

VARMENNEKUVAUS

Väestökisterikeskuksen kansalaisvarmenne
v. 1.1



ISO 9001



ISO/IEC 27001



Väestökisterikeskus



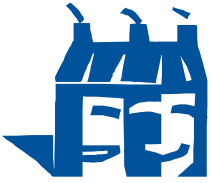
1.1.2017

DOKUMENTINHALLINTA

Omistaja	Jukka Santala
Laatinut	Tuire Saaripuu
Tarkastanut	
Hyväksynyt	

VERSION HALLINTA

versionro	mitä tehty	pvm/henkilö
v. 1.0	Hyväksytty versio 1.0., eIDAS-asetuksen mukainen asiakirja	1.7.2016 TS
v. 1.1	Viestintäviraston M72/2016 vaatimukset, kaksi allekirjoitusvarmennetta (ECC ja RSA). Uuden henkilökortin mukaiset vaatimukset.	1.1.2017 TS

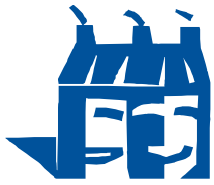


VP/Saaripuu Tuire

1.1.2017

Sisällysluettelo

1 Varmennekuvaus.....	4
1.1 Varmentajan yhteystiedot.....	4
1.2 Varmenteen tyyppi, tarkistamismenettely ja käyttötarkoitus.....	5
1.3 Varmenteeseen luottaminen.....	5
1.4 Varmenteen haltijan velvollisuudet.....	6
1.5 Varmenteeseen luotavan osapuolen varmenteen tarkistamiseen liittyvät velvollisuudet.....	6
1.6 Vastuunrajoitukset.....	6
1.7 Sovellettavat sopimukset, varmennuskäytäntö ja varmennepolitiikka.....	7
1.8 Yksityisyyden suoja.....	8
1.9 Korvauskäytäntö.....	8
1.10 Sovellettava lainsäädäntö ja erimielisyyksien ratkaiseminen	8
1.11 Varmentajan toiminnan tarkastusmenettely	9



1.1.2017

JOHDANTO

Tämä dokumentti kuvaa yleisellä tasolla varmentajan toimintatapoja sekä varmenteen käytön ehtoja ja rajoituksia.

Tämä dokumentti viittaa asiakirjoihin:

Varmennepolitiikka Väestörekisterikeskuksen kansalaisvarmennetta varten

OID:1.2.246.517.1.10.22;

Varmennuskäytäntö sähköisellä henkilökortilla olevaa kansalaisvarmennetta varten

OID: 1.2.246.517.1.10.22.1;

Varmennuskäytäntö kansalaisvarmenne henkilökortilla sairausvakuutustiedoin

OID 1.2.246.517.1.10.22.4;

Väestörekisterikeskus noudattaa EU-asetuksen N:o (EU) 910/2014 luottamuspalveluiden mukaista yleisölle myönnettäviä allekirjoitusvarmenteita koskevaa varmennepolitiikkaa. Asiakirjan viitetiedot ovat ETSI EN 319 411-1 [2], 4.3.5. kohdan 3) QSCD mukaisesti; OID: 0.4.0.194112.1.2. Tämän varmennepolitiikan mukaisesti myönnettäviä allekirjoitusallekirjoitusvarmenteita voi käyttää sellaisten sähköisten allekirjoitusten vahvistamisessa, jotka vastaavat Asetuksessa kuvattuja sähköisten allekirjoitusten hyväksytyjä varmenteita ja luontivälineitä.

1 Varmennekuvaus

1.1 Varmentajan yhteystiedot

Väestörekisterikeskus

Käyntiosoite: Lintulahdenkuja 4, 00530 Helsinki
Postiosoite: PL 123, 00531 Helsinki

Puhelin/Vaihde: +358 295 535 001

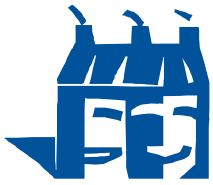
Fax: +358 9 876 4369

E-mail: etunimi.sukunimi@vrk.fi

Kirjaamo: kirjaamo@vrk.fi

www.fineid.fi

Y-tunnus: 0245437-2



1.1.2017

1.2 Varmenteen tyyppi, tarkistamismenettely ja käyttötarkoitus

Kansalaisvarmenne on turvallisen sähköisen asioinnin varmenne, joka voidaan tallettaa erilaisiin viranomaisen myöntämiin teknisiin välineisiin, esimerkiksi sähköiselle henkilökortille tai USB-tokenille.

Kansalaisvarmennetta haetaan käymällä henkilökohtaisesti rekisteröijänä toimivan poliisiviranomaisen tai muun rekisteröintipisteen luona. Käynnin yhteydessä henkilöllisyys tarkistetaan varmennuskäytännössä kuvatulla tavalla. Jos hakijalla ei ole em. asiakirjoja, poliisi tunnistaa hakijan henkilöllisyyden muilla tavoin. Tieto tunnistustavasta merkitään hakemuslomakkeeseen ja rekisteröintipisteen virkailija vahvistaa omalla allekirjoituksellaan, että henkilöllisyyden tunnistus on todella tapahtunut. Henkilön esittämiä tietoja, kuten tunnisteita, nimeä ja virallista osoitetta verrataan Väestötietojärjestelmän tietoihin. Kansalaisvarmenteessa henkilön yksilöintiin käytetään sähköistä asiointia varten erikseen luotua väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetussa laissa (661/2009) määritellyä sähköistä asiointitunnusta (SATU).

Kansalaisvarmenne sisältää allekirjoitus- ja tunnistamisvarmenteet, joista on säädetty laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista.

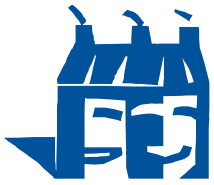
Kansalaisvarmenteita voidaan käyttää henkilön todentamiseen, viestin salaukseen ja sähköiseen allekirjoitukseen. "Varmennepolitiikka valtion kansalaisvarmenteita varten" - dokumentin mukaisesti myönnettyt allekirjoitusvarmenteet täyttävät seuraavan säädöksen mukaiset vaatimukset: Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (Asetus). Kansalaisvarmennetta voidaan käyttää rajoituksitta hallinnollisissa sekä yksityisen organisaation tarjoamissa sovelluksissa ja palveluissa.

Tämän varmennepolitiikan mukaisesti myönnetty allekirjoitusvarmenne täyttää Asetuksen hyväksytyille allekirjoitusvarmenteeille asettamat vaatimukset. Tunnistusvarmenteen taso täyttää Asetuksen ja sen nojalla annetun varmuustasoasetuksen mukaisesti vaatimustason "korkea".

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.

1.3 Varmenteeseen luottaminen

Varmenteen käyttötarkoitus on määritelty kunkin varmenteen varmennepolitiikassa, varmennuskäytännössä sekä varmenteen haltijalle annettavassa käyttöohjeessa. Varmennetta saa käyttää vain sen käyttötarkoituksen mukaisesti. Varmenteeseen luottavan osapuolen on tarkastettava, että käytettävän varmenteen voimassaoloaika ei ole päättynyt. Varmenteeseen luottava osapuoli ei voi vilpittömässä mielessä luottaa varmenteeseen, mikäli varmenteen voimassaoloa ei ole tarkistettu OCSP-palvelusta tai sulkulistalta. Varmenteeseen luottavalla osapuolella on velvollisuus tarkistaa varmenteiden voimassaolo ennen hyväksymistä.



1.4 Varmenteen haltijan velvollisuudet

Varmenteen käyttötarkoitus on määritelty kunkin varmenteen varmennepolitiikassa, varmennuskäytännössä sekä varmenteen haltijan käyttöohjeissa. Varmennetta saa käyttää vain sen käyttötarkoituksen mukaisesti.

Varmenteen haltija vastaa siitä, että varmennetta haettaessa ilmoitetut tiedot ovat oikeita.

Varmenteen haltija on itse vastuussa kansalaisvarmenteen käytöstä, sillä tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista. Allekirjoitusvarmenteen osalta noudatetaan, mitä Asetuksessa ja laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista on määrätty.

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

Sähköistä henkilökorttia ja muita kansalaisvarmenteen sisältäviä teknisiä välineitä tulee käsitellä ja suojata samalla huolellisuudella kuin muita vastaavia kortteja tai asiakirjoja, kuten esimerkiksi luottokortteja, ajokorttia ja passia. Henkilökohtaiset tunnusluvut on säilytettävä fyysisesti eri paikassa kuin kansalaisvarmenteet.

Toimikortin häviämisestä tai väärinkäytön mahdollistumisesta tulee ilmoittaa viivyttämättä Varmentajalle soittamalla maksuttomaan sulkupalveluun 0800 162 622. Vastaavasti kuuroille ja kuulovammaisille on oma tekstipuhelinpalvelunumeronsa 0100 2288.

1.5 Varmenteeseen luottavan osapuolen varmenteen tarkistamiseen liittyvät velvollisuudet

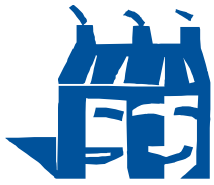
Jos varmenteeseen luottava osapuoli kopioi sulkulistan hakemistosta, sen on varmistettava sulkulistan aitous tarkistamalla sulkulistan sähköinen allekirjoitus. Lisäksi on tarkistettava sulkulistan voimassaoloaika.

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

1.6 Vastuunrajoitukset

Väestörekisterikeskusta koskevat lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista ja sähköisestä asiointista viranomaistoiminnassa annetun lain mukaiset varmentajan vahingonkorvausvastuut. Soveltuvin osin sovelletaan myös vahingonkorvauslakia (412/1974).

Väestörekisterikeskus ei vastaa tunnuslukujen, PUK-koodin ja varmenteen haltijan yksityisten avainten paljastumisen seurauksena syntyvistä vahingoista, ellei paljastuminen välittömästi johdu Väestörekisterikeskuksen toiminnasta.



1.1.2017

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

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

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

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

Väestörekisterikeskus ei vastaa yleisten tietoliikenneyhteyksien eikä tietoverkkojen, esimerkiksi internetin toimivuudesta eikä siitä, jos oikeustoimen suorittaminen estyy kortinhaltijan käyttämän laitteen toimimattomuudesta eikä siitä, että varmenteita käytetään vastoin niiden käyttötarkoitusta.

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

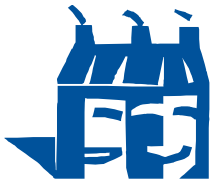
Varmenteen haltijan vastuu varmenteen käyttämisestä päättyy, kun hän on ilmoittanut sulkupalveluun tarvittavat tiedot varmenteen sulkemiseksi ja saatuaan puhelun vastaanottaneelta virkailijalta ilmoituksen varmenteen sulkulistalle viemisestä. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

1.7 Sovellettavat sopimukset, varmennuskäytäntö ja varmennepolitiikka

Varmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa ja yleisissä käyttöohjeissa, jotka muodostavat varmenteen hakijan kanssa tehtävän sopimuksen. Hakemusasiakirjassa on tiedot kummankin osapuolen oikeuksista ja velvollisuuksista. Hakemusasiakirjassa ja käyttöohjeissa mainitaan selkeästi, että kansalaisvarmenteen hakija hyväksyy nimikirjoituksellaan annettujen tietojen oikeellisuuden sekä varmenteen luomisen ja julkaisun julkiseen hakeamiseen. Samalla hakija hyväksyy kansalaisvarmenteen käyttöön liittyvät säännöt ja ehdot sekä huolehtii kansalaisvarmenteen ja sen PIN-tunnusten säilyttämisestä sekä mahdollisen väärinkäytön tai kortin katoamisen ilmoittamisesta.

Varmentajan ja Rekisteröijän, Kortinvalmistajan sekä muiden varmennepalveluiden osa-alueita tuottavien toimittajien kesken on laadittu sopimus, joka ilmaisee kiistattomasti kummankin osapuolen oikeudet, vastuut ja velvoitteet.

Kun Varmentaja myöntää kansalaisvarmenteen, se samalla hyväksyy varmennehakemuksen.



1.1.2017

Väestörekisterikeskus laatii erillisen varmennuskäytännön jokaiselle myöntämälleen varmennetyypille. Varmennuskäytäntö viittaa varmennepolitiikka-asiakirjaan, joka on varmennetyyppiä kuvaava yleisempi säännösto ja ohjeisto ja joka on yhteinen kaikille kansalaisvarmenteille siitä riippumatta, mille tekniselle välineelle varmenne on sijoitettu.

Väestörekisterikeskus julkaisee varmennepolitiikan ja varmennuskäytännön myöntämiensä varmenteiden osalta. Varmennepolitiikka kuvaa varmennetyypin osalta käytettävät menettelytavat, käyttöehdot, vastuiden jaon ja muut varmenteen käyttöönliittyvät näkökulmat. Varmennuskäytäntö kuvaa tarkemmin, miten varmennepolitiikkaa sovelletaan eri teknisillä alustoilla.

Sekä varmennepolitiikka että varmennuskäytäntö ovat saatavilla osoitteesta tai www.fineid.fi.

1.8 Yksityisyyden suoja

Varmentaja ja rekisteröijä noudattavat varmenteen haltijoiden henkilötietojen käsittelyssä hyvää tietojenkäsittelytapaa sekä tietosuojaa. Henkilötietojen käsittelyyn kiinnitetään erityistä huolellisuutta ja Väestörekisterikeskus on julkaissut varmennepalveluiden osalta erityiset henkilötietolain mukaiset käytännesäännöt.

1.9 Korvauskäytäntö

Väestörekisterikeskusta koskevat lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista ja sähköisestä asioinnista viranomaistoiminnassa annetun lain mukaiset varmentajan vahingonkorvausvastuut. Soveltuvin osin sovelletaan myös vahingonkorvauslakia (412/1974).

Väestörekisterikeskus vastaa varmenteen haltijalle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Väestörekisterikeskuksen välittömästä toiminnasta.

1.10 Sovellettava lainsäädäntö ja erimielisyyksien ratkaiseminen

Kansalaisvarmenne täyttää Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta annetun asetuksen (Asetus) allekirjoitusvarmenteelle asettamat vaatimukset.

Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009) on säädetty allekirjoitusvarmenteella tehdyistä sähköisistä allekirjoituksista. Sähköisestä henkilökortista on säädetty henkilökorttilaissa (829/1999) ja Väestörekisterikeskuksen myöntämistä varmenteista on säädetty väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetussa laissa (661/2009). Hallinnon asioinnista on säädetty myös sähköisestä asioinnista viranomaistoiminnassa annetussa laissa (13/2003).

Väestörekisterikeskusta koskevat lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista ja sähköisestä asioinnista viranomaistoiminnassa annetun lain mukaiset varmentajan vahingonkorvausvastuut. Soveltuvin osin sovelletaan myös vahingonkorvauslakia (412/1974).



1.1.2017

Sähköisestä asioinnista viranomaistoiminnassa annetun lain mukaan allekirjoitusvarmenteilla voidaan aina asioida julkisen hallinnon palveluissa.

Kansalaisvarmenteet on luotu noudattaen laissa väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista, laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista, laissa sähköisestä asioinnista viranomaistoiminnassa ja varmennepolitiikassa esitettyjä menettelyjä ja varmenteen haltijan antamien tietojen mukaisesti.

1.11 Varmentajan toiminnan tarkastusmenettely

Allekirjoitusvarmentajia sekä vahvan sähköisen tunnistamispalvelun ja -välineen tarjoajia valvova Viestintävirasto voi tarkastaa varmentajan toiminnan laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista säädetyin edellytyksin. Väestörekisterikeskus voi tarkastaa tekniset toimittajansa sen mukaisesti, kuin teknisten toimittajien kanssa tehdyissä teknisissä toimitussopimuksissa tarkastusmenettely on kirjattu. Tarkastus tehdään vähintään kerran vuodessa ja aina, kun uusi sopimuskausi alkaa.

Tarkastuksen avulla selvitetään toimiiko tekninen toimittaja sopimuksen mukaisesti huomioiden tietoturvastandardien vaatimukset. Pääsääntöisesti teknistä toimittajaa arvioidaan ISO 27001 standardin sekä Viestintäviraston määräysten mukaisesti.

Tarkastuksen suorittaa Väestörekisterikeskuksen tietoturvapäällikkö tai Väestörekisterikeskuksen hankkima ulkopuolinen tarkastaja, joka on erikoistunut varmennepalveluihin liittyvien teknisten toimittajien auditointiin. Tarkastus suoritetaan huomioiden tietoturvan kahdeksan osa-alueen toteutus. Tarkastettavia tietoturvallisuuden ominaisuuksia ovat luottamuksellisuus, eheys ja käytettävyys.

Tarkastus kattaa Viestintäviraston antamat määräykset tietoturvallisuudesta varmentajalle.

Tarkastuksessa verrataan politiikkaa ja soveltamisohjeita koko varmenneorganisaation ja -järjestelmän toimintaan. Väestörekisterikeskuksen vastuulla on soveltamisohjeiden yhdenmukaisuus varmennepolitiikan kanssa.