

Ajankohtaista DVV:llä 16.6.2021

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



DIGI- JA
VÄESTÖTIETO-
VIRASTO



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.
 - Muilta asiakassektoreilta on tullut hajanaisia havaintoja.
 - Ilmaantuvuus suhteessa myönnettyjen korttien kokonaismäärään erittäin pieni.
- **Ongelman juurisyy on selvinnyt, ja johtuu siruprofiilissa olevista standardin mukaisista käyttökertalaskureista, jotka oletuksena sallivat kullekin tunnusluvulle 32 767 käyttökertaa.** Jotkut sovellukset pollaavat PIN1-tunnuslukua tiuhaan, mikä johtaa käyttökertojen epänormaalin nopeaan kulumiseen.



DVV:n ratkaisut lukkiutumisongelmaan

- DigiSignin uusi versio **4.1.4e** suodattaa pois ylimääräisiä PIN-koodin pollauksia, johtaan hitaampaan käyttökertalaskureiden kulumiseen, ja esittää käyttöliittymässä laskurien arvon sekä käyttäjälle varoituksen loppuun kulumisesta.
- **DVV on tuomassa kesän aikana tuotantoon muutetun siruprofiilin, jonka myötä käyttökertalaskurit poistuvat sirulta.**
 - Tekninen kuvaus tahoille, jotka ovat itse toteuttaneet suoran sirutuen ilman DigiSign-sovellusta: IAS-ECC –standardin mukaiset Security Data Object –parametrit Maximum usage counter (9C) ja Remaining usage counter (9D) poistetaan siruprofiilista PIN1- ja PIN2-koodien osalta.
- Laskuriongelman takia lukkiutuneet kortit voi reklamoida DVV:lle.
- DVV pahoittelee ongelmasta asiakkailleen aiheutuvaa haittaa.



DigiSign-kortinlukijaohjelmisto

Uusin versio 4.1.4e julkaistu toukokuussa 2021

- Lievennetty käyttökertalaskurien kulumisesta johtuvaa ongelmaa.
 - Tiuhaan tapahtuvaa PIN1-koodin turhaa sirupollausta suodatetaan pois.
 - Käyttöliittymässä esitetään laskurien tila ja varoitetaan käyttäjää jos määrä laskee alle 1000.
- **Suosittelemme vahvasti asiakkaitamme päivittämään version 4.1.4e käyttöönsä.**
 - <https://dvv.fi/kortinlukijaohjelmisto>

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 uusimpien Safari-versioiden kanssa.
- Sisäänrakennettua PDF-allekirjoituksen toimintoa kehitetty.
- Bugi- ja haavoittuvuuskorjauksia.



DigiSignille suoritettu 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 tuottajan 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 korjataan heinäkuussa julkaistavassa versiossa 4.2.0.
- Tulemme kesän aikana julkaisemaan auditoijan virallisen lausunnon tuotteen tietoturvan tasosta.



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.

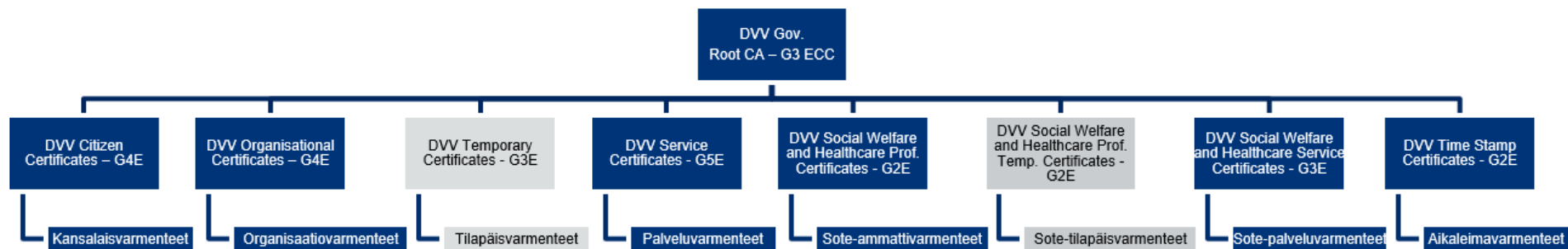
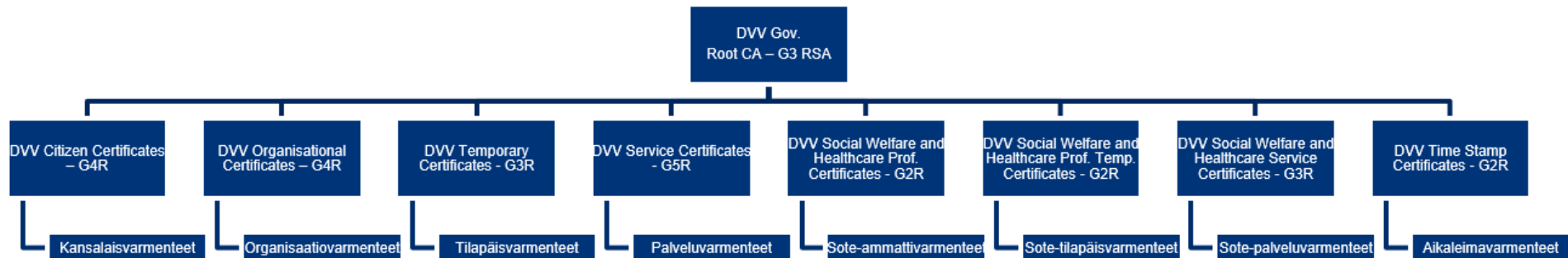


DVV:n varmennehierarkia uudistuu 2021-2022 (I)

- **Uudet G3-varmennehierarkiat tulevat tuotantoon Q4 2021 ja Q1 2022 aikana.**
 - 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 syyskuussa).
 - Tiedotamme asiakkaitamme sähköpostitse ja verkkosivustollamme projektin etenemisestä, ja vielä erikseen muistutamme ennen kuin uudistuotanto alkaa.



DVV:n varmennehierarkia uudistuu 2021-2022 (II)



ECC-testikortteja saatavilla

- DVV alkaa tulevaisuudessa tarjoamaan nykyistä tietoturvalisempia ja suorituskyykyisempia ECC-teknologiaa kyyttavia varmennekortteja.
- Kortin siru (uusi Idemia ID.me) sekä varmenteen tietosisältö ja kyyttötapä pysyvät ennallaan, erona on vain että sirulle generoitavat avaimet luodaan RSA-algoritmin sijaan ECC-algoitmillä. DigiSign Client tukee näitä kortteja versiosta 4.0.18 lähtien.
- Loppukäyttjävarmenteen ECC-käyränä NIST P-384 (secp384r1) ja CA:n allekirjoitusavaimena 4096-bit RSA eli kyseessä on toistaiseksi ECC/RSA-hybridivarmenne. Arviolta syyskuussa tulee tarjolle ECC-täyshierarkian testikortteja.
- ECC-testikortteja on nyt tilattavissa DVV:n verkkoasioinnissa. Tilaus tehdään tavallisena testikorttitilauksena, jonka kommenttikenttään kirjoitetaan pyynnöksi ECC-testikortti. Testikorttien ensisijaisena kohderyhmänä on DVV:n varmennekortti-integraatiota tuotteisiinsa tarjoavat Sote-sektorin tietojärjestelmä- ja sovellustoimittajat.



Aktiiviset SOTE-kortit/-varmenteet 1.6.2021

Tuotantovarmenteet ja –kortit:

SOTE- ja TH-ammattikortit	247 131 (244 694)	↑
SOTE- ja TH-henkilöstökortit	30 130 (29 889)	↑
SOTE- ja TH-toimijakortit	2 186 (2 198)	↓
Yhteensä	279 447 (276 781) kpl	↑

TH-palvelinvarmenteet	1 (1)	-
TH-järjestelmällekirjoitusvarmenteet	0 (0)	-
SOTE-palvelinvarmenteet	1 421 (1 463)	↓
SOTE-järjestelmällekirjoitusvarmenteet	305 (288)	↑
Yhteensä	1 727 (1 752) kpl	↓



Kommentit/kysymykset

Sähköpostilla:

asiakashallinta.th-varmenne@dvv.fi

varmennepalvelut@dvv.fi

Verkkoasiointi:

<https://dvv.fi/verkkoasiointi>



**DIGI- JA
VÄESTÖTIETO-
VIRASTO**

Tehtävänä sujuva
Suomi

