



YRITYKSEN PANKKIYHTEYSKANAVAN TLS-VARMENTEEN UUSIMINEN

OPn Yrityksen pankkiyhteys (Web Services) -kanavan wsk.op.fi-domainin uusi TLS-varmenne otetaan käyttöön tuotannossa 22.5.2018 ja asiakastestiympäristössä (wsk.asiastesti.op.fi) 10.4.2018. Varmenteen myöntäjä on Entrust.

Toivomme, että tarkistatte, että pankkiyhteysohjelmistonne luottaa Entrustin juurivarmen-tajaan ja välivarmentajaan. Lisäksi suosittelemme kokeilemaan (10.4 jälkeen) Web Services -kanavan asiakastestiympäristössä, että palvelun uusi TLS-varmenne toimii asiakasohjel-mistonne kanssa.

Uudet Entrustin CA-varmenteet voi tarvittaessa hakea osoitteesta <https://www.entrustdata-card.com/pages/root-certificates-download>.

Wsk.op.fi käyttää:

Entrust Root Certificate Authority—G2

Entrust Certificate Authority - L1K (Non-EV SSL)

Web Services -palvelun TLS-varmenne:

Asiakastesti: CN=wsk.asiastesti.op.fi

Tuotanto: CN= wsk.op.fi

Lisätietoja:

Mikä on TLS-varmenne?

TLS-varmenteita (aiemmin käytettiin nimeä SSL-varmenne) käytetään tietoliikenteen suo-jaamiseen erityisesti selainkäytössä, mutta myös teknisissä rajapinnoissa. Varmenteen avulla palvelun käyttäjä voi varmistua, että verkkoyhteys on muodostettu oikealle toimijalle eikä kukaan ulkopuolinen esiinny vilpillisesti toisena palveluna. Varmenne mahdollistaa myös tietoliikenteen salaamisen.

Nykytila OPn Web Services -kanavan ympäristöissä

Tällä hetkellä OPssa on käytössä DigiCertin myöntämä varmenne, joka on ristiinvarmen-nettu Symantecin vanhasta juurivarmentajasta. Tällä on väliaikaisesti varmistettu, että Symantecin tai DigiCertin juurivarmentajaan luottavat ohjelmistot toimivat OPn WS-kanavan ympäristöissä.

Tavoitetila OPn Web Services -kanavan ympäristöissä

22.5 käyttöön otettava TLS-varmenteen myöntäjä on Entrust. Jatkossa kuitenkin on huomi-oitava, että varmenteen myöntäjä voi vaihtua myös pankeista riippumattomista syistä. **Tä-män vuoksi suosittelemme, että ohjelmistot luottavat kaikkiin yleisesti luotettuihin varmentajiin.**

Viestintävirasto on julkaissut maaliskuun alussa tiedotteen (<https://www.viestintävirasto.fi/kyberturvallisuus/tietoturvanyt/2018/02/ttn201803011113.html>) osan verkkosivujen varmenteiden luottamisen lakkaamisesta, johon kannattaa tutustua.
