Varmennepalvelu - testipenkki

Kansallisen tulorekisterin perustamishanke

SISÄLLYS

1 JOHDANTO

Varmennepalvelun testipenkin tarkoitus on helpottaa varmennepalvelun rajapintaa käyttävän sovelluksen kehittämistä. Testipenkissä on mahdollista testata varmenteen allekirjoituspyynnön lähetystä, varmenteen uusimispyynnön lähetystä ja varmenteen noutoa.

Testipenkissä käytetään ennakkoon määriteltyjä kertakäyttöisiä tunnisteita, PKI-avaimia ja varmenteita. Tästä johtuen Web Service -pyyntöjä voi toistaa useita kertoja käyttäen samoja parametreja. Esimerkiksi ”Uuden varmenteen allekirjoituspyynnön” siirtotunnusta (TransferId) ja ”kertakäyttösalasanaa” (TransferPassword) voi käyttää monta kertaa.

Testipenkistä saatavia varmenteita ei voi käyttää tulorekisterin rajapinnoissa.

2 TESTIMATERIAALI

Testipenkissä on pysyvästi voimassa oleva varmennetilaus sekä kaksi esivalmisteltua varmennetta ”Varmennepyyntöä” ja ”Varmenteen uusimista” varten. Tämä dokumentti sisältää ohjeet testipenkin käyttöä varten. Lisäksi käyttäjä tarvitsee testausta varten julkaistut testiavaimet (PKI yksityinen avain). Nämä testiavaimet on julkaistu tulorekisterin varmennepalvelun sivuilla:
https://www.vero.fi/globalassets/tulorekisteri/varmennepalvelu-testipenkki.zip

Zip-paketti sisältää seuraavat tiedostot:

- SignNewCertificate_Private.key
  - Tämä yksityinen avain on tarkoitettu uuden varmenteen allekirjoituspyynnön (CSR) luontiin (signNewCertificate-operaatio) ja varmenteen uusimisen (renewCertificate-operaatio) SOAP-sanoman XML-allekirjoituksen muodostamiseen.
- RenewCertificate_Private.key
  - Tämä yksityinen avain on tarkoitettu varmenteen uusimisen yhteydessä varmenteen allekirjoituspyynnön (CSR) luontiin (renewCertificate-operaatio).

2.1 Testipenkin palveluissa käytettävät parametrit

Testipenkin Web Service -palveluissa on käytettävä alla lueteltuja ennalta määriteltyjä tietoja.

1. Uuden varmenteen allekirjoituspyynnön lähetys (signNewCertificate)

```
- Environment: TEST
- CustomerId: 0123456-7
- CustomerName: Ab PKI Developer Company Oy
- TransferId: 12345678903
- TransferPassword: Pw8a1d4u3HhOqhlo
- CertificateRequest: <PKCS#10-muotoinen Base64-koodattu merkkijono>
```

CertificateRequest (CSR) -tiedon muodostus on tehtävä 'SignNewCertificate_Private.key' -avainta käyttäen. Tällöin on mahdollista yhdistää palvelun palauttama varmenne tähän samaan yksityiseen avaimeen. On mahdollista toteuttaa CSR myös itse muodostamallaan avaimella, mutta tällöin palautettua varmennetta ei voida yhdistää käyttäjän avaimeen.

2. Voimassaolevan varmenteen uusimisen allekirjoituspyynnön lähetys (renewCertificate)

- `Environment: TEST`
- `CustomerId: 0123456-7`
- `CustomerName: Ab PKI Developer Company Oy`
- `CertificateRequest: <PKCS#10-muotoinen Base64-koodattu merkkijono>`
- `Signature: <XML Signature mukainen elementti>`

CertificateRequest (CSR) -tiedon muodostus on tehtävä 'RenewCertificate_Private.key' -avainta käyttäen. Tällöin palvelun palauttama varmenne voidaan yhdistää tässä yhteydessä käytettyyn yksityiseen avaimeen. Myös tässä yhteydessä on mahdollista toteuttaa CSR itse muodostamallaan avaimella, mutta sitä ei voida yhdistää käyttäjän avaimeen.

Signature-elementti on muodostettava 'SignNewCertificate_Private.key' -avainta käyttäen. Signature-elementin X509Certificate-tietoon on liitettävä varmennepalvelun testipenkistä noutoavaimella (RetrievalId) 990639930742461205 saatu varmenne (katso kohta 3. Varmenteen noutaminen).

3. Varmenteen noutaminen (getCertificate)

- `Environment: TEST`
- `CustomerId: 0123456-7`
- `CustomerName: Ab PKI Developer Company Oy`
- `RetrievalId: <Uuden varmenteen pyyntöön saatu vastaus>`

Varmenteen nouto-operaatiolla voi hakea kaksi esivalmisteltua varmennetta. Noudettaessa varmennetta, joka on "muodostettu" testipenkin signNewCertificate-operaatiossa käytetyllä yksityisellä avaimella, on käytettävä noutotunnusta (RetrievalId) 990639930742461205. Mikäli haluaa noutaa varmenteen, joka liittyy renewCertificate-operaatiossa käytettyyn yksityiseen avaimeen, käytetään noutotunnusta 11885819811430372306.

Testipenkissä ei ole varmennetta uusitun varmenteen (renewCertificate-operaatiosta saatu varmenne) uusimiseen, vaan testipenkki palauttaa ”Voimassaolevan varmenteen uusimiseen” aina saman esivalmistetun varmenteen.

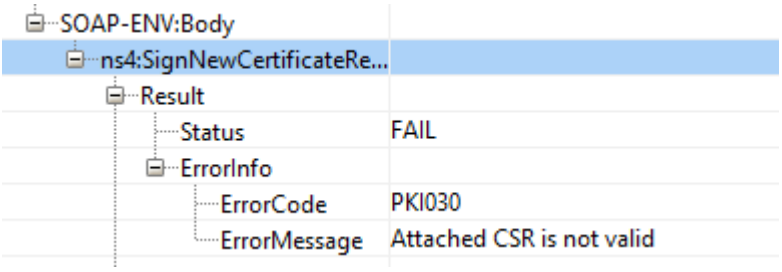
2.2 Testipenkin yhteysosoite

Varmennepalvelun testipenkki sijaitsee varmennepalvelun testiympäristön yhteydessä. Sen osoite poikkeaa varsinaisen testiympäristön osoitteesta palvelun kontekstissa olevan /DEV-kohdan osalta. Osoite kokonaisuudessaan on:
https://pkiws-testi.vero.fi/DEV/2017/10/CertificateServices

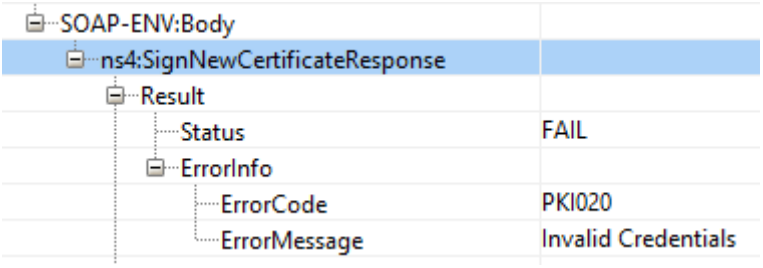
3 TESTIPENKIN PALVELUIDEN VIRHETILANTEET

Testipenkin virhekäsittely ei ole siinä käytettyjen rajallisten varmenteiden ja niiden elinkaaren takia täysin tuotantoa vastaava. Tyypillisimmät virhetilanteet on esitelty tässä kappaleessa. Kattava listaus palvelun virhekoodeista löytyy varmennepalvelun dokumentaatiosta.

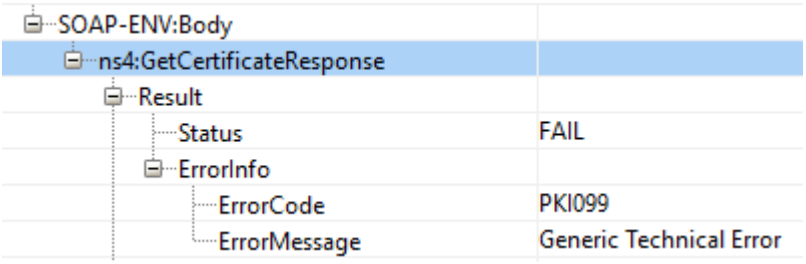
Uuden varmenteen pyynnössä CSR on virheellinen



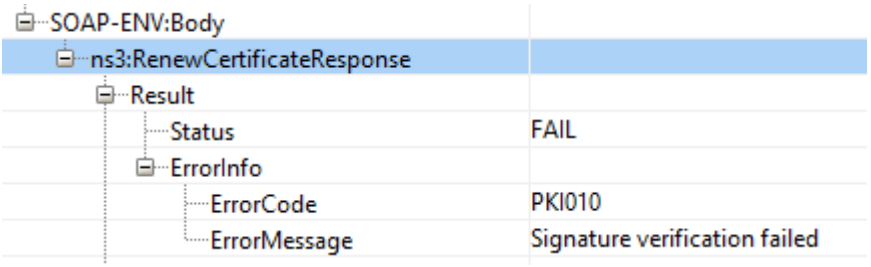
Uuden varmenteen pyynnössä TransferId on virheellinen



Varmenteen noudossa RetrievalId on virheellinen



Varmenteen uusimisen allekirjoitus on virheellinen

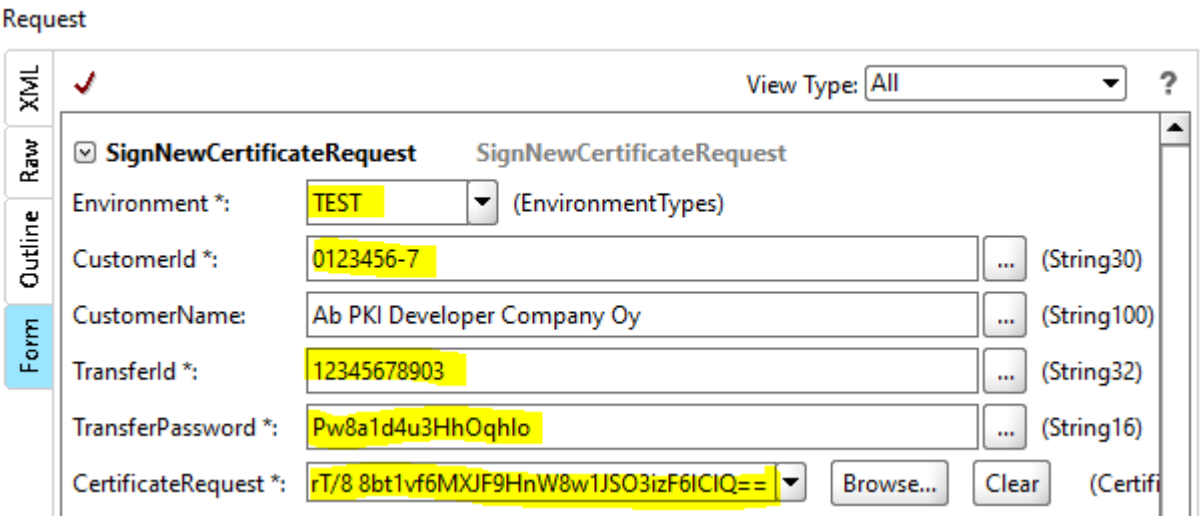


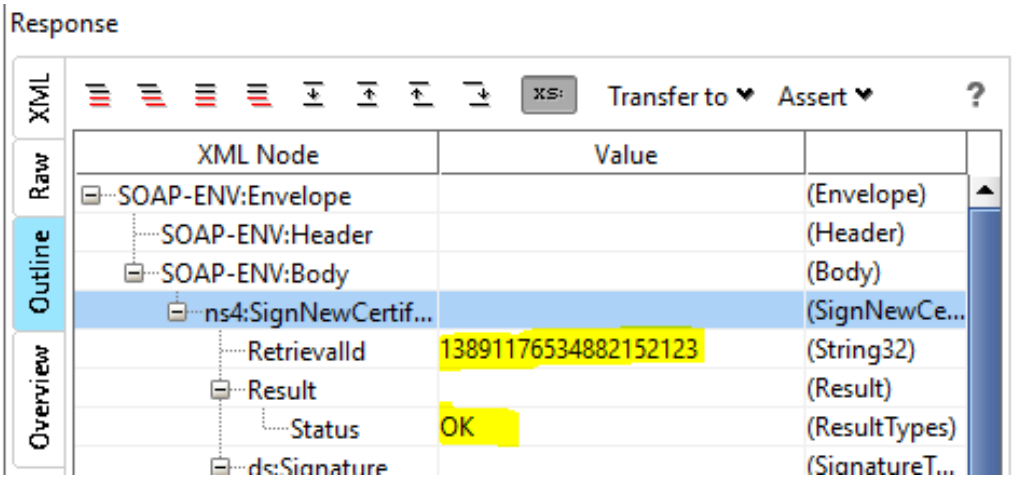
4 ESIMERKKISANOMIA

Seuraaviin esimerkkeihin on käytetty SmartBear Software ReadyAPI -ohjelmaa.

Uusi varmenteen allekirjoituspyyntö (signNewCertificate)

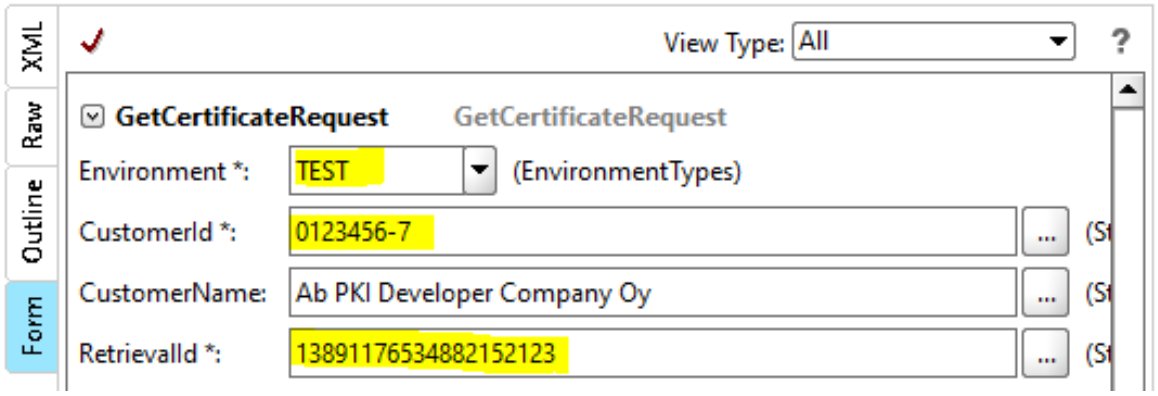
Jos varmenteen allekirjoituspyynnön (CertificateRequest) luonnissa käytetty ohjelma lisää CSR-tiedostoon alku- ja lopputunnisteet (BEGIN ja END), käyttäjän pitää poistaa ne. Vain base64-koodattu osa lähetetään:
-----BEGIN CERTIFICATE REQUEST-----
…. base64-koodattu varmennepyyntö ….
-----END CERTIFICATE REQUEST-----



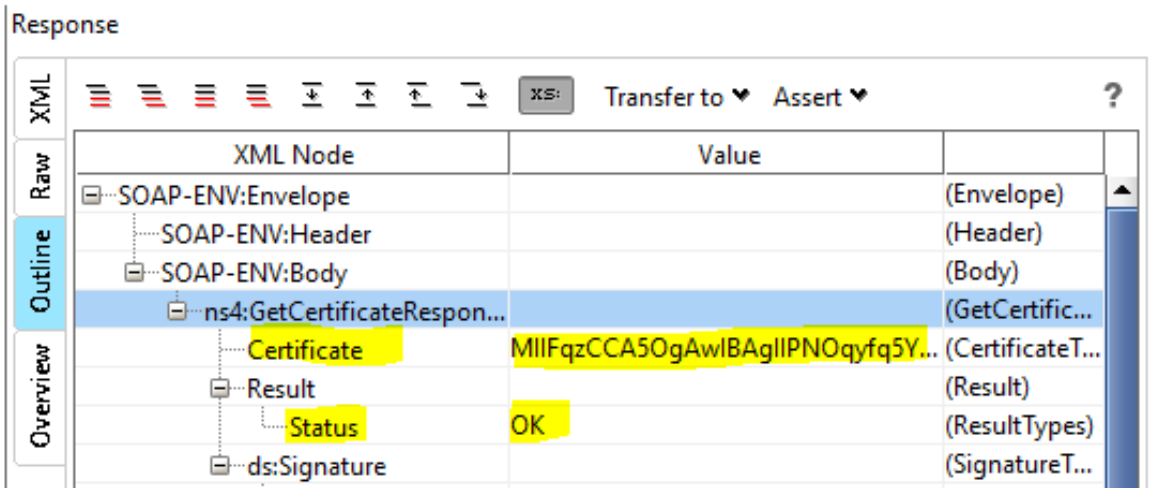


Varmenteen nouto (getCertificate)

Request



Response

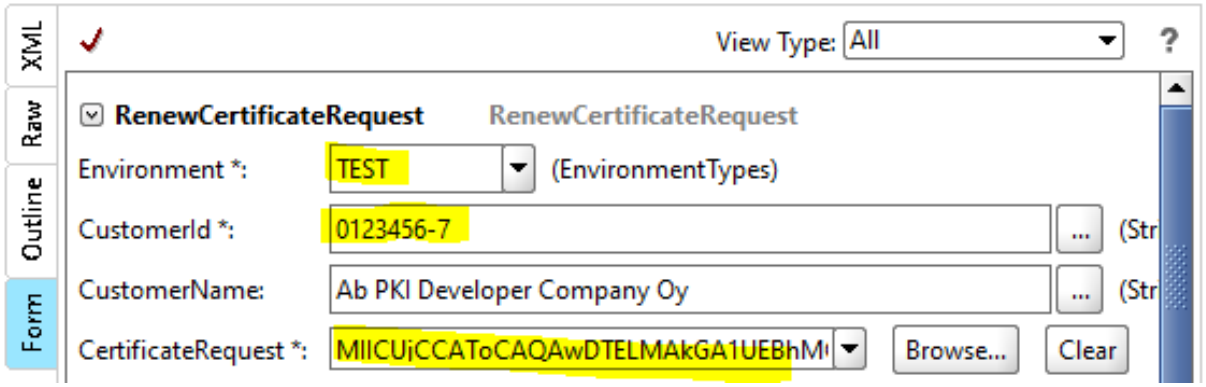


Mikäli käyttäjä tallettaa vastauksena saadun varmenteen tiedostoon, siihen voi joutua lisäämään varmenteen alku- ja lopputunnisteen (BEGIN ja END):
-----BEGIN CERTIFICATE-----
…. base64-koodattu varmenne…
-----END CERTIFICATE-----

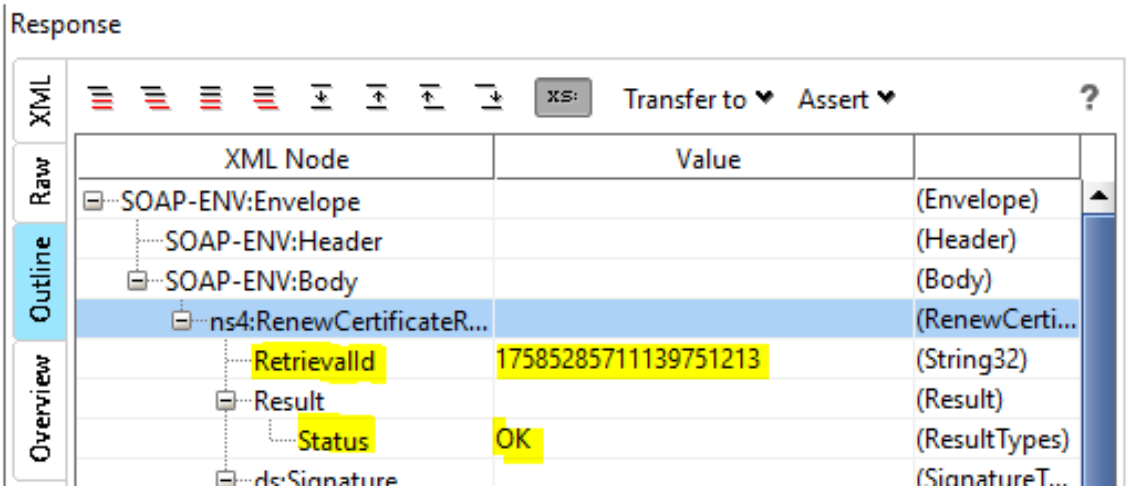
Jotkut ohjelmat ja käyttöjärjestelmät vaativat tunnisteet, että osaavat avata varmenteen.

Varmenteen uusiminen (renewCertificate)

Request



Response



5 ESIMERKKI CSR:N LUOMISESTA OPENSSL-OHJELMALLA

Varmennepyynnön luomisen kaksi vaihetta:

1. Luo 2048 bitin yksityinen avain tai käytä esivalmistelun avainta.
2. Luo pyyntö yksityisellä avaimella.

Yksityisen 2048-bitin RSA-avaimen luonti tiedostoon *yksityisavain*

```
openssl genrsa -out yksityisavain 2048
```

Avain-tiedostoa käytetään varmennepyynnön luomiseen

```
openssl req -new -key yksityisavain -out annavarmenne.csr
```

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:FI
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) [Internet Widgits Pty Ltd]:.
Organizational Unit Name (eg, section) []:.
Common Name (e.g. server FQDN or YOUR name) []:.
Email Address []:.

HUOM. CSR-luonti ei yleensä onnistu, jos kaikki kentät jäävät tyhjiksi. Tämän takia Country Name -kenttään täytetään FI.

Varmennepyynnön tarkastus ”`openssl req -text -noout -verify -in annavarmenne.csr`”

```
verify OK
Certificate Request:
   Data:
      Version: 1 (0x0)
      Subject: C = FI
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
               00:bb:e0:d2:5a:a7:ed:30:1c:fb:43:26:eb:ef:21:
               ……..
               12:a5
            Exponent: 65537 (0x10001)
      Attributes:
         a0:00
   Signature Algorithm: sha256WithRSAEncryption
      9c:e6:6f:c3:bf:9b:c2:e4:43:4f:9e:26:13:25:f6:6a:2d:57:
                        ……..
      14:59:5d:34
```