



DIGI- JA
VÄESTÖTIETO-
VIRASTO

VARMENNEKUVAUS JUURIVAR- MENNE

Digi- ja väestötietoviraston juurivarmentajaa varten

29.9.2022



[Yksikkö] / Kytölä Sanni

29.9.2022

Dokumentinhallinta

| | |
|-------------|----------------|
| Omistaja | |
| Laatinut | Ville Aarnio |
| Tarkastanut | |
| Hyväksynyt | Mikko Pitkänen |

Version hallinta

| versionro | mitä tehty | pvm/henkilö |
|-----------|---|--------------|
| v 1.0 | Versio 1.0 | 1.6.2021/VA |
| v 1.1 | Lisätty kuvaus lokidatasta | 1.10.2021/VA |
| v 1.2 | Päivitetty versio ja linkit varmennepolitiikkasivulle | 29.9.2022/SK |



Sisällysluettelo

| | | |
|----------|---|----------|
| 1 | Johdanto | 3 |
| 2 | Varmennekuvaus | 4 |
| 2.1 | Varmentajan yhteystiedot | 4 |
| 2.2 | Varmenteen tyyppi, tarkistamismenettely ja käyttötarkoitus | 4 |
| 2.3 | Varmenteeseen luottaminen | 5 |
| 2.4 | Varmenteen haltijan velvollisuudet..... | 5 |
| 2.5 | Varmenteeseen luotavan osapuolen varmenteen tarkistamiseen liittyvät velvollisuudet.... | 5 |
| 2.6 | Vastuunrajoitukset | 5 |
| 2.7 | Sovellettavat sopimukset, varmennuskäytäntö ja varmennepolitiikka..... | 6 |
| 2.8 | Yksityisyyden suoja | 7 |
| 2.9 | Korvauskäytäntö | 7 |
| 2.10 | Sovellettava lainsäädäntö ja erimielisyyksien ratkaiseminen..... | 7 |
| 2.11 | Varmentajan toiminnan tarkastusmenettely | 7 |



VARMENNEKUVAUS JUURIVARMENNE

1 Johdanto

Tämä dokumentti kuvaa yleisellä tasolla, kuinka juurivarmentajana toimiva Digi- ja väestötietovirasto toimii myöntäessään (DVV Gov. Root CA – G3 RSA ja DVV Gov. Root CA – G3 ECC) varmentajan varmenteita.

Tässä dokumentissa on kuvattu yleisellä tasolla varmentajan toimintatapoja sekä varmentajan varmenteen käytön ehtoja ja rajoituksia.

Tämä dokumentti viittaa asiakirjoihin:

Varmennepolitiikka Digi- ja väestötietoviraston varmentajan varmennetta varten, OID 1.2.246.517.1.10.301 ja 1.2.246.517.1.10.351.

Varmennuskäytännöt seuraaville alivarmenteille:

DVV Citizen Certificates - G4R, OID: 1.2.246.517.1.10.301.1

DVV Citizen Certificates - G4E, OID: 1.2.246.517.1.10.351.1

DVV Organisational Certificates - G4R, OID: 1.2.246.517.1.10.301.2

DVV Organisational Certificates - G4E, OID: 1.2.246.517.1.10.351.2

DVV Temporary Certificates - G3R, OID: 1.2.246.517.1.10.301.3

DVV Temporary Certificates - G3E, OID: 1.2.246.517.1.10.351.3

DVV Service Certificates - G5R, OID: 1.2.246.517.1.10.301.4

DVV Service Certificates - G5E, OID: 1.2.246.517.1.10.351.4

DVV Social Welfare and Healthcare Prof. Certificates - G2ROID:
1.2.246.517.1.10.301.5

DVV Social Welfare and Healthcare Prof. Certificates - G2E, OID:
1.2.246.517.1.10.351.8

DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2R, OID:
1.2.246.517.1.10.301.6

DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2E, OID:
1.2.246.517.1.10.351.6

DVV Social Welfare and Healthcare Service Certificates - G3R, OID:
1.2.246.517.1.10.301.7

DVV Social Welfare and Healthcare Service Certificates - G3E, OID:
1.2.246.517.1.10.351.7

DVV Time Stamp Certificates - G2R, OID: 1.2.246.517.1.10.301.8



[Yksikkö] / Kytölä Sanni

29.9.2022

~~DVV Time Stamp Certificates - G2EDVV CA for Time Stamp Services - G2 ECG,~~
OID: 1.2.246.517.1.10.351.8

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

2 Varmennekuvaus

2.1 Varmentajan yhteystiedot

Tätä varmennepolitiikkaa koskevat kysymykset lähetetään seuraavaan osoitteeseen:

Digi- ja väestötietovirasto

PL 123 (Lintulahdenkuja 2)

Puh. +358 295 535 001

00531 Helsinki

Fax. +358 9 876 4369

Y-tunnus: 0245437-2

kirjaamo@dvv.fi

Digi- ja väestötietovirasto (DVV) Varmennepalvelut

PL 123

00531 Helsinki

www.dvv.fi

2.2 Varmenteen tyyppi, tarkistamismenettely ja käyttötarkoitus

Varmentajan varmenne on Digi- ja väestötietoviraston myöntämä varmenne, jolla myönnetään loppukäyttäjän varmenteita.

Varmentajan varmennetta haetaan Digi- ja väestötietovirastolta.

Varmennetta myöntäessään DVV tarkistaa hakijan tiedot mm. kaupparekisteristä.

Varmenteen uusiminen noudattaa samaa hakumenettelyä kuin alkuperäinen hakemus.

Varmenteen hinta on palveluhinnaston mukainen maksu / vuosi.

Varmentajan varmennetta voi hakea sekä yksityinen että julkinen organisaatio.

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





2.3 Varmenteeseen luottaminen

Varmenteen käyttötarkoitus on määritelty kunkin varmenteen varmennepolitiikassa ja varmennuskäytännössä sekä varmenteessa. Varmennetta saa käyttää vain sen käyttötarkoituksen mukaisesti. Varmenteeseen luottavan osapuolen on tarkastettava, että käytettävän varmenteen voimassaoloaika ei ole päättynyt eikä varmenne ole sulkulistalla. Varmenteeseen luottava osapuoli ei voi vilpittömässä mielessä luottaa varmenteeseen, mikäli varmenteen voimassaoloa ei ole tarkistettu sulkulistalta. Varmenteeseen luottavalla osapuolella on velvollisuus tarkistaa varmenteet sulkulistalta ennen hyväksymistä mitätöinnin varalta.

2.4 Varmenteen haltijan velvollisuudet

- Varmenteen käyttötarkoitus on määritelty kunkin varmenteen varmennepolitiikassa, varmennuskäytännössä sekä varmenteessa. Varmennetta saa käyttää vain sen käyttötarkoituksen mukaisesti.
- Varmenteen haltija (palveluntarjoaja) vastaa siitä, että varmennetta haettaessa ilmoitetut tiedot ovat oikeita.
- Varmenteen haltija säilyttää yksityisen avaimensa turvallisessa ympäristössä ja estää yksityisen avaimensa katoamisen, joutumisen ulkopuolisten käsiin, muuttamisen tai luvattoman käytön.
- Varmenteen haltijan on ilmoitettava Varmentajalle välittömästi, jos on epäilystä, että varmenteen haltijan yksityinen avain on paljastunut. Tällöin varmentaja sulkee ko. varmenteen.

2.5 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.

2.6 Vastuunrajoitukset

Varmennepalveluiden tuottamiseen liittyvä Digi- ja väestötietoviraston vahingonkorvausvastuu määräytyy vahingonkorvauslain (412/1974) säännösten mukaisesti. Digi- ja väestötietovirastoa koskevat myös lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaiset varmentajan vastuut. Digi- ja väestötietovirasto ei vastaa varmenteen haltijan yksityisen avaimen 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 varmenteen haltijan muun sopimuskumppanin mahdollisesti kärsimistä välillisistä tai seurannaisvahingoista.

Digi- ja väestötietovirasto ei vastaa yleisten tietoliikenneyhteyksien eikä tietoverkkojen, esimerkiksi internetin toimivuudesta.

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

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

Varmenteen haltijan vastuu varmenteen käyttämisestä päättyy, kun hän tai varmenteen haltijan organisaation edustaja on ilmoittanut Varmentajalle tarvittavat tiedot varmenteen sulkemiseksi. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

2.7 Sovellettavat sopimukset, varmennuskäytäntö ja varmennepolitiikka

Varmenteen hakijan oikeudet ja velvollisuudet on mainittu varmennepolitiikka- ja varmennuskäytäntö-asiakirjoissa. Varmennetta hakiessaan hakijaorganisaatio hyväksyy varmenteen käyttöön liittyvät säännöt ja ehdot sekä huolehtii varmenteen säilyttämisestä sekä mahdollisen väärinkäytön ilmoittamisesta.

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

Kun varmentaja myöntää varmentajan varmenteen, se samalla hyväksyy varmennehakemuksen.

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 varmenteiden tuotannossa.

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



2.8 Yksityisyyden suoja

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

2.9 Korvauskäytäntö

Digi- ja väestötietovirastoa koskee vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) annetun lain mukaiset vaatimukset. Eräin osin sovelletaan myös vahingonkorvauslain (412/1974) säännöksiä.

2.10 Sovellettava lainsäädäntö ja erimielisyyksien ratkaiseminen

Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009) on säädetty tunnistamis- ja luottamuspalveluista. Digi- ja väestötietoviraston myöntämistä varmenteista on säädetty laissa väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista (661/2009).

Digi- ja väestötietovirastoa koskee vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) annetun lain mukaiset vaatimukset. Eräin osin sovelletaan myös vahingonkorvauslain (412/1974) säännöksiä.

2.11 Varmentajan toiminnan tarkastusmenettely

Traficom voi tarkastaa varmentajan toiminnan laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista säädetyin 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 mukaisesti.

Tarkastuksen suorittaa Digi- ja väestötietoviraston tietoturvapäällikkö tai Digi- ja väestötietoviraston hankkima ulkopuolinen tarkastaja, joka on erikoistunut varmennepalveluihin liittyvien teknisten toimittajien auditointiin. Tarkastettavia tietoturvallisuuden ominaisuuksia ovat mm. luottamuksellisuus, eheys ja käytettävyys.

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



[Yksikkö] / Aarnio Ville

**Digi- ja väestötietoviraston
juurivarmentajaa varten**
[Tarkenne]

[Numero]
[Liite]

8 (8)

6.5.2021

