Asiakasjärjestelmän liittäminen liityntäpalvelimeen – esuomi.fi

Suomi.fi-palveluväylä – Asiakasjärjestelmän liittäminen liityntäpalvelimeen

Palveluiden kutsuminen

Liityntäpalvelimen asiakasrajapinta, jonka kautta palveluväylän kautta käytettävissä olevien palvelujen kutsuminen tapahtuu, on muotoa ”https://{host}/”. **Osoitteen ”{host}”-osa tulee korvata oman liityntäpalvelimen host-nimellä**. Liityntäpalvelimelle lähetettävien pyyntöjen **Content-Type**-otsikkotiedon arvon tulee olla ”**text/xml**” ja **HTTP-metodin** on oltava **POST**.

> IP-osoitteen käyttö kutsuissa ei ole suositeltavaa, sillä se aiheuttaa varmenteisiin liittyviä ongelmia. Ongelmia ilmenee, mikäli liityntäpalvelin kutsussa käytetty host-nimi ei vastaa liityntäpalvelimen varmenteessa olevaa host-nimeä.

```
Liityntäpalvelimen osoite:
https://{host}/
Method: POST
Content-Type: text/xml
```

Asetukset

Asiakasjärjestelmän (*service client*) liittäminen liityntäpalvelimeen tapahtuu liityntäpalvelimelle luodun alijärjestelmän (*subsystem*) kautta. Alijärjestelmä on käytännössä asiakasjärjestelmän yksilöivä tunnus palveluväylässä ja sitä käytetään palveluiden kutsumisessa sekä palveluväylään liitettyjen palveluiden käyttöoikeuksien määrittelyssä. Alijärjestelmä voi olla asiakasjärjestelmäkohtainen tai vaihtoehtoisesti myös useat yhden loogisen kokonaisuuden muodostavat asiakasjärjestelmät voivat hyödyntää samaa alijärjestelmää palveluiden kutsumiseen. Palveluväylän käyttäoikeuksien määrittely tapahtuu alijärjestelmätasolla, jonka vuoksi lähtökohtaisesti tulisi aina käyttää asiakasjärjestelmäkohtaisia alijärjestelmiä. Liityntäpalvelimen ja asiakasjärjeslmän väliseen yhteyteen liittyvät asetukset löytyvät liityntäpalvelimen ylläpitoliittymästä.

> Liityntäpalvelimen ylläpitoliittymän osoite on https://{host}:4000/, jossa host-korvataan oman liityntäpalvelimen host-nimellä.

1. Kirjaudu sisälle liityntäpalvelimen ylläpitoliittymään. Kirjautumisen jälkeen näytölle avautuu listaus liityntäpalvelimelle lisätyistä oman organisaation alijärjestelmistä (*subsystem*).

2. Valitse listauksesta alijärjestelmä, johon liittyviä asetuksia haluat muokata ja klikkaa rivin oikeassa reunassa olevaa **Internal Servers** -painiketta. **HUOM!** Asetukset ovat alijärjestelmäkohtaisia eli mikäli haluat muokata kaikkien alijärjestelmien asetuksia, on asetukset käytävä muuttamassa jokaiselle alijärjestelmälle erikseen.

3. Oletusarvoisesti asiakasjärjestelmä voi kutsua liityntäpalvelinta HTTP- ja HTTPS-protokollaa käyttäen. HTTPS-protokollaa käytettäessä yhteyden salaamiseen käytetään liityntäpalvelinmen sisäistä varmennetta (*Internal Certificate*). Sisäinen varmenne on liityntäpalvelimen itsensä allekirjoittama (ns. self-signed varmenne), jonka vuoksi

se on erikseen määriteltävä luotetutuksi asiakasjärjestelmän puolella HTTPS-protokollaa käytettäessä. Liityntäpalvelimen sisäisen varmenteen lataaminen tapahtuu alijärjestelmä asetuksien kautta *Internal Servers* -välilehdellä sijaitsevassa *Security Server Certificate* -osiossa olevaa Export-painiketta klikkaamalla.

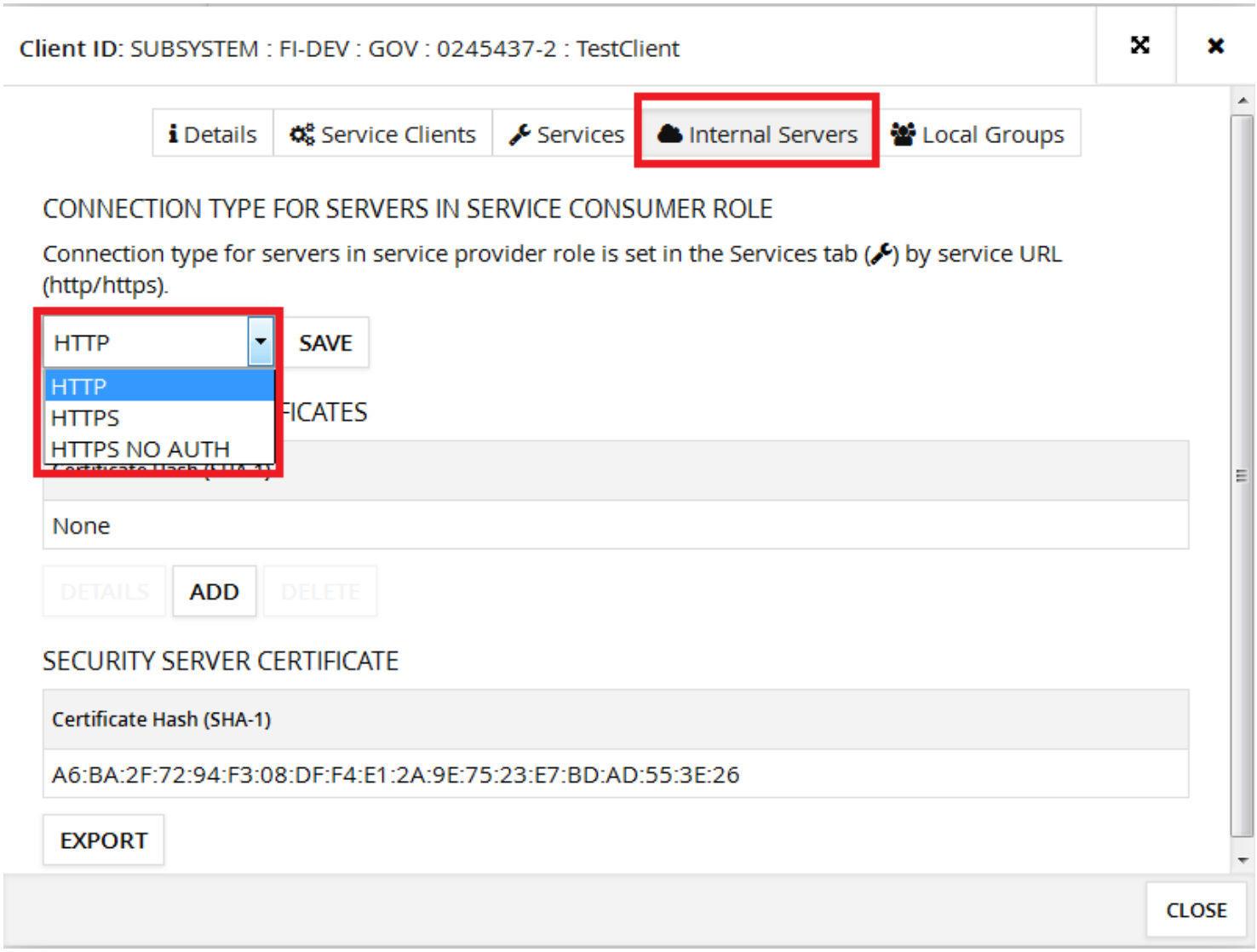
Asiakasjärjestelmän ja liityntäpalvelimen välisessä yhteydessä on vahvasti suositeltavaa käyttää aina HTTPS-protokollaa. HTTP-protokollan käyttö on mahdollista estää asetuksista käyttämällä HTTPS-vaihtoehtoa. HTTPS-vaihtoehtoa käytettäessä on kuitenkin syytä huomioida, että tällöin asiakasjärjestelmän on esitettävä asiakasvarmenne, joka on erikseen lisättävä liityntäpalvelimen *Internal SSL Certificates* -listaukseen.

> **HTTPS-asetuksen ja asiakasvarmenteiden käyttö on pakollista aina, kun useat eri organisaatiot käyttävät samaa liityntäpalvelinta**. Tällaisessa tilanteessa asiakasvarmenteen käyttö on ainoa tapa estää organisaatioita kutsumasta palveluväylän palveluita toistensa alijärjestelmien kautta. Kaikki samaa liityntäpalvelinta käyttävät organisaatiot käyttävät samaa liityntäpalvelimen kutsurajapintaa ja IP-osoitetta, jolloin palvelukutsujen tekoa toisen organisaation nimissä ei ole voida estää palomuuriasetusten kautta.

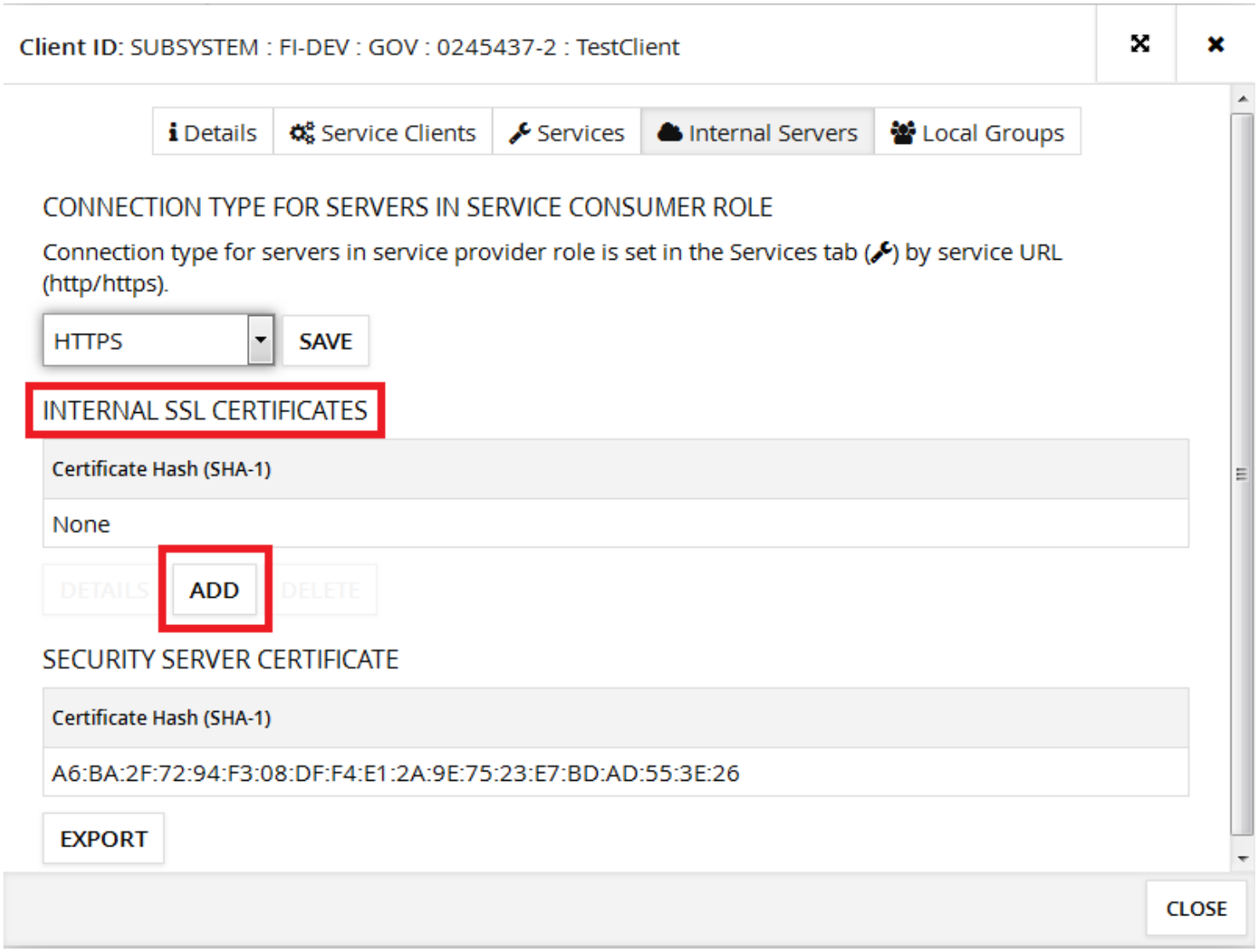
> Liityntäpalvelimen ja asiakasjärjestelmän välisessä liikenteessä on oletuksena sallittu TLS 1.2 ja seuraavat PFS Cipher Suitet.
> TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
> TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*
> TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
> TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*
> TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
> TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
> TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
> TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
> (*) ei käytössä RHEL:ssä jos käytetään OpenJDK:ta.

Asiakasjärjestelmän ja liityntäpalvelimen välisen yhteyden tyyppi määritellään *Connection type for servers in service consumer role* -asetuksen kautta. Asetuksen mahdolliset arvot ovat:

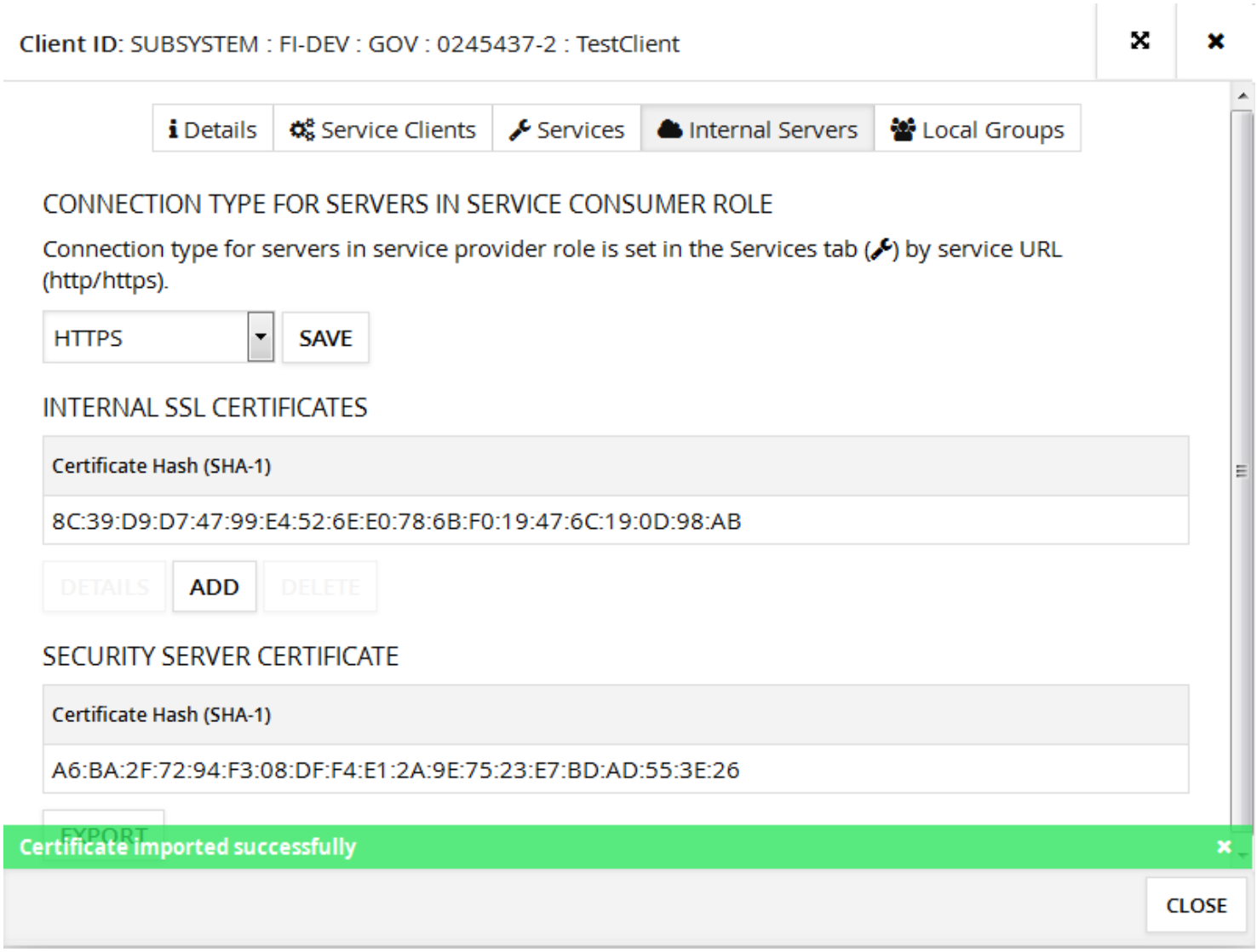
- HTTP: asiakaspalvelin voi tehdä kutsun HTTP tai HTTPS -protokollalla. Varmennetta ei tarvita.
- HTTPS: palvelun käyttäjän täytyy esittää SSL asiakasvarmenne, joka on listattu Internal SSL Certificates -kohdassa.
- HTTPS NO AUTH: asiakaspalvelimen täytyy esittää asiakasvarmenne, mutta liityntäpalvelin ei tarkista on varmennetta lisätty Internal SSL Certificates -listaukseen



4. Asiakasvarmenteiden lisääminen liityntäpalvelimelle tapahtuu *Internal SSL Certificates* -kohdan alla olevaa **Add**-painiketta klikkaamalla. Tämän jälkeen käyttöliittymä ohjeistaa, kuinka asiakasjärjestelmän asiakasvarmenteen lataaminen liityntäpalvelimelle tapahtuu.



5. Kun asiakasvarmenne on onnistuneesti lisätty liityntäpalvelimelle, tulee varmenteen tiivistesumma näkyville *Internal SSH Certificates* -listaukseen. Liityntäpalvelimen sisäisen varmenteen lataaminen tapahtuu *Security Server Certificate* -osiossa olevaa **Export**-painiketta klikkaamalla.



Asiakasvarmenteen testaaminen

Asiakasvarmenteen käyttöä voidaan helposti testata kutsumalla getRandom-testipalvelua Curl-ohjelman avulla.
Vaiheet 1, 2 ja 6 tulee suorittaa jollakin muulla palvelimella kuin liityntäpalvelimella.

1. Luo testissä käytettävä asiakasjärjestelmän yksityinen avain.

```
openssl genrsa -out clientprivatekey.pem
2048
```

2. Luo avaimelle ns. self-signed varmenne.

```
openssl req -new -x509 -key clientprivatekey.pem -out clientcert.pem -days
365
```

3. Kirjaudu liityntäpalvelimen ylläpitoliittymään ja avaa alijärjestelmän asetukset, jota haluat käytttää palvelukutsussa.

Liityntäpalvelimen ylläpitoliittymän osoite on https://{host}:4000/, jossa host-korvataan oman liityntäpalvelimen host-nimellä.

4. Avaa *Internal Servers* -välilehti ja vaihda *Connection type for servers in service consumer role* -asetuksen arvoksi HTTPS.

5. Lisää luomasi clientcert.pem-tiedostoon tallennettu asiakasvarmenne *Internal SSL Certifacetes* -listaukseen.

6. Kutsu kehitysympäristön *getRandom*-testipalvelua käyttäen alijärjestelmää, jonka alle lisäsit asiakasvarmenteen. GetRandom palvelun kutsusanoma löytyy täältä.

```
curl -E ./clientcert.pem --key ./clientprivatekey.pem -k -d @getRandom.xml --
header "Content-Type: text/xml" -X POST https://{host}/
```

7.Yritä kutsua kehitysympäristön testipalvelua myös ilman luomaasi yksityistä avainta ja varmennetta. Lopputuloksena pitäisi olla alla nähtävä virheilmoitus.

```
curl -k -d @getRandom.xml --header "Content-Type: text/xml" -X POST
https://{host}/
```

Virheilmoitus:

```
Server.ClientProxy.SslAuthenticationFailed

Client (SUBSYSTEM:FI-DEV/GOV/0245437-2/TestClient) specifies SSLAUTH but did not
supply SSL certificate
```

Curl-komennossa on käytetty k-optiota, joka tarkoittaa, että kutsutun palvelun varmennetta ei verifioida. Lisätietoja.

Versio	Mitä tehty / muutettu	Pvm/ henkilö
1.0	Dokumentti julkaistu eSuomessa.	22.06.16 / HH

Yksilöintitunnus: 12345