

# Ajankohtaista VRK:lla 24.4.2019

Erikoissuunnittelija Jari Pirinen

Väestörekisterikeskus

[jari.pirinen@vrk.fi](mailto:jari.pirinen@vrk.fi)

0295 535 141

# Digi- ja väestötietovirasto aloittaa 1.1.2020

- Tasavallan presidentti allekirjoitti 15.3.2019 lain Digi- ja väestötietoviraston perustamisesta.
- Väestörekisterikeskus, maistraatit ja maistraattien ohjaus- ja kehittämissyksikkö yhdistyvät yhdeksi virastoksi.
- Virasto edistää yhteiskunnan digitalisaatiota, turvaa tietojen saatavuutta ja tarjoaa palveluja asiakkaiden elämäntapahtumiin.
  - Toiminnassa painottuvat erityisesti valtakunnalliset toimintatavat, yhtenäiset käytännöt ja digitaalisten toimintatapojen tuomat mahdollisuudet.

- <https://vrk.fi/digi-ja-vaestotietovirasto>

# SOTE-kortit/-varmenteet 1.4.2019

SOTE- ja TH-ammattikortit	213 579 (212 824)
SOTE- ja TH-henkilöstökortit	27 236 (27 482)
SOTE- ja TH-toimijakortit	2 339 (2 359)
<b>Yhteensä</b>	<b>243 154</b> (242 665) kpl

TH-palvelinvarmenteet	396 (418)
TH-järjestelmällekirjoitusvarmenteet	123 (144)
epSOS-varmenteet	0 (0)
SOTE-palvelinvarmenteet	1 064 (1 019)
SOTE-järjestelmällekirjoitusvarmenteet	158 (127)

## Testivarmenteet ja -kortit:

SOTE- ja TH-testiammattikortit	8 415 (8 400)
SOTE- ja TH-testihenkilöstökortit	474 (474)
SOTE- ja TH-testitoimijakortit	159 (153)
TH-testipalvelinvarmenteet	92 (101)
TH-testijärjestelmällekirjoitusvarmenteet	33 (36)
epSOS-testivarmenteet	1 (1)
SOTE-testipalvelinvarmenteet	119 (114)
SOTE-testijärjestelmällekirjoitusvarmenteet	96 (93)

# DigiSign-kortinlukijaohjelmisto

Uusin versio 4.0.18b

- Bugikorjauspäivitys marraskuussa julkaistuun 4.0.18-versioon
  - Korjaa harvoin ilmenevän allekirjoitusvarmenteen validointibugin

4.0.18:

- **Tuki tulevalle organisaatiokorttien ja sote-korttien sirulle (Idemia ID.me)**
- Tuki MacOS 10.14:lle
- 32- ja 64-bit Windows 7, 8.1 ja 10 sekä 2008R2, 2012 ja 2016 Server
- 64-bit Linux RPM ja DEB asennuspaketit (ei enää tukea 32-bit Linuxille)

4.0.20:

- Alustava julkaisuajankohta **kesäkuun alkupuolella**
- Useita pienehköjä parannuksia käyttäjystävällisyyteen, asennuksen sujuvoittamiseen, ym

# Toimikorttien uudet sirut

- Taustalla julkinen hankinta; toimittajana Idemia Finland (entinen Oberthur Technologies)
- Siru vaihtuu nykyaikaisempaan
- RSA-avainten pituus kasvaa 2048 -> 3072 bit ja varmenteet myönnetään VRK:n uusilta CA:ilta
- Siru tukee allekirjoitusten osalta SHA2-tiivisteitä (SHA256, SHA384 ja SHA512)
- PKI-toiminnallisuus myös kontaktittomana (Dual Interface, PACE-protokollalla suojattu)
- Emuloitu Mifare-toiminnallisuus (ei 100% taaksepäin yhteensopiva Mifare Classicin kanssa)
- EC-avaimia (NIST SEC P-384) käytäviä kortteja tuotteistetaan tulevaisuudessa
- Aikataulut:
  - Sirumääriykset (FINEID S1 ja S4-2) julkaistaan Q2 / 2019
  - Testikortteja ja kehityskortteja saatavilla Q2 / 2019
  - SoTe-kortit tuotantoon Q3 / 2019 (syyskuu)

# Middleware-toimittajien yhteistyöryhmä

- VRK ehdottaa perustettavan sirukortteja tukevien kortinlukijaohjelmien (middleware) kehittäjätahojen kanssa teknisen yhteistyöryhmän
  - Tiedonvaihtoa ja ajankohtaisten asioiden puimista
  - Kehitystoiveita/palautetta siruasioista
- Säännölliset Skype-kokoontumiset, esim. 3 kk välein
- Ilmoittakaa kiinnostuksenne osoitteeseen [jari.pirinen@vrk.fi](mailto:jari.pirinen@vrk.fi)

# VRK:n uusi varmennehierarkia 2018

- Uusi juurivarmenne VRK Gov. Root CA – G2 ja sen myöntämät subCA-varmenteet otettiin käyttöön loka-marraskuun 2018 aikana
- Miksi?
  - VRK:n aiemman juurivarmenteen käyttöikä loppui henkilövarmenteiden osalta 18.12.2018
  - VRK Gov. Root CA voimassa 18.12.2023 asti
  - SubCA:ilta voitiin siis myöntää 5 vuotta voimassa olevia henkilövarmenteita 18.12.2018 asti
  - Jo myönnettyt varmenteet pysyvät voimassa päättymispäiväänsä asti

# VRK:n uusi varmennehierarkia 2018

## VRK Gov. Root CA – G2

- VRK Gov. CA for Citizen Certificates – G3
- VRK CA for Service Providers – G4
- VRK CA for Organisational Certificates – G3
- VRK CA for Temporary Certificates – G2
- VRK CA for Social Welfare and Healthcare Prof. Certs
- VRK CA for Social Welfare and Healthcare Prof. Temp. Certs
- VRK CA for Social Welfare and Healthcare Service Providers – G2
- VRK CA for Time Stamp Services

## Juurivarmenne

Kansalaisvarmenteet  
Palveluvarmenteet  
Organisaatiovarmenteet  
Varakorttivarmenteet  
SoTe ammattivarmenteet  
SoTe ammattivarakorttivarmenteet  
SoTe palveluvarmenteet  
Aikaleimavarmenteet



# Certificate Transparency käyttöön Q2/2019

- VRK:n palvelinvarmenteille ollaan lisäämässä CT-tuki
- CT:n myötä varmenteet toimivat paremmin SSL-webpalvelinkäytössä
- Ei enää CT-tuen puutteesta johtuvia virheilmoituksia verkkoselaimissa
- Lyhykäisydessään: jokaisen myönnetyn palvelinvarmenteen tiedot julkaistaan julkiseen CT-lokiin, jolloin virheellisesti myönnetyt varmenteet on helpompi havaita
- Parantaa verkkoasioinnin luottamusta ja tietoturvallisuutta

# Taas uusi varmennehierarkia 2019/2020?

- Miksi heti perään uusi?
  - VRK muuttuu 1.1.2020 lähtien Digi- ja väestötietovirastoksi
- Tällä hetkellä epävarmaa, uusiiko VRK varmennehierarkiansa vuodenvaihteessa 2019/2020
- Asia on Viestintäviraston (Traficom) arvioitavana
- Ennakkotapauksia olemassa, jotka vahvistavat ettei varmennehierarkiaa tarvitse uusia vaikka organisaation nimi vaihtuu, kunhan ”juridinen entiteetti” pysyy samana
- Hankkeen mahdollisesta etenemisestä ja aikatauluista tiedotetaan asiakkaita

# Kommentit/kysymykset

Sähköpostilla:

asiakashallinta.th-varmenne@vrk.fi

varmennemyynti@vrk.fi

Verkkoasiointi:

<https://vrk.fi/asiointi>