Version 1.0

Finnish Tax Administration’s certificate service – a description of the PKI system and APIs

The Finnish Tax Administration

Version history

Version	Date	Description
1.0	19.9.2024	New document published, describing the parts of the Finnish Tax Administration’s certificate service, the use of the service, API services and their data content. In addition, the document describes the test bench and presents examples to support use.

TABLE OF CONTENTS

1 GENERAL INFORMATION ABOUT THE FINNISH TAX ADMINISTRATION’S CERTIFICATE SERVICE

1.1 Parts of the certificate service and the use of the service

The Finnish Tax Administration’s certificate service consists of the background public key infrastructure (PKI) system and an e-service, which is the certificate service’s browser-based user interface for customers. Certificates of the Finnish Tax Administration’s certificate service are used by organisations that submit or retrieve records through technical interfaces or request data from systems using application programming interface (API) services. A certificate is issued for organisations that are responsible for submitting data or have the right to access data. The certificate service provides certificates for testing and production.

The Finnish Tax Administration issues certificates to customers for APIs of the Tax Administration, the Incomes Register and the positive credit register. This document describes the use of the system in general and only from the technical perspective. When you use APIs of different parties, always read the instructions of the party whose API you are using. For example, a data permission is required to use data of the Incomes Register or the positive credit register, and it must be requested directly from the party in question.

The Tax Administration’s certificates are based on a PKI solution. A customer has one or more key pairs (private and public key) and a certificate complying with the X.509 standard linked to the key pair. The certificate is used to identify the customer and sign the submitted records with an electronic signature (XML Signature).

Each customer manages their organisation’s API rights and certificates in the certificate service’s e-service. In the service, customers submit API applications, request certificates and maintain certificate data. Certificates are created and stored in the background PKI system. Certificates can either be retrieved in the e-service or through the PKI system’s API.

Log in to the e-service in the Finnish Tax Administration’s certificate service. The same pages provide instructions for submitting API applications and certificate subscriptions in testing and production situations. You can identify yourself in the service using online banking codes, a mobile certificate or a certificate card.

1.2 Intended uses and types of certificates

Certificates are always issued to a specific customer for a specific purpose, and they cannot be used for purposes other than the original. Customers must read the terms of use for API services of the Finnish Tax Administration and the Incomes Register and comply with them.

If a customer uses the Finnish Tax Administration’s technical interfaces for various purposes (including as a provider of earnings or benefits payment data and a user of Incomes Register data), separate certificates must be requested for each purpose. Similarly, separate certificates must be requested for each API. In other words, a single customer can have several certificates. If a customer uses several certificates in single software, special attention must be paid to the management of certificates.

APIs	Channel	Certificate authority
Provider of earnings payment data (Web Service)	Web Service (SOAP)	Data Providers Issuing CA
Provider of earnings payment data (SFTP)	SFTP	Data Providers SFTP Issuing CA
Provider of benefits payment data (WS)	Web Service (SOAP)	IR Benefit Data Providers Issuing CA
Provider of benefits payment data (SFTP)	SFTP	IR Benefit Data Providers SFTP Issuing CA
Data user (WS)	Web Service (SOAP)	IR Income Data Users Issuing CA
Data user (SFTP)	SFTP	IR Income Data Users SFTP Issuing CA
Support services outside the Incomes Register	Web Service (SOAP)	IR External Data Providers Issuing CA
	SFTP	IR External Data Providers SFTP Issuing CA
Vero API	Web Service (REST)	Data Providers Issuing CA
APItamoPKI	Web Service (SOAP)	Data Providers Issuing CA
Credit data provider	Web Service (REST)	Data Providers Issuing CA
Credit data user	Web Service (REST)	PCR Credit Data Users Issuing CA v1

Table 1: Certificate types and authorities.

Certificates are created in accordance with the certificate authorities (CA) mentioned above, and corresponding packages can be downloaded on the certificate service’s pages under Documentation.

1.3 Requesting certificates

Certificates are always requested in the certificate service’s e-service. When placing their subscription, customers must name a technical contact person for certificates, after which the certificate service will send the information required to retrieve certificates to the contact person: the transfer ID (TransferId) and a one-time password (TransferPassword). They will be sent to the technical contact person by secure email, and the contact person will receive a PIN code as a text message to open the secure email message. The one-time password is valid for 14 days. If a certificate is not retrieved during this time, the one-time password will expire, and the customer must place a new certificate subscription.

The process of requesting a new certificate is presented in Figure 1. More detailed instructions for requesting a certificate in the e-service are available in the Finnish Tax Administration’s certificate service.

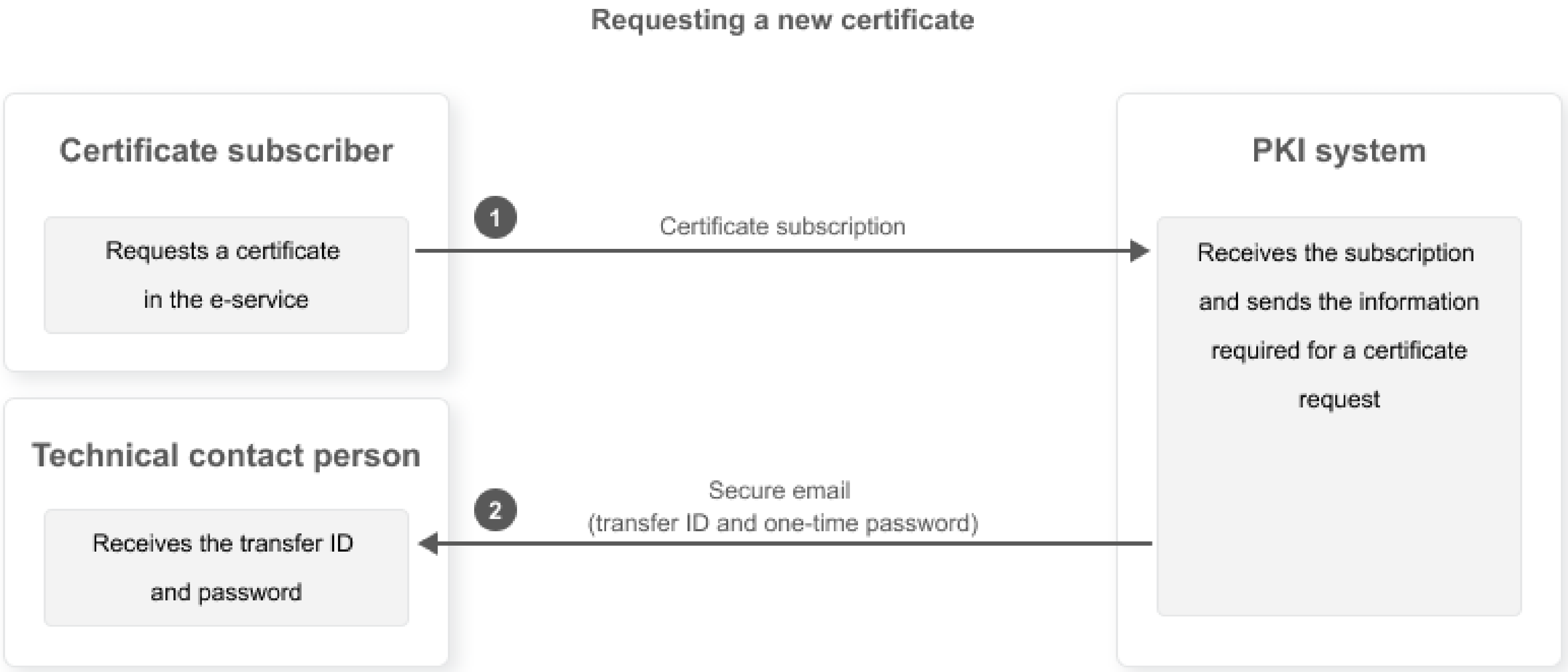

Requesting a new certificate
Certificate subscriber
Requests a certificate in the e-service
Technical contact person
Receives the transfer ID and password
PKI system
Receives the subscription and sends the information required for a certificate request
1
Certificate subscription
2
Secure email (transfer ID and one-time password)

Figure 1: Requesting a certificate.

1.4 Retrieving certificates

Certificates can be retrieved using an API or the e-service. Both options require the transfer ID, a one-time password and a certificate signing request (CSR). For a certificate request, the customer generates a 2,048-bit key pair using the RSA algorithm. In addition, the customer generates a certificate signing request, complying with the PKCS#10 specification, which includes the customer's public key.

When the certificate is retrieved using the e-service (Figure 2), the customer enters the transfer ID, password and the generated signing request in the user interface. The certificate is downloaded on a computer.

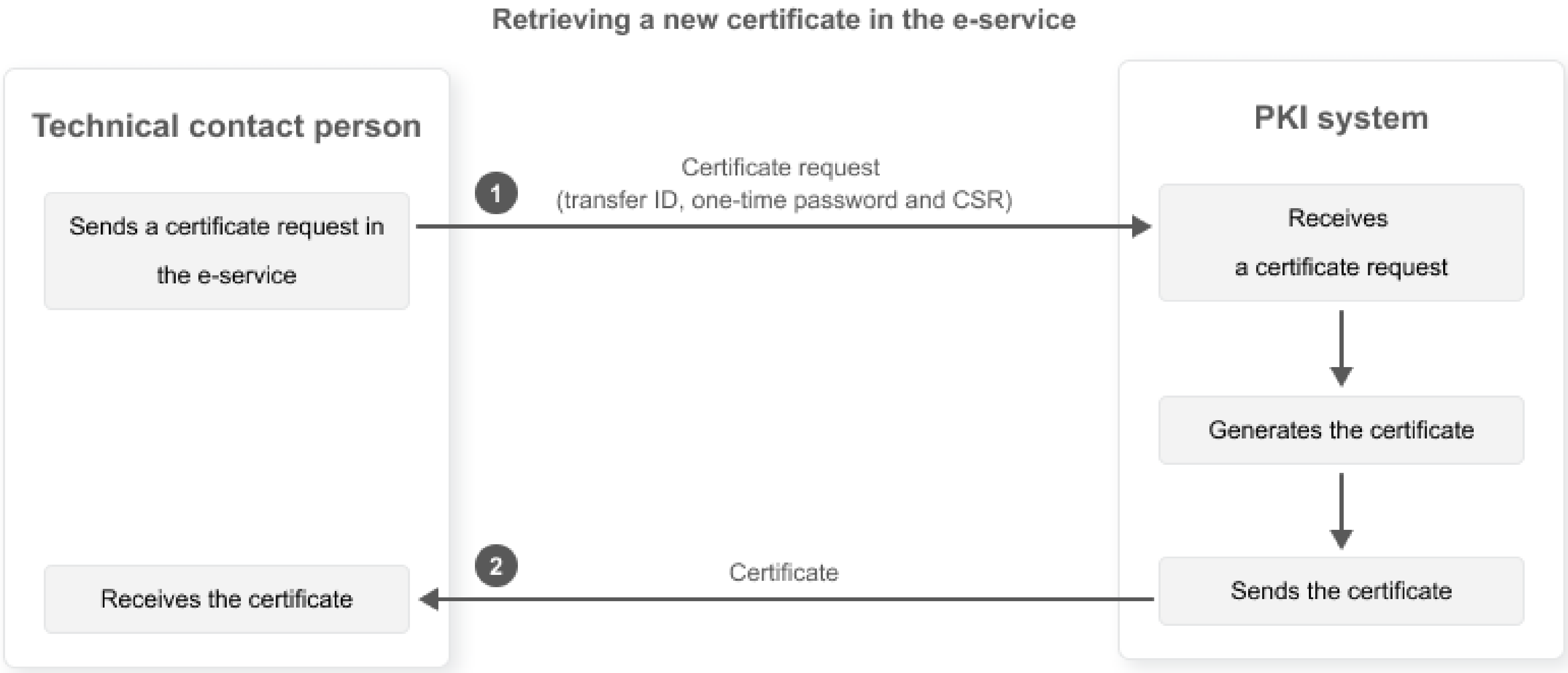

Retrieving a new certificate in the e-service
Technical contact person
Sends a certificate request in the e-service
Receives the certificate
1
Certificate request
(transfer ID, one-time password and CSR)
2
Certificate
PKI system
Receives a certificate request
Generates the certificate
Sends the certificate

Figure 2: Retrieving a certificate using the e-service.

When the certificate is retrieved using an API (Figure 3), the customer attaches the transfer ID, password and signing request to a service call for a new certificate request (SignNewCertificateRequest). The service call returns the retrieval ID (RetrievalID) to the customer through the acknowledgement of receipt. After receiving the retrieval ID, the customer has to wait for 10–30 seconds. After this, the customer creates a service call for retrieving the certificate (GetCertificateRequest) and attaches the retrieval ID to it. As a response to the service call, the customer receives the certificate. If the certificate cannot be generated due to an error, the retrieval service call will return an error message instead of the certificate.

Address of the production certificate API: https://pkiws.vero.fi/2017/10/CertificateServices

Address of the testing certificate API: https://pkiws-testi.vero.fi/2017/10/CertificateServices

Retrieving a new certificate through the PKI system’s API

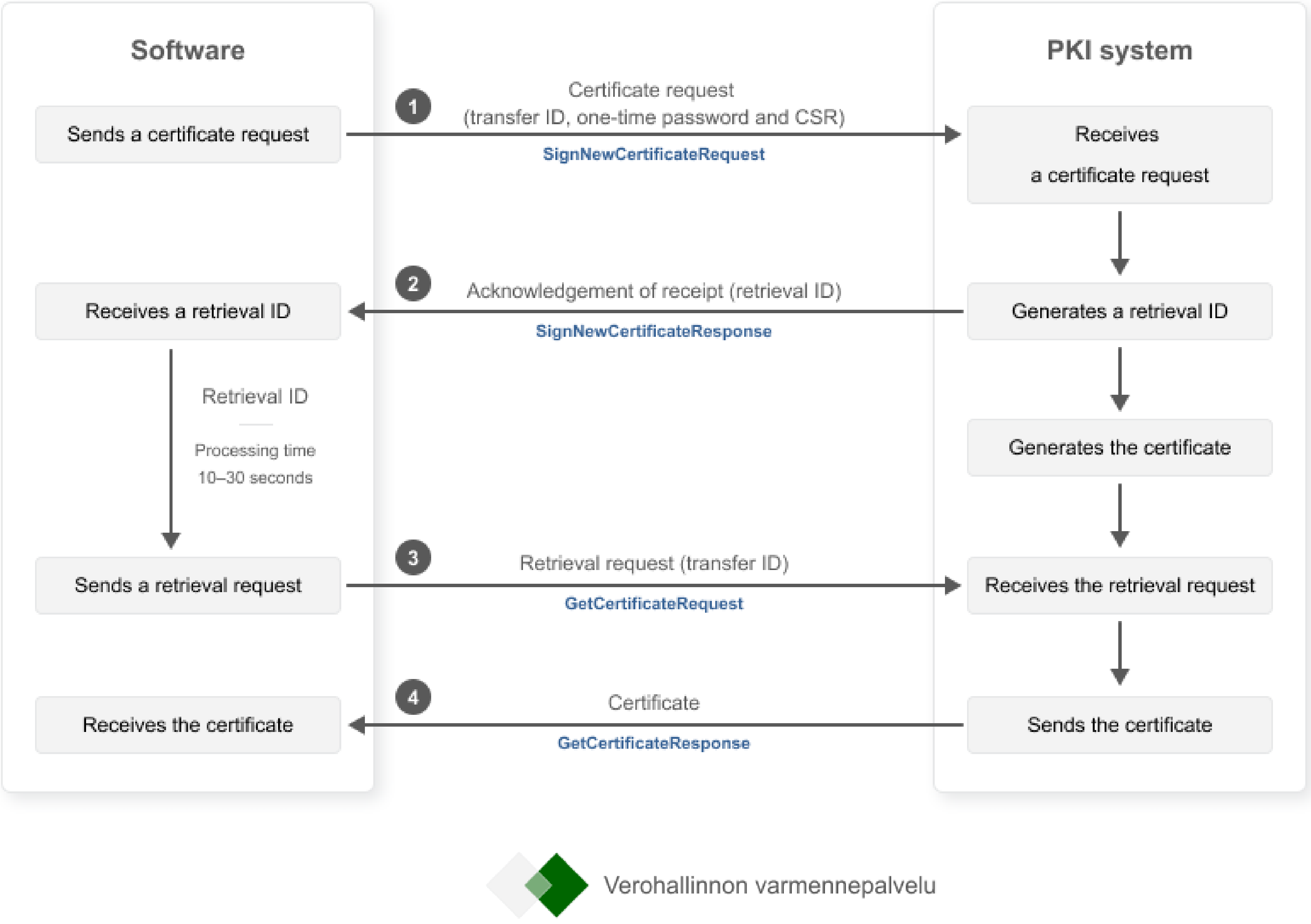

Software
PKI system
Sends a certificate request
1
Certificate request
(transfer ID, one-time password and CSR)
SignNewCertificateRequest
Receives
a certificate request
Receives a retrieval ID
2
Acknowledgement of receipt (retrieval ID)
SignNewCertificateResponse
Generates a retrieval ID
Retrieval ID
Processing time
10–30 seconds
Generates the certificate
Sends a retrieval request
3
Retrieval request (transfer ID)
GetCertificateRequest
Receives the retrieval request
Receives the certificate
4
Certificate
GetCertificateResponse
Sends the certificate
Verohallinnon varmennepalvelu

Figure 3: Retrieving a certificate using an API.

1.5 Revoking certificates

The customer must request a production certificate to be revoked if it is known or suspected that the certificate holder’s private key has been misplaced or ended up in the wrong hands. A certificate must also be revoked if it is no longer needed. The certificate issuer, i.e. the Finnish Tax Administration, can revoke a certificate when, for example, the agreement entitling to the use of the service ends or it is apparent that the issued certificate has been misused.

The customer can revoke a production certificate by contacting the Incomes Register’s customer service. Detailed instructions are available on the page Revoking certificates. The Incomes Register’s customer service is responsible for revoking production certificates of the Finnish Tax Administration, the Incomes Register and the positive credit register.

Production certificates can be requested to be revoked at any time. When a customer requests a certificate to be revoked outside office hours, the certificate will first be revoked temporarily (a temporary prohibition of use is issued). This means that the use of the certificate is prevented but the certificate can still be reactivated. If the customer confirms the revocation, the certificate will be revoked permanently. The customer must confirm the revocation or reactivate the certificate within 14 days of the issuance of the temporary prohibition of use. If the customer does not confirm the reactivation during this time, the Tax Administration will permanently revoke the certificate.

A permanently revoked certificate cannot be returned for use or renewed; the customer must request a new certificate. The customer must then submit a new API application in the certificate service’s e-service and retrieve it in the same way as when requesting a certificate for the first time.

Testing certificates can be revoked by completing the certificate service’s observation form.

1.6 Lifecycle and renewal of certificates

Customers’ production and testing certificates are valid for two years. If a certificate needs to be renewed, it must be renewed before it expires. Certificate holders must check the validity of their certificates regularly. The final validity date can be checked in the certificate service’s e-service or the certificate.

Certificates are renewed using the PKI system’s API. A certificate can be renewed at the earliest sixty (60) days before the end of their validity. The certificate remains valid until the end of the original validity period. If the certificate is renewed on time, a new certificate does not need to be requested, and the customer does not require a new transfer ID or one-time password.

The renewal of a certificate using an API is presented in Figure 4.

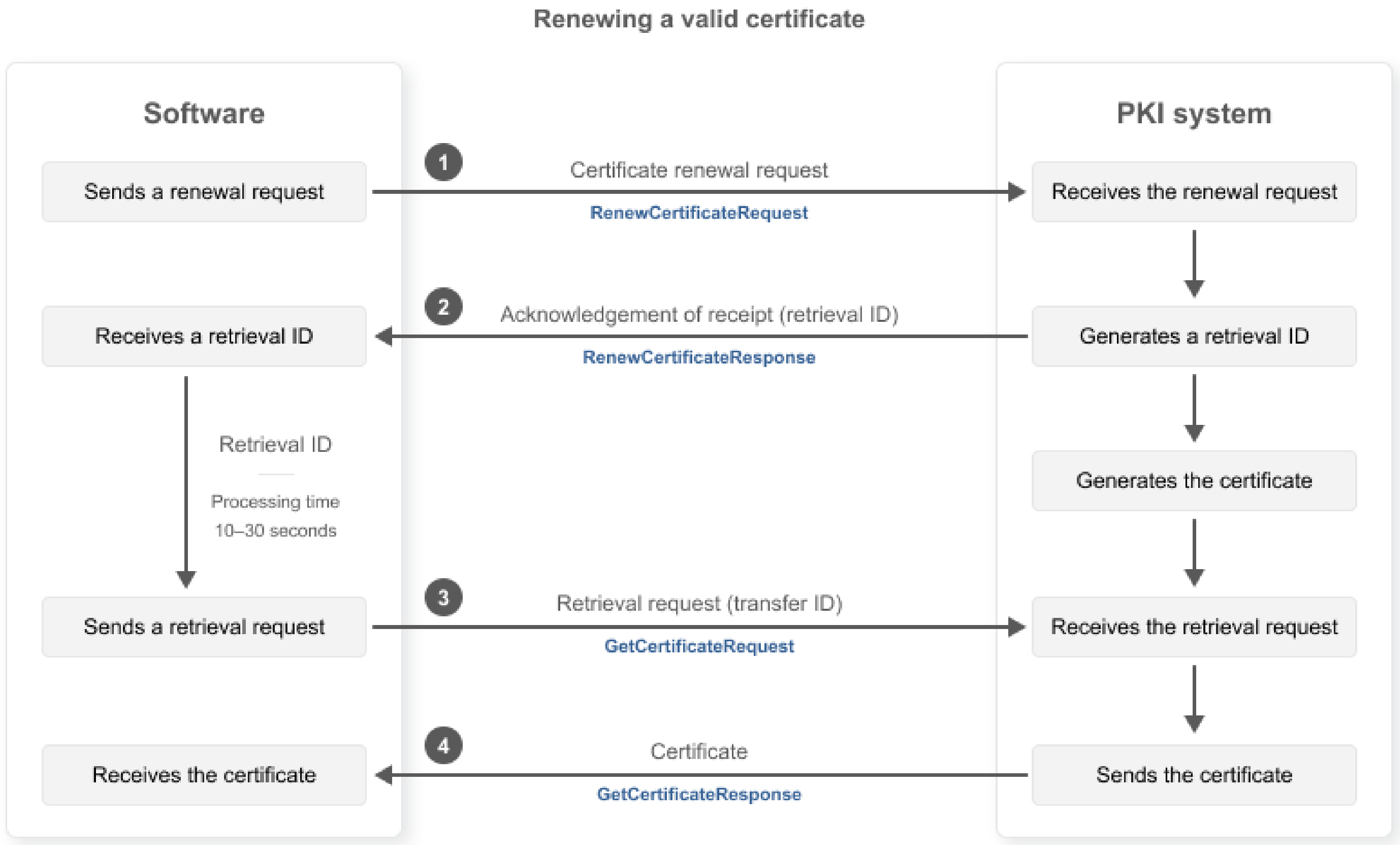


Figure 4: Renewing a certificate using an API.

The API includes a separate service for renewing certificates (RenewCertificate). For the renewal, the customer must generate a new key pair and a certificate signing request and sign the service call using a private key linked to the valid certificate.

The certificate is signed in the same format as when the customer submits records through APIs using a valid certificate. The request to renew a certificate returns the certificate retrieval ID to the customer through the acknowledgement of receipt. The customer retrieves the certificate similarly to a new certificate. This means that the customer has to wait for 10–30 seconds. After this, the customer creates a service call for retrieving the certificate (GetCertificateRequest) and attaches the retrieval ID to it. As a response to the service call, the customer receives the certificate.

Note: The previous certificate must be replaced by the new certificate immediately; however, no later than when the validity of the previous certificate ends. If a single certificate has been used in more than one location, all copies of the previous certificate must be replaced with the new one to avoid errors caused by an expired certificate.

If a certificate expires, the customer must request a new certificate in the e-service. In this case, the new certificate is requested and retrieved in the same way as when requesting a certificate for the first time.

2 TERMINOLOGY AND ABBREVIATIONS

The abbreviations and key terminology used in the certificate service.

Abbreviation or term	Description
CSR (Certificate Signing Request)	A certificate signing request placed by a certificate service user. The CSR is a Base64-encoded character string in PKCS#10 format.
Public key infrastructure (PKI)	Asymmetrical encryption, in which one encryption key is public and the other is private.
Retrieval ID (RetrievalID)	An ID that can later be used to retrieve a certificate.
PKCS#10 (Public Key Cryptography Standards # 10)	A standard that specifies the format and content of the certificate signing request.
PKI (Public Key Infrastructure)	A system utilising the public key method that the certificate authority uses to offer and maintain certificates.
Private key	The secret part of an asymmetric key pair used in public key encryption. Private keys are typically used for electronic signatures or the decryption of a message encrypted with a public key.
Public key	The public part of an asymmetric key pair. Public keys are typically used in the encryption of messages and the authentication of a signature generated with a private key.
Application programming interface (API)	A standard-compliant practice or connection point enabling data transfer between devices, software or the user.
RSA encryption	A public key infrastructure based on the encryption algorithm developed by Rivest, Shamir and Adleman.
SFTP (Secure File Transfer Protocol)	A file transfer protocol that allows an encrypted data transfer connection between two systems.
SGML (Standard Generalized Markup Language)	A markup language used to mark the different sections of a record and their interrelations.
Transfer ID (TransferID)	The ID delivered to the customer for requesting a certificate.
Certificate subscription	A subscription placed for a certificate in the e-service of the Finnish Tax Administration's certificate service.
Certificate request	A request message in the SignNewCertificate service of the API, with which the customer starts the retrieval of a previously requested certificate.
Certificate retrieval request	A request message in the GetCertificate service of the API, with which the customer retrieves a previously requested certificate.
Certificate renewal request	A request message in the RenewCertificate service of the API, with which the customer renews a valid certificate.
WS (Web Service)	Software running on a web server, offering services for applications through standardised Internet communication protocols. The services offered by the certificate service are certificate request, retrieval and renewal.
XML (Extensible Markup Language)	A markup language that is a subset of SGML, particularly designed for Internet use and easily extensible.

XML Signature	An XML signature generated by a customer using a valid certificate.
X.509	The standard defining the structure of the certificate.

Table 2: Terminology and abbreviations.

3 API NAMESPACES, CHARACTER SET AND READING INSTRUCTIONS

The implementation of the Web Service API for the PKI system of the Finnish Tax Administration’s certificate service is described below from the system integrator’s perspective. The document describes the API services and the data content of the services (XML schemas).

The technical implementation of the PKI system’s API is presented in such detail that the parties can specify and implement the integration of their own systems with the PKI system.

3.1 The PKI system’s Web Service API

API services are specified in the description **CertificateServices.wsdl**.

The namespaces used in the description are as follows:

File name	Prefix	Namespace
XMLSchema	xmlns:xs	http://www.w3.org/2001/XMLSchema
WSDL	xmlns:wsdl	http://schemas.xmlsoap.org/wsdl/
WSDL SOAP binding	xmlns:soap	http://schemas.xmlsoap.org/wsdl/soap/
CertificateServices.wsdl	xmlns:tns	http://certificates.vero.fi/2017/10/certificateservices

3.2 Schema

Elements in accordance with the XML schema **CertificateServices.xsd** are used in the lifecycle management of the certificates issued by the PKI system.

The namespaces used in the schema are as follows:

File name	Prefix	Namespace
XMLSchema	xmlns:xs	http://www.w3.org/2001/XMLSchema
CertificateServices.xsd	xmlns:ser	http://certificates.vero.fi/2017/10/certificateservices

Blank elements are not allowed in the messages. If an element has no value, the element will be left out from the message entirely. Furthermore, blank character strings are not allowed, i.e. the minimum length of all values is 1.

3.3 Character set

The schemas use UTF-8, which is the default character set of XML. The file must not contain the Byte Order Mark (BOM) character.

The following table presents the requirements for the conversion of special characters appearing in messages.

Character	Description	Presentation format as an entity
&	ampersand	&amp; conversion is mandatory
<	less than	&lt; conversion is mandatory
>	greater than	&gt; conversion is not mandatory, but conforms with best practices
'	apostrophe	&apos; conversion is not mandatory, but conforms with best practices
"	quotation mark	&quot; conversion is not mandatory, but conforms with best practices
--	double dash	This character must not appear in an XML file
/*	slash asterisk	This character must not appear in an XML file
&#	ampersand hash	This character must not appear in an XML file

3.4 Reading instructions for diagrams

The marking 0 .. ∞ in the bottom right-hand corner of an element in the document's diagrams means that the element may appear several times or not at all. The marking 1 .. ∞ means that the element may appear several times, but it must always appear at least once. The mandatory elements are highlighted with a solid border line and voluntary elements with a dashed border line.

In the document tables, the mandatory nature and the number of occurrences are depicted in the 'Element mandatoriness' column. The number of the elements is indicated in format A:B, where A is the minimum number of the elements in question that the message must contain (minOccurs), and B is the maximum number of the elements that the message may contain (maxOccurs). The values are as follows:

0 = element can be missing altogether

1 = element occurs once

N = N is a numerical value, and the element occurs N times

unbounded = element occurs a previously undefined number of times

4 API SERVICES AND ERROR PROCESSING

4.1 API services

See the table below for a description of the API services:

Operation	Request message	Response message	Description
Requesting a new certificate (SignNewCertificate)	SignNewCertificateRequestMessage	SignNewCertificateResponseMessage	A certificate request with which the customer starts the retrieval of a new certificate. Before the certificate request, the customer must request a new certificate in the e-service of the Finnish Tax Administration’s certificate service. The certificate request is used when • a customer is retrieving their organisation’s first certificate; • a customer already has a valid certificate or valid certificates, but their organisation requires more certificates; • a customer’s previous certificate has expired or has been revoked.
Renewing a valid certificate (RenewCertificate)	RenewCertificateRequestMessage	RenewCertificateResponseMessage	A certificate renewal request, when a user’s certificate is about to expire and the renewal is carried out before the currently valid certificate expires.
Retrieving a certificate (GetCertificate)	GetCertificateRequestMessage	GetCertificateResponseMessage	Retrieving a previously requested new or renewed certificate. There must be a delay of at least 10 seconds between the certificate request or the response message for the renewal of a valid certificate and the request message for retrieving a certificate.

The data content of API services and messages is described in Section 5.

4.2 Signing messages

Electronic signatures (XML Signature) are used in services of the Web Service API. They are used to verify the creator of the data content of the message for the messages defined in Section 5. A signature also guarantees the integrity of the message. Signatures are implemented using the XML Enveloped Signature mechanism; its processing rules and structure are described in the document XML Signature Syntax and Processing (http://www.w3.org/TR/xmldsig-core/). An example of an electronic signature is presented in Section 9 of this document.

4.3 Processing errors

In error situations, the services return related error messages with the response message in accordance with the structure described in the data content. The ‘Error information’ element contains the error code and its description. If an error is detected before the processing of the actual service request (processing of the SOAP message), the service returns an HTTP error only. The HTTP error can be, for example, ‘HTTP 404 Not found’. The service can also return an error message in accordance with the SOAP 1.1 Fault structure, with the HTTP 500 error code (Internal Server Error). Situations in which a SOAP Fault can be returned include those where the SOAP framework is invalid, the received message cannot be parsed into an XML document, or the document does not pass schema validation.

As a rule, information about errors is returned immediately with the service’s response. However, some errors can only be detected during the processing of certificate requests, in which case the service call for retrieving a certificate returns an error message instead of the certificate.

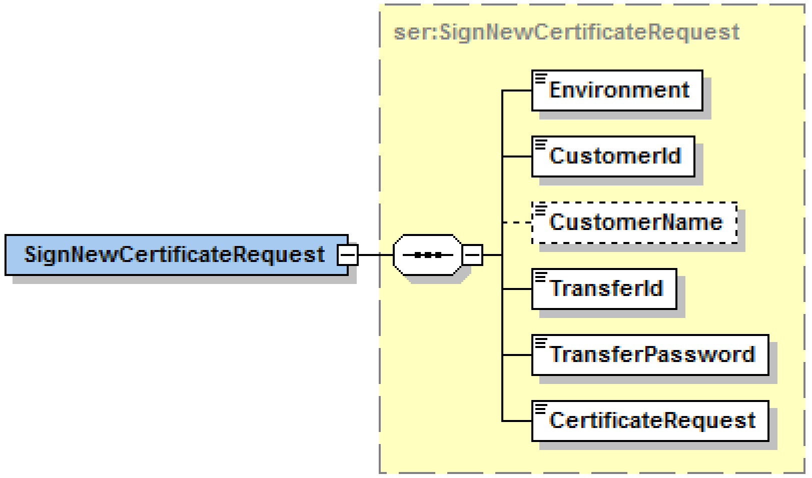
Information about an error is returned immediately in the service call’s acknowledgement of receipt, when

- the service call does not comply with the service schema;
- the transfer ID is incorrect;
- the certificate signing request possibly attached to the request is incorrectly formed;
- checking the electronic signature used in the certificate renewal fails; or
- some other technical error caused by an exceptional situation occurs.

If the generation of a certificate fails, any error, including incorrect IDs, must be corrected. After this, the certificate request service call, which ended due to the error, must be repeated. Exceptions include situations where the system has not yet processed the certificate request before the certificate is tried to be retrieved. In this case, the retrieval can be tried again after a processing time of 10–30 seconds.

5 DATA CONTENT OF API SERVICES

5.1 Requesting a new certificate – request message (SignNewCertificateRequest)

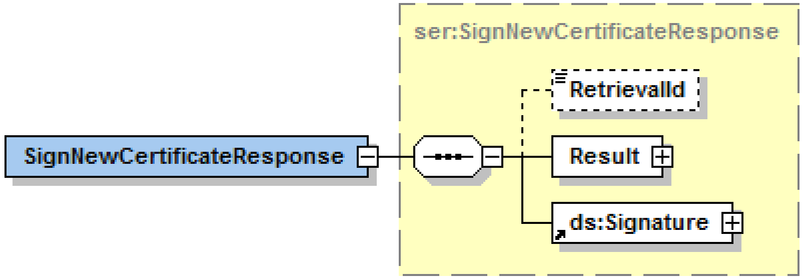


Details of the *SignNewCertificateRequest* data group:

Record name	Type	Allowed values	Element mandatoriness (minOccurs: maxOccurs)	Data description
Environment	ser:EnvironmentTypes	PRODUCTION, TEST	1:1	In the production environment, the value must be PRODUCTION, and in a testing environment, it must be TEST.
Customer identifier (CustomerId)	ser:String30		1:1	Customer identifier. The organisation’s official identifier used in interaction with the Finnish Tax Administration is used as the identifier. The identifier can be, for example, the Business ID. If

Record name	Type	Allowed values	Element mandatoriness (minOccurs: maxOccurs)	Data description
				the Business ID is used, the identifier must be in the Business Information System (BIS) and include the dash.
Customer's name (CustomerName)	ser:String100		0:1	The customer's name. This data is not used in the certificate as such, but it will help should troubleshooting be required.
Transfer ID (TransferId)	ser:String32		1:1	The ID delivered to the customer for requesting a certificate.
One-time password (TransferPassword)	ser:String16		1:1	The one-time password delivered to the customer for requesting a certificate.
Certificate signing request (CertificateRequest)	ser:CertificateRequestType		1:1	A certificate signing request placed by the customer; a Base64-encoded character string in PKCS#10 format.

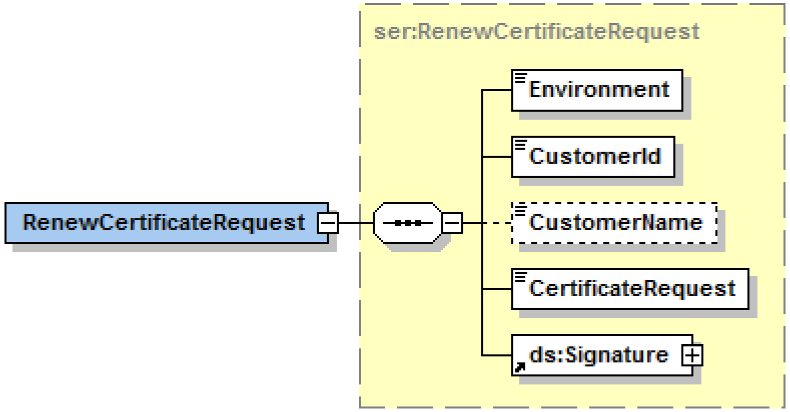
5.2 Requesting a new certificate – response message (SignNewCertificateResponse)



Details of the *SignNewCertificateResponse* data group:

Record name	Type	Allowed values	Element mandatoriness (minOccurs: maxOccurs)	Data description
Certificate retrieval ID (RetrievalId)	ser:String32		0:1	An ID that can later be used to retrieve the certificate.
Result of the processing (Result)	ser:Result		1:1	The result of the processing; see a more detailed content in the description of the 'Result of the message processing' message.
XML signature (Signature)	ds:Signature		1:1	An XML signature that the PKI system generates using its own certificate.

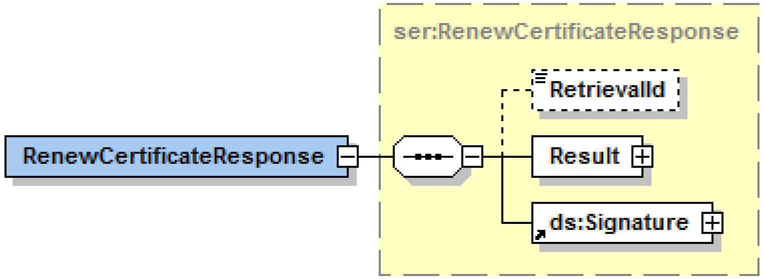
5.3 Renewing a valid certificate – request message (RenewCertificateRequest)



Details of the *RenewCertificateRequest* data group:

Record name	Type	Allowed values	Element mandatoriness (minOccurs: maxOccurs)	Data description
Environment	ser:EnvironmentTypes	PRODUCTION, TEST	1:1	In the production environment, the value must be PRODUCTION, and in a testing environment, it must be TEST.
Customer identifier (CustomerId)	ser:String30		1:1	Customer identifier. The organisation's official identifier used in interaction with the Finnish Tax Administration is used as the identifier. The identifier can be, for example, the Business ID. If the Business ID is used, the identifier must be in the Business Information System (BIS) and include the dash.
Customer's name (CustomerName)	ser:String100		0:1	The customer's name. This data is not used in the certificate as such, but it will help should troubleshooting be required.
Certificate request (CertificateRequest)	ser:CertificateRequestType		1:1	A certificate signing request placed by the customer; a Base64-encoded character string in PKCS#10 format.
XML signature (Signature)	ds:Signature		1:1	An XML signature that the customer generates using its valid certificate.

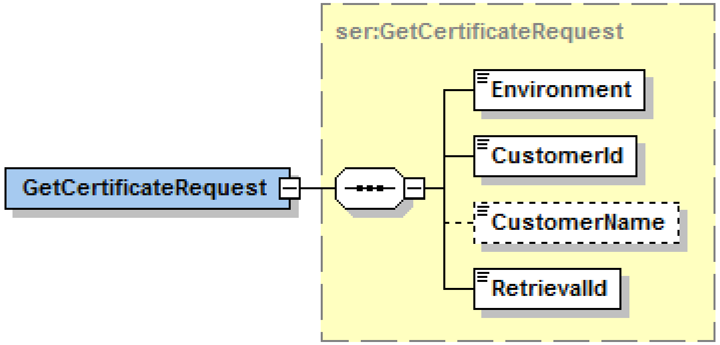
5.4 Renewing a valid certificate – response message (RenewCertificateResponse)



Details of the *RenewCertificateResponse* data group:

Record name	Type	Allowed values	Element mandatoriness (minOccurs: maxOccurs)	Data description
Certificate retrieval ID (RetrievalId)	ser:String32		0:1	An ID that can later be used to retrieve the certificate.
Result of the processing (Result)	ser:Result		1:1	The result of the processing; see a more detailed content in the description of the ‘Result of the message processing’ message.
XML signature (Signature)	ds:Signature		1:1	An XML signature that the PKI system generates using its own certificate.

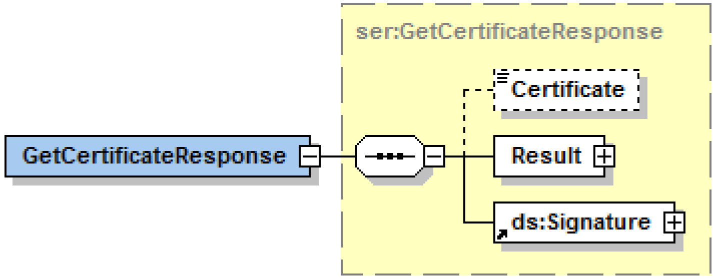
5.5 Retrieving a certificate – request message (GetCertificateRequest)



Details of the *GetCertificateRequest* data group:

Record name	Type	Allowed values	Element mandatoriness (minOccurs: maxOccurs)	Data description
Environment	ser:EnvironmentTypes	PRODUCTION, TEST	1:1	In the production environment, the value must be PRODUCTION, and in a testing environment, it must be TEST.
Customer identifier (CustomerId)	ser:String30		1:1	Customer identifier. The organisation’s official identifier used in interaction with the Finnish Tax Administration is used as the identifier. The identifier can be, for example, the Business ID. If the Business ID is used, the identifier must be in the Business Information System (BIS) and include the dash.
Customer’s name (CustomerName)	ser:String100		0:1	The customer’s name. This data is not used in the certificate as such, but it will help should troubleshooting be required.
Certificate retrieval ID (RetrievalId)	ser:String32		1:1	A retrieval ID that the PKI system returns for a certificate request message or certificate renewal message.

5.6 Retrieving a certificate – response message (GetCertificateResponse)

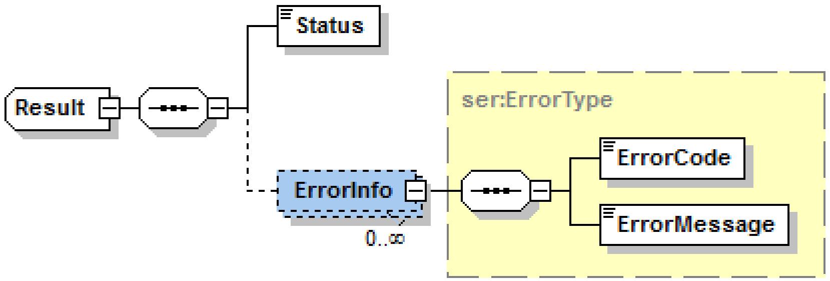


Details of the *GetCertificateResponse* data group:

Record name	Type	Allowed values	Element mandatoriness (minOccurs: maxOccurs)	Data description
Customer’s certificate (Certificate)	ser:CertificateType		0:1	The customer’s certificate signed by the PKI system. The certificate is delivered in Base64-encoded format.
Result of the processing (Result)	ser:Result		1:1	The result of the processing; see a more detailed content in the description of the ‘Result of the message processing’ message.
XML signature (Signature)	ds:Signature		1:1	An XML signature that the PKI system generates using its own certificate.

5.7 Result of the message processing (Result)

This data structure indicates the data content of the ‘Result’ element. The element gives the result of the processing for response messages related to certificate requests, renewals and retrievals. In an error situation, this element also includes the error details in addition to the processing result.



Details of the *Result* data group:

Record name	Type	Allowed values	Element mandatoriness (minOccurs: maxOccurs)	Data description
Result of the message processing (Status)	ser:ResultTypes	FAIL, OK	1:1	Result of the message processing. In an error situation, the value FAIL is returned, and more details of the error are delivered in the 'Error information' element. If the processing is successful, the value OK is returned, and the 'Error information' element is not returned.
Error information (ErrorInfo)	ser:ErrorType		0:unbounded	The error messages are returned in this element.
Error code (ErrorCode)	ser:String10		1:1	The error code is returned in this element.
Error code description (ErrorMessage)	ser:String255		1:1	A description of the error code is returned in this element.

The error codes and their descriptions are described in Section 6.

6 ERROR CODES AND THEIR DESCRIPTIONS

Requesting a new certificate – errors possibly returned by the response message

Error code	Description of the error code	Description of the error
PKI005	Wrong environment type specified	The value of the environment parameter of the request message does not correspond to the value specified in the target system. Once the parameter value has been corrected, the function can be tried again.
PKI020	Invalid credentials	Any of the given credentials – the customer identifier (CustomerID), transfer ID (TransferId) or one-time password (TransferPassword) – is invalid. Once the entered parameters have been checked and corrected, a new certificate request must be placed.
PKI030	Attached CSR is not valid	The certificate signing request (CSR) attached to the request message is incorrect. Once a new CSR has been created, the function can be tried again.
PKI040	The certificate signing request (CSR) is invalid or has been used already.	The certificate signing request (CSR) is invalid or has been used already. Please make a new signing request and try again. If the problem persists, please contact us using the certificate service’s observation form.
PKI099	Generic technical error	An error that has no separately specified error code. The format and details of the incorrect call must be checked. If the error recurs often, contact the Finnish Tax Administration’s certificate service using the observation form.

Renewing a valid certificate – errors possibly returned by the response message

Error code	Description of the error code	Description of the error
PKI005	Wrong environment type specified	The value of the environment parameter of the request message does not correspond to the value specified in the

Error code	Description of the error code	Description of the error
		target system. Once the parameter value has been corrected, the function can be tried again.
PKI010	Signature verification failed	Checking the signature in the content of the request message for renewing a certificate failed. The message must be signed using the certificate that is to be renewed. Once any incorrect signature has been corrected, the call can be repeated.
PKI015	Invalid certificate to be renewed received	The certificate the request message has been signed with is incorrect or does not include the details required. Once the message has been signed using the correct certificate, the certificate request can be repeated.
PKI030	Attached CSR is not valid	The certificate signing request (CSR) is incorrect. Once a new CSR has been created, the function can be tried again.
PKI040	The certificate signing request (CSR) is invalid or has been used already.	The certificate signing request (CSR) is invalid or has been used already. Please make a new signing request and try again. If the problem persists, please contact us using the certificate service's observation form.
PKI080	Certificate renewal not yet allowed	The certificate can only be renewed when there are at most 60 days until it expires.
PKI099	Generic technical error	An error that has no separately specified error code. The format and details of the incorrect call must be checked. If the error recurs often, contact the Finnish Tax Administration's certificate service using the observation form.

Retrieving a certificate – errors possibly returned by the response message

Error code	Description of the error code	Description of the error
PKI005	Wrong environment type specified	The value of the environment parameter of the request message does not correspond to the value specified in the

Error code	Description of the error code	Description of the error
		target system. Once the parameter value has been corrected, the function can be tried again.
PKI020	Invalid credentials	Any of the given credentials – the customer identifier (CustomerID), transfer ID (TransferId) or one-time password (TransferPassword) – is invalid when requesting a new certificate or renewing a certificate. Once the credentials have been checked, the original certificate request or the renewal of a valid certificate and the retrieval of a certificate must be repeated. If the retrieval of a certificate alone is repeated, the original PKI020 error will be returned.
PKI099	Generic technical error	An error that has no separately specified error code. The format and details of the incorrect call must be checked. An error occurs when, for example, a certificate is retrieved too quickly after the request message to request or renew a certificate so that the PKI system has not yet been able to process the request message. If the error recurs often, contact the Finnish Tax Administration’s certificate service using the observation form. Because the service is asynchronous, the error may have already occurred earlier. For example, incorrect information may have been given when requesting or renewing a certificate, due to which the certificate cannot be created.

7 TEST BENCH INSTRUCTIONS

The purpose of the certificate service test bench is to facilitate the development of the application that uses the certificate service's API. 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 APIs of the Finnish Tax Administration, Incomes Register or positive credit register.

7.1 Test materials

The test bench has a permanently valid certificate subscription and two prepared certificates for "Certificate request" and "Certificate renewal". This section presents instructions for using the test bench. In addition, users will require test keys published for testing (PKI private keys).

These test keys are published as ZIP: https://vero.fi/globalassets/tietoa-verohallinnosta/ohjelmistokehittajille/varmennepalvelu/varmennepalvelu-testipenkki.zip

The ZIP archive contains the following files:

- SignNewCertificate_Private.key
  - This private key is intended to create 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 to create the certificate signing request (CSR) in conjunction with certificate renewal (renewCertificate operation).

The testing certificates related to the test keys were renewed in July 2020 and remain valid until July 2030. At the same time, the RetrievalId identifiers required to retrieve the testing certificate were replaced. The new identifiers are listed in this document.

7.1.1 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 conjunction. In this case, the CSR can also 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. Retrieving certificates).

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”.

7.2 Test bench contact address

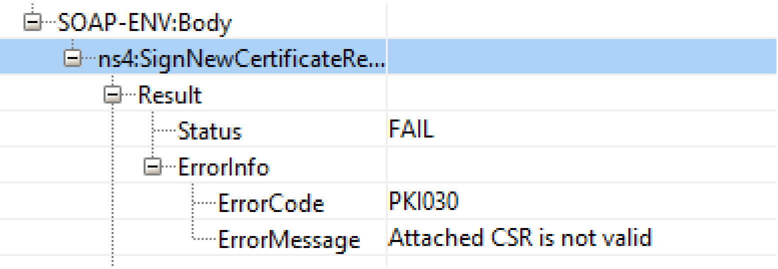
The certificate service’s test bench is connected to the certificate service’s testing environment. Its address differs from that of the actual testing environment by adding /DEV to the service context. The complete address is: https://pkiws-testi.vero.fi/DEV/2017/10/CertificateServices

Note: The address cannot be opened in a browser, as it can be used with API testing software, including SoapUI and Curl.

7.3 Errors in test bench services

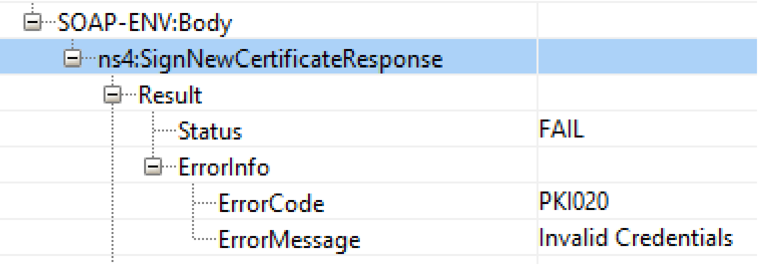
Due to the limited certificates used in the test bench and their limited lifecycles, error processing does not fully correspond to the production environment. The most typical errors are presented in this section. A comprehensive list of the service’s error codes is presented in Section 6.

Incorrect CSR in a new certificate request: error code PKI030 (Attached CSR is not valid) is returned.



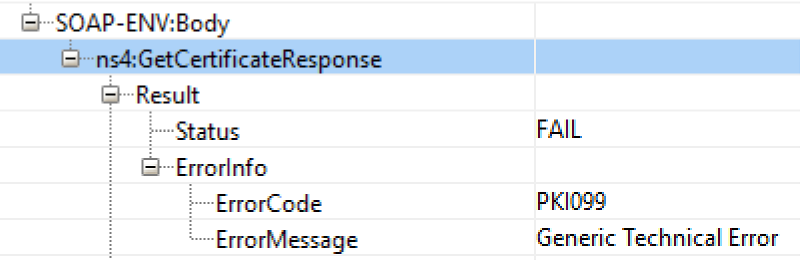
```
⊟ SOAP-ENV:Body
  ⊟ ns4:SignNewCertificateRe...
    ⊟ Result
        Status            FAIL
      ⊟ ErrorInfo
          ErrorCode       PKI030
          ErrorMessage    Attached CSR is not valid
```

Incorrect TransferId in a new certificate request: error code PKI020 (Invalid credentials) is returned.



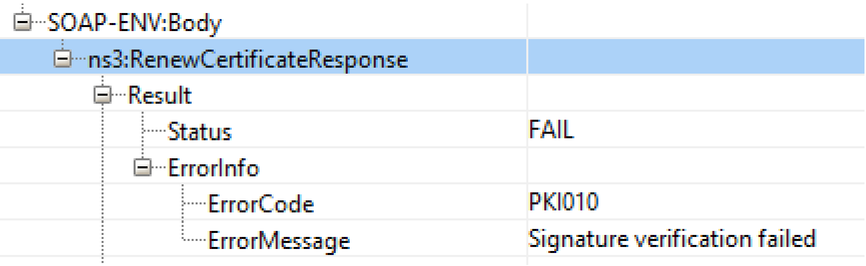
```
SOAP-ENV:Body
  ns4:SignNewCertificateResponse
    Result
      Status                FAIL
      ErrorInfo
        ErrorCode           PKI020
        ErrorMessage        Invalid Credentials
```

Incorrect RetrievalId in certificate retrieval: error code PKI099 (Generic technical error) is returned.



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

Incorrect signature for certificate renewal: error code PKI010 (signature verification failed) is returned.

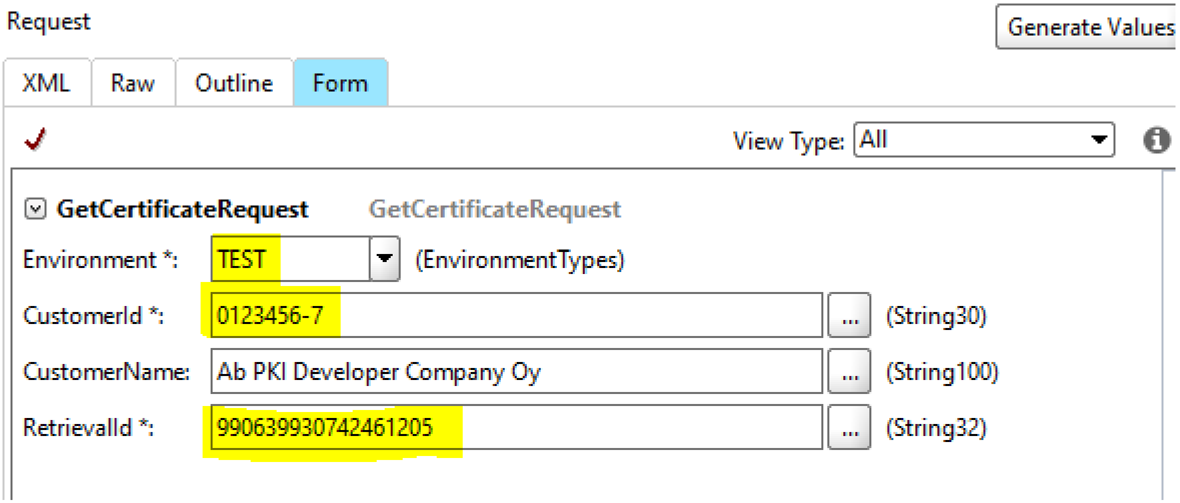


```
SOAP-ENV:Body
  ns3:RenewCertificateResponse
    Result
      Status                FAIL
      ErrorInfo
        ErrorCode           PKI010
        ErrorMessage        Signature verification failed
```

8 EXAMPLE MESSAGES

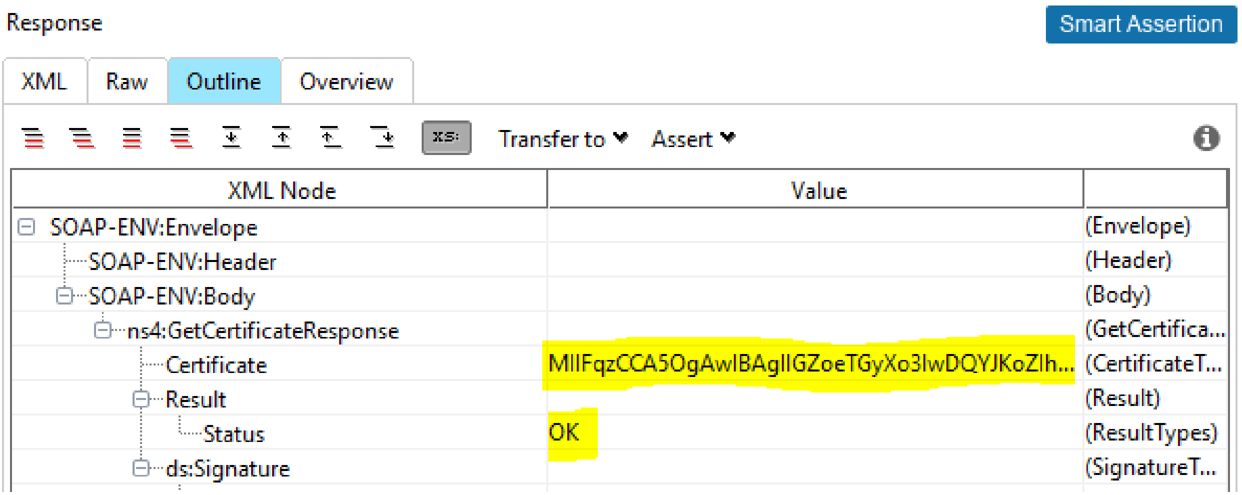
SmartBear Software ReadyAPI has been used in the following examples.

8.1 Certificate retrieval (getCertificate)



GetCertificateRequest GetCertificateRequest

Environment *:	TEST	(EnvironmentTypes)
CustomerId *:	0123456-7	(String30)
CustomerName:	Ab PKI Developer Company Oy	(String100)
RetrievalId *:	990639930742461205	(String32)



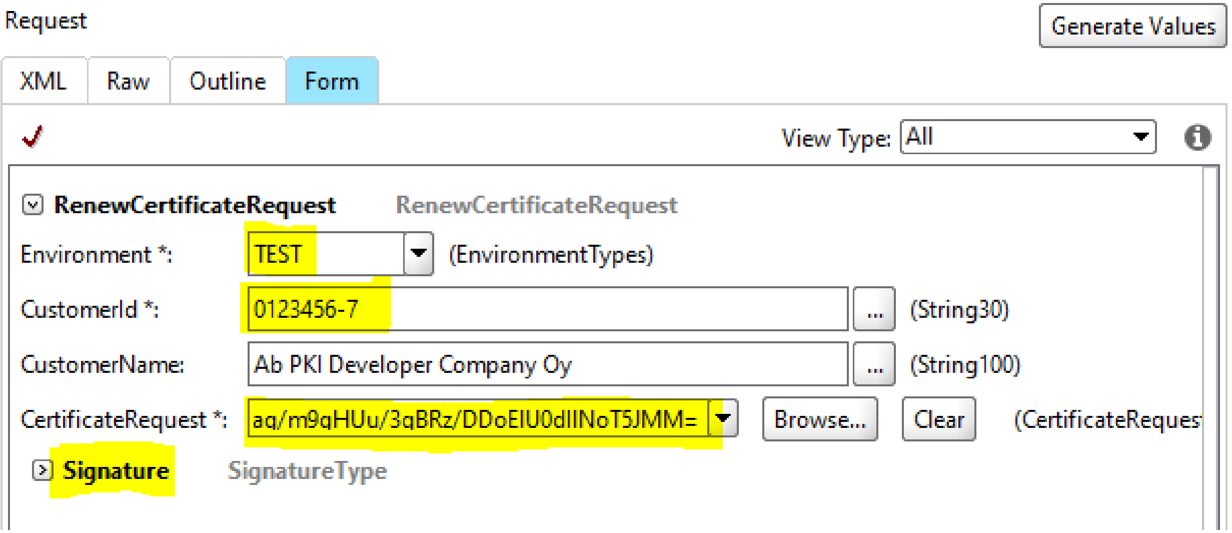
XML Node	Value	
SOAP-ENV:Envelope		(Envelope)
SOAP-ENV:Header		(Header)
SOAP-ENV:Body		(Body)
ns4:GetCertificateResponse		(GetCertifica...
Certificate	MIIFqzCCA5OgAwIBAgIIGZoeTGyXo3lwDQYJKoZIh...	(CertificateT...
Result		(Result)
Status	OK	(ResultTypes)
ds:Signature		(SignatureT...

If the customer saves the certificate received as a response in 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 to open the certificate.

8.2 Renewing a certificate (renewCertificate)

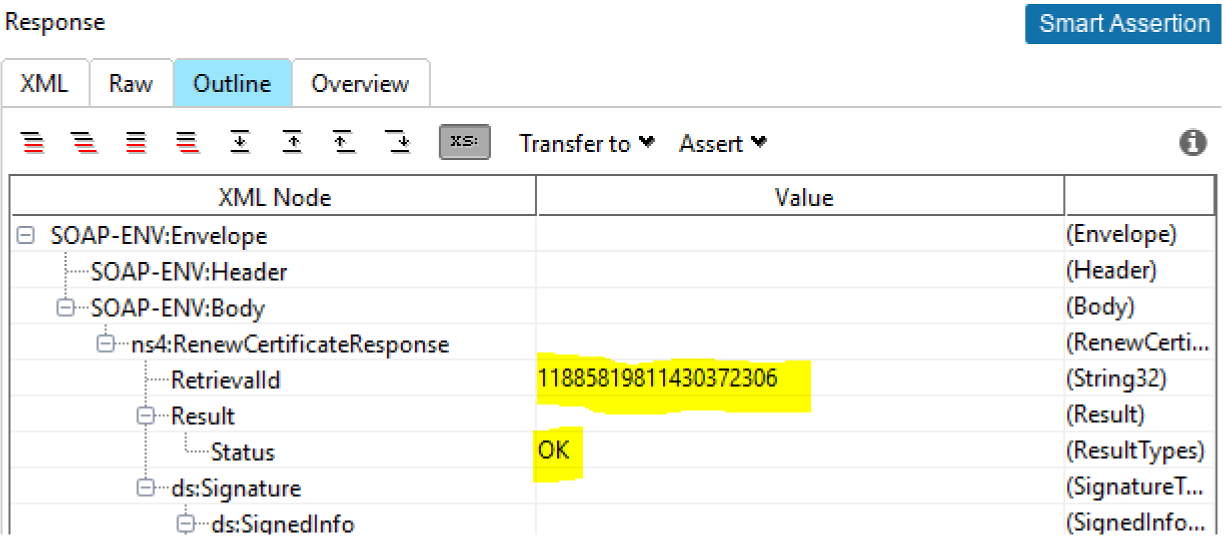
If the program used to create the certificate signing request (CertificateRequest) adds identifiers to the beginning and end (BEGIN and END) of the CSR file, **the user must delete them**. Only the base64-encoded part is sent:
-----BEGIN CERTIFICATE REQUEST-----
.... base64-encoded certificate signing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



View Type: All

RenewCertificateRequest RenewCertificateRequest

Environment *:	TEST	(EnvironmentTypes)
CustomerId *:	0123456-7	(String30)
CustomerName:	Ab PKI Developer Company Oy	(String100)
CertificateRequest *:	aq/m9qHUu/3qBRz/DDoEIU0dlINoT5JMM=	(CertificateReques
Signature	SignatureType	



XML Node	Value	
SOAP-ENV:Envelope		(Envelope)
SOAP-ENV:Header		(Header)
SOAP-ENV:Body		(Body)
ns4:RenewCertificateResponse		(RenewCerti...
RetrievalId	11885819811430372306	(String32)
Result		(Result)
Status	OK	(ResultTypes)
ds:Signature		(SignatureT...
ds:SignedInfo		(SignedInfo...

The message looks like this in XML format:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:cer="http://certificates.vero.fi/2017/10/certificateservices"
xmlns:xd="http://www.w3.org/2000/09/xmldsig#">
<soapenv:Header/>
<soapenv:Body>
<cer:RenewCertificateRequest>
<Environment>TEST</Environment>
<CustomerId>0123456-7</CustomerId>
<CustomerName>Ab PKI Developer Company Oy</CustomerName>
<CertificateRequest>MIICUjCCf.......kEwVXN30KnChlGw2fI79uB5W0HvyQdY69Y6uqbf6P3SGe7g==</CertificateRequest>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/><SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/><Reference URI=""><Transforms><Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><DigestValue>/R8PqacpnI39cWR3Yzrszu4gDzR3Jv6FjXo8gP95viM=</DigestValue></Reference></Sign
edInfo><SignatureValue>nlW0x+q5IEIDtoD5z0MXS60ThEtSWChv7FGFssq6Y8J0K86CazBltZleGG28r7C0OT4rFIIM3bbk
eP3wfgHXpA74cS6UWl0Bv132/HmrgE4kEGZ4Hk8B0SaFcMeyF5UY23dHor+V+VJ7OeuSgosMyJAt
WUD2GERpWFsB+L6zuj5poihoW0yGW88dxi+J3I9VekbyPXErFbWtw5VaJaiL+s6rX22puGevM/Ah
8VL7+eiOgzhjF87p01Yh+WpodMSHvPA5IprrCE1gUxlgKpMl7iWSs0GiogpoqU5g6TxW/SZYZySm
aD0OSL38aPa/Nz/xC2naianFWe/SDhTI5/wE9Q==</SignatureValue><KeyInfo><KeyValue><RSAKeyValue><Modulus>yt/5ZTHae5gE54bc/GrMh4yYxVHCWqYFMf+N
1bQCZFnfhy6H4Oj9PpTSaqD0biVWyPxZozx+aHu1
0JDfFwI+eqlCuR4a5ZBXiciGiTviQOdBvXYWs4oKwsg4w40dLb70TwcrBLyCIVfMo/xRSckrw+am
0lCj4TqOUTL6/NKwei5/RQwKCn0y6031GUC2OpLqXIe2qnwEufaF0QzWysioJcFGKCQAfnDWapsF
KJWSCwJpgn4jkBjbTVlNSVvXfxJj9tiT2B8tLVpjWAQX7rrsGbKzRomTglEse6Myp+QS4et9FajW
mzvf0f7xQ+qRGYl83JsYVQ+gkTBx8YiRd1gY9Q==</Modulus><Exponent>AQAB</Exponent></RSAKeyValue></KeyValue><X509Data><X509SubjectName>C=FI,
O=Ab PKI Developer Company Oy, SERIALNUMBER=C46819107B4015B41B31041111A4DA6D, CN=0123456-7
</X509SubjectName><X509Certificate>MIIFqzCCA5OgAwIBAgIIPNOqyfq5YUgwDQYJKoZIhvcNAQELBQAwSjEkMCIGA1UEAwwbUEtJIFNl
cnZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQKDAxWZXJvaGFsbGludG8xCzAJBgNVBAYTAkZJ
MB4XDTE4MDQxNjEzMjA0M1oXDTIwMDQxNTEzMjA0M1owcjESMBAGA1UEAwwJMDEyMzQ1Ni03MSkw
JwYDVQQFEyBDNDY4MTkxMDdCNDAxNUI0MUIzMTA0MTExMUE0REE2RDEkMCIGA1UECgwbQWIgUEtJ
IERldmVsb3BlciBDb21wYW55IE95MQswCQYDVQQGEwJGSTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAMrf+WUx2nuYBOeG3PxqzIeMmMVRwlqmBTH/jdW0AmRZ34cuh+Do/T6U0mqg9G4l
Vsj8WaM8fmh7tdCQ3xcCPnqpQrkeGuWQV4nIhok74kDnQb12FrOKCsLIOMONHS2+9E8HKwS8giFX
```

```
zKP8UUnJK8PmptJQo+E6jlEy+vzSsHouf0UMCgp9MutN9RlAtjqS6lyHtqp8BLn2hdEM1srIqCXB
RigkAH5w1mqbBSiVkgsCaYJ+I5AY201ZTUlb138SY/bYk9gfLS1aY1gEF+667Bmys0aJk4JRLHuj
MqfkEuHrfRWo1ps739H+8UPqkRmJfNybGFUPoJEwcfGIkXdYGPUCAwEAAaOCAWswggFnMAwGA1Ud
EwEB/wQCMAAwHwYDVR0jBBgwFoAUZeehBs4guH858QDh/4DceYSqbCAwUwYIKwYBBQUHAQEERzBF
MEMGCCsGAQUFBzAChjdodHRwOi8vY3JsLXRlc3RpLnZlcm8uZmkvY2EvUEtJU2VydmljZURldmVs
b3BlckNBdjEuY2VyMBMGA1UdJQQMMAoGCCsGAQUFBwMCMIGcBgNVHR8EgZQwgZEwgY6gPKA6hjho
dHRwOi8vY3JsLXRlc3RpLnZlcm8uZmkvY3JsL1BLSVNlcnZpY2VEZXZlbG9wZXJDQXYxLmNybKJO
pEwwSjEkMCIGA1UEAwwbUEtJIFNlcnZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQKDAxWZXJv
aGFsbGludG8xCzAJBgNVBAYTAkZJMB0GA1UdDgQWBBQwtQwXI5AZJVyZf4DEemCYLnw+mzAOBgNV
HQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQELBQADggIBAEWSy5VOm5gsk7YYAesYRCB3IMAR1VTGtbKH
s+oZxUJKHl8/K2bgGMLKyYbAySxDMd/SFnxO4TXU/1IOedBYp4D9oe8eKIyBmWwG1XdpJ8W2LCvx
+CMrolcwF/5D38pMnxW5sFebTFp7v7m2ZnI5nrdDLNG1XGdF/A4M3ZJ8RymJYG8jC/F3dTao1LWx
9wAevsRwzYm2Y4+CdW/J1wN28vHXJKG6qJsMLrpeBRC27MAqgN2h9NsJnimLKCKdXHPqrW4HKNEe
uXs2bxzHLN17A45RxBpTGnDY3Y6seu4Uw/4U/1ptFyeE8cdC8Gsu++3oOWRfJv5O4mVczGtX4iEk
hgmZTJNYRDEmKqtDN7aNxKoHZ66IgU31vK6M/aiu0FTWr7tugdKVydfNy65XBixM4GCYyGtWRuwu
89ojQnrSQ3h6a4N6jtweAaui0T04UCTr0aZFL6TiGBicjMez/8w1YzAmJ3+a0/ZGL6Q/WU5jPiJf
vNldJoNqyk+IKESr01IoT5Cy+kg2Bzt5Pk+R4KdOERX8TedTxH5U/L/QfUXqGtyfl1768QxB7kaF
9T1CSuXAdR2O+JeYUkekV7WgtrbXA/Y8mZ04HZe7kglH4WJRAkdZXIhPJqS4GudEx6YKZsrC6W0T
wQ9x/30aaIdulABePI3nVEUkGOYRetjoRBOQNckW</X509Certificate></X509Data></KeyInfo></Signature></cer:RenewCertificateRequest></soapenv:Body>
```

9 EXAMPLE OF RENEWING A CERTIFICATE AND GENERATING A SIGNATURE (CSR)

These instructions describe one way to renew a certificate issued by the Finnish Tax Administration’s certificate service and generating a signature using the Web Service API of the PKI system of the Finnish Tax Administration’s certificate service. Based on the example, you can generate the renewal of a certificate in your software.

These instructions describe the renewal of a testing certificate. These instructions also apply to the renewal of a production certificate. In this case, actual customer data and the certificate service’s production address must be used. Production customer data cannot be used in the testing environment.

Requirements:

- PKI expertise to generate a key pair and a signing request
- Programming skills, compiling and executing the signing program
- The certificate service’s message structures, WSDL package: https://vero.fi/globalassets/tietoa-verohallinnosta/ohjelmistokehittajille/varmennepalvelu/varmennepalvelu-rajapinta_v1.01.zip
- A new key pair for the certificate signing request (CSR)
- The current certificate and the private key linked to it for signing the XML message
- The artificial Business ID and the artificial company name for the Web Service certificate used by your organisation
- Any PFX file which contains the private key linked to the current certificate
- The password of the current PFX file

Required tools:

- OpenSSL: https://wiki.openssl.org/index.php/Binaries
- .NET Core 3.1 or newer: .NET Downloads (Linux, macOS, and Windows) (microsoft.com)
- Visual Studio Code: https://code.visualstudio.com/
- Example solution of the Finnish Tax Administration’s signing program, available for download here (SignXmlNew.cs): https://www.vero.fi/globalassets/tietoa-verohallinnosta/ohjelmistokehittajille/swaggerui/verohallinto_program.zip
- SoapUI https://www.soapui.org/downloads/soapui/ or Curl https://curl.se/download.html

Further information:

- Renewal instructions: Renewing certificates
- Documentation on the pages of the Finnish Tax Administration’s certificate service: Documentation
- Instructions for the certificate service’s test bench (in Section 7 of this document)
- A Slack channel is available for Vero API and ApitamoPKI customers: https://vero-api.slack.com

  - You can join the channel using the API observation form.
    - [Observation form of the Finnish Tax Administration’s certificate service]

Renewing a testing certificate

1. Generate a new private key for a new certificate

Generate the private key in OpenSSL using the following command:
openssl genrsa -out newprivate.key 2048

The new private key will be generated in the file newprivate.key.

2. Generate a new certificate signing request for renewal

Generate the certificate signing request (CSR) using the private key generated in step 1 in OpenSSL using the following command:
openssl req -new -key newprivate.key -out certificaterequest.csr

Enter the following information in OpenSSL in accordance with the details of the certificate to be renewed:
Country Name = *FI*
Organization Name = *The name of your testing company*
Common Name = *Your artificial Business ID*

The new certificate signing request will be generated in the file certificaterequest.csr.

3. Generate an XML message for signing

Generate the content of the XML message for renewing a certificate for the renewal API. **Only this part of the message is signed.** Use the attached template. Note that editors may add line breaks. It is **recommended** that any line breaks be removed from the template before generating the signature:

```
<cer:RenewCertificateRequest xmlns:cer="http://certificates.vero.fi/2017/10/certificateservices" xmlns:xd="http://www.w3.org/2000/09/xmldsig#">
  <Environment>TEST</Environment>
  <CustomerId>Your artificial Business ID</CustomerId>
  <CustomerName>Name of the testing company</CustomerName>
```

<CertificateRequest>*The certificate signing request generated in step 2, i.e. the base64 character string contained by the CSR file without --- begin certificate request --- and --- end certificate request ---*</CertificateRequest>
</cer:RenewCertificateRequest>

Enter your testing certificate's Business ID (artificial identifier), the artificial company name and the new certificate signing request generated in step 2 (base64 character string without --- begin certificate request --- and --- end certificate request ---) in the fields of the example message. Save the XML file on a disk without any line breaks for signing.

4. Sign the XML message

Generate a signature for the message's content, i.e. the part generated in step 3. You can use readily available solutions (e.g. XML Signer), build your own solution or use the Finnish Tax Administration's example solution. These instructions are based on the Finnish Tax Administration's C# solution. The example solution assumes that the current certificate is in the PFX file.

Download the signing program's example solution on the Documentation page or at the beginning of Section 9.

To run the program, download .net core 3.1 libraries and a suitable development environment, e.g. Visual Studio Code: https://code.visualstudio.com/

4.1 Generate a PFX file for the signing program using OpenSSL

You do not need to generate a new PFX file if you already have one for using Vero API. In this case, proceed directly to step 4.2.

Run the command below to generate a PFX file. The current certificate and the private key with which it was generated are added to the file.

If no PFX file exists, generate it using the following command, in which case the private key and current certificate are added to it (saved in the cert.cer file in base64 format):
openssl.exe pkcs12 -export -out test.pfx -inkey private.key -in cert.cer

The private key of the currently used certificate is unencrypted in base64 format in the command input in the private.key file, and the certificate's public part (i.e. the signed public key) is in base64 format in the cert.cer file.

OpenSSL asks you to enter a password to encrypt the PFX file. The password is required in the signing program. A new test.pfx file will be generated.

If you are testing in the test bench:
Generate the PFX file using the command above, in which case the private key, the test bench’s SignNewCertificate_Private.key file and the current certificate retrieved from the test bench and saved in the cert.cer file in base64 format are added to it.

4.2 Run the signing program

Compile and run the signing program (SignXmlNew.exe) and enter the XML message to be signed and generated in step 3, the PFX file and the password created for it as command row parameters:
SignXmlNew.exe renew.xml test.pfx password

The signed XML file renew_signed.xml will be generated; see the test bench example below:

```
<cer:RenewCertificateRequest xmlns:cer="http://certificates.vero.fi/2017/10/certificateservices" xmlns:xd="http://www.w3.org/2000/09/xmldsig#">
  <Environment>TEST</Environment>
  <CustomerId>0123456-7</CustomerId>
  <CustomerName>Ab PKI Developer Company Oy</CustomerName>
  <CertificateRequest>MIICjTCCAXUCAQAwSDELMAkGA1UEBhMCRkkxEzARBgNVBAgMClNvbWUtU3RhdGUx
JDAiBgNVBAoMG0FiIFBLSSBEZXZlbG9wZXIgQ29tcGFueSBPeTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAJkBP88eLdbxbJfPluDI/rNP0EUpluRohxgx
MNfuYVV9kXgrMsOZpCsV/QjwZFpWBSFy6PDJIKyvAqe83XSfoGPt9apy3QaUJuXR
4/P5H6VT+eZpt1TCf5CEaKb0aW4bZ1kN9BLerrJ81HsR6cutpE/t0bzArc4kna/l
rz/yB3tlU34YoHyx9bXNwKSPsUdL7N32vIuSO8Me/3NjFzA9CBYRrP58qnXIyTmm
0x5GJXGBJqJM2xBRCmpMWg5WGUOF8mAGxkPDxyEfZpaHXbSLaBQ1nJyDPg0+n/Ak
rcweydE0BKmMh3rSITH/M5DYZ6yKgHABEWERg1Nz06ei+a+KJUcCAwEAAaAAMA0G
CSqGSIb3DQEBCwUAA4IBAQBsIqCulgyrfU+DVZxS60Hvu4d8GcKKRGCtFBt508BM
c+NSnevgakWZXXMWKOJStsDHsOPnwfaIvlmFLWRkAsqxt2dIGgWMzFh9NaX0Anwm
CbiUruot9C8zguP7Y/67AFSeageNYrHmgIBHoZyNIe+tPR4Y5DxcQBl/6HtyzJ/q
Nej5mp2zSlW5P1QoEkS3MU8Gm0mpCBylyAvCzeYHOop6caZMQctVCmPto+0PYx0T
qEmO15vGj/rIN4btjEKSYfjNj56MMN8lsIc/6vqdikKKmMwTLRXjq73liOYyJ11s
9433VK1J/UMvay3y2jYKVDUUw567HD8C3lsT+A+ifkCo</CertificateRequest>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/><SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /><Reference URI=""><Transforms><Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" /></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/><DigestValue>i13a6CV9yr+uqy/qx4yhvyysDvcKnoiNIjUdj7Arr1A=</DigestValue></Reference></SignedInfo><SignatureValue>VEja46Y17IaMXHMJfcZMRM+3zPTL
```

Sepv/zWeR2JLMMCz3nWldJynhs1MjGMbqJ3gLsebomkE3UX10ToZ0LObtbeACFYz78dDKbWHTc4cU1IWkZU3DpXQ5svgJWNk1L+B2SDH7V+ethFNqBmwLCgsE2dT8p
t7rXwsBOnZe/Rt30flEMd5sSWYYJeb1FzMXAcafVIoVs31T9HcoCFupgMH9YWsgzpknQHTSTKfjBZbhsjBnvnDIwSceFhxxNpcmY/zVjRVB56WeC2qhQgZFN7PsnCJ6KnNO
TkYr2w7CVCFNwofCMU3eXUl+n5khTJmNQV+SZ2S0qPzBSp6TD/reCVJHA==</SignatureValue><KeyInfo><X509Data><X509Certificate>MIIFqzCCA5OgAwIBAgIIGZoe
TGyXo3IwDQYJKoZIhvcNAQELBQAwSjEkMCIGA1UEAwwbUEtJIFNlcnZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQKDAxWZXJvaGFsbGludG8xCzAJBgNVBAYTAk
ZJMB4XDTIwMDcwNjA4MzYzMloXDTMwMDcwNDA4MzYzMlowcjESMBAGA1UEAwwJMDEyMzQ1Ni03MSkwJwYDVQQFEyBDNDY4MTkxMDdCNDAxNUI0MUIzMTA
0MTExMUE0REE2RDEkMCIGA1UECgwbQWIgUEtJIERldmVsb3BlciBDb21wYW55IE95MQswCQYDVQQGEwJGSTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggE
BAMrf+WUx2nuYBOeG3PxqzIeMmMVRwlqmBTH/jdW0AmRZ34cuh+Do/T6U0mqg9G4lVsj8WaM8fmh7tdCQ3xcCPnqpQrkeGuWQV4nIhok74kDnQb12FrOKCsLIOM
ONHS2+9E8HKwS8giFXzKP8UUnJK8PmptJQo+E6jlEy+vzSsHouf0UMCgp9MutN9RlAtjqS6lyHtqp8BLn2hdEM1srIqCXBRigkAH5w1mqbBSiVkgsCaYJ+I5AY201ZTUlb138
SY/bYk9gfLS1aY1gEF+667Bmys0aJk4JRLHujMqfkEuHrfRWo1ps739H+8UPqkRmJfNybGFUPoJEwcfGIkXdYGPUCAwEAAaOCAWswggFnMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAUT1PJe8BCr9h+uQE8W6CNC7/QfeYwUwYIKwYBBQUHAQEERzBFMEMGCCsGAQUFBzAChjdodHRwOi8vY3JsLXRlc3RpLnZlcm8uZmkvY2EvUEtJU2
VydmljZURldmVsb3BlckNBdjEuY3J0MBMGA1UdJQQMMAoGCCsGAQUFBwMCMIGcBgNVHR8EgZQwgZEwgY6gPKA6hjhodHRwOi8vY3JsLXRlc3RpLnZlcm8uZmkvY3Js
L1BLSVNlcnZpY2VEZXZlbG9wZXJDQXYxLmNybKJOpEwwSjEkMCIGA1UEAwwbUEtJIFNlcnZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQKDAxWZXJvaGFsbGludG
8xCzAJBgNVBAYTAkZJMB0GA1UdDgQWBBQwtQwXI5AZJVyZf4DEemCYLnw+mzAOBgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQELBQADggIBADZkkj4T+rVlAe9a53/
9zrWLuJqe+WePxIoEk5ozXWDb2FeR0uEyUS2Ba0gVJwPm9Go6CAia3J9nFGyVUUNCm2ofdDGxEX4JkrRc7cO8JPaMY74tJR9wwj8R5sshAXPDVMWh9Ml8LHG6hqz0ic
0lK9cSsAHBGJ3GBlckS/6y+SPWGKMHOf0QIm5of63qQ8aI950y4aUjL7td2Yxiu6jKUfP4haL0BvJFM///o6Ge5LxT3nfPZxESBLbLE21D0ksyO+fZIjleflxIeQk9rWY7zYq/Go9
+EIvElLXE2aDjqQrwoNIQHmqLgG0DuKpJKzSi7nRvDVHaB5YldtLDJ4PXZlTkib8QBOZWmHCw58IvfEdL0WfuRpzJmlCf8oyzLWRagtnEQhwnWnkXOtPqivRq3Rh35M4mQ
PNVPikduzYlhvQzwCAVkzgspEZVT5hQlTEXBiZZQ8jC8Mb6U1u7G/NndHGwdWn0WtNYDMrhqEZGoHxgLTLwaU4d5suHzkv0gIxkreR4fnVdiVWd4zCNQk6rt9Jo3p0yLF
GM49G3kszHPcYxxBmzqSrSBoBKX5Sn9+jOF39fxE6LNCmJBiZz49WhSOTSLjX/kL8B0T4NBCtz6EdhQk0lz1JC5GvNuVVnmKeZYElt3qLvx4ktc6QxlH2zZ48BR+m/cXycvyLz
y2fgyAlW</X509Certificate></X509Data></KeyInfo></Signature></cer:RenewCertificateRequest>

Note that the signing program adds the Signature block to the end of the RenewCertificateRequest block.

It is important that the content of the file is not changed in any way before it is sent to the PKI system’s API so that the signed content remains unchanged. Changes are also caused by line breaks and other formatting, due to which the signature is no longer valid and the certificate service returns the error code PKI010.

5. Send the signed message to the certificate service’s PKI system API

Send the signed message for renewing a testing certificate using SoapUI, for example, to the testing address of the certificate service’s PKI system: https://pkiws-testi.vero.fi/2017/10/CertificateServices

You can download message structure templates based on the WSDL description in SoapUI. Download the signing program’s API package on the Documentation page or at the beginning of Section 9. Open the WSDL file using SoapUI.

Generate the outgoing message so that the signed content remains unchanged in the body element of soap-envelope. Do not add any formatting to the signed content.

Example of soap-envelope and the part in which the content is entered:

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xs="http://www.w3.org/2001/XMLSchema" ><env:Body>
the signed content as generated in step 4
</env:Body></env:Envelope>
```

Check the URL and send the message. ‘OK’ and ‘retrievalID’, with which the renewed certificate can be retrieved using the GetCertificate operation, will be sent as the response.

Curl can be used instead of SoapUI, in which case you need to ensure in the Windows environment that there are no line breaks in the signed content and that all content is on a single row. Remember to add soap-envelope to the signed file. A renewal request can be sent with the Curl command below:

```
curl -i -v -d @template_signed_env.xml --header "SOAPAction:renewCertificate" -H "Content-Type: text/xml;charset=UTF-8" -H "Accept-Encoding: gzip,deflate
https://pkiws-testi.vero.fi/2017/10/CertificateServices
```

6. Retrieve the renewed certificate using the GetCertificate operation

Use the certificate service’s instructions when retrieving.

Store the PFX file and private key with care.

10 GENERATING A SIGNATURE (CSR) USING THE WINDOWS MMC TOOL

If you cannot use OpenSSL, the CSR can also be generated using Microsoft Management Console (MML) in the Windows environment. Detailed instructions are available at:

https://knowledge.digicert.com/solution/SO29005.html