Version 1.01

Certificate service – General 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 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.

CONTENTS

1 FOREWORD

All organisations providing records to and retrieving records from the Incomes Register use the certificate service. 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 a separate document.

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, the Unemployment Insurance Fund (TVR), 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, the Education Fund, 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. A certificate requested from the certificate service and issued by the Incomes Register is used in the authentication of the customer and the signing of records submitted to the Incomes Register with an electronic signature (XML Signature). The certificates are issued for a specific purpose, and they cannot be used for purposes differing from the original. If a user of the Incomes Register's services acts as both a data provider and a data user, the service user must request certificates for both purposes.

3.1 Requesting a new certificate

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

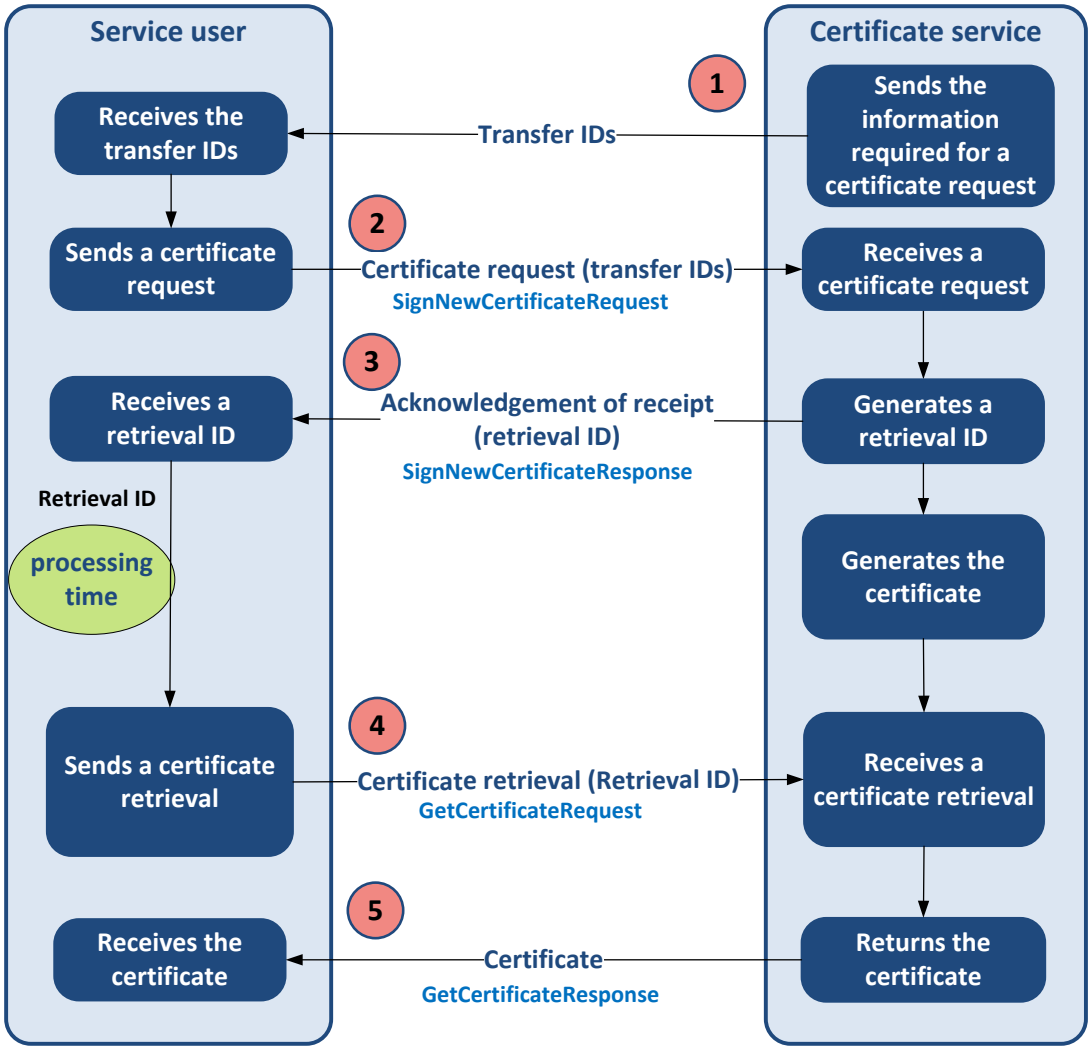

Figure 1. Requesting and retrieving a new certificate.

The customer agrees with the Incomes Register on the use of the services. The certificate service sends the information required for making a certificate request: the transfer ID and a one-time password. 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 signing request is not made within this time period, the one-time password will expire and the customer must begin certificate generation from the start. The transfer ID and one-time password are delivered to the customer in a secure e-mail 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 being generated for retrieval. The certificate is obtained as a response to a certificate retrieval service call to which the retrieval ID has been attached. The customer now has the certificate required to use the services of the Incomes Register.

3.2 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 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 can be revoked by contacting the Incomes Register. The contact details for certificate revocation will be specified at a later date. When a customer asks for a certificate to be revoked, it is first revoked temporarily, i.e., set on hold (Certificate Hold). This means that the use of the certificate is prevented but the certificate can still be reactivated. The Incomes Register processes the revocation request during office hours. If the revocation request is confirmed, the certificate is revoked permanently. A certificate revocation request found to be incorrect or unnecessary can be cancelled, and the certificate reactivated.

A permanently revoked certificate cannot be returned to use or renewed; the customer must request a new certificate. The request and retrieval of the new certificate is then performed in the same way as when ordering a certificate for the first time.

3.3 Life cycle and renewal of certificates

Customer certificates remain valid for a maximum of two years. Certificate holders must check the validity of their certificates regularly. Certificates about to expire can be renewed using the certificate renewal function of the certificate service no earlier than sixty (60) days before the expiration of the certificate. The old certificate remains valid until the end of the original validity period. When a certificate is renewed during the validity period of an existing certificate, there is no need to order a new transfer ID and one-time password.

If the certificate expires, the customer must contact the Incomes Register and order a new certificate. The request and retrieval of the new certificate is then performed in the same way as when ordering a certificate for the first time.

The renewal of a certificate is presented in Figure 2.

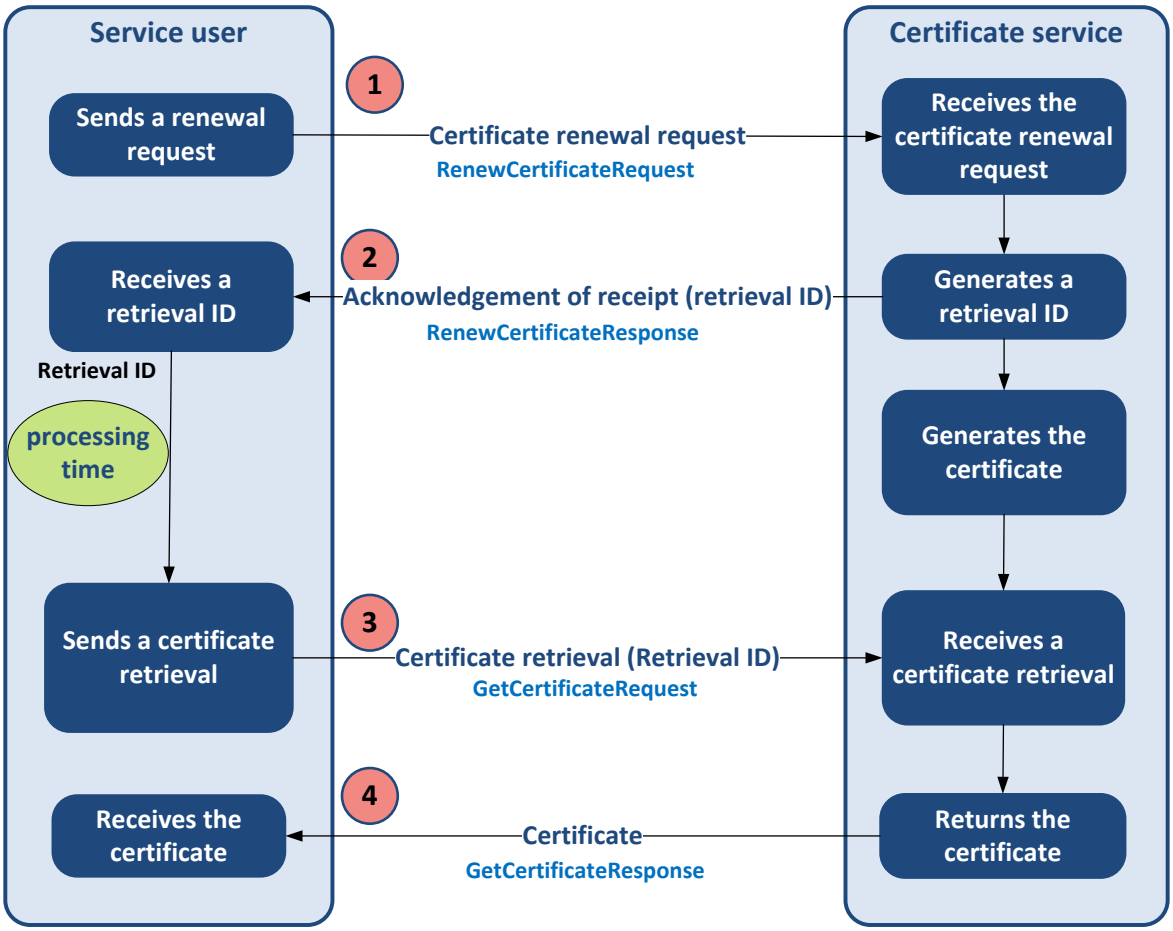

Figure 2. Renewal of a certificate.

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.

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.

3.4 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 processed, and the error is returned in connection with certificate retrieval.

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 service call that resulted in an error must be repeated after the possible correction of the error situation.

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 SFTP CHANNEL

A PKI key pair is used for customer authentication in the Incomes Register's SFTP channel. Authentication takes place as follows: the Incomes Register possesses the public key of the key pair, and the customer authenticates himself/herself by using his/her private key.

The certificate is issued in the same way as the other certificates. The purpose of use of the SFTP channel certificate (and the related key pair) is different from other certificates. The certificate can be used to sign records, and the connected key pair can be used for authentication in the SFTP channel. However, it cannot be used for authentication in the Web Service channel.

5 TESTING THE SERVICE

The testing of the technical interface is agreed with the Incomes Register. Testing occurs in the testing environment of the certificate service, from where a testing certificate is issued to the customer for testing the Incomes Register's technical interface. More detailed instructions and the terms and conditions of use for stakeholder testing will be published on page Stakeholder testing.