

Ajankohtaista DVV:llä 8.12.2021

Jari Pirinen
Erikoissuunnittelija
Digi- ja väestötietovirasto
jari.pirinen@dvv.fi
029 553 5141



DIGI- JA
VÄESTÖTIETO-
VIRASTO



DigiSign-kortinlukijaohjelmisto

Uusin versio 4.2.0b julkaistu lokakuussa 2021

- Bugikorjausversio, jossa korjattu kaksi 4.2.0-versiossa ilmennyttä bugia:
 - Toinen vaikutti 1.8.2021 jälkeen myönnettyihin uusiin henkilökortteihin (kansalaisvarmenne).
 - Toinen aiheutti DigiSignin kaatumisen virtualisoiduissa ja image-yksilöidyissä ympäristöissä.
- Suosittelemme asiakkaitamme päivittämään uusimman version käyttöönsä.
 - <https://dvv.fi/kortinlukijaohjelmisto>
 - Release Notes –dokumentit sisältävät aina tarkat tiedot versioiden välisistä muutoksista.

Seuraava versio 4.2.2 julkaistaan alustavasti helmikuussa 2022. Suunnitellut muutokset:

- Virallinen tuki Windows 11:lle ja MacOS 12:lle.
- Tuki SCS-rajapinnan uudelle versiolle 1.2, jossa mm. allekirjoitusvarmenteen pyyntö etukäteen.
- Asennusprosessin sujuvoittaminen.
- Selkeytetty käyttöliittymän kielivalintaa.
- Bugikorjauksia.
- DigiSignin julkaisusykli muuttuu jatkossa nykyisestä joulukuu/heinäkuu → helmikuu/syyskuu.



DVV:n varmennehierarkia uudistuu 2021-2022

- DVV on käynnistänyt projektin, jossa uudistetaan viraston varmennehierarkia DVV:n nimiin nykyisestä VRK:sta.
 - Nykyiset varmennehierarkiat G1 ja G2 ovat edelleen VRK:n nimissä, ja DVV tuottaa niillä varmenteita auditoijan myöntämän siirtymäajan puitteissa.
 - Projektissa tuotetaan ja käyttöön otetaan erilliset RSA- ja ECC-varmennehierarkiat.
 - Mahdollistaa jatkossa nykyistä tietoturvallisemmän ECC-täyshierarkian käytön.
 - RSA-avaimen pituus 4096 bittiä juuressa ja CA-varmentajissa.
 - ECC-avaimen pituus 384 bittiä (*NIST P-384*) juuressa ja CA-varmentajissa.
 - Uudet varmennehierarkiat ovat läpäisseet eIDAS-auditoinnin 6/2021.



DVV:n varmennehierarkia uudistuu 2021-2022

- **Uudet G3-varmennehierarkiat tulevat tuotantoon 12/2021 (palveluvarmenteet) ja 2/2022 (sote-kortit). Tarkat uudistuotannon aloituspäivät seuraavalla dialla.**
 - Tämä tulee edellyttämään konfiguraatiomuutoksia sote-sektorin tietojärjestelmiin ja työasemiin, joten asia on huomioitava kaikkien niiden tahojen toimesta, jotka tavalla tai toisella hyödyntävät DVV:n myöntämiä varmenteita.
 - Juurivarmenteet ja CA-varmentajat ovat ladattavissa verkkosivustoltamme: <https://dvv.fi/ca-varmenteet> sekä testipuolen osalta <https://dvv.fi/testi-ca-varmenteet>
 - Uuden testihierarkian mukaisia testikortteja on tilattavissa [DVV:n verkkoasioinnissa](#). Saatavilla on sekä RSA- että ECC-testikortteja. Kirjoitathan korttitilauksen Lisätietoja-kenttään ”Uuden CA:n testikortti” tai ”Uuden CA:n ECC-testikortti”.
 - Tiedotamme asiakkaitamme sähköpostitse ja [verkkosivustollamme](#) projektin etenemisestä, ja vielä erikseen muistutamme ennen kuin uudistuotanto alkaa. Asiakasinfo järjestettiin 30.9.2021.



DVV:n varmennehierarkia uudistuu 2021-2022

- Uudet CA:t tulevat tuotantoon seuraavan aikataulun mukaisesti:
 - Palveluvarmenteet ja Sote-palveluvarmenteet: **9.12.2021**
 - Organisaatiokortti: **3.2.2022**
 - Sote-ammattikortti, -henkilöstökortti ja -toimijakortti: **10.2.2022**
 - Henkilökortti (kansalaisvarmenne): **17.2.2022**
- Näiden päivämäärien jälkeen ei ole enää mahdollista tilata DVV:ltä nykyisillä CA:illa tuotettuja varmenteita.
- Varmistattehan, että organisaationne tietojärjestelmät ja työasemat luottavat uusiin varmentajiin ennen näitä päivämääriä.
- Huomioittehan myös, että uusissa varmenteissa käytetään nykyistä pidempiä sarjanumeroita (CA/Browser Forum compliant serial number format).
 - hex 0bf4eab0 / dec 200600240
 - hex 0100000168f0a805c366b43b5de968c691fb / dec 87112293252494463413683796322992020427259



ECC-testikortteja nyt tilattavissa

- DVV alkaa tarjoamaan nykyistä tietoturvalisempia ja suorituskykyisempiä ECC-teknologiaa käyttäviä varmennekortteja. **ECC-teknologialla varustetut Sote-kortit eivät ole vielä tulossa tuotantoon.**
- Kortin siru (uusi Idemia ID.me) sekä varmenteen tietosisältö ja käyttötapa pysyvät ennallaan, erona on vain että sirulle generoitavat avaimet luodaan RSA-algoritmin sijaan ECC-algoritmillä. DigiSign Client tukee näitä kortteja versiosta 4.0.20 lähtien.
- Loppukäyttäjävarmenteen sekä CA-varmenteen ECC-käyränä käytetään NIST P-384 (secp384r1).
- ECC-testikortteja on nyt tilattavissa [DVV:n verkkoasioinnissa](#). Tilaus tehdään tavallisena testikorttitilauksena, jonka Lisätietoja-kenttään kirjoitetaan pyynnöksi "Uuden CA:n ECC-testikortti".
- Testikorttien ensisijaisena kohderyhmänä on DVV:n varmennekortti-integraatiota tuotteisiinsa tarjoavat Sote-sektorin tietojärjestelmä- ja sovellustoimittajat. **Kela tiedottaa erikseen ECC-varmenteiden käyttöönnotosta Kanta-palveluissa.**



Sulkulistahakemiston tekninen muutos

- Vuonna 2009 rekisteröity sote-ammattikorttien LDAP-hakemiston osoite **ldap.shpca.fi** on edelleen voimassa DNS-entrynä ja ohjaa eteenpäin varsinaiseen LDAP-hakemistoomme osoitteessa **ldap.fineid.fi**.

DNS entry: ldap.shpca.fi

IP address: 195.226.202.184

- DVV on luopumassa domainista shpca.fi, joten **mikäli teillä on vielä jossain järjestelmässä osoite ldap.shpca.fi määriteltynä, pyydämme teitä muuttamaan sen osoittamaan osoitteeseen ldap.fineid.fi tai 195.226.202.184.**
- Yhdessäkään voimassa olevassa sote-varmenteessa ei ole suoraa sulkulistaviittausta osoitteeseen ldap.shpca.fi.
- LDAP on muutenkin ”poistuvaa kansanperinnettä”, joten suosittelemme hakemaan varmenteen tilatiedon joko OCSP:tä tai HTTP-CRL:ää (proxy.fineid.fi) käyttäen.



Aktiiviset SOTE-kortit/-varmenteet 1.12.2021

Tuotantovarmenteet ja –kortit:

SOTE- ja TH-ammattikortit	250 355 (251 798)	↓
SOTE- ja TH-henkilöstökortit	29 889 (29 901)	↓
SOTE- ja TH-toimijakortit	2 073 (2 064)	↑
Yhteensä	282 317 (283 763) kpl	↑

SOTE-palvelinvarmenteet	1 360 (1 390)	↓
SOTE-järjestelmällekirjoitusvarmenteet	323 (317)	↑
Yhteensä	1 683 (1 708) kpl	↓



Kommentit/kysymykset

Sähköpostilla:

`varmennepalvelut@dvv.fi`

Verkkoasiointi:

<https://dvv.fi/verkkoasiointi>



**DIGI- JA
VÄESTÖTIETO-
VIRASTO**

Tehtävänä sujuva
Suomi

