Ajankohtaista DVV:llä 26.10.2021

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

DIGI- JA VÄESTÖTIETO-VIRASTO

Uusien sote-korttien lukkiutumisongelma

- Sote-korttien uusi siruprofiili on otettu tuotantoon 6.9.2021.
  - Potentiaalinen ongelma koskee siis 1.4.2020 – 5.9.2021 tuotettuja sote-kortteja.
  - Uusi siruprofiili vaatii DigiSign-version 4.0.20 (julkaistu 7/2019) tai sitä uudemman.
- DigiSign-versio 4.1.4e ja sitä uudemmat esittävät käyttäjälle jäljellä olevien PIN-käyttökertojen määrän ja ohjaavat uusimaan kortin jos ne ovat loppumassa.
- Tietoomme tulleita lukkiutumistapauksia on ollut vähän ja pääasiassa apteekkisektorilla.
- Laskuriongelman takia lukkiutuneet kortit voi reklamoida DVV:lle.
- DVV pahoittelee ongelmasta asiakkailleen aiheutuvaa haittaa.

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 joulukuussa 2021. Suunnitellut parannukset:

- 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 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 sovelluksen toimittajan Fujitsu Finland Oy:n kanssa teettänyt DigiSignille kattavan tietoturva-auditoinnin kolmannen osapuolen toimesta.
  - Toteutusajankohtana oli Q2 2021.
  - Auditoinnin suoritti tietoturva-auditointeihin ja penetraatiotestaukseen erikoistunut suomalainen yhtiö.
- Auditoinnissa ei tullut ilmi yhtään vakavaa tietoturvahaavoittuvuutta. Havaitut lievät haavoittuvuudet/bugit korjattiin heinäkuussa julkaistussa versiossa 4.2.0.
- Auditoijan lausunto on julkinen ja jaossa DVV:n verkkosivustolla (linkki).

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 käyttöönotetaan erilliset RSA- ja ECC-varmennehierarkiat.
    - Mahdollistaa jatkossa nykyistä tietoturvallisemman 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 aloituspäivät tiedotetaan myöhemmin.**

  - 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 on jo tuotettu ja ovat ladattavissa verkkosivustoltamme: https://dvv.fi/ca-varmenteet sekä testipuolen osalta https://dvv.fi/testi-ca-varmenteet

  - Tiedotamme, kun uuden testihierarkian mukaiset testikortit ovat tilattavissa (alustavasti lokakuussa).

  - Tiedotamme asiakkaitamme sähköpostitse ja verkkosivustollamme projektin etenemisestä, ja vielä erikseen muistutamme ennen kuin uudistuotanto alkaa. Teams-infotilaisuus järjestettiin 30.9.2021.

  - Kaikki asiakasmateriaali löytyy sivulta https://dvv.fi/varmennehierarkian-uudistus.

ECC-testikortteja pian saatavilla

- DVV alkaa tulevaisuudessa tarjoamaan nykyistä tietoturvallisempia ja suorituskykyisempiä ECC-teknologiaa käyttäviä varmennekortteja.

- 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-algoritmilla. DigiSign Client tukee näitä kortteja versiosta 4.0.18 lähtien.

- Loppukäyttäjävarmenteen sekä CA-varmenteen ECC-käyränä käytetään NIST P-384 (secp384r1).

- ECC-testikortteja on pian tilattavissa DVV:n verkkoasioinnissa. Tiedotamme vielä erikseen, kun kortit ovat tilattavissa. Tilaus tehdään tavallisena testikorttitilauksena, jonka kommenttikenttään 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 käyttöönotosta 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.

Tulevia tuotekehitysuutisia: eIDAS-hyväksytty sähköinen leimapalvelu

- DVV:llä on suunnitelmissa kehittää eIDAS-hyväksytty sähköinen leimavarmenne (*Qualified Certificate for Electronic Seal*) ja tuotteistaa se kansallisen allekirjoituspalvelun (*Remote Signing Service*) muodossa. Sähköinen leima on oikeushenkilön (organisaation) nimissä tehty sähköinen allekirjoitus.

- Helposti integroitavissa asiakasjärjestelmiin REST-rajapinnan kautta.

- Tietoturvallisempi vaihtoehto nykyiselle järjestelmäallekirjoitusvarmenteelle:
  - Yksityistä avainta säilytetään aina laitepohjaisesti suojattuna (eIDAS-vaatimus).
    - VP:n korkean tietoturvatason ympäristössä sijaitseva eIDAS-sertifioitu (*QSCD*) HSM.

- Rajat ylittävä yhteensopivuus: eIDAS-hyväksytty sähköinen leima on juridisesti pätevä koko EU:ssa.

- Alustava aikataulu tuotannon aloitukselle 8/2022.

Aktiiviset SOTE-kortit/-varmenteet 1.10.2021

Tuotantovarmenteet ja –kortit:		
SOTE- ja TH-ammattikortit	251 798 (247 131)	↑
SOTE- ja TH-henkilöstökortit	29 901 (30 130)	↓
SOTE- ja TH-toimijakortit	2 064 (2 186)	↓
Yhteensä	**283 763** (279 447) kpl	↑
TH-palvelinvarmenteet	1 (1)	-
TH-järjestelmäallekirjoitusvarmenteet	0 (0)	-
SOTE-palvelinvarmenteet	1 390 (1 421)	↓
SOTE-järjestelmäallekirjoitusvarmenteet	317 (305)	↑
Yhteensä	**1 708** (1 727) kpl	↓

Kommentit/kysymykset

Sähköpostilla:

~~asiakashallinta.th-varmenne@dvv.fi~~

varmennepalvelut@dvv.fi

Verkkoasiointi:

https://dvv.fi/verkkoasiointi

DIGI- JA VÄESTÖTIETO-VIRASTO

Tehtävänä sujuva Suomi