

Ajankohtaista VRK:lla 25.9.2019

Erikoissuunnittelija Jari Pirinen

Väestörekisterikeskus

jari.pirinen@vrk.fi

0295 535 141

Digi- ja väestötietovirasto (DVV) aloittaa

1.1.2020

- Väestörekisterikeskus, maistraatit ja maistraattien ohjaus- ja kehittämissyksikkö yhdistyvät yhdeksi virastoksi.
- DVV 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 1.9.2019

SOTE- ja TH-ammattikortit	218 209 (213 579)	↑
SOTE- ja TH-henkilöstökortit	27 011 (27 236)	↓
SOTE- ja TH-toimijakortit	2 265 (2 339)	↓
Yhteensä	247 485 (243 154) kpl	↑

TH-palvelinvarmenteet	277 (396)	↓
TH-järjestelmällekirjoitusvarmenteet	66 (123)	↓
epSOS-varmenteet	0 (0)	–
SOTE-palvelinvarmenteet	1 176 (1 064)	↑
SOTE-järjestelmällekirjoitusvarmenteet	216 (158)	↑

Testivarmenteet ja –kortit:

SOTE- ja TH-testiammattikortit	8 522 (8 415)	↑
SOTE- ja TH-testihenkilöstökortit	524 (474)	↑
SOTE- ja TH-testitoimijakortit	209 (159)	↑
TH-testipalvelinvarmenteet	80 (92)	↓
TH-testijärjestelmällekirjoitusvarmenteet	27 (33)	↓
epSOS-testivarmenteet	1 (1)	–
SOTE-testipalvelinvarmenteet	134 (119)	↑
SOTE-testijärjestelmällekirjoitusvarmenteet	99 (96)	↑

DigiSign-kortinlukijaohjelmisto

Uusin versio 4.0.20e

(Tarkka muutosloki löytyy aina [Release Notes –tiedostosta](#))

- Bugikorjauspäivitys 4.0.20-versioon
 - Korjaa joukon bugeja, mm. varakorttia yksilöittäessä ilmenevä PIN-dialogin ongelma

4.0.20:

- Julkaistu kesäkuussa. Vedetty pois jakelusta havaittujen bugien ja julkaistun korjausversion takia
- Uusi aktivointiruutu ja muita parannuksia käyttäjäystävällisyyteen, asennuksen sujuvoittamiseen

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)

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)
- ECC-avaimia (NIST P-384) käyttäviä kortteja ollaan tuotteistamassa, ensin varakorttien osalta
- Aikataulut: Sirumääritykset (FINEID S1 ja S4-2) julkaistu: <https://vrk.fi/fineid-maaritykset>
Testikortteja tilattavissa: <https://vrk.fi/asiointi>
SoTe-kortit tuotantoon Q1 / 2020

SCS-sovelluksesta uusi versio

- VRK:n tuottamasta SCS Signer –allekirjoitussovelluksesta julkaistaan Q4 2019 aikana uusi versio Androidille
- Uusina ominaisuuksina mm. tuki uudelle Idemia ID.me –sirulle sekä uudemmille Android-versioille
- Sovelluksen sekä SCS-protokollan tulevaisuuden roadmapit edelleen auki ja osittain riippuvaisia muista mobiilikehityshankkeista

Certificate Transparency otettu käyttöön huhtikuussa 2019

- VRK:n palvelinvarmenteissa otettu käyttöön Certificate Transparency
- CT:n myötä varmenteet toimivat paremmin SSL-webpalvelinkäytössä
- Ei enää CT-tuen puutteesta johtuvia virheilmoituksia verkkoselaimissa
- Pähkinänkuoressa: Jokaisen myönnetyn palvelinvarmenteen tiedot julkaistaan julkiseen CT-lokiin, jolloin virheellisesti myönnetyt varmenteet on helpompi havaita kolmansien osapuolten toimesta
- Parantaa verkkoasioinnin luottamusta ja tietoturvallisuutta

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

Taas uusi varmennehierarkia 2020?

- Miksi heti perään pitäisi tehdä uusi?
 - VRK muuttuu 1.1.2020 lähtien Digi- ja väestötietovirastoksi
- VRK ei uusi varmennehierarkiaansa vielä vuodenvaihteessa 2019/2020
- Siirtymäaika ”muutama vuosi”
- Nimenmuutos indikoidaan varmennepolitiikkadokumentaatiossa
- Tulevan hankkeen etenemisestä ja aikatauluista tiedotetaan asiakkaita

Aikaleimapalvelun tuotteistaminen (TSA)

- Varmennettu aikaleima on sähköiseen allekirjoitukseen liitettävä tarkka aikaleima, joka kiistämättömästi todistaa allekirjoituksen tekohetken.
- Aikaleimapalvelun tuotteistaminen on VRK:lla selvityksen alla. Asiakaskysyntää kartoitetaan kyselyllä jonka tulokset valmistuvat pian.
- Varmennepalveluilla on jo toiminnassa oleva aikaleimapalvelu jota käyttää mm. Palveluväylä sekä muutama pilottiasiakas, mutta sitä ei ole vielä virallisesti auditoitu eikä tuotteistettu.
- Jos olette kiinnostuneita hyödyntämään aikaleimapalvelua tuotteessanne tai asiakkaallanne, ottakaa yhteyttä jari.pirinen@vrk.fi

Kommentit/kysymykset

Sähköpostilla:

asiakashallinta.th-varmenne@vrk.fi

varmennemyynti@vrk.fi

Verkkoasiointi:

<https://vrk.fi/asiointi>