

17.4.2020 TN-HedsamX-Webserver-Sertifikaatin-Asennus-FI-V1.0

Ohjelmisto toimitetaan allekirjoittamattomilla sertifikaateilla **unsigned.key** ja **unsigned.crt**. Kun otat ensimmäistä kertaa yhteyttä graafiseen käyttöliittymään selaimella, saat seuraavan ilmoituksen. Ilmoituksen tarkka sisältö riippuu käytetystä selaimesta. Tässä esimerkissä käytetään Chrome-selainta.



Yhteytesi ei ole salattu

Sivustolle **127.0.0.1** hyökännyt taho voi yrittää varastaa tietojasi (esimerkiksi salasanoja, viestejä tai luottokorttitietoja). [Lisätietoja](#)

NET::ERR_CERT_AUTHORITY_INVALID

[Lisäasetukset](#)[Takaisin suojaukseen](#)

Valitse **Lisäasetukset**.

Jotta saat yhteyden käyttöliittymään, salli poikkeus valitsemalla **Siirry sivustoon 127.0.0.1 (tämä ei ole turvallista)**.

[Piilota lisäasetukset](#)[Takaisin suojaukseen](#)

Palvelin ei voinut todistaa olevansa **127.0.0.1**; tietokoneesi käyttöjärjestelmä ei luota sen suojausvarmenteeseen. Tämä voi johtua määrittämisvirheestä tai verkkoyhteytesi siepanneesta hyökkääjästä.

[Siirry sivustoon 127.0.0.1 \(tämä ei ole turvallista\)](#)

Yllä oleva ilmoitus tulee aina kun tyhjennät selaimen historian tai käytät yhteyteen ns. yksityistä ikkunaa.

Selaimen osoiterivillä näkyy myös yhteyden aikana seuraava varoitus:

 **Ei turvallinen** | 127.0.0.1/wsgi/chameleon/index.html

Jotta pääset eroon yllä mainituista ilmoituksista ja varoituksista, kopioi allekirjoitetut sertifikaatit palvelimelle ja ota ne käyttöön. Näiden allekirjoitettujen sertifikaattien hankinta on aina loppuasiakkaan tehtävä. Tässä esimerkissä asiakas (customer) on hankkinut omat allekirjoitetut sertifikaatit.

1. Avaa seuraava kulunvalvontapalvelimen kansio:
C:\Hedengren\Hedsam\Webserver\<versio>\core\apache2\server_certs
2. Kopioi allekirjoitetut sertifikaattitiedostot kansioon. Tiedostojen tulee olla seuraavaa muotoa:
 - **sertifikaatin_nimi.crt** (esim. **customer.crt**)
 - **sertifikaatin_nimi.key** (esim. **customer.key**)

17.4.2020 TN-HedsamX-Webserver-Sertifikaatin-Asennus-FI-V1.0

3. Avaa seuraava kulunvalvontapalvelimen kansio:

C:\Hedengren\Hedsam\Webserver\<versio>\core\apache2\conf

4. Muokkaa **httpd.conf**-tiedostoa esim. Notepad-tekstieditorilla. Joissakin serveriympäristöissä Notepad tulee käynnistää ensin *Suorita järjestelmänvalvojana* ja vasta tämän jälkeen avata **httpd.conf**-tiedosto.

Etsi tiedostosta kohta Listen 443, jossa on määritetty sertifikaattitiedostojen sijainti ja nimet.

Listen 443

<VirtualHost *:443>

 SSLEngine on

 SSLCertificateFile "\${US_ROOTF}/core/apache2/server_certs/customer.crt"

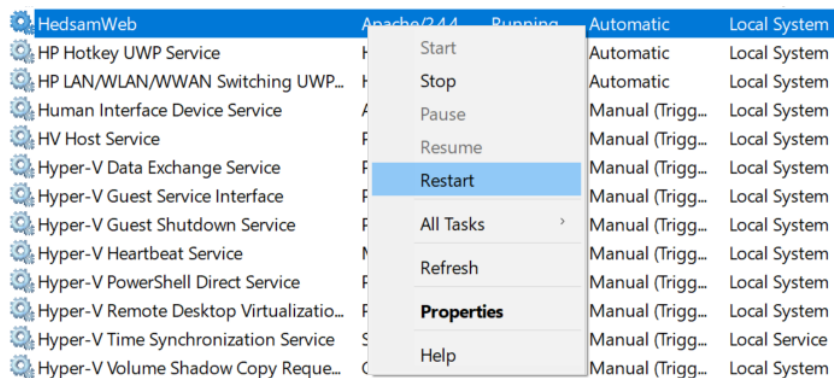
 SSLCertificateKeyFile "\${US_ROOTF}/core/apache2/server_certs/customer.key"

</VirtualHost>

Oletuksena tiedostojen nimet ovat **unsigned.crt** ja **unsigned.key**. Muuta nimet vastamaan käyttämiäsi allekirjoitettuja sertifikaattitiedostoja ja tallenna muutokset.

5. Uudelleenkäynnistä HedsamWeb-palvelu Windowsin palveluiden kautta tai komentokehotteella (CMD).

- a. Windowsin Palvelut-ikkunan kautta:



- b. Komentokehote (järjestelmänvalvoja)-ikkunan kautta seuraavilla komennoilla:

net stop hedsamweb

net start hedsamweb

