Ajankohtaista DVV:llä 02.10.2020

Erikoissuunnittelija Jari Pirinen
Digi- ja väestötietovirasto
jari.pirinen@dvv.fi
0295 535 141

DIGI- JA VÄESTÖTIETO-VIRASTO

Uudet Sote-kortit Citrix-ympäristöissä

- DVV:n uudet sote-kortit (Idemia ID.me –siru) otettiin tuotantoon 1.4.2020.
- Olemme asiakasyhteydenoton seurauksena saaneet tietoomme yhteensopivuus-ongelmasta uusien korttien käyttämien 3072-bittisten RSA-varmenteiden ja **Citrix VPX** –tuotteen kanssa.
- Citrix VPX tukee client-varmenteita vain 2048-bittisiin RSA-varmenteisiin asti.
- Ongelma on selvityksessä yhdessä asiakkaan ja Citrixin kanssa ja siitä on erikseen tiedotettu myös Kelan Kanta-tiimiä.

DigiSign-kortinlukijaohjelmisto

Uusin versio 4.1.2 julkaistu heinäkuussa 2020 (Tarkka muutosloki löytyy Release Notes –tiedostosta)

- Sisäänrakennettua PDF-asiakirjan allekirjoitustoimintoa nopeutettu ja kehitetty.
- Automaattinen versiontarkistustoiminto huomauttaa käyttäjää jos uudempi versio on saatavilla (oletuksena päällä vain .exe-asennuspaketissa, ei massa-asennuksiin tarkoitetussa .msi-paketissa).
- Tuki MacOS 10.15 Catalinalle sekä parempi tulevien MacOS-versioiden eteenpäin yhteensopivuus.
- Windows-asennuspaketti allekirjoitettu uudella koodin allekirjoitusvarmenteella (edellinen vanheni tammikuussa) ja MacOS-asennuspaketti notarisoitu Applella asennuksen sujuvoittamiseksi.
- Useita bugikorjauksia.

Varmenteiden sähköiset tukipalvelut uudistettu kevään 2020 aikana

- DVV:n julkinen varmenne- ja sulkulistahakemisto sekä varmenteen- ja SCS-allekirjoituksen testauspalvelut on uudistettu kevään 2020 aikana.
- Lisäksi kokonaisuuteen on tullut uutena palveluna sähköisesti allekirjoitetun PDF-asiakirjan tarkastuspalvelu.
- Syynä uudistukseen on, että aiempi palvelukokonaisuus oli alusta- ja teknologia-ratkaisultaan sekä tietoturvaltaan ja käyttöliittymältään vanhanaikainen.
- Uusi palvelukokonaisuus avattiin vaiheittain osoitteeseen https://dvv.fineid.fi
  - Vaihe 1 (avattu 2/2020): Varmenne- ja sulkulistahakemisto
  - Vaihe 2 (avattu 4/2020): Tunnistusvarmenteen testaus (client authentication)
  - Vaihe 3 (avattu 4/2020): Allekirjoituksen testaus (SCS signature)
  - Vaihe 4 (avattu 5/2020): Sähköisesti allekirjoitetun PDF:n validointipalvelu (PAdES)

Sähköisesti allekirjoitetun PDF-asiakirjan tarkastuspalvelu

- Palvelu tarkastaa PDF-asiakirjan sähköisen allekirjoituksen (PAdES-standardi):
  - Teknisen kelvollisuuden (allekirjoituksen/tiivisteen oikeellisuus, standardinmukaisuus).
  - Allekirjoittajan identiteetin luotettavuuden (varmenteen myöntäjä).
  - Tarkastuksen tulos ilmoitetaan helppotajuisilla liikennevaloväreillä vihreä/keltainen/punainen.
  - Tarkempi kuvaus palvelun suorittamista tarkastuksista: https://dvv.fi/tarkasta-pdf-asiakirja

- Luottaa allekirjoituksiin jotka on tehty kaikilla DVV:n sekä EU-komission Trusted Listilla (EUTL) olevien varmentajien myöntämillä varmenteilla. Palveluun on tulevaisuudessa mahdollista lisätä luotetuiksi myös kolmannen osapuolen varmentajia.

- Palvelu on saatavilla sekä web-käyttöliittymänä että REST-rajapinnan kautta, jolloin se on helposti integroitavissa muihin tietojärjestelmiin automatisoitua tarkastusta varten.

- Palvelun käyttö on maksutonta ja se on vapaasti saatavilla (ainakin toistaiseksi).

PDF-asiakirja tarkastettu. Asiakirja sisältää seuraavat allekirjoitukset:

1 kpl kelvollisia allekirjoituksia, joiden varmenteen myöntäjä on EU-hyväksytty ja joiden avainta säilytetään hyväksytyssä turvalaitteessa.

Allekirjoitus 1/1:[S-BFF949F198F79A17771573BE9F315BD54862C1D92A1BCC372DB40A85BADA2A66]

- **Sähköinen allekirjoitus on kelvollinen eikä sitä ole jälkikäteen muutettu tai väärennetty. Allekirjoituksen taso on PKCS7_T (aikaleima).**
- **Allekirjoituksen on tehnyt DVV:n luottama taho.**
- **Allekirjoitus on tehty EU:n hyväksytyn tason varmenteella.**
- **Allekirjoituksessa käytettyä avainta säilytetään EU-hyväksytyssä turvalaitteessa (QSCD).**

Allekirjoittaja: Pirinen Jari 91170404S | Digi- ja väestotietovirasto

Varmenteen myöntäjä ja juurimyöntäjä: VRK CA for Organisational Certificates - G3 | VRK Gov. Root CA - G2 (**Luotettu**)

Allekirjoituksen ajankohta: 11.5.2020 14:43:44 +03:00 (**Varmennettu aikaleima (TSA)**)

Palvelinvarmenteiden voimassaoloajat lyhenivät 1.9.2020 lähtien

- DVV:n myöntämien TLS-palvelinvarmenteiden (ml. Sote- ja hyvinvointisovellus-) voimassaoloajat lyhenivät 1.9.2020 lähtien **yhteen vuoteen** aiemmasta kahdesta vuodesta. Asiasta tiedotettiin asiakkaita heinäkuussa.

- Muutoksen syynä on CA/Browser Forumin 16.7.2020 hyväksymä päätösesitys. DVV:n palvelinvarmennetuotanto auditoidaan CA/Browser Forumin Baseline Requirements (BR) –kriteerejä vasten, joten päätös sitoo myös meitä.

- Muutos ei vaikuta ennen 1.9. voimaan tulleisiin palvelinvarmenteisiin, eikä myöskään järjestelmäallekirjoitus-, sähköposti- tai henkilövarmenteisiin.

ECC-avaimia käyttävät varmennekortit

- DVV:llä on suunnitelmissa alkaa tarjoamaan nykyistä tietoturvallisempia ja suoritus-kykyisempiä 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-algoritmilla. 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 Q4/2020 aikana. Testikorttien ensisijaisena kohderyhmänä DVV:n varmennekortti-integraatiota tuotteisiinsa tarjoavat Sote-sektorin tietojärjestelmä- ja sovellustoimittajat.

Aktiiviset SOTE-kortit/-varmenteet 1.9.2020

Tuotantovarmenteet ja –kortit:

SOTE- ja TH-ammattikortit	234 185 (233 092)	↑
SOTE- ja TH-henkilöstökortit	28 349 (28 103)	↑
SOTE- ja TH-toimijakortit	2 242 (2 224)	↑
Yhteensä	**264 776** (263 419) kpl	↑

TH-palvelinvarmenteet	103 (114)	↓
TH-järjestelmäallekirjoitusvarmenteet	14 (16)	↓
SOTE-palvelinvarmenteet	1 358 (1 351)	↑
SOTE-järjestelmäallekirjoitusvarmenteet	266 (260)	↑
Yhteensä	**1 741** (1 741) kpl	–

Kommentit/kysymykset

Sähköpostilla:
asiakashallinta.th-varmenne@dvv.fi
varmennemyynti@dvv.fi

Verkkoasiointi:
https://dvv.fi/verkkoasiointi

DIGI- JA VÄESTÖTIETO-VIRASTO

Tehtävänä sujuva Suomi