Version 1.01

Certificate service – Interface description

Implementation project of a national Incomes Register

Version history

Version	Date	Description
1.0	30/10/2017	Document published.
1.01	15/12/2017	Document updated in Sections 1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 3.3, 3.7 and 4. Section 2.2.1 removed.

CONTENTS

1 GENERAL

This document describes the implementation of the Web Service interface of the certificate service, from the perspective of the system integrator. The document describes the interface services and data contents of the services (XML schemas).

The document presents the implementation of the certificate service interface with sufficient precision for the parties to specify and implement the integration of their own systems with the certificate service.

1.1 Web Service interface

The services of the certificate service interface 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

1.2 Schema

Elements in accordance with the XML schema **CertificateServices.xsd** are used in the life cycle management of the certificates issued by the certificate service.

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/schemas/certificateservices

Empty elements are not allowed in the messages. If an element receives no value, the element is left out of the message entirely. Empty character strings are also not allowed, i.e., the minimum length of all values is 1.

1.3 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	& conversion is mandatory
<	less than	< conversion is mandatory
>	greater than	> conversion is not mandatory, but conforms with best practices
'	apostrophe	' conversion is not mandatory, but conforms with best practices
"	quotation mark	" 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

1.4 Document reading instructions

In the document diagrams, the 0 .. ∞ marking in the bottom right-hand corner of an element means that the element may appear several times, or not at all. The 1 .. ∞ marking 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 the form 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

2 THE CERTIFICATE SERVICE'S WEB SERVICE -INTERFACE

The use cases of the certificate service's Web Services and the links between the services are described in the document Certificate service – General description.

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

Operation	Request message	Response message	Description
Request for a new certificate (SignNewCertificate)	SignNewCertificateRequestMessage	SignNewCertificateResponseMessage	Requesting a new certificate, when • the user requests a certificate for the first time • the user already has one or more valid certificates, but needs more certificates • the user's previous certificate has expired or has been revoked.
Renewing a valid certificate (RenewCertificate)	RenewCertificateRequestMessage	RenewCertificateResponseMessage	Certificate renewal request, when a user's certificate is about to expire and the renewal is performed before the currently valid certificate expires.
Certificate retrieval (GetCertificate)	GetCertificateRequestMessage	GetCertificateResponseMessage	Retrieval of a previously requested new or renewed certificate.

The data contents of the request and response messages of the interface services are described in more detail in Chapter 3.

2.1 Message signing

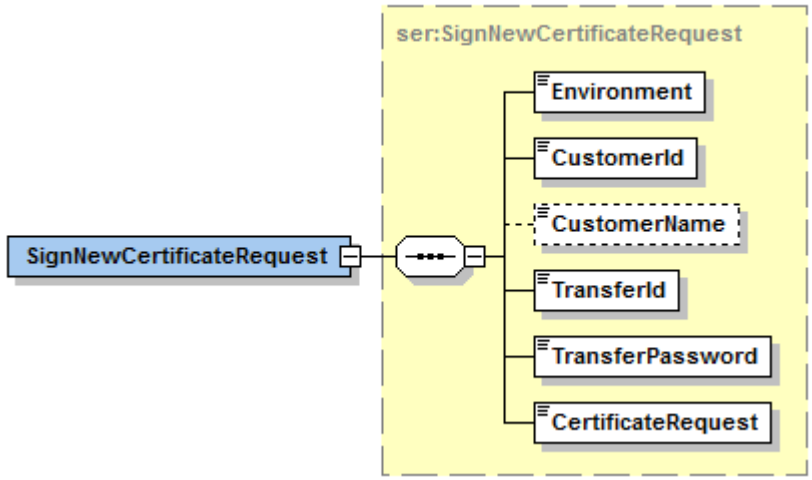
The certificate service's Web Service interface services use electronic signatures (XML Signature). These are used to verify the creator of the data contents of the message for messages defined in Chapter 3. A signature also guarantees the integrity of the message. A signature is implemented using the 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/). The signature generation procedures and related details (such as the algorithms and canonicalisation methods to be used) will be published at a later date in connection with the generation of the Incomes Register's XML signature.

2.2 Error handling in the Web Services

In error situations, the services return the relevant error messages with the response message, in accordance with the structure described in the data contents. 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. The error codes and their descriptions are described in Chapter 4.

3 DATA CONTENTS OF THE INTERFACE SERVICES

3.1 Requesting a new certificate – request message (SignNewCertificateRequest)

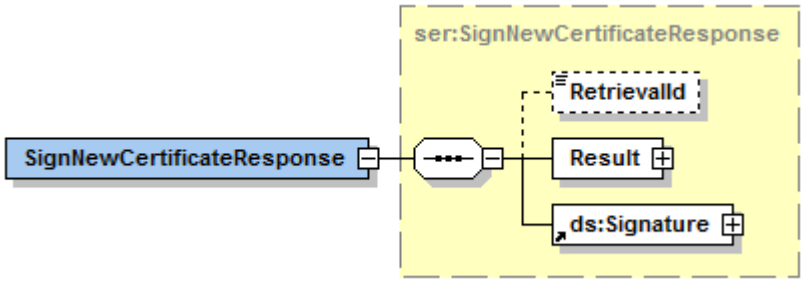


Details of the *SignNewCertificateRequest* data group:

Data designation	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 transactions with the Incomes Register, is used as the identifier. The identifier can be, for example, the Business ID.

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 request (CertificateRequest)	ser:CertificateRequestType		1:1	The certificate request made by the customer. The CSR is a Base64-encoded character string in PKCS#10 format.

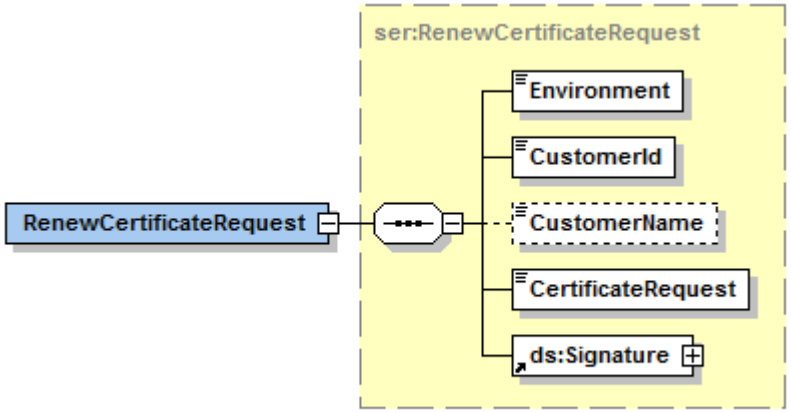
3.2 Requesting a new certificate – response message (SignNewCertificateResponse)



Details of the *SignNewCertificateResponse* data group:

Data designation	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 the more detailed contents in the description of the element Result of the message processing.
XML signature (Signature)	ds:Signature		1:1	XML signature that the certificate service generates using its own certificate.

3.3 Renewing a valid certificate – request message (RenewCertificateRequest)

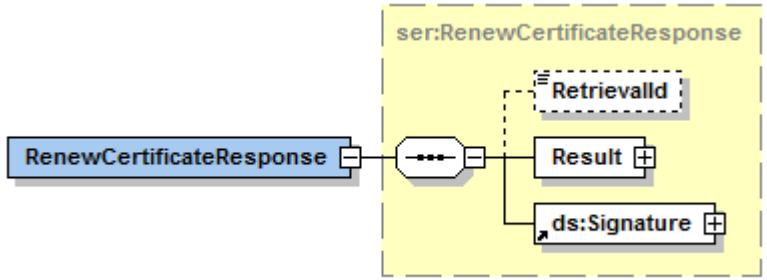


Details of the *RenewCertificateRequest* data group:

Data designation	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 transactions with the Incomes Register, is used as the identifier. The identifier can be, for example, the Business ID.
Customer's name (CustomerName)	ser:String100		0:1	The customer's name. This data is not used in the certificate as such, but will help should troubleshooting be required.
Certificate request (CertificateRequest)	ser:CertificateRequestType		1:1	The certificate request made by the customer. The CSR is a Base64-encoded character string in PKCS#10 format.

XML signature (Signature)	ds:Signature		1:1	XML signature that the customer generates using its valid certificate.

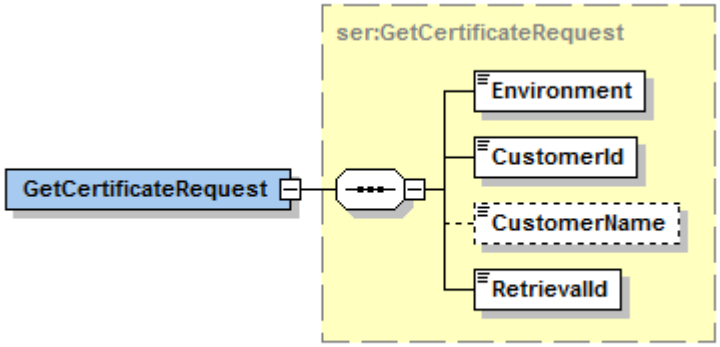
3.4 Renewing a valid certificate – response message (RenewCertificateResponse)



Details of the *RenewCertificateResponse* data group:

Data designation	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 the more detailed contents in the description of the element Result of the message processing.
XML signature (Signature)	ds:Signature		1:1	XML signature that the certificate service generates using its own certificate.

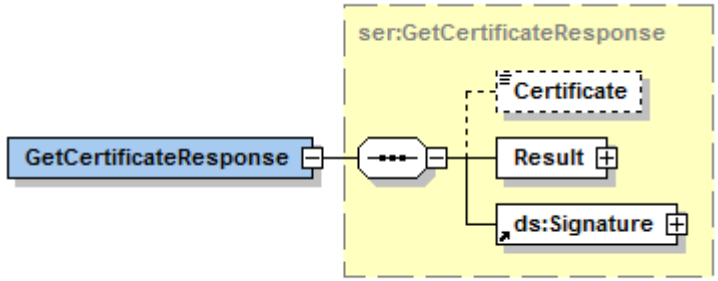
3.5 Retrieving the certificate – request message (GetCertificateRequest)



Details of the *GetCertificateRequest* data group:

Data designation	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 transactions with the Incomes Register, is used as the identifier. The identifier can be, for example, the Business ID.
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	Retrieval ID that the certificate service returns for a certificate request message or certificate renewal message.

3.6 Retrieving the certificate – response message (GetCertificateResponse)

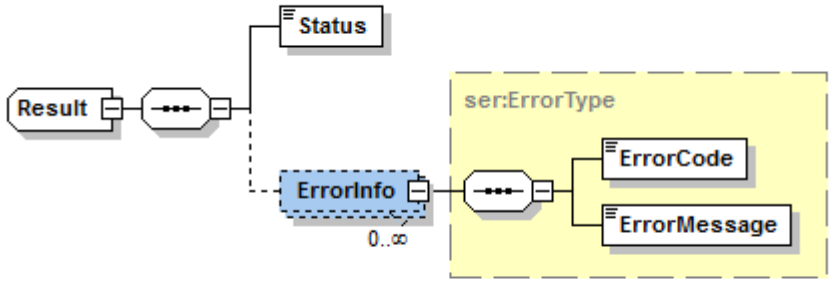


Details of the *GetCertificateResponse* data group:

Data designation	Type	Allowed values	Element mandatoriness (minOccurs: maxOccurs)	Data description
Customer's certificate (Certificate)	ser:CertificateType		0:1	Customer's certificate signed by the certificate service. The certificate is delivered in Base64-encoded format.
Result of the processing (Result)	ser:Result		1:1	The result of the processing, see the more detailed contents in the description of the element Result of the message processing.
XML signature (Signature)	ds:Signature		1:1	XML signature that the certificate service generates using its own certificate.

3.7 Result of the message processing (Result)

This data structure indicates the data contents of the Result element. The element gives the result of the processing on 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:

Data designation	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 on the error are delivered in the element Error information. If the processing is successful, the value OK is returned, and the element Error information 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	The description of the error code is returned in this element.

The error codes and their descriptions are described in Chapter 4.

4 ERROR CODES AND THEIR DESCRIPTIONS

Requesting a new certificate – error situations possibly returned in the response message:

Error code	Error code description	Description of the error situation
PKI005	Wrong environment type specified	The value of the Environment parameter in the request message does not match the value defined in the target system. You may retry the operation after correcting the parameter value.
PKI020	Invalid credentials	One of the provided identifiers – Customer identifier (CustomerId), Transfer ID (TransferId) or One-time password (TransferPassword) is invalid. You may retry the operation after checking and correcting the entered parameters.
PKI030	Attached CSR is not valid	The certificate signing request (CSR) attached to the request message is invalid. You may retry the operation after generating a new certificate signing request.
PKI099	Generic Technical Error	An error situation for which there is no separately defined error code. You must check the format and data of the invalid request. If this error recurs often, please contact the Incomes Register.

Renewing an existing certificate – error situations possibly returned in the response message:

Error code	Error code description	Description of the error situation
PKI005	Wrong environment type specified	The value of the Environment parameter in the request message does not match the value defined in the target system. You may retry the operation after correcting the parameter value.
PKI010	Signature verification failed	The checking of the electronic signature used in the certificate renewal request message failed. The message must be signed with the certificate you wish to renew. You may retry the request after correcting the possibly invalid signature.
PKI015	Invalid certificate to be renewed received	The certificate used to sign the request message is invalid or does not contain the required data. You may retry the certificate request after signing the message with the correct certificate.
PKI030	Attached CSR is not valid	The certificate signing request (CSR) is invalid. You may retry the operation after generating a new certificate signing request.
PKI080	Certificate renewal not yet allowed	The certificate cannot be renewed until there are no more than 60 days until its expiration.
PKI099	Generic Technical Error	An error situation for which there is no separately defined error code. You must check the format and data of the invalid request. If this error recurs often, please contact the Incomes Register.

Retrieving a certificate – error situations possibly returned in the response message:

Error code	Error code description	Description of the error situation
PKI005	Wrong environment type specified	The value of the Environment parameter in the request message does not match the value defined in the target system. You may retry the operation after correcting the parameter value.
PKI020	Invalid credentials	One of the provided identifiers – Customer identifier (CustomerId), Transfer ID (TransferId) or One-time password (TransferPassword) is invalid when requesting a new certificate or renewing a certificate. After checking the identifying information, you must retry the original operation and the retrieval of the certificate.
PKI099	Generic Technical Error	An error situation for which there is no separately defined error code. You must check the format and data of the invalid request. If this error recurs often, please contact the Incomes Register. Because the service is of an asynchronous nature, the error may have occurred earlier. For example, you may have provided invalid data when requesting or renewing a certificate, and the generation of the certificate failed.