Certificate service - test bench

Project to establish the National Incomes Register

CONTENTS

Version history

Version	Date	Description
1.0	30/4/2018	Document published.
1.01	9/7/2020	Changed the retrieval IDs in Section 2.1.
1.02	18/9/2020	Added a paragraph on testing certificates to Section 2. Changed the example pictures in Section 4.

1 FOREWORD

The purpose of the certificate service test bench is to facilitate the development of the application that uses the certificate service interface. The test bench can be used to test the sending of certificate signing requests and certificate renewal requests and the retrieval of certificates.

The test bench uses pre-defined, single-use identifiers, PKI keys and certificates. This enables repeating Web Service requests multiple times with the same parameters. For example, you can use the ”New certificate signing request” transfer identifier (TransferId) and ”one-time password” (TransferPassword) multiple times.

The certificates obtained from the test bench cannot be used in the Incomes Register's interfaces.

2 TEST MATERIALS

The test bench has a permanently valid certificate subscription and two prepared certificates for ”Certificate request” and ”Certificate renewal”. This document contains the instructions for using the test bench. In addition, users will require test keys published for testing (PKI private keys).
The test keys have been published on the Incomes Register's certificate service site:
https://www.vero.fi/globalassets/tulorekisteri/varmennepalvelu-testipenkki.zip

The ZIP archive contains the following files:

- SignNewCertificate_Private.key
  - This private key is intended for creating new certificate signing requests (CSR, signNewCertificate operation) and generating the XML signature for the certificate renewal SOAP message (renewCertificate operation).
- RenewCertificate_Private.key
  - This private key is intended for the creation of the certificate signing request (CSR) in connection with certificate renewal (renewCertificate operation).

The testing certificates related to test keys were renewed in July 2020 and they will be valid up until July 2030. The retrieval IDs (RetrievalId) needed to retrieve the testing certificates were changed at the same time. The new IDs are listed in this document.

2.1 Parameters used in the test bench services

The predefined data listed below must be used in the test bench's Web Service services.

1. Sending a new certificate signing request (signNewCertificate)

```
- Environment: TEST
- CustomerId: 0123456-7
- CustomerName: Ab PKI Developer Company Oy
- TransferID: 12345678903
- TransferPassword: Pw8a1d4u3HhOqhlo
- CertificateRequest: <Base64-encoded character string in PKCS#10 format>
```

The CertificateRequest (CSR) data item must be generated with the 'SignNewCertificate_Private.key' key. This enables linking the certificate returned by the service with the above-mentioned private key. The CSR can also be executed with a self-generated key, but the returned certificate cannot then be linked to the user's key.

2. Sending a signing request for the renewal of a valid certificate (renewCertificate)

- `Environment: TEST`
- `CustomerId: 0123456-7`
- `CustomerName: Ab PKI Developer Company Oy`
- `CertificateRequest: <Base64-encoded character string in PKCS#10 format>`
- `Signature: <element corresponding to the XML Signature>`

The CertificateRequest (CSR) data item must be generated with the 'RenewCertificate_Private.key' key. The certificate returned by the service can then be linked to the private key used in this connection. In this case too, the CSR can be executed with a self-generated key, but cannot then be linked to the user's key.

The signature element must be generated with the 'SignNewCertificate_Private.key' key. The certificate obtained from the certificate service's test bench with the retrieval key (RetrievalId) 990639930742461205 must be attached to the signature element's X509Certificate data item (see section 3. Certificate retrieval).

3. Certificate retrieval (getCertificate)

- `Environment: TEST`
- `CustomerId: 0123456-7`
- `CustomerName: Ab PKI Developer Company Oy`
- `RetrievalId: <Reply received for the new certificate request>`

The certificate retrieval operation can be used to retrieve two prepared certificates. When retrieving a certificate “generated” with the private key used in the signNewCertificate operation, you must use the retrieval ID (RetrievalId) 990639930742461205. If you want to retrieve the certificate linked to the private key used in the renewCertificate operation, use retrieval ID 11885819811430372306.

The test bench does not contain a certificate for renewing a renewed certificate (a certificate obtained from the renewCertificate operation). Rather, the test bench will always return the same prepared certificate for ”Renewal of a valid certificate”.

2.2 Test bench contact address

The certificate service's test bench is connected to the certificate service test environment. Its address differs from that of the actual test environment by adding /DEV to the service context. The complete address is:
https://pkiws-testi.vero.fi/DEV/2017/10/CertificateServices

3 ERRORS IN TEST BENCH SERVICES

Due to the limited certificates used in the test bench and their limited lifecycles, error processing does not fully correspond to the production environment. The most typical errors are presented in this section. A comprehensive list of the service's error codes can be found in the certificate service documentation.

Incorrect CSR in a new certificate request

SOAP-ENV:Body	
ns4:SignNewCertificateRe...	
Result	
Status	FAIL
ErrorInfo	
ErrorCode	PKI030
ErrorMessage	Attached CSR is not valid

Incorrect TransferId in a new certificate request

SOAP-ENV:Body	
ns4:SignNewCertificateResponse	
Result	
Status	FAIL
ErrorInfo	
ErrorCode	PKI020
ErrorMessage	Invalid Credentials

Incorrect RetrievalId in certificate retrieval

SOAP-ENV:Body	
ns4:GetCertificateResponse	
Result	
Status	FAIL
ErrorInfo	
ErrorCode	PKI099
ErrorMessage	Generic Technical Error

Incorrect signature for certificate renewal

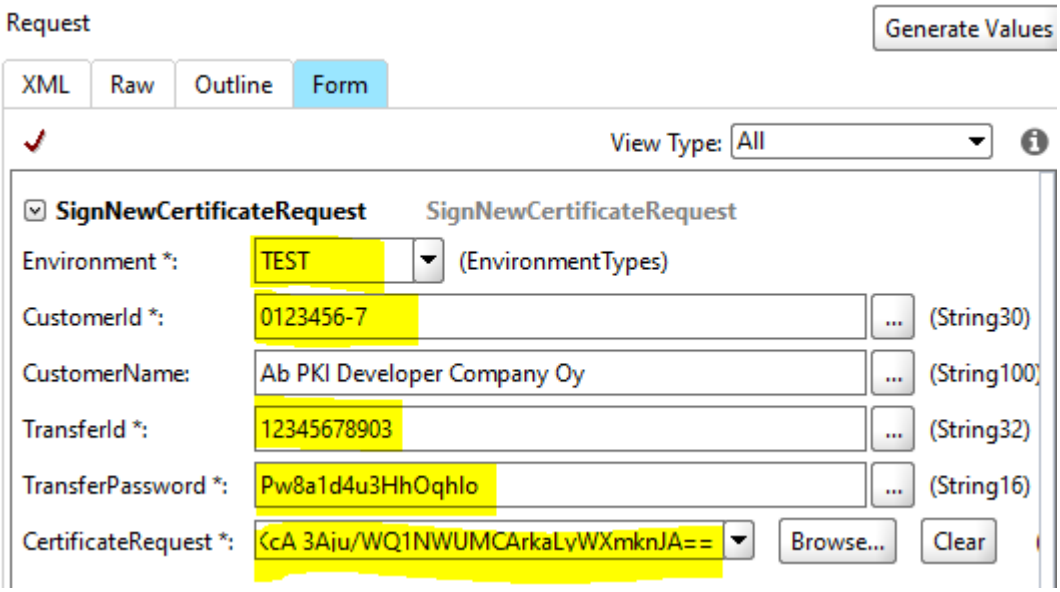
SOAP-ENV:Body	
ns3:RenewCertificateResponse	
Result	
Status	FAIL
ErrorInfo	
ErrorCode	PKI010
ErrorMessage	Signature verification failed

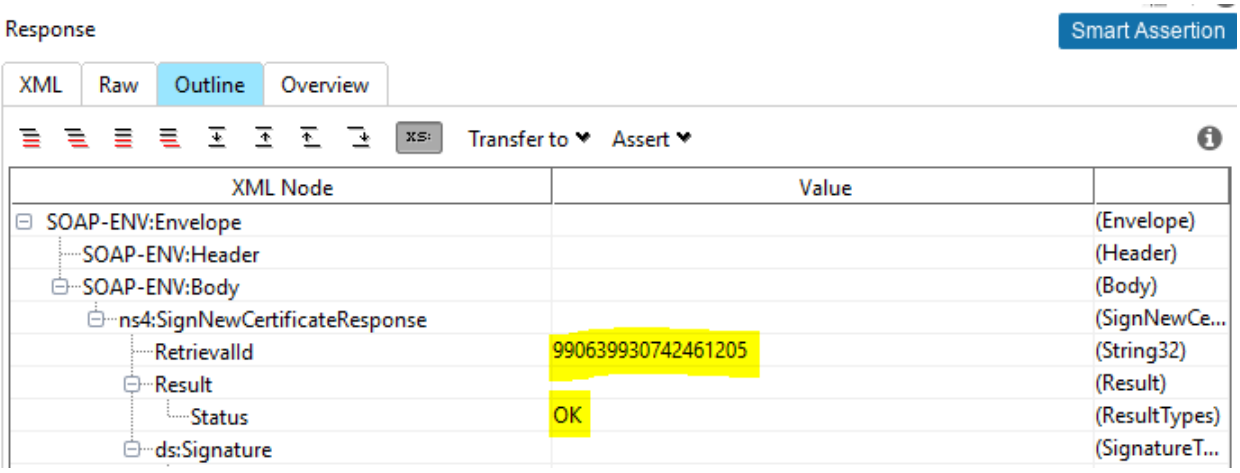
4 SAMPLE MESSAGES

SmartBear Software ReadyAPI was used in the following examples.

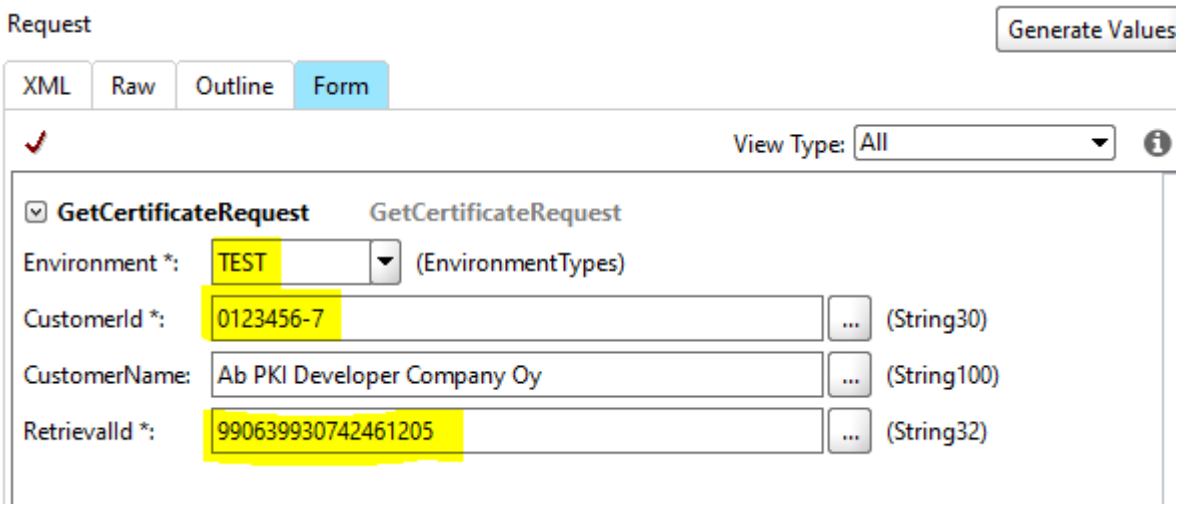
New certificate signing request (signNewCertificate)

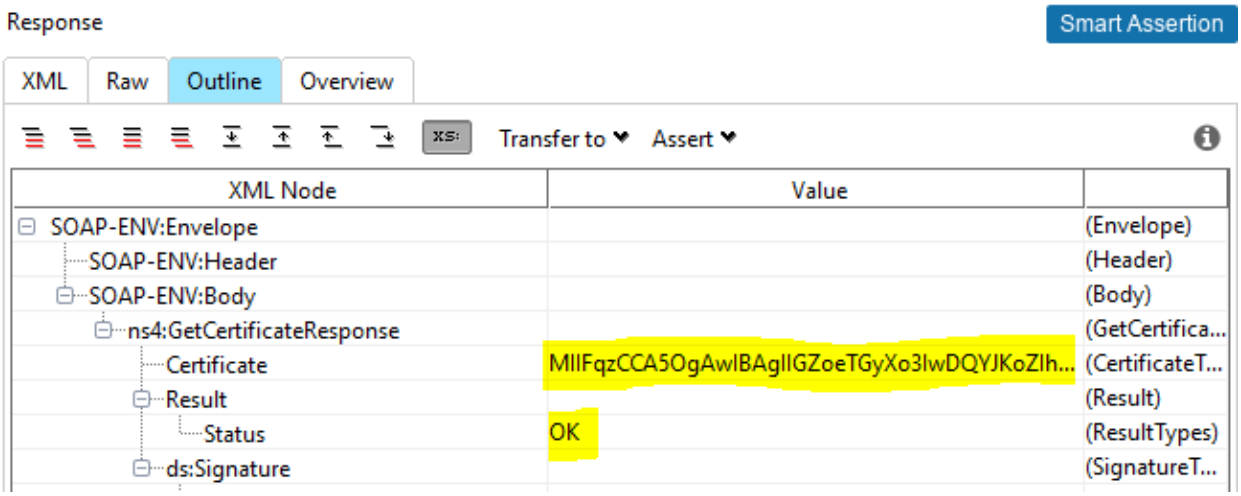
If the program used to create the certificate signing request (CertificateRequest) adds identifiers to the beginning and end (BEGIN and END) of the CSR file, the user must delete these. Only the base64-encoded part is sent:
-----BEGIN CERTIFICATE REQUEST-----
…. base64-encoded certificate request….
-----END CERTIFICATE REQUEST-----





Certificate retrieval (getCertificate)

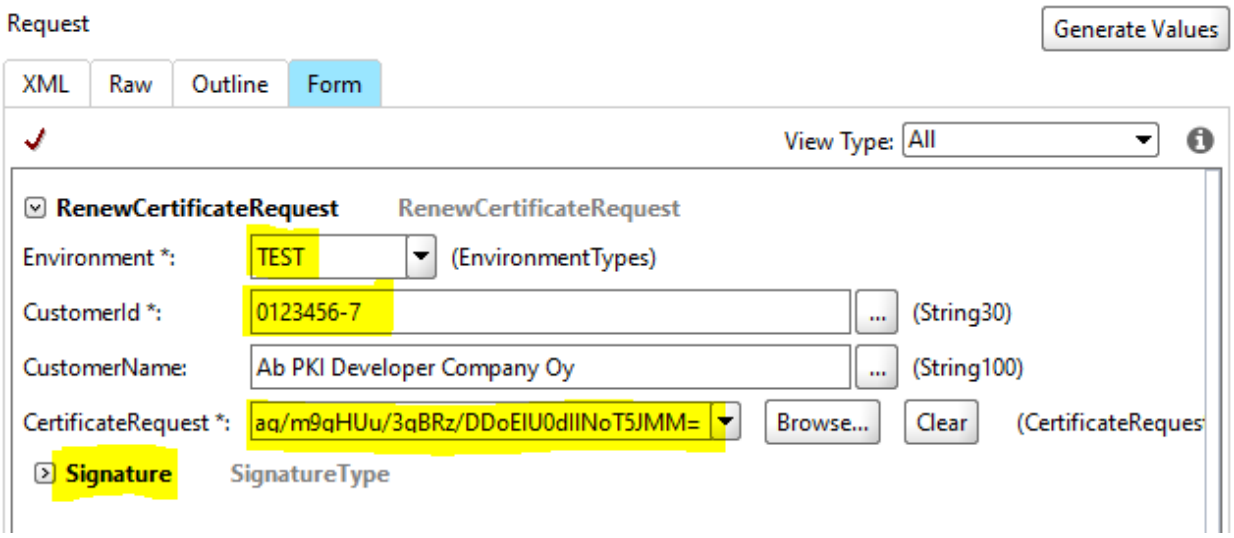


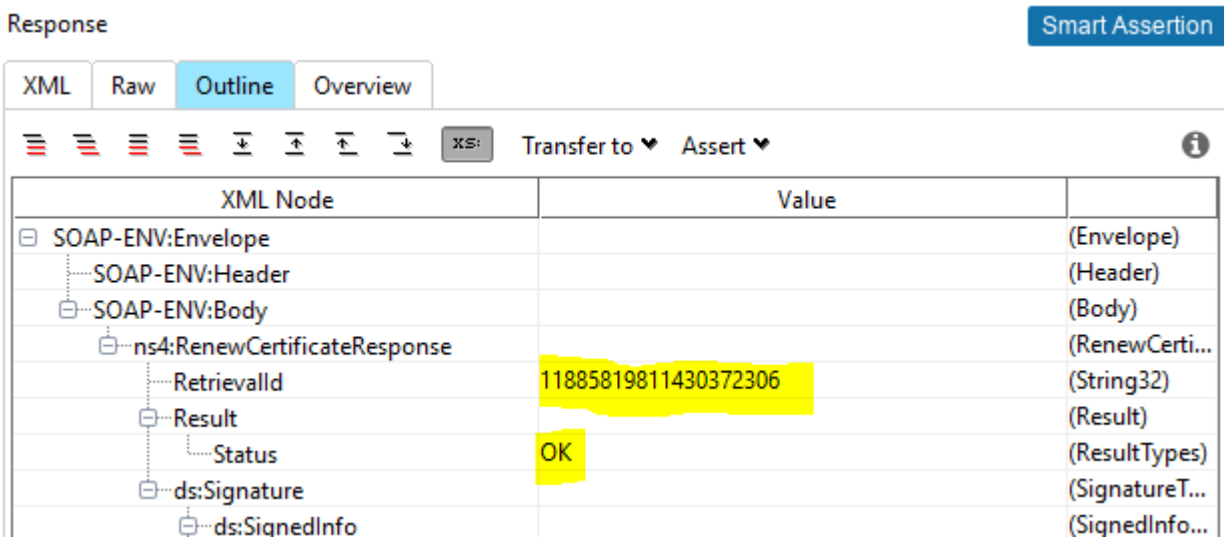


If the user saves the certificate received in response to a file, it may be necessary to add identifiers to the beginning and end of the certificate (BEGIN and END):
-----BEGIN CERTIFICATE-----
…. base64-encoded certificate…
-----END CERTIFICATE-----

Certain programs and operating systems require these identifiers for opening the certificate.

Renewing a certificate (renewCertificate)





5 EXAMPLE OF CSR CREATION WITH OPENSSL

The two stages of certificate request creation:

1. Create a 2048-bit private key or use the prepared key.
2. Create a request with the private key.

Creation of the 2048-bit RSA key into the file *private key*

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

The key file is used to create the certificate request

```
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 []:.

NOTE! CSR will normally fail if all fields are left blank. This is why you should enter FI in the Country Name field.

Certificate request verification ”`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
```