Version 1.04

Certificate service – General description

Incomes Register Unit

Version history

Version	Date	Description
1.0	30/10/2017	Document published.
1.01	15/12/2017	Document updated in the following sections: 2. Terminology and abbreviations, 3.1 Requesting a new certificate, 3.3. Life cycle and renewal of certificates, 3.4. Error situations, 4. Using certificates in the Incomes Register's SFTP channel, 5 Testing the service. The previous section 3, Service access rights and agreeing on its use, has been removed.
1.02	16/10/2018	Document updated in the following sections: 1. Foreword, 3. Certificate service, 3.4 Life cycle and renewal of certificates, 4. Certificate use in the Incomes Register's technical interfaces, 4.1 Web Service channel, 4.2 SFTP channel Added: 3.1 Certificate types
1.03	10/4/2019	Document updated in the following sections: 3 Certificate service, 3.1 Certificate types, 3.2 Requesting a new certificate, 3.4 Life cycle and renewal of certificates, 3.5 Error situations, 4 Using certificates in the Incomes Register's technical interfaces, 5 Testing the service.
1.04	20/1/2020	Document updated in Section 3.4 Life cycle and renewal of certificates.

CONTENTS

1 FOREWORD

The certificate service is utilised by organisations that submit records to the Incomes Register or retrieve records from the Incomes Register via technical interfaces. The Incomes Register's technical interface channels are the SFTP channel and the Web Service channel. A certificate is issued to an organisation that is responsible for delivering data to the Incomes Register, or that has the right to receive data from the Incomes Register. The Incomes Register's certificate service issues the certificates.

The purpose of this document is to describe the Incomes Register's certificate service on a general level. The technical functionalities and schemas used in requesting, retrieving and renewing the certificate are described in the separate document, Certificate service – Interface description.

2 TERMINOLOGY AND ABBREVIATIONS

The abbreviations and key terminology used in the service description are presented in Table 1.

Abbreviation or term	Description
CSR (Certificate Signing Request)	A request for a certificate made by a user of the certificate service. The CSR is a Base64-encoded character string in PKCS#10 format.
Public Key Method	An asymmetric encryption scheme where one of the encryption keys is a public key and the other is a private key.
PKCS#10 (Public Key Cryptography Standards # 10)	A standard that specifies the format and contents 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 the 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.
Interface	A standard-compliant practice or connection point enabling data transfer between devices, software or the user.
RSA encryption	A Public Key Method 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.
Data users	Actors who have a statutory right to obtain income or other data from the Incomes Register for the purpose of performing their duties. During the first stage, beginning from 1 January 2019, the data users will be the Tax Administration, the Social Insurance Institution of Finland Kela, Employment Fund, the earnings-related pension providers, and the Finnish Centre for Pensions ETK. In the second stage, beginning from 1 January 2020, the data users will also include Statistics Finland, Employment Fund (adult education benefits), non-life insurance providers, unemployment funds, the administrative sector of the Ministry of Economic Affairs and Employment, the municipalities, and the labour protection authorities.
Data providers	All companies and other actors under the obligation to report wage, pension or benefit data to an Incomes Register data user in Finland.
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 1. The abbreviations used and key terminology.

3 CERTIFICATE SERVICE

The certificate service of the Incomes Register is based on a PKI solution (Public Key Infrastructure). In the certificate service, 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 customer requests a certificate from the Incomes Register's certificate service, and the certificate service issues one. The certificate is used in the identification of the customer and the signing of records submitted to the Incomes Register with an electronic signature (XML Signature) in the Incomes Register's technical interfaces. The certificates are issued for a specific purpose for a specific customer, and they cannot be used for purposes differing from the original. Certificate users must accept and comply with the terms and conditions of the Finnish Tax Administration's and the Incomes Register's interface services (pdf).

If a user of the Incomes Register's services acts as both a data provider and a data user of earnings payment data and benefits payment data, separate certificates must be requested for the different purposes. If a customer uses both the SFTP and Web Service channels of the technical interface, separate certificates for the different channels must also be requested. A single actor can thus have several certificates. If a customer uses several certificates meant for different purposes and channels, for example, in the same software, attention should be particularly paid to the management of certificates.

3.1 Certificate types

Role	Channel	Certificate issuer
Provider of earnings payment data	Web Service	Data Providers Issuing CA
	SFTP	Data Providers SFTP Issuing CA
Provider of benefits payment data	Web Service	IR Benefit Data Providers Issuing CA
	STFP	IR Benefit Data Providers SFTP Issuing CA
Data user	Web Service	IR Income Data Users Issuing CA
	SFTP	IR Income Data Users SFTP Issuing CA
Support services outside the Incomes Register	Web Service	IR External Data Providers Issuing CA
	SFTP	IR External Data Providers SFTP Issuing CA

3.2 Requesting a new certificate

Requesting a new certificate and the retrieval of the certificate are presented in Figure 1.

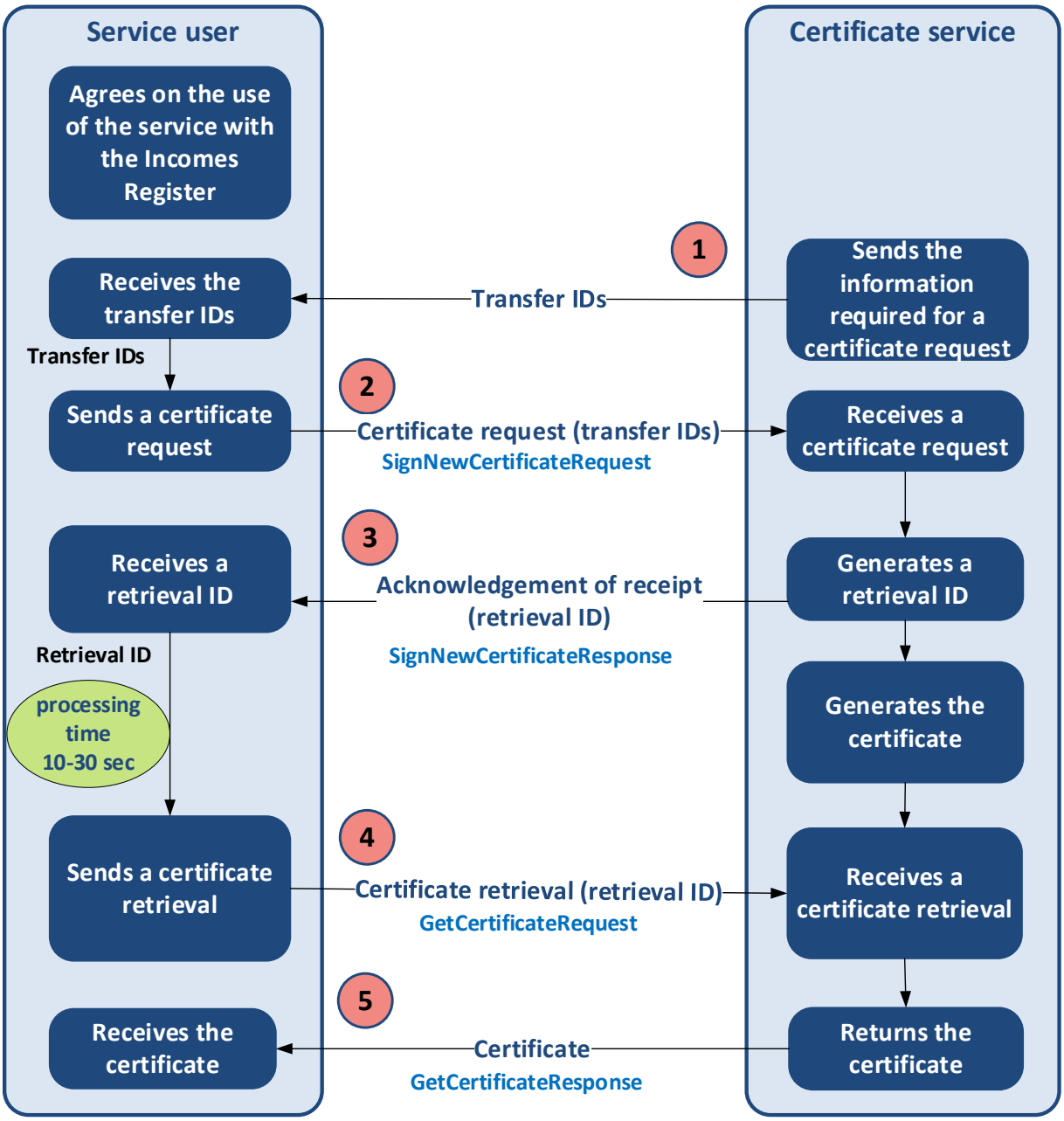

Figure 1. Requesting and retrieving a new certificate.

Access rights to the technical interfaces needed for data provision are applied for in the Incomes Register's e-service. When an organisation submits an application for the deployment of the technical interface, it accepts the terms and conditions of the Finnish Tax Administration's and the Incomes Register's interface services. The application triggers a certificate request. Access rights to the technical interface needed for data use are applied for by filling in the report by the Incomes Register data user for data permission purposes.

The certificate service sends the information required for making a certificate request to the customer: the transfer ID (TransferId) and a one-time password (TransferPassword). A customer can make a certificate request after receiving the transfer ID and one-time password sent for the certificate request. The one-time password is valid for 14 days.

- If a certificate request is not made within this time period, the one-time password will expire and the customer must submit a new application for the deployment of the technical interface.

- The transfer ID and one-time password are delivered to the certificate's technical contact person in a secure e-mail message that the customer can open with a code sent in a text message.

For the certificate request, the customer generates a 2048-bit key pair using the RSA algorithm. Furthermore, the customer generates a Certificate Signing Request (CSR) complying with the PKCS#10 specification, containing the customer's public key.

The generated CSR is attached to the certificate request service call. Additionally, the transfer ID and one-time password separately delivered to the customer are attached to the service call, in order to uniquely identify and secure the request. In the acknowledgement of receipt, the certificate request service call to the certificate service returns a retrieval ID that uniquely identifies the certificate request feedback and the certificate being generated for retrieval in connection with a successful request. When retrieving a certificate, the processing time of a certificate request must be taken into account, and the certificate should not be retrieved immediately after a successful certificate request. The certificate is obtained as a response to a certificate retrieval service call to which the retrieval ID has been attached. After a successful retrieval of a certificate, the customer has the certificate required to use the services of the Incomes Register. If a certificate cannot be generated due to an error situation, the service call for a certificate request returns an error notification instead of a certificate.

3.3 Revocation of certificates

A certificate must be revoked if it is known or suspected that the certificate holder's private key has been lost or ended up in the wrong hands. A certificate must also be revoked if it is no longer needed. The Incomes Register Unit can revoke a certificate when, for example, the agreement entitling to use the service ends, or it is apparent that the issued certificate has been misused.

A certificate is revoked by contacting the Incomes Register Unit. For more detailed instructions on revoking a certificate, see the website of the certificate service. Certificate revocation can be requested at any time. When a customer requests the revocation of a certificate outside office hours, the certificate is first revoked temporarily (suspended). This means that the use of the certificate is prevented but the certificate can still be reactivated. If the customer confirms the revocation request, the certificate is revoked permanently. The customer must confirm the revocation or reactivation of a suspended certificate within 14 days of the certificate being suspended. If the customer does not confirm the reactivation during this period, the certificate service will permanently revoke the certificate.

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

3.4 Life cycle and renewal of certificates

A customer's certificate is valid for two years, after which it must be renewed. . Certificate holders must check the validity of their certificates regularly. The last date of validity can be checked in the e-service or on the certificate. The certificate can be renewed via the interface of the certificate service. The interface has a specific service (RenewCertificate) for this purpose. For the renewal of a certificate, a new key pair is created, a certificate signing request is generated and the service request is signed using the key associated with the valid certificate. A certificate that is about to expire can be renewed no earlier than sixty (60) days before its expiry. The old certificate will remain valid until the end of the original period of validity. If the certificate is renewed on time, there will be no need to request a new certificate and the Incomes Register will not send you transfer IDs (transfer ID and one-time password).

The renewal of a certificate is presented in Figure 2.

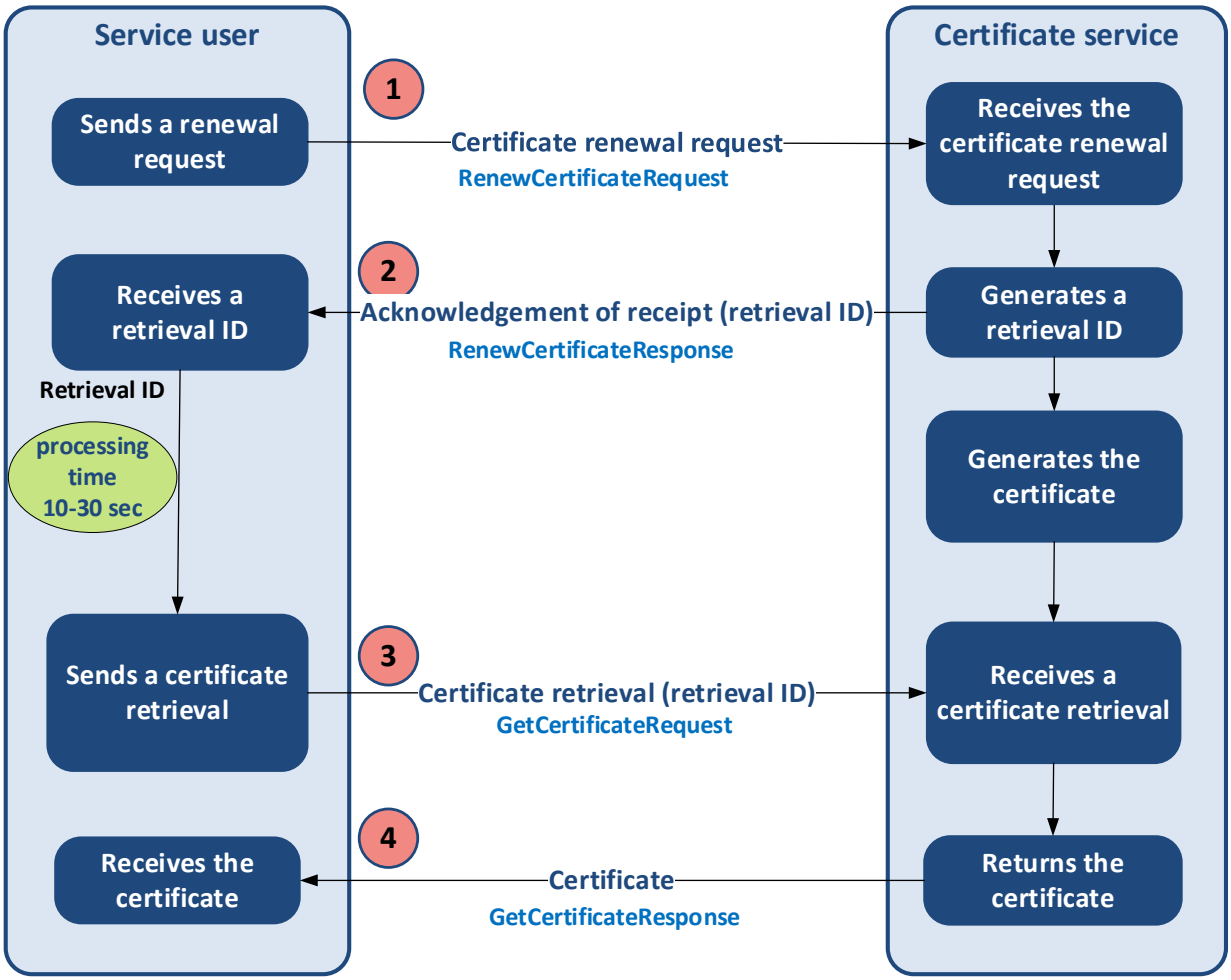

Figure 2. Renewal of a certificate.

For the renewal of a certificate, the customer must create a new key pair and Certificate Signing Request (CSR) in the same way as when requesting a new certificate.

The service user attaches the generated CSR to the certificate renewal service call. The service call is electronically signed using the private key linked to the previous certificate that is still valid.

The certificate signature uses the same format as when submitting records to the Incomes Register with a valid certificate. The certificate renewal function returns a certificate retrieval ID that can be used to retrieve the new certificate with a certificate retrieval service call, in the same way as when a certificate is retrieved for the first time. When retrieving a certificate, the processing time of a certificate request must be taken into account, and the certificate should not be retrieved immediately after a successful certificate request.

Note! The previous certificate must be replaced with the new certificate without delay and no later than its expiration date. If the same certificate has been used in more than one location, all copies of the old certificate must be replaced with the new one in order to avoid errors caused by an expired certificate.

If the certificate expires, the customer must request a new certificate via the Incomes Register's e-service. The request and retrieval of the new certificate is then performed in the same way as when ordering a certificate for the first time.

3.5 Error situations

As a rule, the certificate service returns information on errors immediately, with the service response. However, some of the errors are not detected until the certificate request is being processed. In such a case, the service call for a certificate request returns an error notification instead of a certificate.

Information on an error is returned immediately in the service call acknowledgement of receipt, when

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

If the certificate generation fails, the possible error situation, such as the invalid IDs, must be corrected. After that, the service call for a certificate request that resulted in an error must be repeated. The only exception is a situation where the system has not had time to process the certificate request before the customer attempts to retrieve it. In this case, you can try retrieving the certificate request again after 10–30 seconds.

The returned error codes and their descriptions are described in the interface description of the certificate service.

4 USING CERTIFICATES IN THE INCOMES REGISTER'S TECHNICAL INTERFACES

When forming a connection, the technical interfaces of the Incomes Register will check the validity and purpose of use of the certificate. If the certificate has expired, been revoked or issued for a different channel, the connection will fail. For further information about the use of the Incomes Register's interfaces, identification of customers, and the electronic signature, see document: Technical interface – Application guidelines.

4.1 Web Service channel

In the Incomes Register's Web Service channel, certificates are used for customer identification. Certificates and private keys are used in the electronic signing of records.

4.2 SFTP channel

In the Incomes Register's SFTP channel, user IDs and certificate key pairs are used for customer identification. Identification takes place as follows: the Incomes Register's certificate service and the SFTP server possess the public key of the key pair, and the customer identifies himself/herself by using his/her private key. Certificates and private keys are used in the electronic signing of records.

5 TESTING THE SERVICE

The certificate service and the certificates issued by it can be tested before the deployment of the service. The software solutions utilising the interface of the certificate service can be tested in the certificate service test bench before the use of the actual testing certificates. In the test bench, it is possible to test repeatedly the most important functions of the interfaces with the help of pre-specified test keys. See Certificate service's stakeholder testing for further information on the test bench and the testing of the certificate service.