

Ajankohtaista DVV:llä 7.4.2021

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



**DIGI- JA
VÄESTÖTIETO-
VIRASTO**



DigiSign-kortinlukijaohjelmisto

Uusin versio 4.1.4c julkaistu tammikuussa 2021

- Korjattu versiossa 4.1.4 ilmennyt vakava bugi joka joissakin tapauksissa esti kortin käytön.
 - Syynä virheellisesti generoitu RSA-padding.
 - Koskee vain Windows-versiota. Mac- ja Linux-puolella uusin versio edelleen 4.1.4.

Seuraava versio 4.2.0 julkaistaan heinäkuussa 2021. Suunnitellut parannukset:

- Tuki TLS 1.3:lle.
- Tuki RSA-PSS –allekirjoitusmenetelmälle.
- Parannettu tukea uusille M1-prosessoria käyttäville Maceille.
- Korjattu yhteensopivuusongelma uusien Safari-versioiden kanssa.
- Sisäänrakennettua PDF-allekirjoituksen toimintoa kehitetty.
- Bugikorjauksia.



DigiSignille suoritetaan tietoturva-auditointi

- Koska DigiSign on käytössä useilla suomalaisen yhteiskunnan kriittisillä toimialoilla, kuten terveydenhuollossa ja turvallisuusviranomaisilla, on tuotteen tietoturvan korkea taso korostetun tärkeä.
- DVV on yhdessä ohjelman tuottajan Fujitsu Finland Oy:n kanssa teettämässä DigiSignille kattavaa tietoturva-auditointia kolmannen osapuolen toimesta.
 - Ajankohtana Q2 2021.
 - Auditoinnin suorittaa tietoturva-auditointeihin ja penetraatiotestaukseen erikoistunut suomalainen yhtiö.
- Auditoinnissa ilmi tulevat mahdolliset havainnot pyritään korjaamaan mahdollisimman pian normaalin bugikorjausprosessin mukaisesti.
- Auditoinnin päätyttyä julkaisemme auditoijan lausunnon tuotteen tietoturvan tasosta.



DVV:n varmennehierarkia uudistuu 2022 1/2

- **DVV on aloittanut projektin, jossa uudistetaan viraston varmennehierarkia DVV:n nimiin nykyisestä VRK:sta.**
 - Nykyiset varmennehierarkiat (G1- ja G2-juuret) ovat edelleen VRK:n nimissä, ja DVV tuottaa niillä varmenteita auditoijan myöntämän siirtymäajan puitteissa.
 - Projektissa tuotetaan 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.



DVV:n varmennehierarkia uudistuu 2022 2/2

- **Uusi G3-varmennehierarkia tulee näillä näkymin tuotantoon vuoden 2022 alkupuolella (Q1/Q2).**
 - Tämä tulee edellyttämään konfiguraatiomuutoksia tietojärjestelmiin ja työasemiin, joten asia on huomioitava kaikkien niiden tahojen toimesta, jotka tavalla tai toisella hyödyntävät DVV:n myöntämiä varmenteita.
 - Juurivarmenne ja CA-varmentajien varmenteet pyritään julkaisemaan verkkosivustollamme mahdollisimman pian luomisen jälkeen.
 - Tiedotamme asiakkaitamme sähköpostitse ja verkkosivustollamme projektin etenemisestä, ja vielä erikseen muistutamme ennen kuin uudistuotanto alkaa.



ECC-avaimia käyttävät sote-varmennekortit

- DVV:llä on suunnitelmissa alkaa tarjoamaan nykyistä tietoturvalisempia ja suorituskykyisempiä ECC-varmennekortteja, sekä varakortteina että tehdastuotettuina kortteina.
- Siru (uusi Idemia ID.me) sekä varmenteen tietosisältö ja käyttötapa pysyvät ennallaan, erona on vain että sirulle generoitavat avaimet luodaan RSA-algoritmin sijaan ECC-algoritmeilla. DigiSign Client tukee näitä kortteja versiosta 4.0.18 lähtien.
- Loppukäyttäjävarmenteen ECC-käyränä NIST P-384 (secp384r1) ja CA:n allekirjoitusavaimena 4096-bit RSA eli kyseessä on ECC/RSA-hybridivarmenne.
- ECC-testikortteja tilattavissa Q2/2021 aikana. Testikorttien ensisijaisena kohderyhmänä DVV:n varmennekortti-integraatiota tuotteisiinsa tarjoavat Sote-sektorin tietojärjestelmä- ja sovellustoimittajat.



eIDAS-aikaleimapalvelun myöhästyminen

- DVV tiedotti viime vuonna suunnitelmistaan tuotteistaa asiakkailleen eIDAS-hyväksytty aikaleimapalvelu (Qualified Time Stamp) vuoden 2021 aikana.
- Aikaleimapalvelu mahdollistaisi mm. seuraavat sähköisen allekirjoituksen oheispalvelut:
 - Pitkäaikaisarkistoitava sähköinen allekirjoitus (LTA, Long Term Archival).
 - Sähköisen allekirjoituksen ajoittainen virkistäminen tulevaisuuden tietoturvaohjeiden varalta.
 - Allekirjoituksen tarkan tapahtuma-ajankohdan varmistaminen.
- Valitettavasti kyseisen palvelun auditointi ja asiakastuotteistus ovat näillä näkymin myöhästymässä vuodelle 2022.
- Aikaleimapalvelun eIDAS-auditointi ja tuotteistus on edelleen DVV:n kehitysroadmapilla osana sähköisen allekirjoituksen strategiaamme.



Uusissa sote-korteissa ilmennyt ongelma

- Olemme saaneet joiltakin asiakkailta havaintoja, että DVV:n myöntämän uuden sote-kortin siru (1.4.2020 lähtien tuotettu Idemia ID.me) menee lukkoon kesken käytön.
 - Valtaosa havainnoista on tullut apteekkisektorilta.
 - Myös muilta asiakassektoreilta on tullut hajanaisia havaintoja.
- Ongelman ilmaantuvuus suhteessa myönnettyjen korttien kokonaismäärään on pieni, mutta suhtaudumme asiaan erittäin vakavasti ja selvitämme juurisyytä yhdessä korttitoimittajan, kortinlukijaohjelman toimittajan ja asiakkaidemme kanssa.
- **Alustavien selvitysten perusteella vaikuttaa siltä, että lukittumisongelmaa ei ilmene enää uusimmalla DigiSign-versiolla 4.1.4c.**
 - Lopullisten johtopäätösten vetäminen on kuitenkin vielä liian aikaista.
- Toimimattomat kortit voi reklamoida DVV:lle (rekisteröijällä lomake, kirjatkaa syy).
- DVV pahoittelee ongelmasta asiakkailleen aiheutuvaa haittaa.



DVV:n asema suomalaisen virallisen tiedon varmentajana vahvistuu entisestään

- DVV:n varmennetietojärjestelmä alkaa tuottaa allekirjoitusvarmenteita useisiin uusiin käyttökohteisiin, joilla varmistetaan suomalaisen viranomaistiedon oikeellisuus ja väärentämättömyys:
 - Henkilökorttien sirutietojen allekirjoittaminen (ICAO CSCA Document Signer).
 - Passit ja oleskeluluvat allekirjoitetaan jo samalla menetelmällä.
 - Sähköisten viisumien allekirjoittaminen (ICAO CSCA Visa Signer).
 - Rokotustodistusten allekirjoittaminen (EU-komission Digital Green Certificate).



Aktiiviset SOTE-kortit/-varmenteet 1.4.2021

Tuotantovarmenteet ja –kortit:

SOTE- ja TH-ammattikortit	244 694 (239 908)	↑
SOTE- ja TH-henkilöstökortit	29 889 (29 151)	↑
SOTE- ja TH-toimijakortit	2 198 (2 192)	↑
Yhteensä	276 781 (271 250) kpl	↑

TH-palvelinvarmenteet	1 (47)	↓
TH-järjestelmällekirjoitusvarmenteet	0 (6)	↓
SOTE-palvelinvarmenteet	1 463 (1 395)	↑
SOTE-järjestelmällekirjoitusvarmenteet	288 (286)	↑
Yhteensä	1 752 (1 734) kpl	↑



Kommentit/kysymykset

Sähköpostilla:

asiakashallinta.th-varmenne@dvv.fi

varmennepalvelut@dvv.fi

Verkkoasiointi:

<https://dvv.fi/verkkoasiointi>



**DIGI- JA
VÄESTÖTIETO-
VIRASTO**

Tehtävänä sujuva
Suomi

