

Configuration Guide

KATRE

Document Version: 1.0 – 2018-11-05

CUSTOMER

Reporting to the Incomes Register (KATRE)

Using Web Services with SAP Cloud Platform Integration

Typographic Conventions

Type Style	Description
<i>Example</i>	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Textual cross-references to other documents.
Example	Emphasized words or expressions.
EXAMPLE	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
Example	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
Example	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example>	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
EXAMPLE	Keys on the keyboard, for example, F2 or ENTER.

Document History

Version	Date	Change
1.0	2018-11-05	Initial instructions for the Pilot version.

Contents

1	Prerequisites.....	5
2	SOAMANAGER configuration	6
2.1	Certificate service.....	6
2.2	Wage Report service	11
2.3	Status service	11
2.4	Invalidation service.....	11
3	Obtaining a certificate.....	12
3.1	Creating a new identity in STRUST	12
3.2	Saving Certificate Request (CSR).....	13
3.3	Certificate Service report	14
3.4	Exporting certificate to PKCS#12	17
4	SAP Cloud Platform Integration (CPI)	18
4.1	Uploading Key Pair to Keystore.....	18
4.2	Uploading Certificates to Keystore	19
4.3	Configuring iFlows	21
5	Resources	24

1 Prerequisites

The main SAP Note with the KATRE solution:

- **2679935** - HRFI: The National Incomes Register project (KATRE)



Please, make sure that the *SAP Cloud Platform Integration* is setup as a **trusted system** (i.e. all certificates are in place).

2 SOAMANAGER configuration

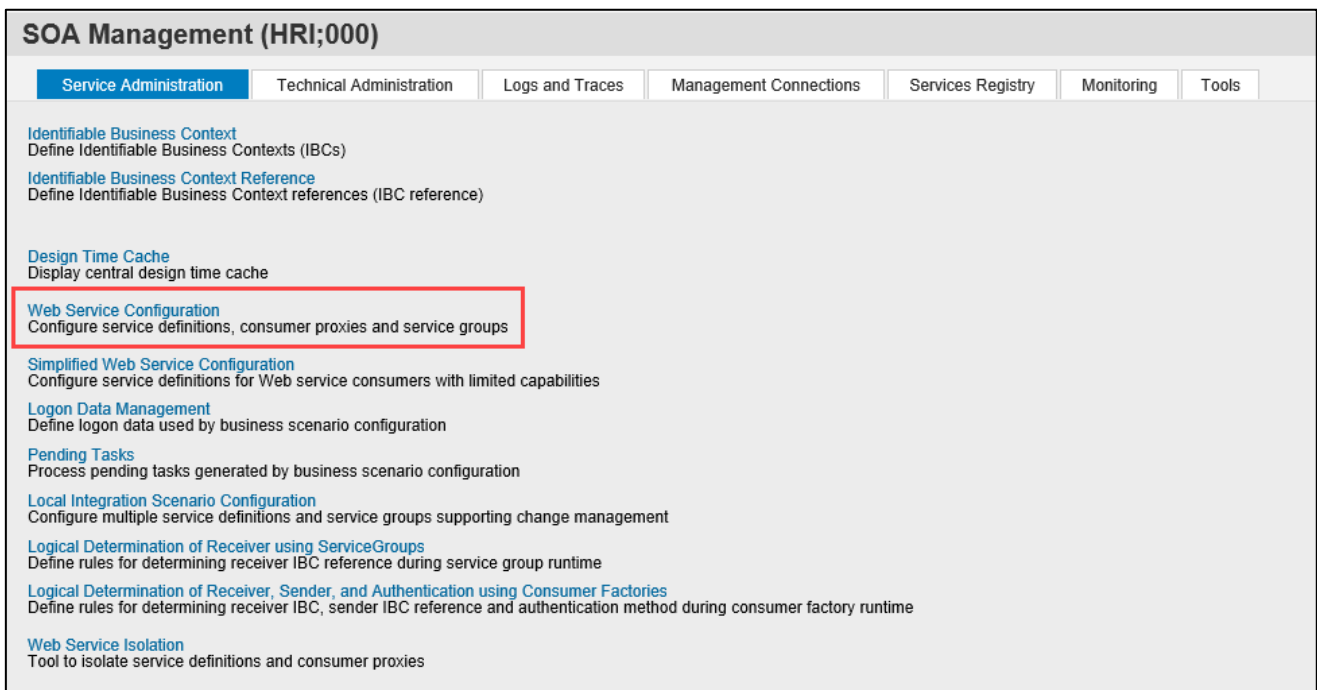
SOA Manager is a transaction for configuring and monitoring Web Services. It is run in a web browser.

Note

Some details (names of tabs etc.) might be slightly different depending on your release version.

2.1 Certificate service

1. Execute the transaction code **SOAMANAGER**. This opens a new window in your web browser.
2. In the **Service Administration** tab, click [Web Service Configuration](#) link.



The screenshot shows the SOA Management (HRI;000) interface. At the top, there is a title bar and a navigation menu with tabs: Service Administration (selected), Technical Administration, Logs and Traces, Management Connections, Services Registry, Monitoring, and Tools. Below the tabs, the main content area lists several configuration options:

- [Identifiable Business Context](#)
Define Identifiable Business Contexts (IBCs)
- [Identifiable Business Context Reference](#)
Define Identifiable Business Context references (IBC reference)
- [Design Time Cache](#)
Display central design time cache
- [Web Service Configuration](#)
Configure service definitions, consumer proxies and service groups
- [Simplified Web Service Configuration](#)
Configure service definitions for Web service consumers with limited capabilities
- [Logon Data Management](#)
Define logon data used by business scenario configuration
- [Pending Tasks](#)
Process pending tasks generated by business scenario configuration
- [Local Integration Scenario Configuration](#)
Configure multiple service definitions and service groups supporting change management
- [Logical Determination of Receiver using ServiceGroups](#)
Define rules for determining receiver IBC reference during service group runtime
- [Logical Determination of Receiver, Sender, and Authentication using Consumer Factories](#)
Define rules for determining receiver IBC, sender IBC reference and authentication method during consumer factory runtime
- [Web Service Isolation](#)
Tool to isolate service definitions and consumer proxies

The [Web Service Configuration](#) link and its description are highlighted with a red rectangular box.

- Then in the *Search Criteria* section, type the Object Name **CO_HRPAYFIIR_CERTIFICATE_SERVI**.

Web Service Configuration (HRI;000)

Design Time Object Search Configuration Search

Search Criteria

Object Type is All

Object Name contains **CO_HRPAYFIIR_CERTIF**

Maximum Number of Results: 100

Search Clear Values Reset Search Criteria

Search Result

Internal Name	Name
CO_HRPAYFIIR_CERTIFICATE_SERVI	CertificateServicesPortType

- Click the Internal name **CO_HRPAYFIIR_CERTIFICATE_SERVI**.
- In the **Configurations** tab, click the *Create* button and select *Manual Configuration*.

Web Service Configuration (HRI;000)

Details of Consumer Proxy: CO_HRPAYFIIR_CERTIFICATE_SERVI

Overview Configurations Details

Define Logical Ports

Create Set Log Port Default Activate Deactivate Delete

WSDL Based Configuration Logical Port

Manual Configuration

Process Integration Runtime

Local Shortcut Configuration

Service Registry Based Configuration

Template Based Configuration

WSDL based Configuration with Template

- Step 1 - **Logical Port name:**
 - Logical Port Name:* **CPI_SIGN**
 - Description:* **CPI port for SignNewCertificate**

Web Service Configuration (HRI;000)

New Manual Configuration of Logical Port for Consumer Proxy 'CO_HRPAYFIIR_CERTIFICATE_SERVI'

1 2 3 4 5 6

Logical Port Name Consumer Security HTTPSettings SOAP Protocol Identifiable Business Context Operation Settings

Back Next Finish Cancel

General Configuration Settings

* Logical Port Name: CPI_SIGN

Description: CPI port for SignNewCertificate operation|

7. Click *Next*.

8. Step 2 - **Consumer Security**:

- o *Authentication Settings*: **User ID / Password**
- o *User Name*: <CPI admin's user name>
- o *Password*: <CPI admin's password>

9. Click *Next*.

10. Step 3 - **HTTPSettings**:

- o *URL*: <URL to your CPI tenant>/**cx**f/HCI/PAYROLL/FI/KATRE/SIGN_NEW_CERTIFICATE
- o *Proxy*: setup the proxy if it's used in your company
- o Leave other fields with their default values.

11. Click *Next*.

12. Step 4 - **SOAP Protocol**:

- o *Message ID Protocol*: **Suppress ID Transfer**
- o *Data transfer scope*: **Enhanced Data Transfer**
- o *Transfer protocol*: **Transfer via SOAP header**
- o *Process Attachments*: **No**

Web Service Configuration (HRI;000)
New Manual Configuration of Logical Port for Consumer Proxy 'CO_HRPAYFIIR_CERTIFICATE_SERVI'

1 Logical Port Name 2 Consumer Security 3 HTTPSettings 4 **SOAP Protocol** 5 Identifiable Business Context 6 Operation Settings

Back Next Finish Cancel

Message ID (Synchronous)
Message ID Protocol: Suppress ID Transfer

Metering of Service Calls
Data transfer scope: Enhanced Data Transfer
Transfer protocol: Transfer via SOAP header

Message Attachment Handling
Process Attachments: No

13. Click *Next*.

14. Step 5 - **Identifiable Business Context**:

- o *Leave everything blank*

Web Service Configuration (HRI;000)
New Manual Configuration of Logical Port for Consumer Proxy 'CO_HRPAYFIIR_CERTIFICATE_SERVI'

1 Logical Port Name 2 Consumer Security 3 HTTPSettings 4 SOAP Protocol 5 **Identifiable Business Context** 6 Operation Settings

Back Next Finish Cancel

Identifiable Business Context
Sender IBC Identifier:
Receiver IBC Identifier:
Suppress sending of IBC Identifier:

15. Click *Next*.

16. Step 6 - **Operation Settings**:

- o *Leave everything default*

Web Service Configuration (HRI;000)
New Manual Configuration of Logical Port for Consumer Proxy 'CO_HRPAYFIIR_CERTIFICATE_SERVI'

1 Logical Port Name 2 Consumer Security 3 HTTPSettings 4 SOAP Protocol 5 Identifiable Business Context 6 **Operation Settings**

Back Next Finish Cancel

Operation
getCertificate
renewCertificate
signNewCertificate

Transport Binding
 Use non-default value for SOAP Action
SOAP Action:

WS Addressing
 Use non-default value for Inbound Message Action
Inbound Message Action:

17. Click *Finish*.

Define another two logical ports (repeat points 5 to 17) for this Proxy. The only differences are below:

Port CPI_GET

- Step 1 - **Logical Port name:**
 - *Logical Port Name:* **CPI_GET**
 - *Description:* **CPI port for GetCertificate**
- Step 3 - **HTTPSettings:**
 - *URL:* **<URL to your CPI tenant>/cxf/HCI/PAYROLL/FI/KATRE/GET_CERTIFICATE**

Port CPI_RENEW

- Step 1 - **Logical Port name:**
 - *Logical Port Name:* **CPI_RENEW**
 - *Description:* **CPI port for RenewCertificate**
- Step 3 - **HTTPSettings:**
 - *URL:* **<URL to your CPI tenant>/cxf/HCI/PAYROLL/FI/KATRE/RENEW_CERTIFICATE**

Note

The following chapters describe the same process, only with different values in some of the parameters.

2.2 Wage Report service

Proxy CO_HRPAYFIIR_WAGE_REPORT_PORT

Port CPI_WR

- Step 1 - Logical Port name:
 - *Logical Port Name:* CPI_WR
 - *Description:* CPI port for WageReportsToIR
- Step 3 - HTTPSettings:
 - *URL:* <URL to your CPI tenant>/cxf/HCI/PAYROLL/FI/KATRE/SEND_WAGE_REPORTS

2.3 Status service

Proxy CO_HRPAYFIIR_STATUS_PORT

Port CPI_STATUS

- Step 1 - Logical Port name:
 - *Logical Port Name:* CPI_STATUS
 - *Description:* CPI port for StatusRequestToIR
- Step 3 - HTTPSettings:
 - *URL:* <URL to your CPI tenant>/cxf/HCI/PAYROLL/FI/KATRE/GET_STATUS

2.4 Invalidation service

Proxy CO_HRPAYFIIR_INVALIDATION_PORT

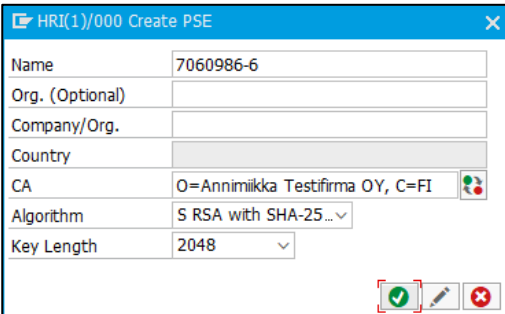
Port CPI_WR

- Step 1 - Logical Port name:
 - *Logical Port Name:* CPI_INV
 - *Description:* CPI port for InvalidationsToIR
- Step 3 - HTTPSettings:
 - *URL:* <URL to your CPI tenant>/cxf/HCI/PAYROLL/FI/KATRE/SEND_INVALIDATIONS

3 Obtaining a certificate

3.1 Creating a new identity in STRUST

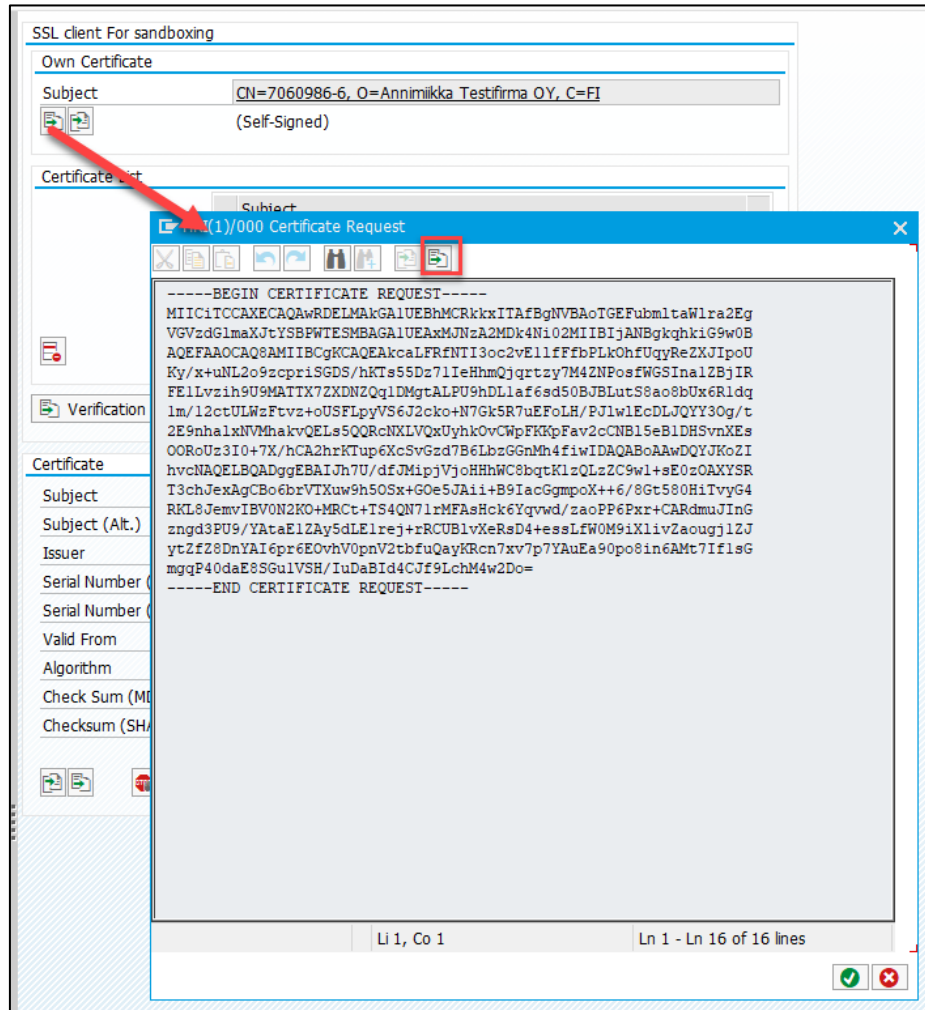
1. Open the transaction **STRUST** in the *Change mode*.
2. Create a new **SSL Client Identity**:
 - o In the menu: *Environment* → *SSL Client identities*
 - o Click *New entries* and enter identity **name** and **description**.
 - o *Right-click* the newly created identity
 - o Choose **Create**
 - o Fill the fields:
 - o *Name*: <Business ID>
 - o *CA*: O=<Name of your organization>, C=FI
 - o *Algorithm*: RSA with SHA-256
 - o *Key Length*: 2048



HRI(1)/000 Create PSE	
Name	7060986-6
Org. (Optional)	
Company/Org.	
Country	
CA	O=Annimikka Testifirma OY, C=FI
Algorithm	S RSA with SHA-25...
Key Length	2048

3.2 Saving Certificate Request (CSR)

1. In the **STRUST** transaction, double-click your **SSL Client Identity (PSE)**.
2. In the **Own certificate** section, click the *Create certificate request* button.
3. Save the **Certificate Request (CSR)** as a *local file* by click the rightmost button in the pop-up.



3.3 Certificate Service report

The Certificate Service report **HFIIRCERT** (transaction **PC00_M44_IR_CERT**) can be used for obtaining a new certificate or renewing an existing one.

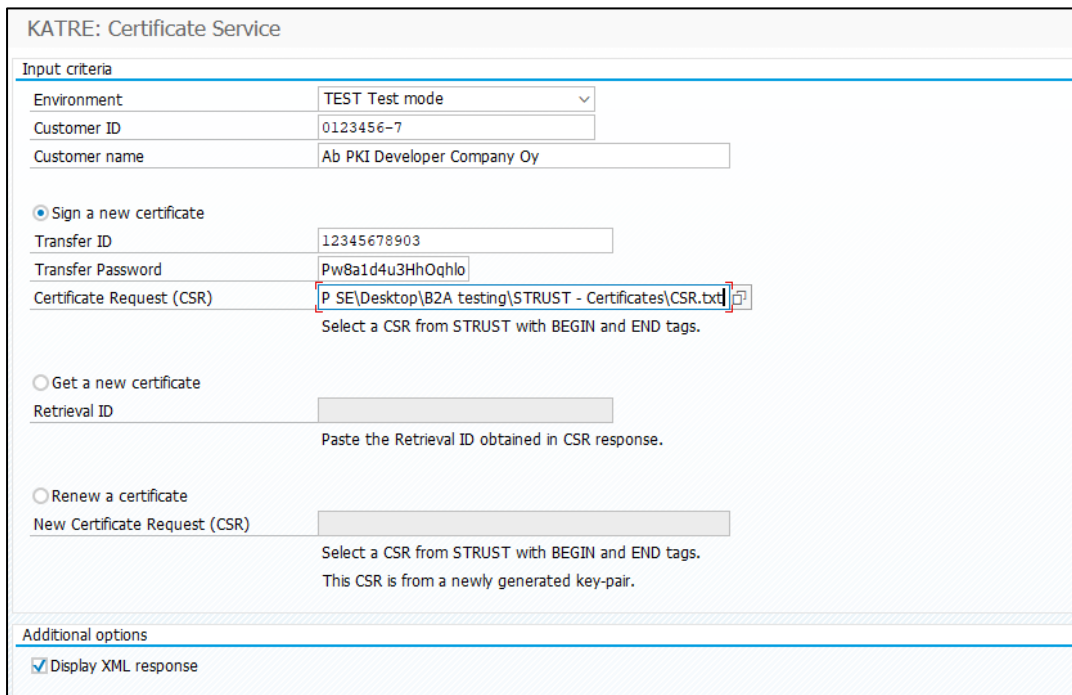
Note

A certificate is needed for signing submission with an *XML digital signature* and for *SSL communication*.

1. Open the transaction **PC00_M44_IR_CERT**.
2. Fill the selection screen with **your data** and select the first radiobutton *Sign a new certificate*.
3. Press **F4** to select a *Certificate Request (CSR)* saved from the **STRUST** transaction.

Example

This is an example of how you can call the KATRE's Certificate Test Bench (for testing the Certificate Service):



KATRE: Certificate Service	
Input criteria	
Environment	TEST Test mode
Customer ID	0123456-7
Customer name	Ab PKI Developer Company Oy
<input checked="" type="radio"/> Sign a new certificate	
Transfer ID	12345678903
Transfer Password	Pw8a1d4u3HhOqhlo
Certificate Request (CSR)	P SE\Desktop\B2A testing\STRUST - Certificates\CSR.txt
Select a CSR from STRUST with BEGIN and END tags.	
<input type="radio"/> Get a new certificate	
Retrieval ID	
Paste the Retrieval ID obtained in CSR response.	
<input type="radio"/> Renew a certificate	
New Certificate Request (CSR)	
Select a CSR from STRUST with BEGIN and END tags. This CSR is from a newly generated key-pair.	
Additional options	
<input checked="" type="checkbox"/> Display XML response	

4. If you run the report with the option *Display XML response*, the **XML** received from the authority is displayed in the next screen. Press *Back* (F3) to continue.

- Copy/Save the **Retrieval ID** from the next screen.

KATRE: Certificate Service	
KATRE: Certificate Service	
Sign a new certificate request	
Status:	OK
Retrieval ID:	13891176534882152123
Please, save the Retrieval ID for the next step in the process!	



Caution

Please, make sure to **save the Retrieval ID**, it will be needed in the next step of the process!



Caution

If an error in the process occurs, it is displayed on the screen. Please, check the configuration and try again.

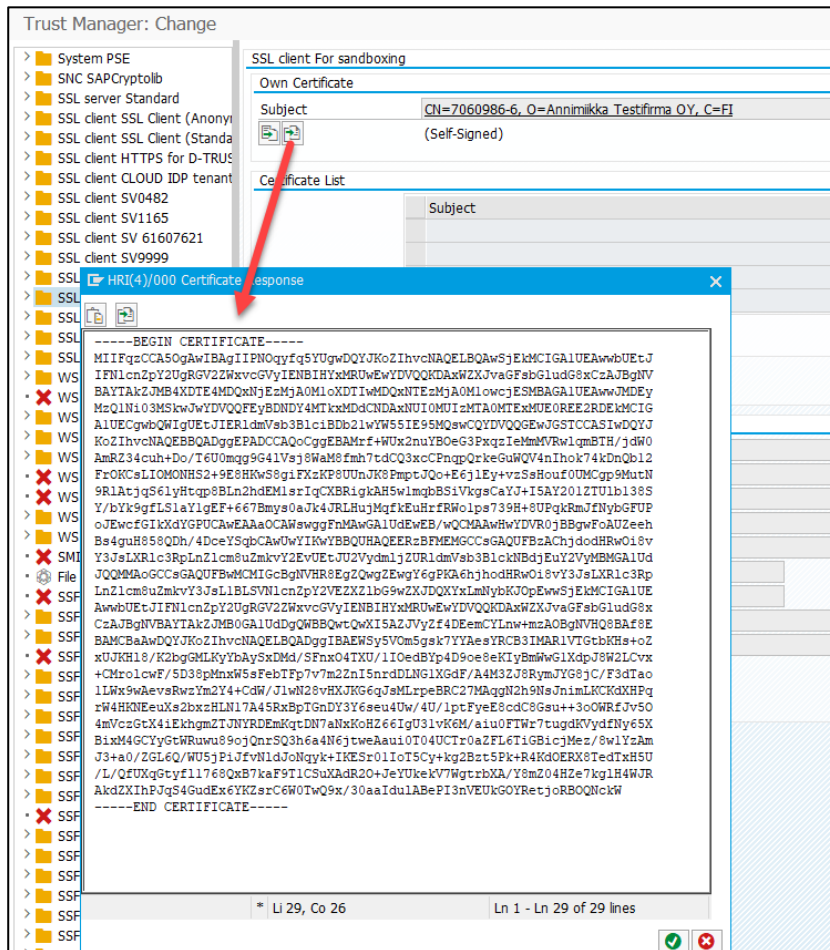
- Return (F3) to the selection screen and select the second radiobutton *Get a new certificate* to finish the process of obtaining a new certificate.
- Enter the **Retrieval ID** from the previous steps.
- After running the report, you should get a screen with a **certificate** itself.

KATRE: Certificate Service	
KATRE: Certificate Service	
Get a new certificate request	
Status:	OK
Certificate:	
-----BEGIN CERTIFICATE-----	
<pre> MIIFqzCCAS0gAwIBAgIIPN0yqf5YUgWdQYJKoZIhvcNAQELBQAwSjEKMCIgA1UEAwBUEtJ IFNlcnZpY2UgRGV2ZWxvcGVyIENBIHxMRUwEwYDVQQKDAxWZXJvaGFsbG8xZm9udG8x CzAxBgNVBAYTAkZJMB4XDTE4MDQxNjEzMDUxMjEwMDQxNTEzMDUxMjEwMDUxMjEwMDUx MzQ1Ni03MSkwYVYVQ0FEyBDNDY4MTkxMDcNDAAxNUIzMTA0MTExMUE0REER2ERDEKMCIG A1UECgwBQWVtJER1dmVsb3BlciBDb2lW55IE95MQswCQYDVQQGEwJGStCCAS1wDQYJ KoZIhvcNAQEBBQADggEPADCCAQoCggEBAMrf+WUx2nuYBOeG3PqxqIeMmVrWlqmBTH/jdW0 AmRZ34cuh+Do/T6U0mqg9G41Vsj8WaM8fmh7tdCQ3xcCPnqpQrkeGuWQV4nIhok74kDnQb12 FrOKCsLIOMONHS2+9E8HKwS8giFXzKP8UUnJK8PmptJQo+E6j1Ey+VzSsHouf0UMCqp9MutN 9R1RtjqS61yHtqp8BLn2hdEM1srIqCXBRIgkAH5wlmqBBSiVkgScaYJ+I5AY201ZTU1b138S Y/bYk9gfLS1aYlgEF+667Bmys0aJk4JRLHujMgfkEuHrfRw0lps739H+8UPqkRmJfNybgFUP oJEwfgIkXdyGpUCAwEAaOCAswggFnMAwGAlUdEwEB/wQCMAAwHwYDVR0jBBgwFoAUZeeh Be4guH858Qdh/4DceYSqbCawUwYIKwYBBQUHAQEERzBFMEMGCCsGAQUFBzAChjdodHRwOi8v Y3JseLXRlc3R3LnZlcm8uZmkvY2EvUEtJU2VydmljZUR1dmVsb3BlckNBdJEUy2VyMBMGA1Ud JQMMAoGCCsGAQUFBwMCMIGcBgnVHR8EgZQwgZEwgY6gPKA6hjhodHRwOi8vY3JseLXRlc3R3 LnZlcm8uZmkvY3JseL1BL5VN1cnZpY2VEZXZlbG9wZXJkXGdF/A4M3Zj8RymJYg6jC/F3dTao 1LWx9wAevsRwzYm2Y4+Cdw/J1wN28vHXJKG6qJmLrpeBRC27MAqgN2h9NsJnimLKCKdXHPq rW4HKNEuXs2bxsHLN17A45RxBpTGNdy3Y6seu4Uw/4U/lptFyeE8cdC8Gsu++3oOWRFJv50 4mVczGtX4iEkghmZTjNVRDEmKqtDN7aNXK0h266IqU31vK6M/aiu0FTw7tugdkVdyfNy65X BixM4GcYyGtWruw89ojQnrS3h6a4N6jtweAaui0T0UCTr0aZFL6TiGbicjMez/6w1YzAm J3+a0/ZGL6Q/WU5pPiJfVn1dJoNqyk+IKEsr01IoT5Cy+kg2Bzt5Pk+R4KdOERX8TedTxH5U /JL/QfUXgGtyf11768QxB7kaF9T1CSuXAdR20+JeYUkeKv7WgtrbXA/Y8m204Hze7kg1H4WJR Akd2XhPjS4GudEx6YKzsrC6W0Tq9x/30aaIduLABEPI3nVEUKGOYRetjorBBOQnckW -----END CERTIFICATE----- </pre>	
Please, copy the whole Certificate into STRUST as a Certificate response!	

Caution

Please, make sure to **save the Certificate**, it will be needed in the next step of the process!

- Copy the whole certificate (including the BEGIN/END sections) to your clipboard.
- Open the **STRUST** transaction in the edit mode and double-click your **SSL Client Identity (PSE)**.
- In the **Own certificate** section, click the *Import certificate response* button.
- Paste the copied certificate to the pop-up window.



- Confirm the pup-up window and *Save* the PSE.

Note

To **renew an existing certificate**, follow the same procedure; only choose the third radiobutton and select a CSR generated from a *new SSL Client Identity*. For more information about the process, please, refer to the Incomes Register website.

3.4 Exporting certificate to PKCS#12

To be able to upload the obtained certificate to the *SAP Cloud Platform Integration*, it needs to be exported to the **PKCS#12 format**. To do so, you need to get the **SAP GenPSE command-line tool**.

Note

The SAP GenPSE command-line tool can be downloaded from the SAP Support portal.

1. Open the **STRUST** transaction in the edit mode and select your *SSL Client identity (PSE)*.
2. In the menu, select *PSE* → *Export* and save the PSE file to a local file system.

Example

The default location is `C:\Users\<>your_user>\AppData\Local\sec\<>pse_file>.pse`

3. Open the command line and perform the following command:

```
sapgenpse export_p12 [options] -p <pse_file> <filename>.p12
```

```
C:\Users\<user>\AppData\Local\SAPCRYPTOLIB>sapgenpse.exe export_p12 -v -p STRUST.pse CERTIFICATE.p12
Trying to open PSE STRUST.pse
Opening PSE "C:\Users\<user>\AppData\Local\sec\STRUST.pse"...
No SSO credentials found for this PSE.
PSE (v2) open ok.
PSE "C:\Users\<user>\AppData\Local\sec\STRUST.pse" opened ok.
Please enter PKCS#8 encryption password:
For verification, please reenter password:

!!! WARNING: For security reasons it is recommended to use a PIN/passphrase
!!! WARNING: which is at least 8 characters long and contains characters in
!!! WARNING: upper and lower case, numbers and non-alphanumeric symbols.

Trying to build PKCS#12 container...
PKCS#12 container creation OK.
Trying to write PKCS#12 container (10490 Bytes)
to file "CERTIFICATE.p12" ... OK.
```

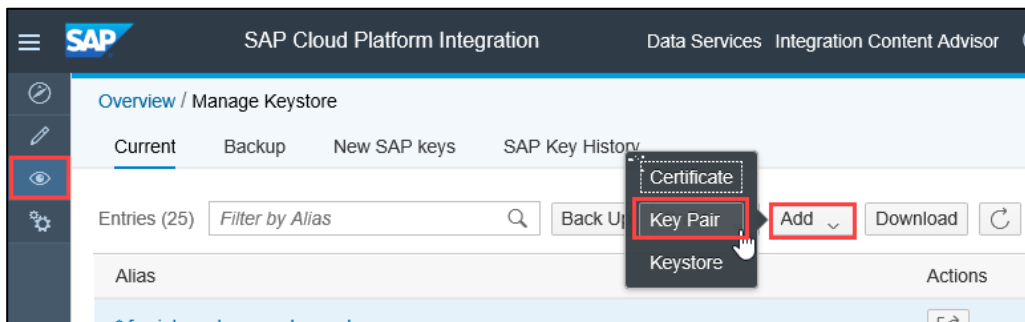
4. Enter the **password**, which will be needed later.
5. Now you have the certificate exported in the desired format for the CPI.

4 SAP Cloud Platform Integration (CPI)

SAP Cloud Platform Integration (CPI) cockpit can be accessed via a link provided with your CPI tenant. Keep in mind that you have to configure the **Test** tenant as well as the **Productive** one (after the testing phase).

4.1 Uploading Key Pair to Keystore

1. In the CPI, open the *Overview* section.
2. In the *Manage Security* section, click the **Keystore** tile.
3. Click the *Add* button and select **Key Pair**.



4. In the pop-up window, enter the **Alias** for the Key Pair (e.g. *katre_customer_pk*). Then select the **.p12 file** extracted from the **STRUST** and enter the **password to the .p12 file**.
5. Press *Deploy*.

Now you have a Key Pair deployed in the CPI that can be used for XML Digital Signature and the SSL communication.

i Note

For renewing an existing certificate, you need to deploy a new Key Pair under a different Alias, or you can rename the old one to prevent re-configuration of the iFlows.

4.2 Uploading Certificates to Keystore

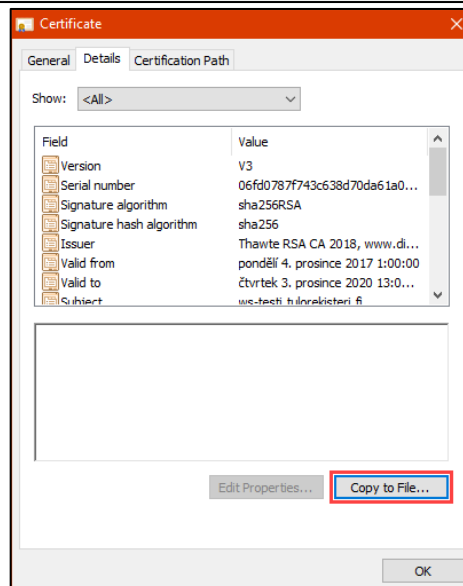
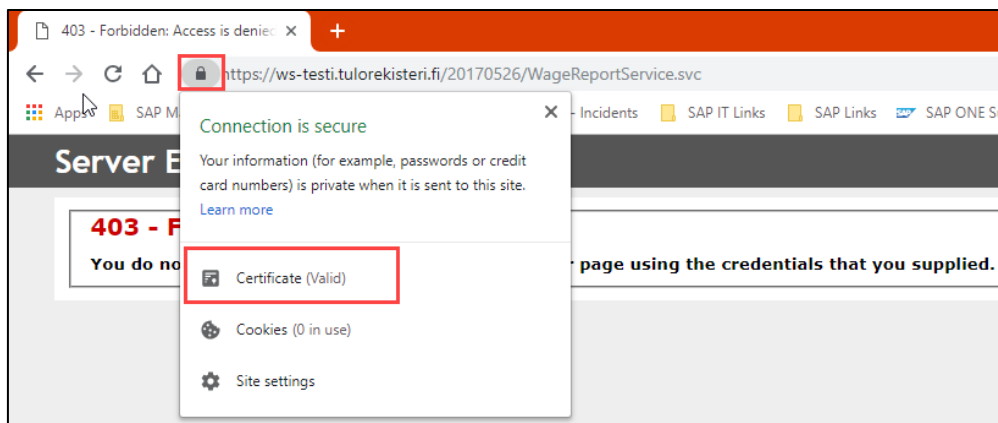
You also need two additional Certificates for the communication with:

- **Incomes Register's Web Services** (Wage report, Invalidation and Status service)
- **Certificate Service**

To do so, you have to download the certificates using your **Web browser**. Just open the address of the web service (e.g. <https://ws-testi.tulorekisteri.fi/20170526/WageReportService.svc>) and download the certificate from there.

Example

An example in the Google Chrome:

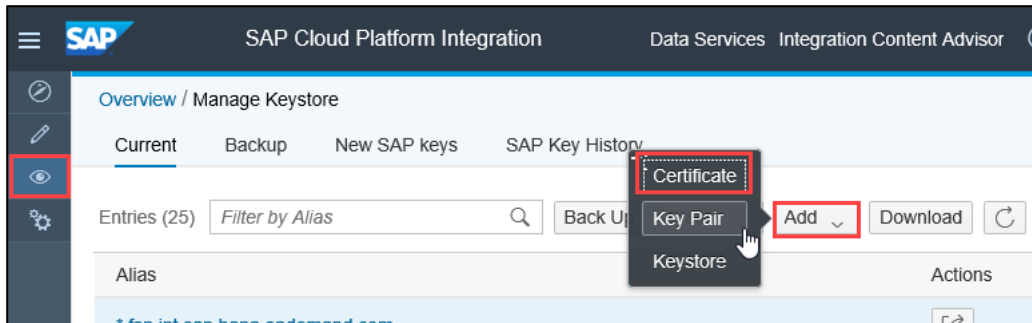


Note

The Incomes Register may supply these certificates in another way in the future (e.g. download from KATRE website).

After you have downloaded the certificates, perform the following steps for both of them:

1. In the CPI, open the *Overview* section.
2. In the *Manage Security* section, click the **Keystore** tile.
3. Click the *Add* button and select **Certificate**.



4. In the pop-up window, enter the *Alias* and choose the *File* with a certificate.

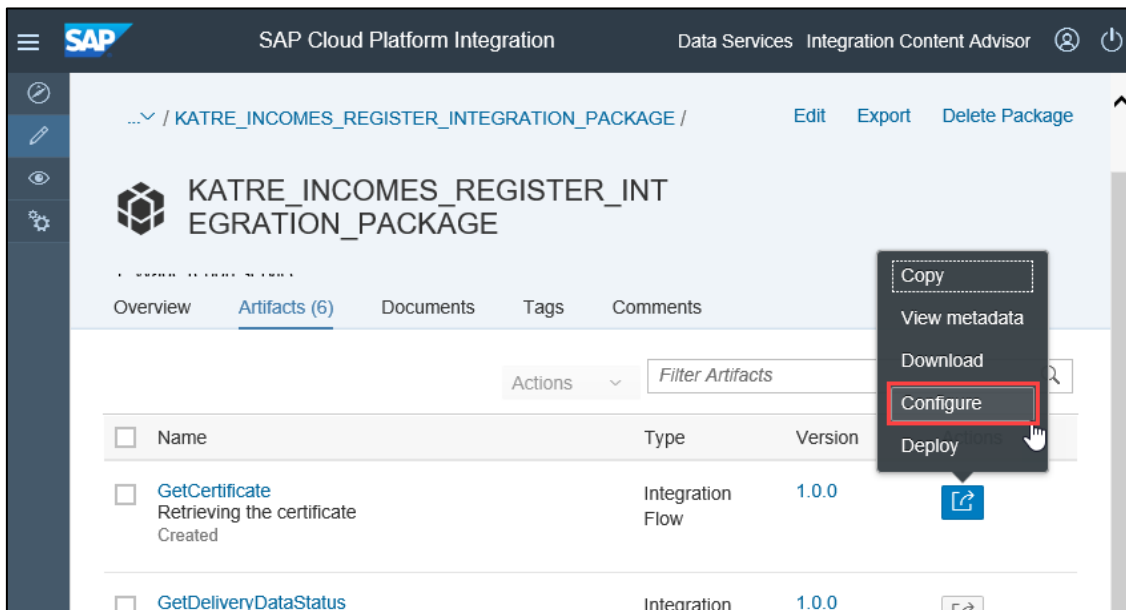
 **Caution**

Remember that the **Aliases** of Certificates and Key Pairs will be used in the iFlow configurations.

4.3 Configuring iFlows

After you have downloaded the **KATRE Integration Package** in the *Discover* section of the SAP Cloud Platform Integration cockpit, you have to configure the Integration flows (iFlows) contained in it.

1. In the CPI, open the KATRE Integration Package and select the *Artifacts* section.
2. For every iFlow, click the button *Actions* and choose **Configure**.



3. Configure so-called **Externalized Parameters** according to your preferences (e.g. certificate's Aliases). The parameters' details are shown in the table below.

Caution

The default values are set up for the **Testing environment**. In your **Productive tenant**, you have to configure these iFlows according to authority's specifications provided for the productive environment.

GetCertificate

Parameter name	Default value	Section
URL to WSDL	/wsdl/CertificateServices.wsdl	Sender
Address	https://pkiws-testi.vero.fi/DEV/2017/10/CertificateServices	Receiver
URL to WSDL	/wsdl/CertificateServices.wsdl	Receiver
Private Key Alias	katre_cert_service	Receiver

GetDeliveryDataStatus

Parameter name	Default value	Section
URL to WSDL	/wsdl/StatusService.wsdl	Sender
Address	https://ws-testi.tulorekisteri.fi/20170526/StatusService.svc	Receiver
URL to WSDL	/wsdl/StatusService.wsdl	Receiver
Private Key Alias	katre_customer_pk	Receiver
Private Key Alias	katre_customer_pk	More
Namespace	http://www.tulorekisteri.fi/2017/1/StatusRequestToIR	More

RenewCertificate

Parameter name	Default value	Section
URL to WSDL	/wsdl/CertificateServices.wsdl	Sender
Address	https://pkiws-testi.vero.fi/DEV/2017/10/CertificateServices	Receiver
URL to WSDL	/wsdl/CertificateServices.wsdl	Receiver
Private Key Alias	katre_old_customer_pk	Receiver
Private Key Alias	katre_old_customer_pk	More
Namespace	http://certificates.vero.fi/2017/10/certificateservices	More

SendInvalidations

Parameter name	Default value	Section
URL to WSDL	/wsdl/InvalidationService.wsdl	Sender
Address	https://ws-testi.tulorekisteri.fi/20170526/InvalidationService.svc	Receiver
URL to WSDL	/wsdl/InvalidationService.wsdl	Receiver
Private Key Alias	katre_customer_pk	Receiver
Private Key Alias	katre_customer_pk	More
Namespace	http://www.tulorekisteri.fi/2017/1/InvalidationsToIR	More

SendWageReports

Parameter name	Default value	Section
URL to WSDL	/wsdl/WageReportService.wsdl	Sender
Address	https://ws-testi.tulorekisteri.fi:443/20170526/WageReportService.svc	Receiver
URL to WSDL	/wsdl/WageReportService.wsdl	Receiver
Private Key Alias	katre_customer_pk	Receiver
Private Key Alias	katre_customer_pk	More
Namespace	http://www.tulorekisteri.fi/2017/1/WageReportsToIR	More

SignNewCertificate

Parameter name	Default value	Section
URL to WSDL	/wsdl/CertificateServices.wsdl	Sender
Address	https://pkiws-testi.vero.fi/DEV/2017/10/CertificateServices	Receiver
URL to WSDL	/wsdl/CertificateServices.wsdl	Receiver
Private Key Alias	katre_cert_service	Receiver

Explanation of Private Key Aliases

Private Key Alias	Explanation
katre_customer_pk	Key Pair downloaded from the STRUST. Obtained by the Certificate Service report.
katre_old_customer_pk	Key Pair from the currently valid certificate that is about to be renewed.
katre_cert_service	Certificate for the Certificate service downloaded from a web browser.
katre_web_services	Certificate for the KATRE's Web services downloaded from a web browser.

4. After you configure all the iFlows, select *Actions* → *Deploy*.

5 Resources

- Incomes Register website:
 - <https://www.vero.fi/en/incomes-register/>

A background image of dandelion seeds floating in the air against a light blue sky. The seeds are in various stages of dispersal, with some showing their characteristic white, feathery parachutes and others showing the dark, oval-shaped seed heads.

www.sap.com/contactsap

© 2016 SAP SE or an SAP affiliate company. All rights reserved.
No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.
SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices.

Material Number:

