Certifikattjänsten - testbädd

Anläggningsprojekt för ett nationellt inkomstregister

INNEHÅLL

Version	Datum	Beskrivning
1.0	30.4.2018	Dokumentet har publicerats.
1.01	9.7.2020	Hämtningskoderna i kapitel 2.1 har ändrats.
1.02	18.9.2020	Ett stycke om testcertifikat har lagts till i kapitel 2. Exempelbilderna i kapitel 4 har ändrats.

1 INLEDNING

Syftet med testbädden för certifikattjänsten är att underlätta utvecklingen av en applikation som använder certifikattjänstens gränssnitt. I testbädden kan man testa sändningen av en signaturbegäran för certifikatet, sändningen av en begäran om förnyande av ett certifikat och hämtningen av ett certifikat.

I testbädden används på förhand specificerade engångsidentifierare, PKI-nycklar och certifikat. På grund av detta kan Web Service-begäran upprepas flera gånger med samma parametrar. Till exempel överföringskoden (TransferId) för ”Signaturbegäran för ett nytt certifikat” och ”engångslösenord” (TransferPassword) kan användas flera gånger.

Certifikat från testbädden kan inte användas i inkomstregistrets gränssnitt.

2 TESTMATERIAL

Testbädden har en stående certifikatbeställning samt två förberedda certifikat för ”Certifikatbegäran” och ”Förnyelse av certifikatet ”. Detta dokument innehåller anvisningar för användningen av testbädden. Användaren behöver även testnycklarna som publicerats för testningen (PKI privat nyckel). Dessa testnycklar har publicerats på webbplatsen för inkomstregistrets certifikattjänst: https://www.vero.fi/globalassets/tulorekisteri/varmennepalvelu-testipenkki.zip

Zip-paketet innehåller följande filer:

- SignNewCertificate_Private.key
    - Denna privata nyckel är avsedd för skapande av en signaturbegäran för ett nytt certifikat (CSR, signNewCertificate) och en XML-signatur för SOAP-meddelandet för förnyelsen av certifikatet (renewCertificate).
- RenewCertificate_Private.key
    - Denna privata nyckel är avsedd för skapande av en signaturbegäran för certifikatet (CSR) i samband med förnyelse av certifikatet (renewCertificate).

Testcertifikaten som anknyter till testnycklar förnyades i juli 2020 och de gäller fram till juli 2030. Samtidigt ändrades hämtningskoderna (RetrievalId) som behövs för hämtning av testcertifikat. De nya hämtningskoderna har listats i detta dokument.

2.1 Parametrar som används i testbäddens tjänster

I testbäddens Web Service-tjänster ska de på förhand definierade uppgifter som listas nedan användas.

1. Sändning av en signaturbegäran för ett nytt certifikat (signNewCertificate)

```
- Environment: TEST
- CustomerId: 0123456-7
- CustomerName: Ab PKI Developer Company Oy
- TransferID: 12345678903
- TransferPassword: Pw8a1d4u3HhOqhlo
- CertificateRequest: <en Base64-kodad teckensekvens i PKCS#10-format>
```

Skapandet av uppgiften CertificateRequest (CSR) ska ske med nyckeln 'SignNewCertificate_Private.key'. Då är det möjligt att förknippa det certifikat som tjänsten returnerar till samma privata nyckel. Man

kan skapa CSR även med en nyckel som man själv har skapat, men då kan det returnerade certifikatet inte förknippas med användarens nyckel.

2. Sändning av en signaturbegäran för förnyelse av ett giltigt certifikat (renewCertificate)

- `Environment: TEST`
- `CustomerId: 0123456-7`
- `CustomerName: Ab PKI Developer Company Oy`
- `CertificateRequest: <en Base64-kodad teckensekvens i PKCS#10-format>`
- `Signature: <element som motsvarar XML Signature>`

Skapandet av uppgiften CertificateRequest (CSR) ska ske med nyckeln 'RenewCertificate_Private.key'. Då är det möjligt att förknippa det certifikat som tjänsten returnerar till den privata nyckel som används i detta sammanhang. Också i detta fall är det möjligt att skapa CSR med en nyckel som man själv har skapat, men då kan den inte förknippas med användarens nyckel.

Elementet Signature ska skapas med nyckeln 'SignNewCertificate_Private.key'. Ett certifikat som returnerats från certifikattjänstens testbädd med hämtningsnyckeln (RetrievalId) 990639930742461205 ska fogas till Signature-elementets uppgift X509Certificate (se punkt 3. Hämtning av certifikat).

3. Hämtning av certifikat (getCertificate)

- `Environment: TEST`
- `CustomerId: 0123456-7`
- `CustomerName: Ab PKI Developer Company Oy`
- `RetrievalId: <Svar till begäran om ett nytt certifikat>`

Två förberedda certifikat kan hämtas genom hämtning av certifikat. Vid hämtning av ett certifikat som ”skapats” med den privata nyckel som använts vid testbäddens operation signNewCertificate ska hämtningskoden (RetrievalId) 990639930742461205 användas. Vill man hämta ett certifikat som förknippas med en privat nyckel som använts vid operationen renewCertificate, ska hämtningskoden 11885819811430372306 användas.

Testbädden har inget certifikat för förnyelse av ett förnyat certifikat (dvs. ett certifikat från operationen renewCertificate), utan testbädden returnerar alltid samma förberedda certifikat som respons till ”Förnyelse av ett giltigt certifikat”.

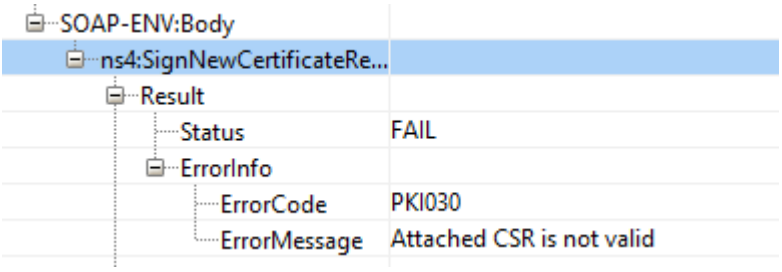
2.2 Testbäddens kontaktadress

Certifikattjänstens testbädd finns i certifikattjänstens testmiljö. Testbäddens adress avviker från adressen till den egentliga testmiljön på /DEV-sekvensen av tjänstens kontext. Hela adressen är: https://pkiws-testi.vero.fi/DEV/2017/10/CertificateServices

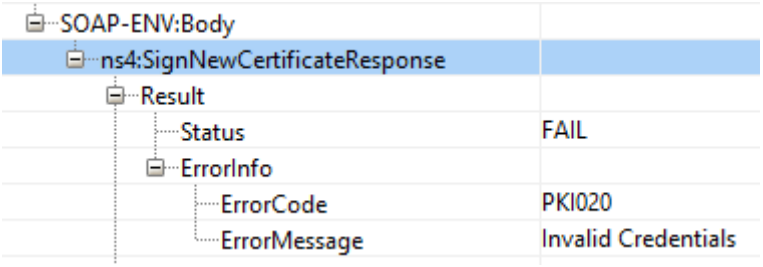
3 FELSITUATIONER HOS TESTBÄDDENS TJÄNSTER

Testbäddens felhantering motsvarar på grund av dess begränsade certifikat och deras livscykel inte helt produktionen. De vanligaste felsituationerna presenteras i detta kapitel. En omfattande förteckning över tjänstens felkoder finns i dokumentationen för certifikattjänsten.

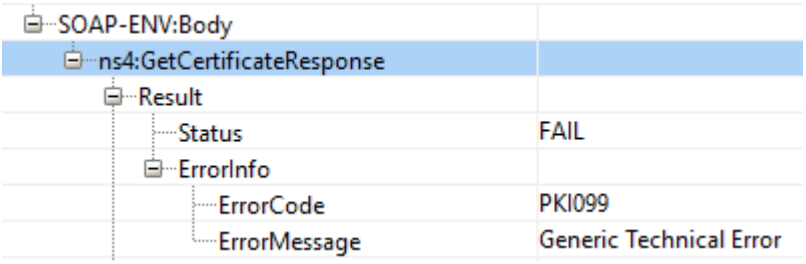
Felaktig CSR i begäran om ett nytt certifikat



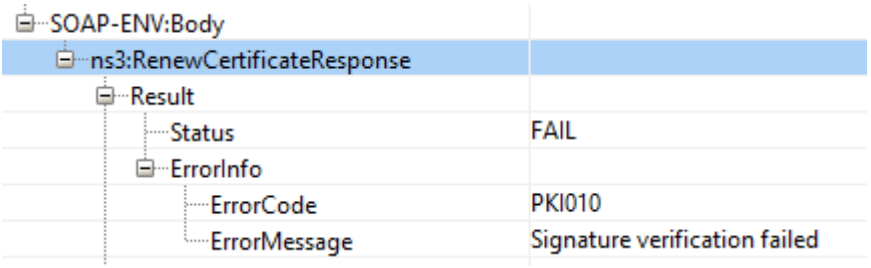
Felaktig TransferId i begäran om ett nytt certifikat



Felaktig RetrievalId vid hämtning av certifikatet



Felaktig signatur för förnyelse av ett certifikat

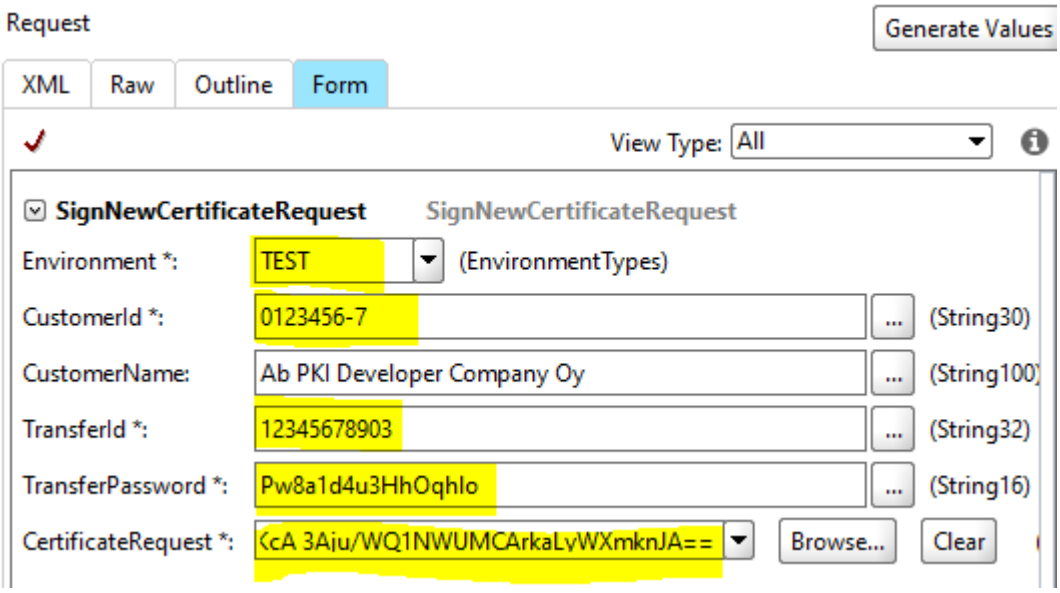


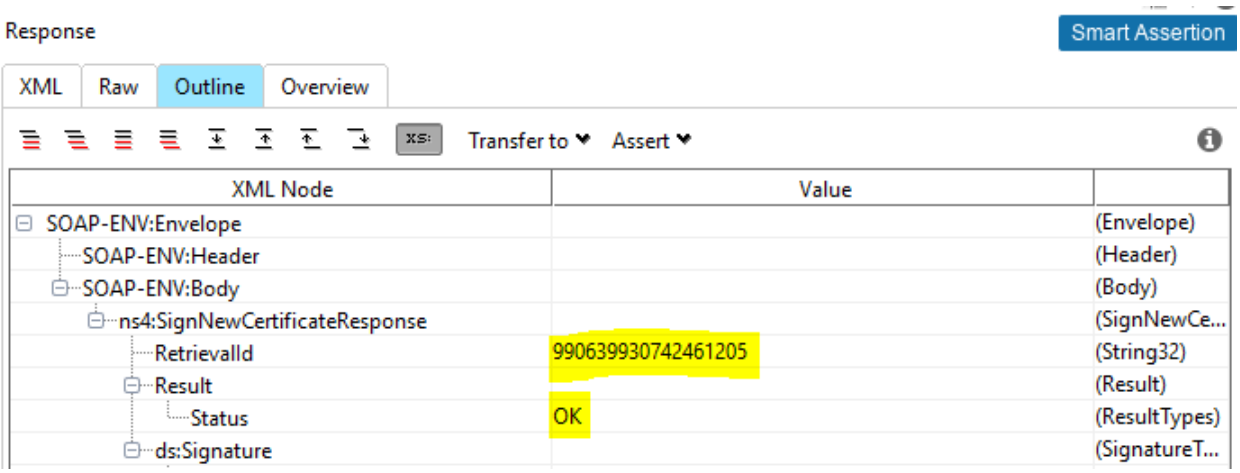
4 EXEMPEL PÅ MEDDELANDEN

I följande exempel har man använt programmet SmartBear Software ReadyAPI.

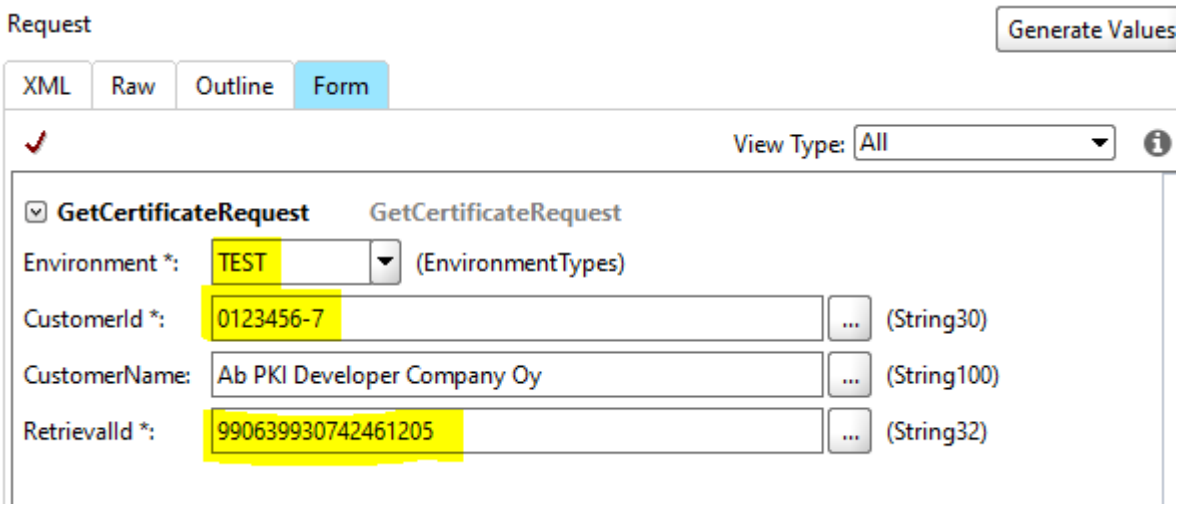
Signaturbegäran för ett nytt certifikat (signNewCertificate)

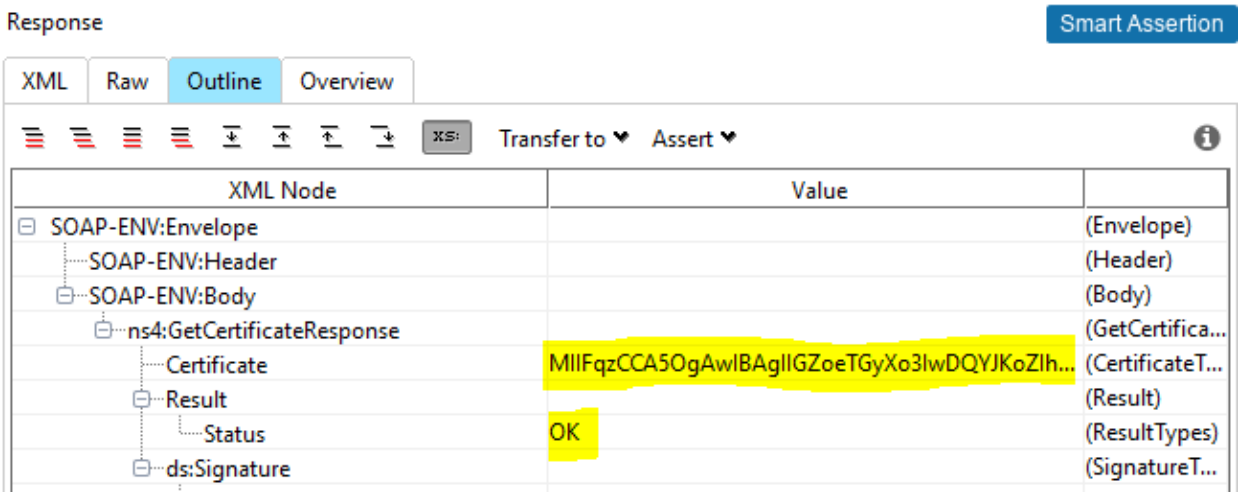
Om programmet med vilket en signaturbegäran för certifikatet (CertificateRequest) har skapats lägger till identifierare (BEGIN och END) på CSR-filen, ska användaren radera dem. Endast den base64-kodade sekvensen sänds:
-----BEGIN CERTIFICATE REQUEST-----
…. base64-kodad certifikatbegäran….
-----END CERTIFICATE REQUEST-----





Hämtning av certifikat (getCertificate)

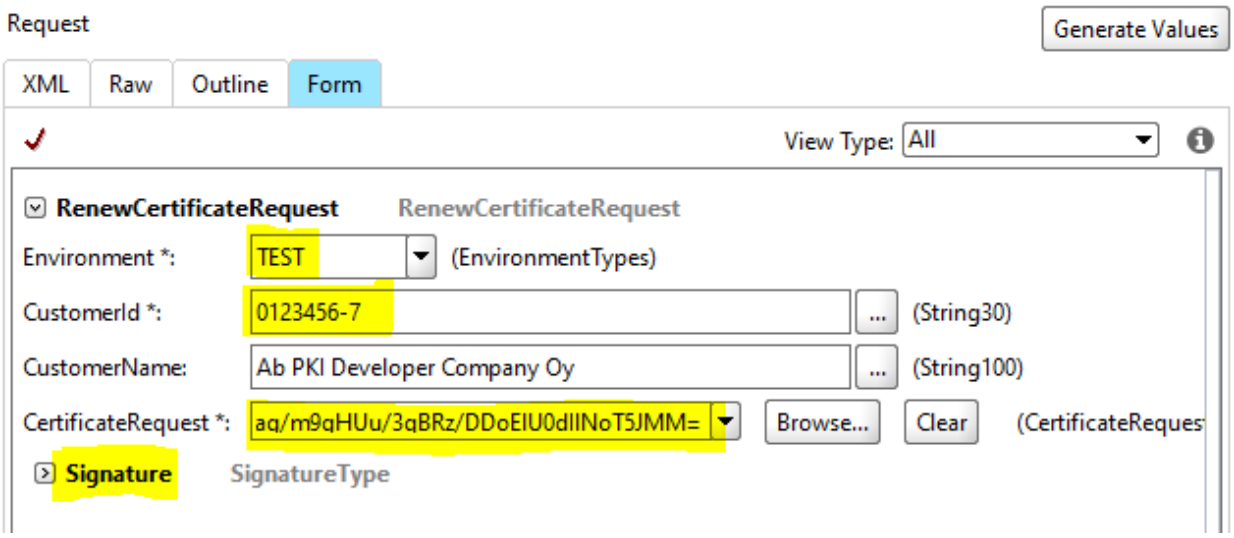


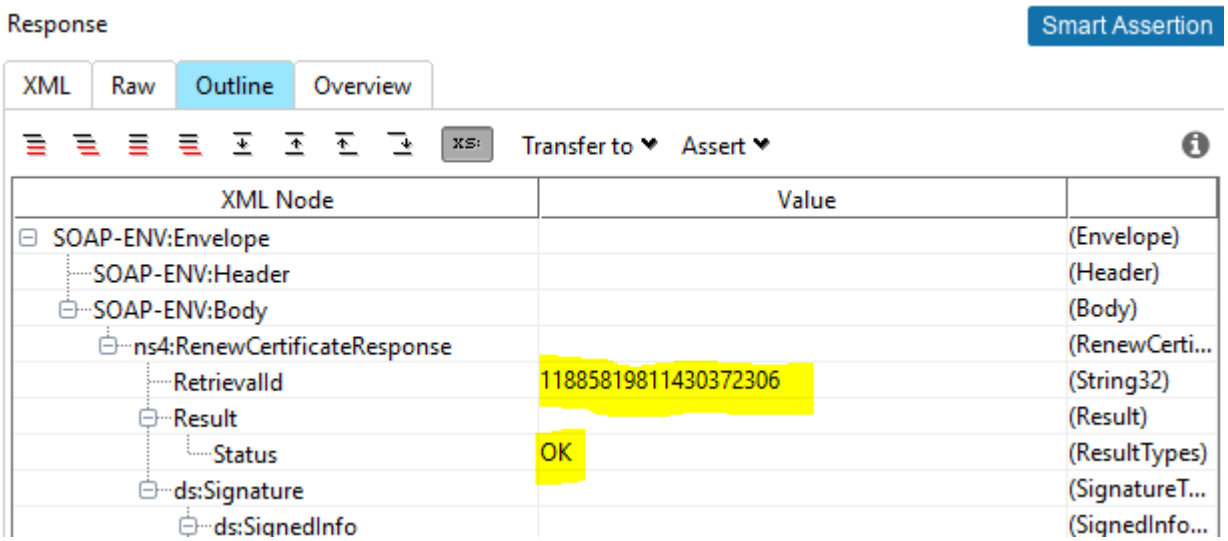


Om användaren sparar det certifikat som returnerats som respons till filen, kan hen bli tvungen att lägga till identifierare (BEGIN och END) på certifikatet:
-----BEGIN CERTIFICATE-----
…. base64-kodat certifikat…
-----END CERTIFICATE-----

Vissa program och operativsystem kräver identifierare för att kunna öppna certifikatet.

Förnyande av ett certifikat (renewCertificate)





5 EXEMPEL OM SKAPANDE AV CSR MED PROGRAMMET OPENSSL

En certifikatbegäran skapas i två steg:

1. Skapa en 2048-bits privat nyckel eller använd den förberedda nyckeln.
2. Skapa en begäran med den privata nyckeln.

Skapande av en privat 2048-bits RSA-nyckel till filen *privat nyckel*

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

Filen Nyckel används för skapande av en begäran om certifikat

```
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 []:.

OBS! Det brukar inte gå att skapa CSR om alla fält är tomma. Därför ska man fylla i FI i fältet Country Name.

Kontroll av certifikatbegäran ”`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
```