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
Example	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

The main SAP Note with the KATRE solution:

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

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

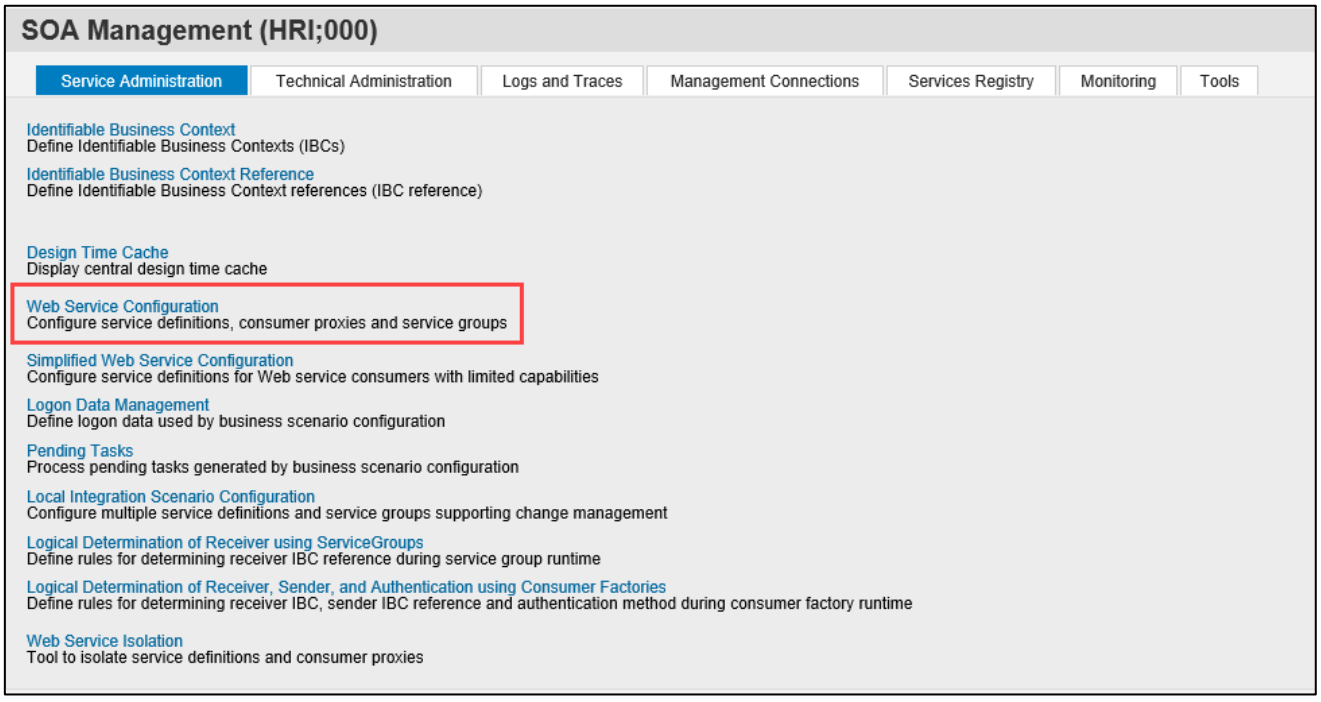
2 SOAMANAGER configuration

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

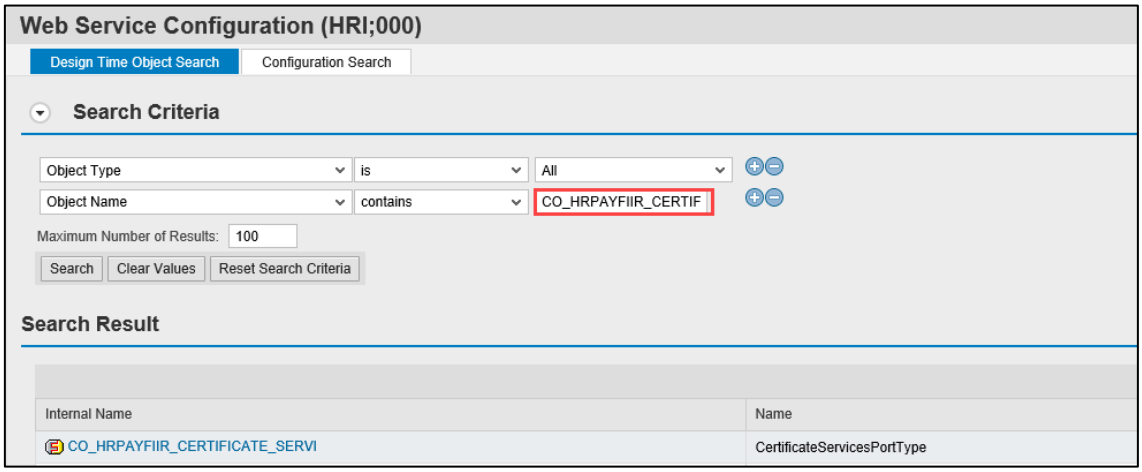
> **Note**
>
> Some details (names of tabs etc.) might be slightly different depending on your release version.

2.1 Certificate service

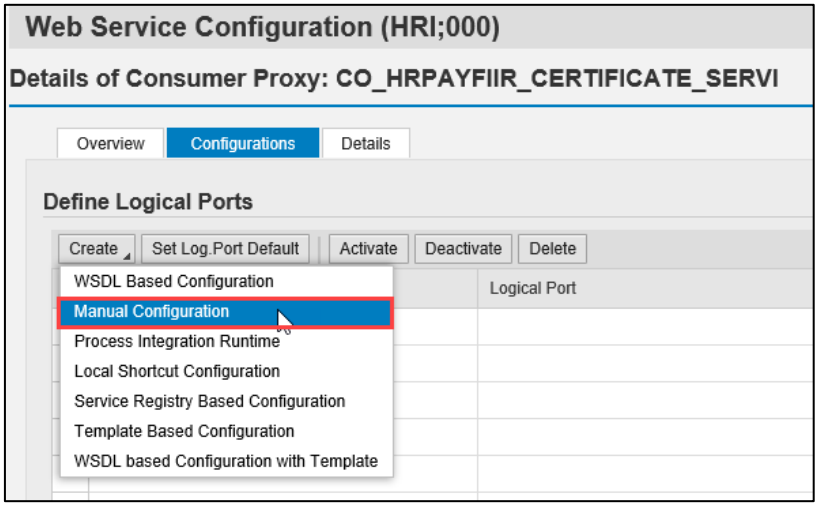
1. Execute the transaction code **SOAMANAGER**. This opens a new window in your web browser.
2. In the **Service Administration** tab, click *Web Service Configuration* link.



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

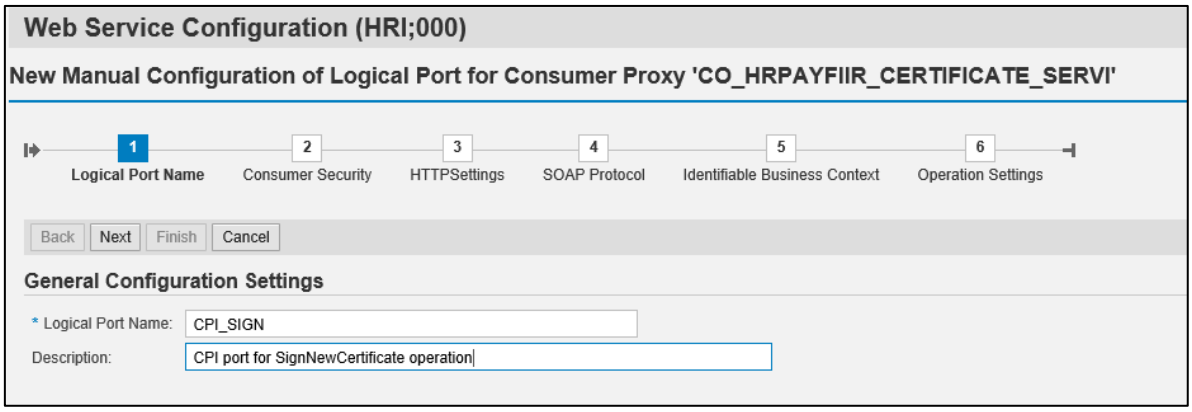


4. Click the Internal name **CO_HRPAYFIIR_CERTIFICATE_SERVI**.
5. In the **Configurations** tab, click the *Create* button and select *Manual Configuration*.

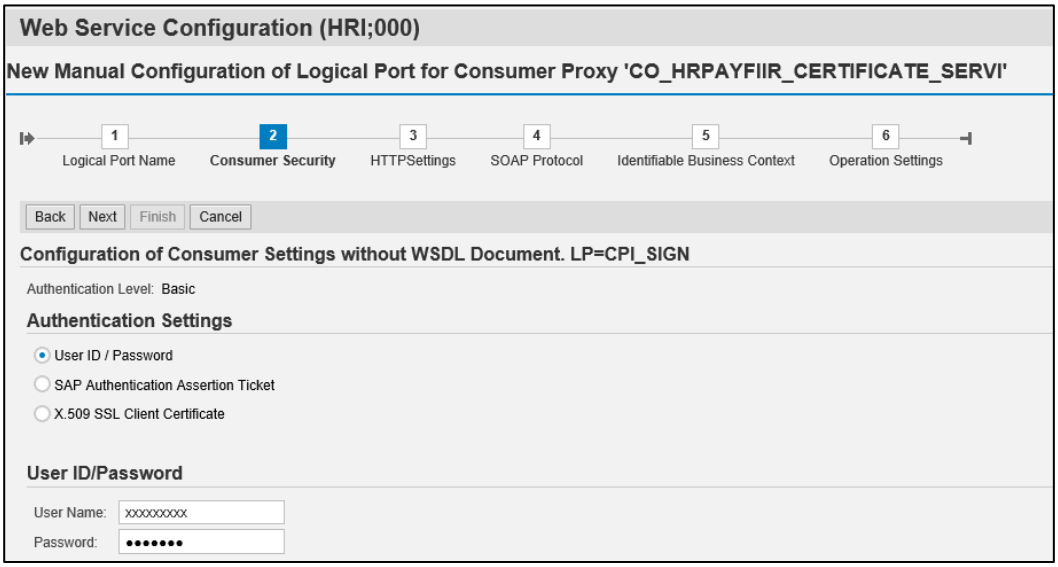


6. Step 1 - **Logical Port name**:
   - *Logical Port Name:* **CPI_SIGN**

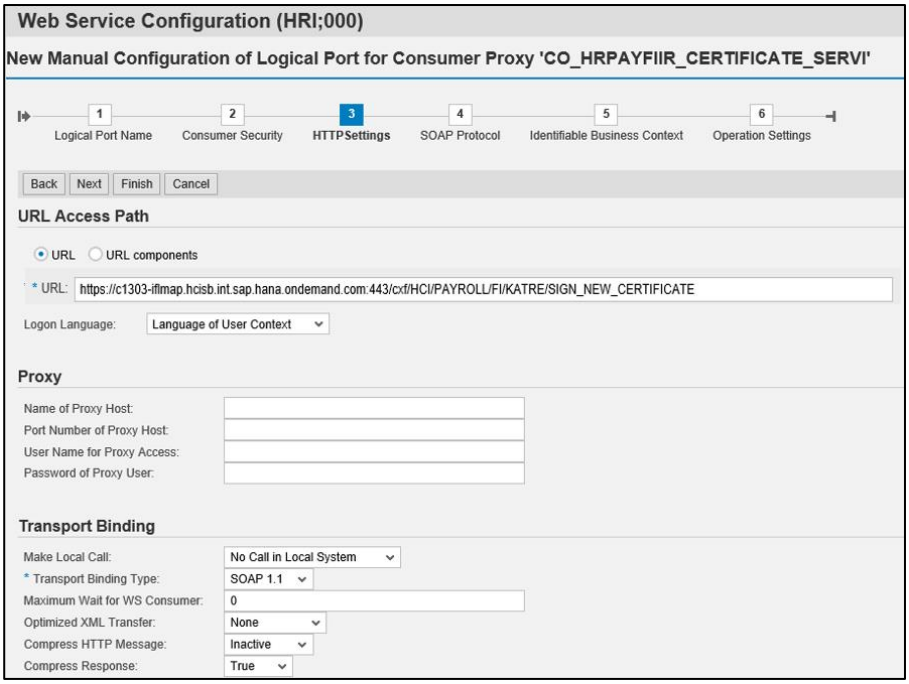
     Description: **CPI port for SignNewCertificate**



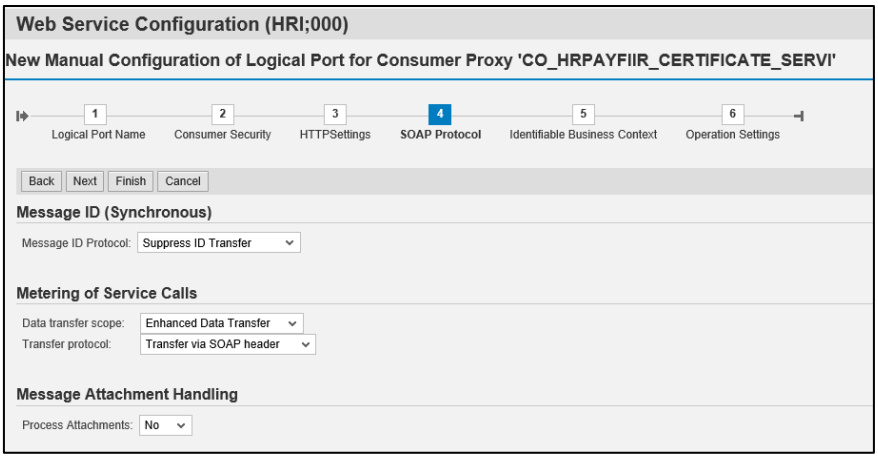
7. Click *Next*.
8. Step 2 - **Consumer Security**:
   - *Authentication Settings:* **User ID / Password**
   - *User Name:* **<CPI admin's user name>**
   - *Password:* **<CPI admin's password>**



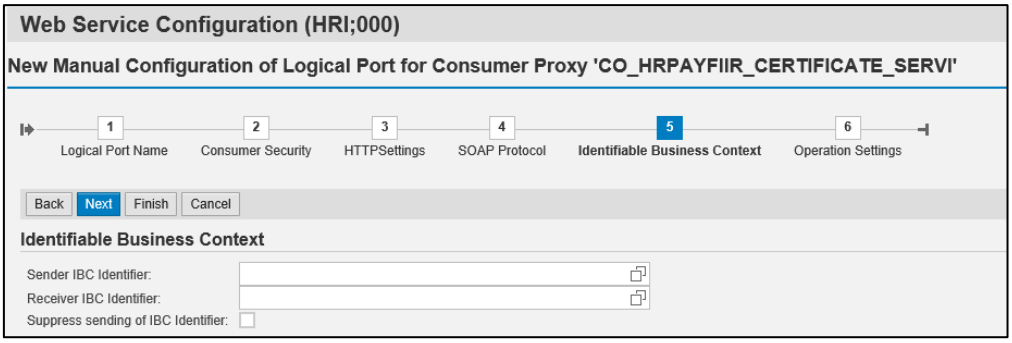
9. Click *Next*.
10. Step 3 - **HTTPSettings**:
    - *URL: <URL to your CPI tenant>***/cxf/HCI/PAYROLL/FI/KATRE/SIGN_NEW_CERTIFICATE**
    - *Proxy: setup the proxy if it's used in your company*
    - *Leave other fields with their default values.*



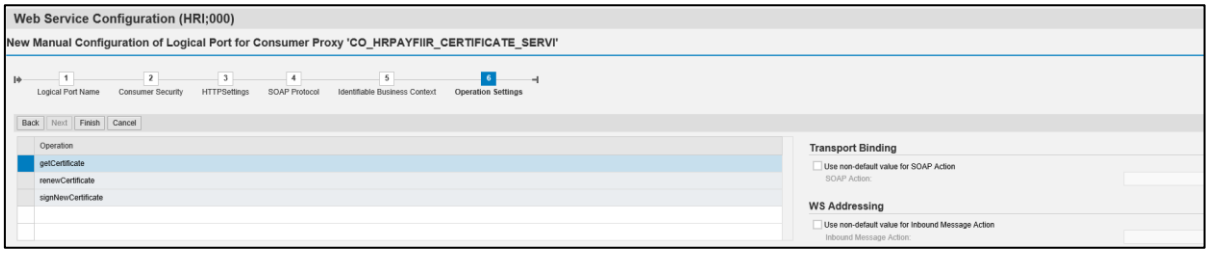
11. Click *Next*.
12. Step 4 - **SOAP Protocol**:
    - *Message ID Protocol:* **Suppress ID Transfer**
    - *Data transfer scope:* **Enhanced Data Transfer**
    - *Transfer protocol:* **Transfer via SOAP header**
    - *Process Attachments:* **No**



13. Click *Next*.
14. Step 5 - **Identifiable Business Context**:
    - *Leave everything blank*



15. Click *Next*.
16. Step 6 - **Operation Settings**:
    - *Leave everything default*



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

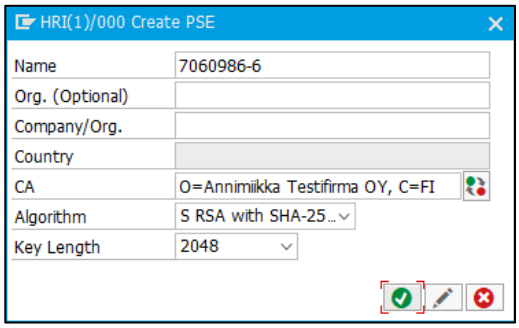
Port CPI_WR

- 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

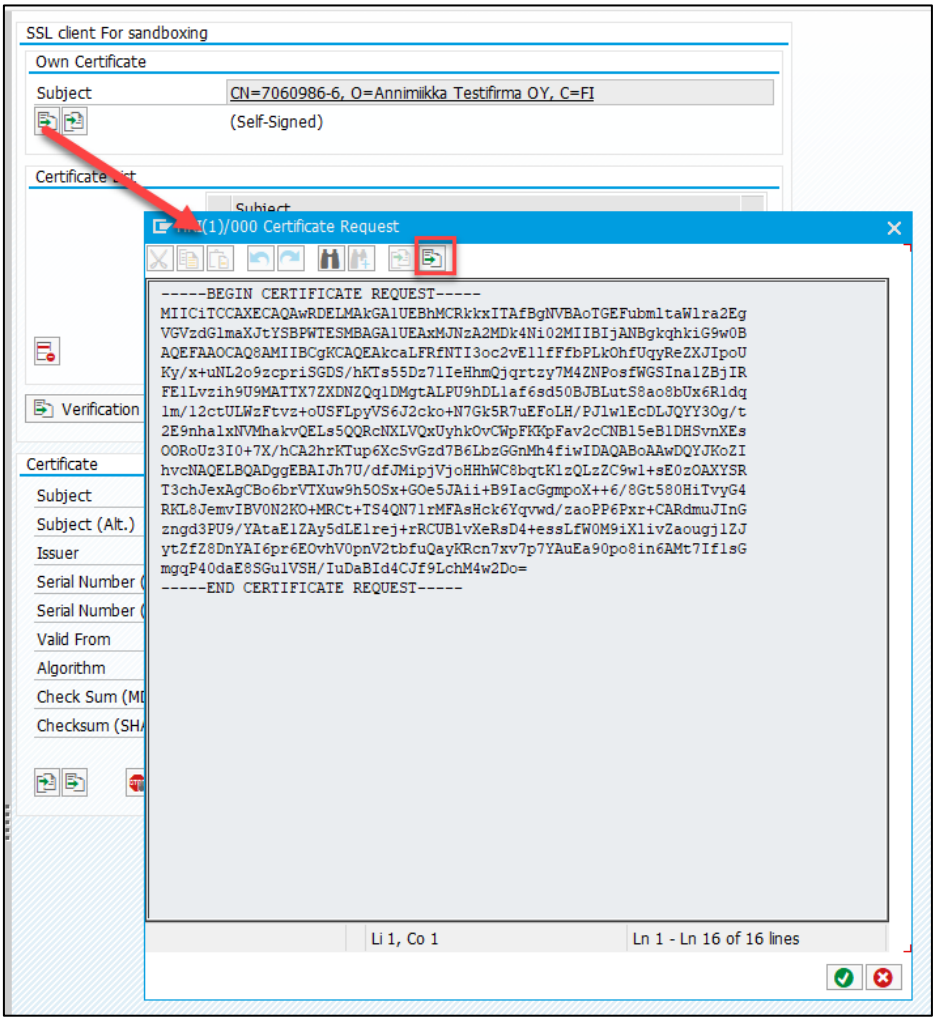
3.1 Creating a new identity in STRUST

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



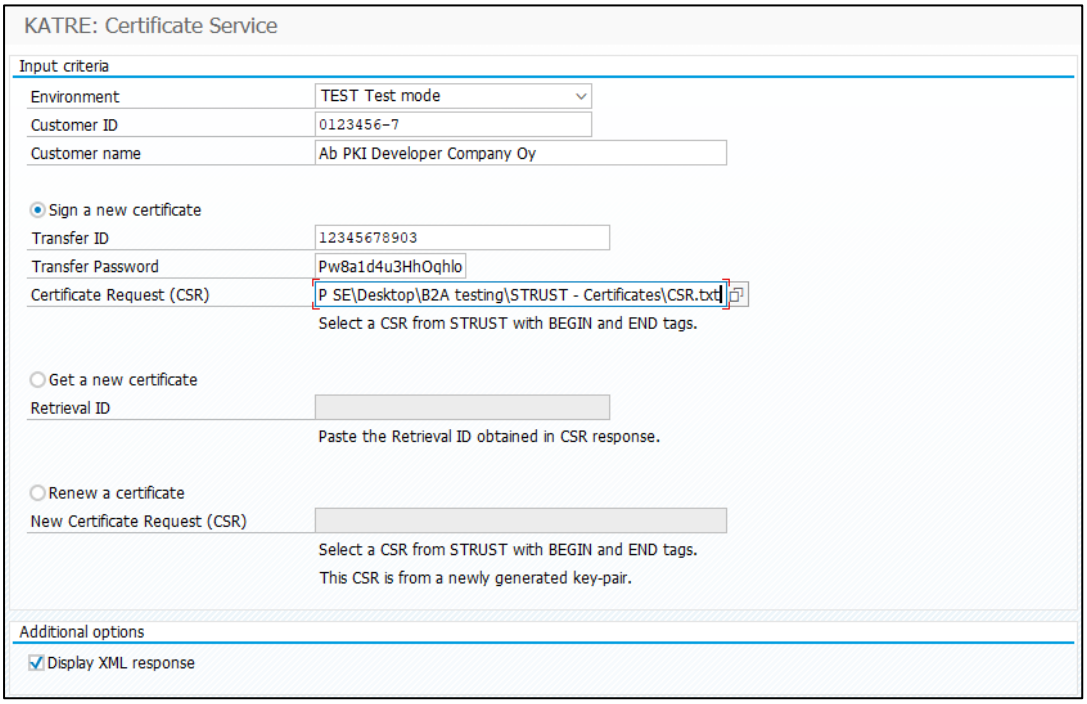
3.3 Certificate Service report

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*.

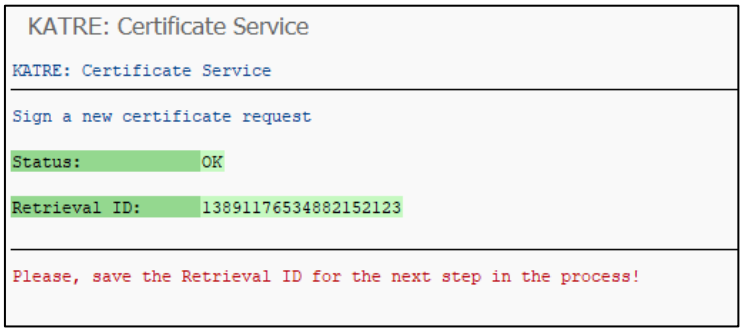
1. Open the transaction PC00_M44_IR_CERT.
2. Fill the selection screen with **your data** and select the first radiobutton *Sign a new certificate*.
3. Press **F4** to select a *Certificate Request (CSR)* saved from the **STRUST** transaction.

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



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.

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



Caution

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

Caution

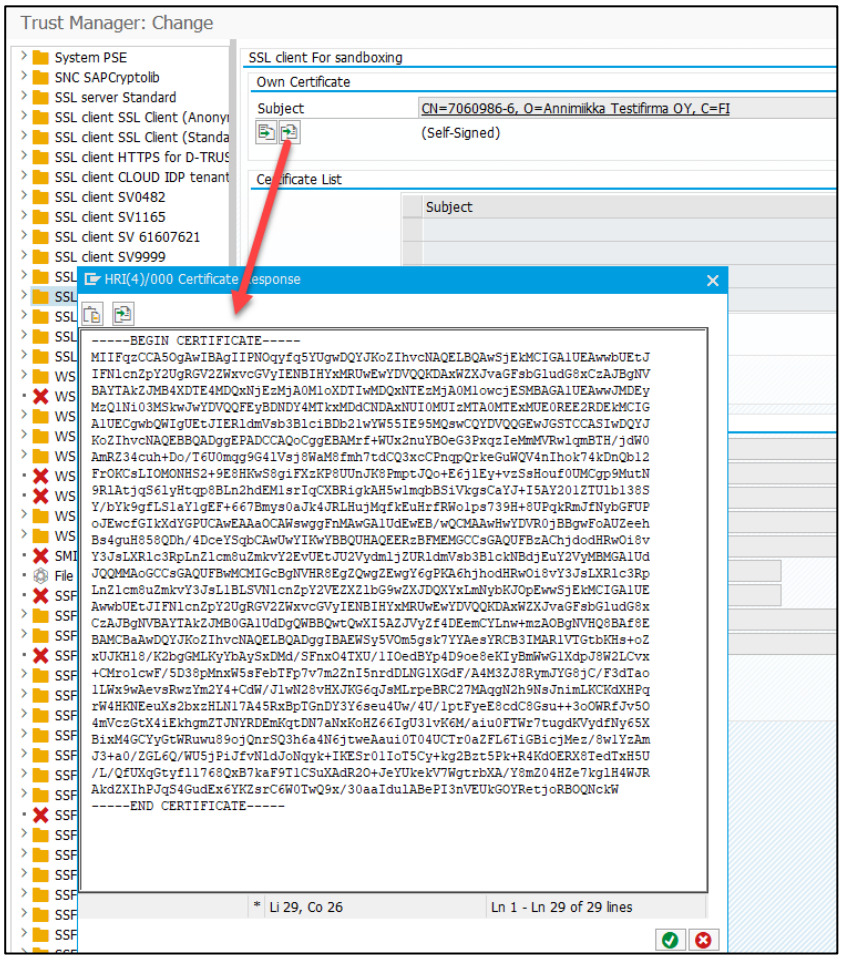
If an error in the process occurs, it is displayed on the screen. Please, check the configuration and try again.

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

Caution

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

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



13. 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**.

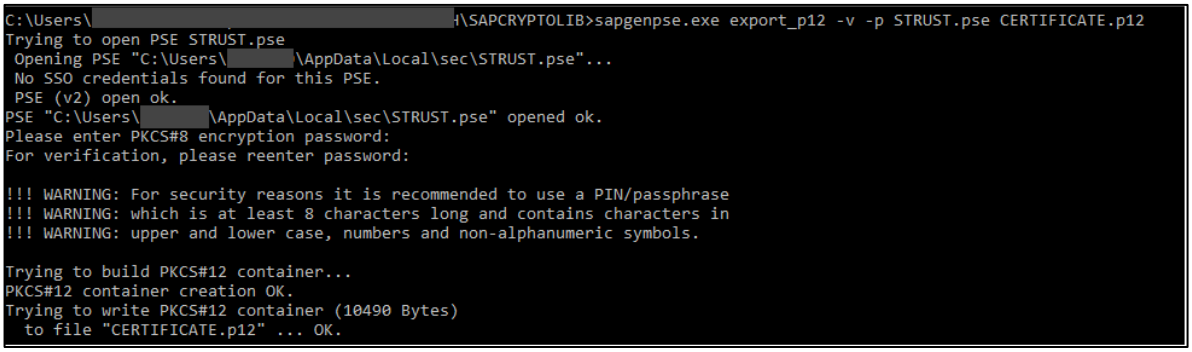
> **Note**
>
> The SAP GenPSE command-line tool can be downloaded from the SAP Support portal.

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
```



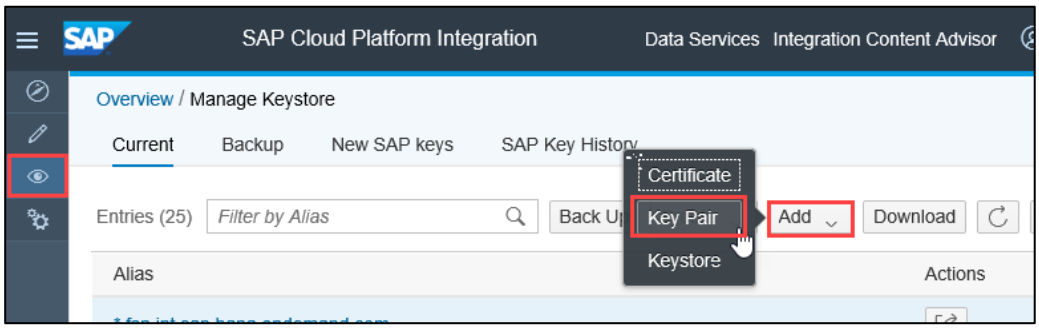
4. Enter the **password**, which will be needed later.
5. Now you have the certificate exported in the desired format for the CPI.

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.

> **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

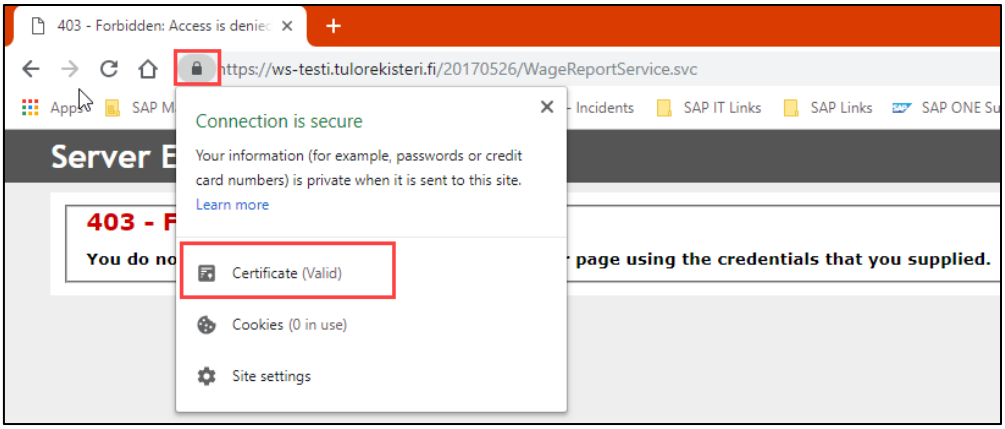
You also need two additional Certificates for the communication with:

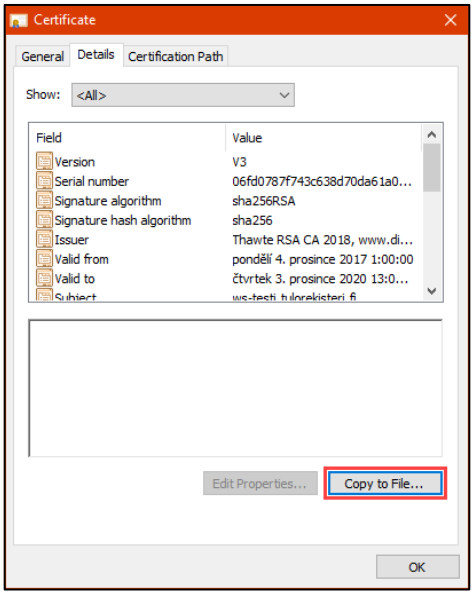
- **Incomes Register's Web Services** (Wage report, Invalidation and Status service)
- **Certificate Service**

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:



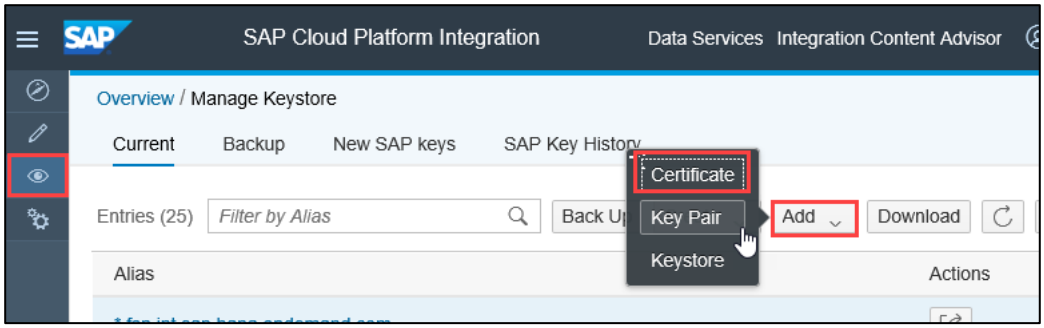


Note

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**.



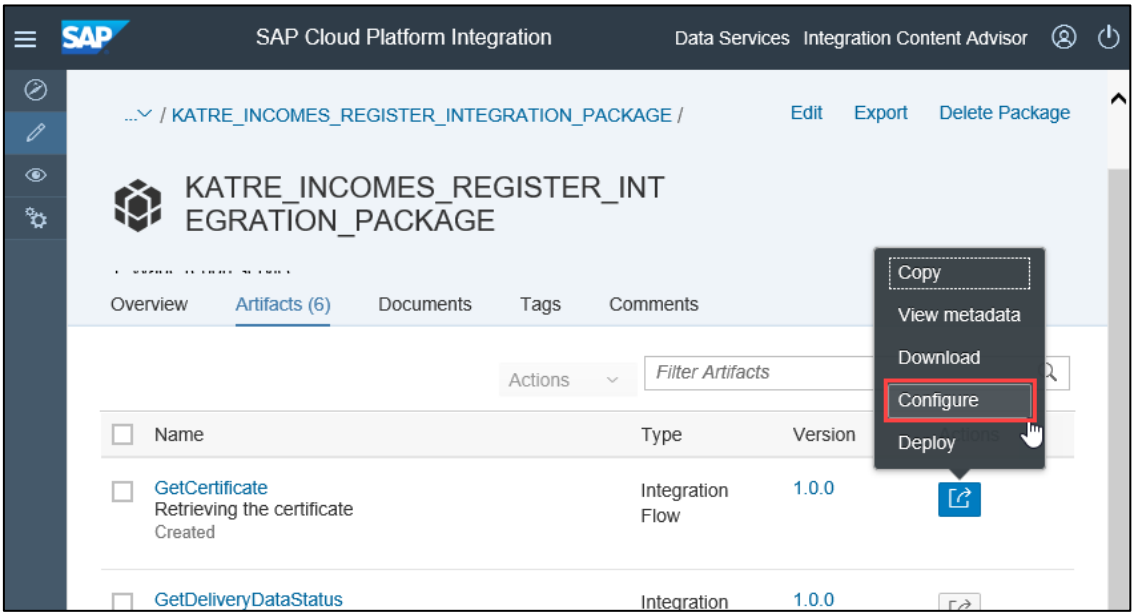
4. In the pop-up window, enter the *Alias* and choose the *File* with a certificate.

> **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/

www.sap.com/contactsap

Material Number: