



DIGI- JA
VÄESTÖTieto-
VIRASTO

VARMENNEKUVAUS

Digi- ja väestötietoviraston kansalaisvarmenne

13.9.2024



ISO 9001



ISO/IEC 27001



13.9.2024

Dokumentinhallinta

Omistaja	
Laatinut	Ville Aarnio, Taija Malinen, Tuire Saaripuu
Tarkastanut	
Hyväksynyt	Mikko Pitkänen

Version hallinta

versionro	mitä tehty	pvm/henkilö
v. 1.0	Hyväksytty versio 1.0., eIDAS-asetuksen mukainen asiakirja	3.5.2018 TS
v. 1.1	Päivitetty versio, viraston nimenmuutos.	1.1.2020
v 1.2	Päivitetty versio, saavutettavuusominaisuudet	6.5.2021
v 1.3	Lisätty kuvaus lokidatasta	1.10.2021/VA
V 1.4	Päivitetty versio ja linkit varmennepolitiikkasivulle	21.9.2022/SK
V 1.5	Muutettu termi "PUK-koodi" termiksi "aktivointitunnusluku".	8.3.2023/AG
V 1.6	Päivitetty uusi päivämäärä	15.9.2023/TM
v.1.7	Yhdistetty asiakirjat G2 ja G3. Yhdenmukaistettu viittaus eIDAS-asetukseen. Päivitetty viittaukset henkilötietolakiin (523/1999) -> tietosuojalaki (1050/2018)	13.9.2024/TV





13.9.2024

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	7
1.7	Sovellettavat sopimukset, varmennuskäytäntö ja varmennepolitiikka.....	7
1.8	Yksityisyyden suoja	8
1.9	Korvauskäytäntö	8
1.10	Sovellettava lainsäädäntö ja erimielisyyksien ratkaiseminen.....	9
1.11	Varmentajan toiminnan tarkastusmenettely	9





13.9.2024

Johdanto

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

Tämä dokumentti viittaa asiakirjoihin:

Varmennepolitiikka Digi- ja väestötietoviraston kansalaisvarmennetta varten

OID: 1.2.246.517.1.10.202, 1.2.246.517.1.10.302 ja 1.2.246.517.1.10.352

Varmennuskäytäntö sähköisellä henkilökortilla olevaa kansalaisvarmennetta varten

OID: 1.2.246.517.1.10.202.1, 1.2.246.517.1.10.302.1 ja 1.2.246.517.1.10.352.1

Digi- ja väestötietovirasto noudattaa EU-asetuksen N:o (EU) 910/2014 luottamuspalveluiden mukaista yleisölle myönnettäviä allekirjoitusvarmenteita koskevaa varmennepolitiikkaa. Asiakirjan viitetiedot ovat ETSI EN 319 411-1 [2] 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

Digi- ja väestötietovirasto

PL 123 (Lintulahdenkuja 2)

00531 Helsinki

Y-tunnus: 0245437-2

Puh. +358 295 535 001

Fax. +358 9 876 4369

kirjaamo@dvv.fi

Digi- ja väestötietovirasto (DVV) Varmennepalvelut

PL 123

00531 Helsinki

www.dvv.fi/



13.9.2024

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 toimivien poliisiviranomaisen tai Suomen ulkomaan edustuston luona. Käynnin yhteydessä henkilöllisyys tarkistetaan varmennuskäytännössä kuvatulla tavalla. Jos hakijalla ei ole em. asiakirjoja, rekisteröijä 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 verratetaan Väestötietojärjestelmän tietoihin. Kansalaisvarmenteessa henkilön yksilöintiin käytetään sähköistä asiointia varten erikseen luotua väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa (304/2019) määriteltyä sähköistä asiointitunnusta (SATU).

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

Kansalaisvarmenteita voidaan käyttää henkilön todentamiseen ja sähköiseen allekirjoitukseen. G3 RSA ja ECC varmenteita voidaan käyttää lisäksi viestin salaukseen. ”Varmennepolitiikka valtion kansalaisvarmenteita varten” -dokumentin mukaisesti myönnetty 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 (eIDAS-asetus). Kansalaisvarmennetta voidaan käyttää rajoituksitta hallinnollisissa sekä yksityisen organisaation tarjoamissa sovelluksissa ja palveluissa.

Tämän varmennepolitiikan mukaisesti myönnetty allekirjoitusvarmenne täyttää eIDAS-asetuksen hyväksytyille allekirjoitusvarmenteele asettamat vaatimukset. Tunnistusvarmenteen taso täyttää eIDAS-asetuksen ja sen nojalla annetun varmuus-tasoasetuksen 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 hake-mistoon samoin kuin muu kansalaisvarmenteen tietosisältö. Sähköpostiosoitetta ei voi muuttaa kansalaisvarmenteen voimassaoloaikana.

Varmenteiden myöntämiseen sekä peruuttamiseen liittyvää lokidataa säilytetään vähintään seitsemän (7) vuotta varmenteen voimassaoloajan jälkeen.

1.3 Varmenteeseen luottaminen

Varmenteen käyttötarkoitus on määritelty kunkin varmenteen varmennepolitiikassa, varmennuskäytännössä sekä varmenteen haltijalle annettavassa käyttöohjeessa.

13.9.2024

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. Henkilökortin 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.

Henkilökortin häviämisestä tai väärinkäytön mahdollistumisesta tulee ilmoittaa viivyttelemättä Varmentajalle soittamalla maksuttomaan sulkupalvelunumeroon 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.

13.9.2024

1.6 Vastuunrajoitukset

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

Digi- ja väestötietovirasto ei vastaa tunnuslukujen, aktivointitunnusluvun ja varmenteen haltijan yksityisten avainten paljastumisen seurauksena syntyvistä vahingoista, ellei paljastuminen välittömästi johdu Digi- ja väestötietoviraston toiminnasta.

Digi- ja väestötietovirasto ei vastaa varmenteen haltijalle aiheutuneista välillisistä tai seurannaisvahingoista. Digi- ja väestötietovirasto ei myöskään vastaa varmenteeseen luottavan osapuolen tai henkilökortin haltijan muun sopimuskumppanin mahdollisesti kärsimistä välillisistä tai seurannaisvahingoista.

Digi- ja väestötietovirasto vastaa kansalaisvarmenteen haltijalle ja kansalaisvarmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Digi- ja väestötietoviraston välittömästä toiminnasta.

Varmentajalla on oikeus keskeyttää palvelu muutos- tai huoltotoimien ajaksi. Sulkulistaa koskevista muutos- ja huoltotoista 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.

Digi- ja väestötietovirasto 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 verkkopalvelun tai sovelluksen virheistä tai niistä loppukäyttäjälle 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

13.9.2024

kansalaisvarmenteen hakija hyväksyy nimikirjoituksellaan annettujen tietojen oikeellisuuden sekä varmenteen luomisen ja julkaisun. 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.

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

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

Sekä varmennepolitiikka että varmennuskäytäntö ovat saatavilla osoitteesta www.dvv.fi/cps.

1.8 Yksityisyyden suoja

Varmentaja ja rekisteröijä noudattavat varmenteen haltijoiden henkilötietojen käsittelyssä hyvää tietojenkäsittelytapaa sekä tietosuojaa. Henkilötietojen käsittelyyn kiinnitetään erityistä huolellisuutta ja Digi- ja väestötietovirasto on julkaissut varmennepalveluiden osalta erityiset tietosuojalain mukaiset käytäntönsäännöt. Tietojen käsittelyssä noudatetaan henkilötietojen käsittelyä ja yksityisyydensuojaa koskevaa lainsäädäntöä, mm. EU:n yleistä tietosuoja-asetusta (EU) 2016/679 ja tietosuojalakea (1050/2018).

1.9 Korvauskäytäntö

Digi- ja väestötietovirastoa koskevat lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) ja sähköisestä asioinnista viranomaistoinnassa annetun lain mukaiset varmentajan vahingonkorvausvastuut. Soveltuvien osin sovelletaan myös vahingonkorvauslakia (412/1974).

Digi- ja väestötietovirasto vastaa varmenteen haltijalle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Digi- ja väestötietoviraston välittömästä toiminnasta.

13.9.2024

1.10 Sovellettava lainsäädäntö ja erimielisyyksien ratkaiseminen

Kansalaisvarmenne täyttää eIDAS-asetuksen allekirjoitusvarmenteelle asettamat vaatimukset. Tietojen käsittelyssä noudatetaan henkilötietojen käsittelyä ja yksityisyydensuojaa koskevaa lainsäädäntöä, mm. EU:n yleistä tietosuoja-asetusta (EU) 2016/679 ja tietosuojalakia (1050/2018).

Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009) on säädetty allekirjoitusvarmenteella tehdyistä sähköisistä allekirjoituksista. Sähköisestä henkilökortista on säädetty henkilökorttilaissa (663/2016) ja Digi- ja väestötietoviraston myöntämistä varmenteista on säädetty väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa (304/2019). Hallinnon asioinnista on säädetty myös sähköisestä asioinnista viranomaistoiminnassa annetussa laissa (13/2003).

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

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

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

1.11 Varmentajan toiminnan tarkastusmenettely

Allekirjoitusvarmentajia sekä vahvan sähköisen tunnistamispalvelun ja -välineen tarjoajia valvova Traficom voi tarkastaa varmentajan toiminnan laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista säädettyin edellytyksin. Digi- ja väestötietovirasto 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 Traficomien määräysten mukaisesti.

Tarkastuksen suorittaa Digi- ja väestötietoviraston tietoturvapääällikkö tai Digi- ja väestötietoviraston 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 Traficomien antamat määräykset tietoturvallisuudesta varmentajalle.



13.9.2024

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

