoamaan välitettäviä tietoja. Korttitehdas ei saa kopioida, tallettaa eikä luovuttaa DVV:n varmenteen hakijalle luovutettavia yksityisiä avaimia eikä niiden luomisessa käytettyjä tietoja. Jos yksityiset avaimet luodaan sirun ulkopuolella, korttitehdas hävittää yksityiset avaimet omista järjestelmistään viivytyksettä sirulle tallettamisen jälkeen. Julkiset, mutta vielä varmentamattomat avaimet säilytetään turvallisesti. Varmennealustan ja varmenteiden tiedot on toimitettava luotettavalla tavalla korttitehtaan, Poliisin ja DVV:n järjestelmien välillä.

7 Valvonta ja laadunseuranta

Digi- ja väestötietovirasto vastaa myös kansalaisvarmenteen valvonnasta ja jatkokehityksestä saamansa palautteen ja ilmenneiden kehitystarpeiden perusteella. Myös alihankkijoiden uudet innovaatiot (teknologian kehittyminen) vaikuttavat jatkokehitykseen.

Kansalaisvarmenteen laatua seurataan laaturyhmässä, jossa edustettuina ovat kortinvalmistaja, Poliisi, Ulkoministeriö ja Digi- ja väestötietovirasto. Huomioon otetaan tällöin kansalaisvarmenteen valmistukseen liittyvien prosessien ja niitä ylläpitävien yhteistyökumppaneiden toiminta ja siinä esiintyvät poikkeamat. Poikkeamista raportoidaan sovitun menettelytavan mukaisesti DVV:n johdolle ja sidosryhmille.

Kansalaisvarmenteen luovutusta seurataan seurantaryhmässä, jossa edustettuina ovat kortinvalmistaja, Poliisi, jakelija ja Digi- ja väestötietovirasto.