Configuration Guide
KATRE
Document Version: 5.1 – 2025-09-25

CUSTOMER

Reporting to the Incomes Register (KATRE)

Using Web Services with SAP Cloud 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.
2.0	2019-01-10	Added instructions about the Database in STRUST.
3.0	2019-01-24	Certificate service address corrected. Certificates in the Database changed.
4.0	2019-01-30	Additional changes after the Pilot phase.
5.0	2024-12-19	Updated URL in iFlow configuration, additional options for certificates creation
5.1	2025-09-25	Adding configurable field Address to all integration flows

Contents

1 Introduction

You use SAP Cloud Integration to establish the communication with external systems and transfer to them the electronic documents you have created using the Human Capital Management solutions from SAP for Finland. This document lists the required setup steps you perform in the SAP ERP or SAP SuccessFactors Employee Central Payroll and the SAP Cloud Integration tenant so that the integration between the systems works.

The setup steps are typically done by an SAP Cloud Integration consulting team, which is responsible for configuring the SAP back-end systems and the connection with SAP Cloud Integration. This team may be also responsible for maintaining the integration content and certificates/credentials on the SAP Cloud Integration tenant.

> **Note**
>
> *This document describes functionality that is provided by the Integration Package itself, that is, by the artifacts that are deployed in the SAP Cloud Integration tenant. It may happen, however, that in the SAP back-end systems the access to such functionality is only partially implemented. Additionally, it may also happen that the Vero servers do not provide all services that are described in this document. Please refer to the relevant SAP back-end systems documentation and to the relevant Vero information, respectively.*

For the sake of simplicity in this guide, we mention SAP back-end systems when something refers to both SAP ERP and SAP SuccessFactors Employee Central Payroll.

2 Prerequisites

2.1 Installation of KATRE solution

The main SAP Note with the KATRE solution:

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

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

> **Note**
>
> To configure the SAP Cloud Integration correctly (users, authorizations, etc.), please, refer to the SAP Help Portal (e.g. https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/73af55cff75342a8a8ca3a22f22b5283.html).

2.2 Set Up SAP Cloud Integration Tenants

SAP Cloud Integration test and production tenants are live and users in the tenants have the rights to copy the integration package and to configure and deploy the integration flows (iFlows).

When your tenants are provisioned, you receive an email with the Tenant Management (TMN) URL. You need this URL for the configuration of the SAP back-end systems.

To be able to deploy the security content, you must be assigned the `AuthGroup.Administrator` role.

If you are a first-time user, you must first set up your users (members) and their authorizations in the SAP BTP Cockpit.

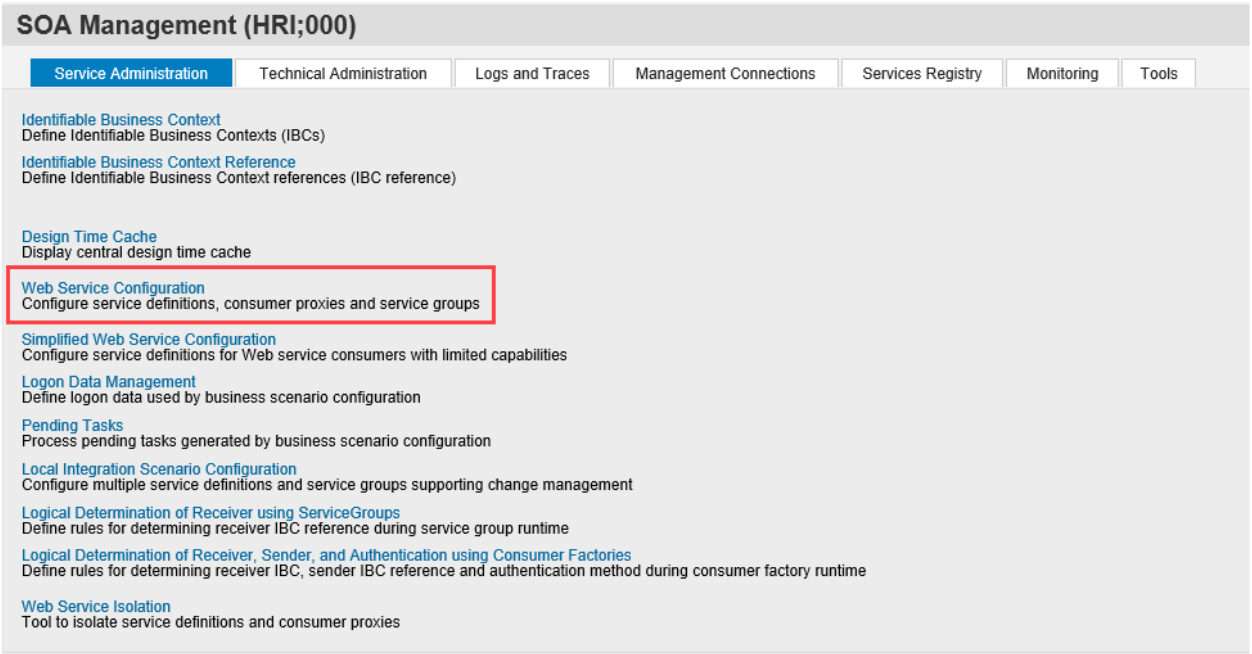
3 SOAMANAGER configuration

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

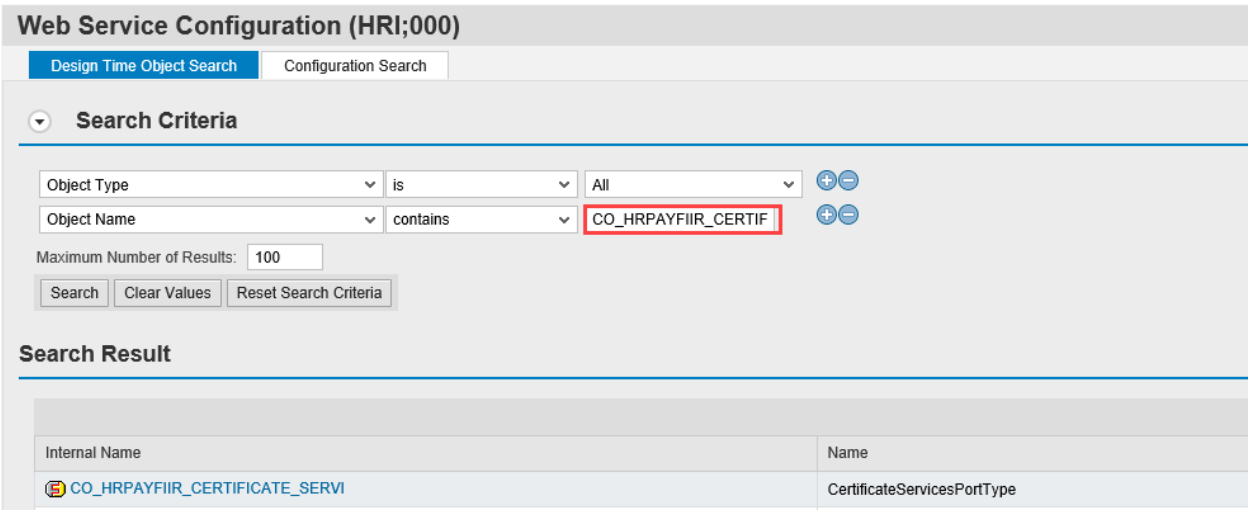
> **Note**
>
> Some details (names of tabs etc.) might be slightly different depending on your release version.

3.1 Certificate service

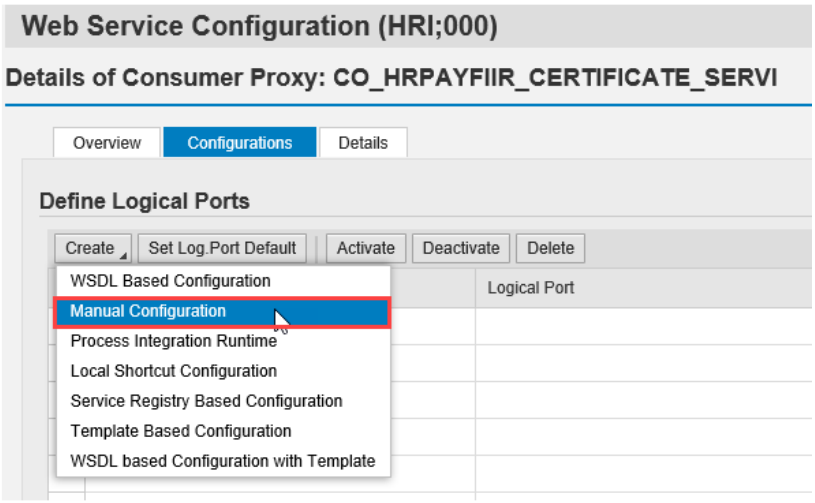
1. Execute the transaction code SOAMANAGER. This opens a new window in your web browser.
2. In the Service Administration tab, click *Web Service Configuration* link.



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

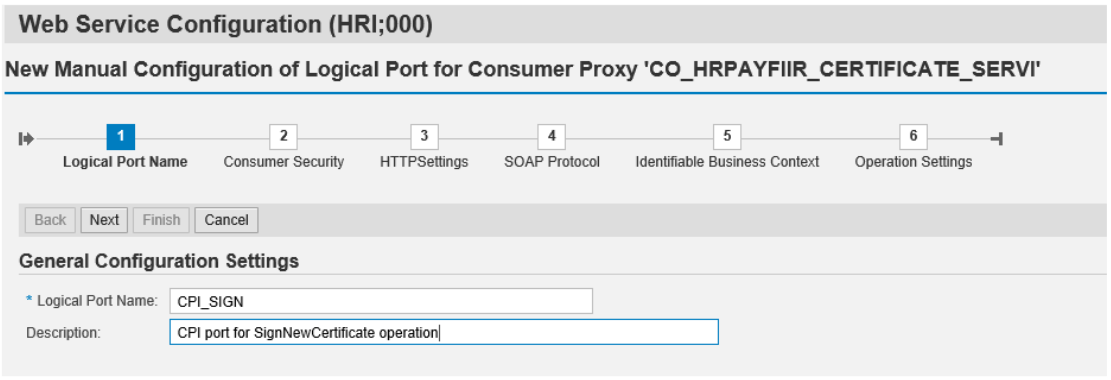


4. Click the Internal name CO_HRPAYFIIR_CERTIFICATE_SERVI.
5. In the Configurations tab, click the Create button and select *Manual Configuration*

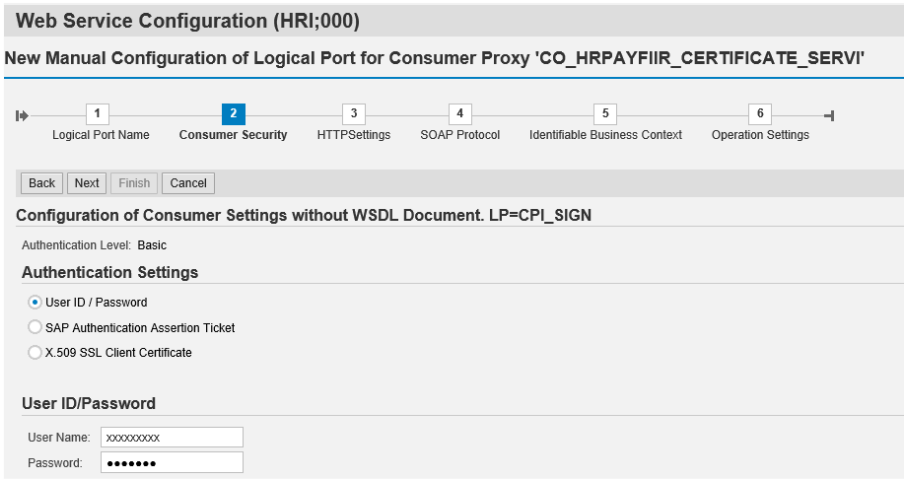


6. Step 1 - Logical Port name:
   - *Logical Port Name*: CPI_SIGN

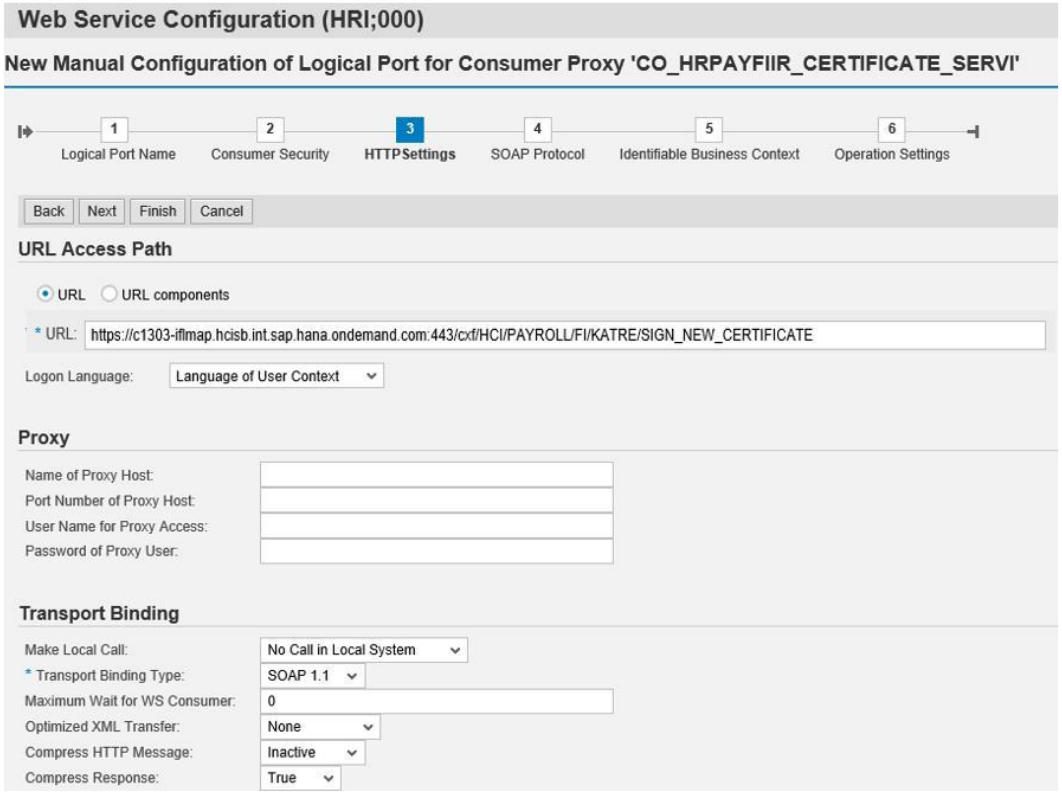
     Description: CPI port for SignNewCertificate



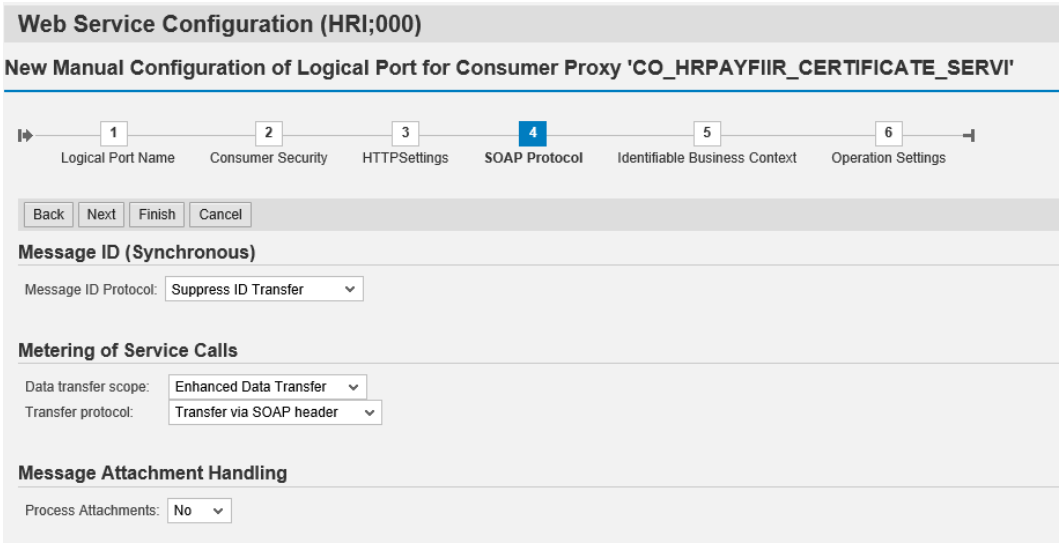
7. Click *Next*.
8. Step 2 - Consumer Security:
    - *Authentication Settings:* User ID / Password
    - *Username:* <CI admin's user name>
    - *Password:* <CI admin's password>



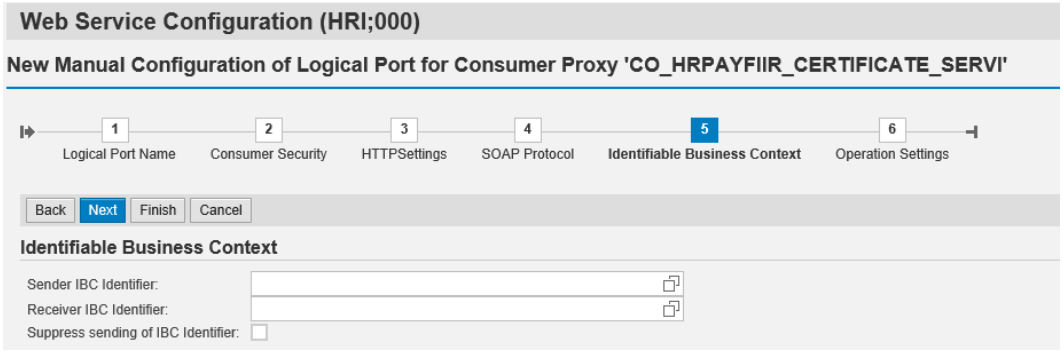
9. Click *Next*.
10. Step 3 - HTTPSettings:
    - *URL:* <URL to your CI>/cxf/HCI/PAYROLL/FI/KATRE/SIGN_NEW_CERTIFICATE
    - *Proxy:* setup the proxy if it's used in your company
    - *Leave other fields with their default values.*



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 CI>/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 CI>/cxf/HCI/PAYROLL/FI/KATRE/RENEW_CERTIFICATE

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

3.2 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 CI>/cxf/HCI/PAYROLL/FI/KATRE/SEND_WAGE_REPORTS

3.3 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 CI>/cxf/HCI/PAYROLL/FI/KATRE/GET_STATUS

3.4 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 CI>/cxf/HCI/PAYROLL/FI/KATRE/SEND_INVALIDATIONS

4 Configuration Steps in SAP Cloud Integration

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

4.1 Uploading Certificates to Keystore

You will need two Income Register Certificates for the communication with:

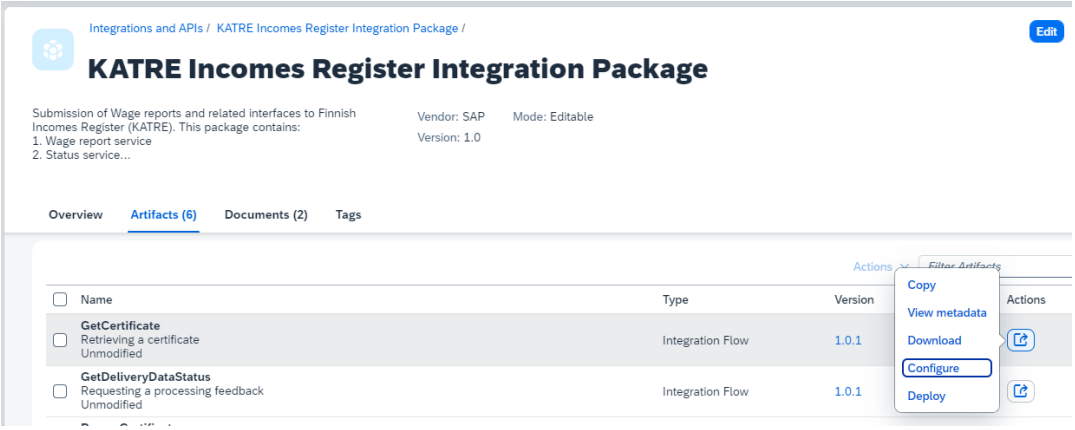
- Incomes Register's Web Services
  (for testing e.g. from https://ws-testi-2.tulorekisteri.fi/20170526/WageReportService.svc port 443)
  (for production e.g. from https://ws.tulorekisteri.fi/20170526/WageReportService.svc port 443),
- Certificate Service
  (for testing https://pkiws-testi.vero.fi/2017/10/CertificateServices port 443)
  (for production https://pkiws.vero.fi/2017/10/CertificateServices port 443)

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-testi2.tulorekisteri.fi/20170526/WageReportService.svc*) and download the certificate from there

4.2 Configuration of iFlows

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

1. In the CI, 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.

Note

A new configurable field *Address* was added to the sender tab in the package version 1.0.3. Changing the default value in this field needs to be reflected in SOAMANAGER configuration – sections 3.1-3.4 (in HTTP Settings step, use URL to the CI for each changed iflow as */cxf/<your configured value>*),

GetCertificate

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

Explanation of Private Key Aliases

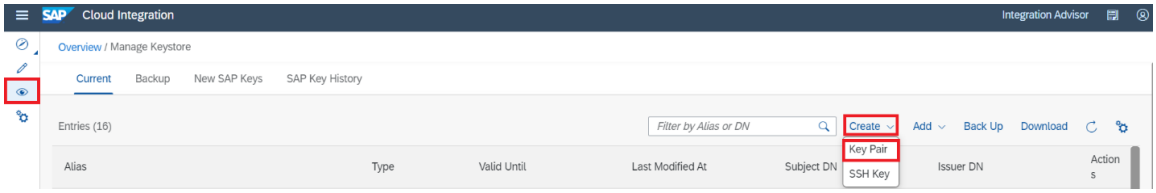
Private Key Alias	Explanation
katre_customer_pk	Key Pair downloaded from the STRUST. Obtained by the Certificate Service report.
katre_old_customer_pk	Key Pair from the currently valid certificate that is about to be renewed.
katre_cert_service	Certificate for the Certificate service downloaded from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

5 Obtaining a certificate

> **Note**
> There are currently two supported options how to create a certificate in SAP environment. This guide describes both the new process in SAP CI (section 5.1) and original process with STRUST (section 5.2). Following either section of the guide should lead to the same result.

5.1 Creating a new certificate in CI

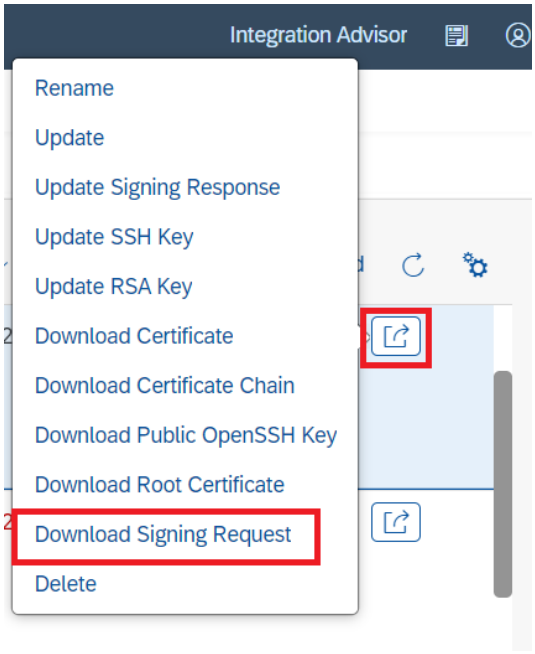
1. In the SAP CI, open the *Overview* section
2. In the *Manage Security* section, click the **Keystore** tile
3. Click the *Create* button and select **Key Pair**



4. Fill the fields:
   - Key Type: RSA
   - KeySize: 204
   - Algorithm: RSA with SHA-512
   - CN: <Business ID>
   - O: <Name of your organization>
   - C: FI

5.1.1 Saving Certificate Request (CSR)

1. On the newly created certificate, click the action button
2. In the menu, choose *Download Signing Request*
3. Save the CSR file



5.1.2 Certificate Service report

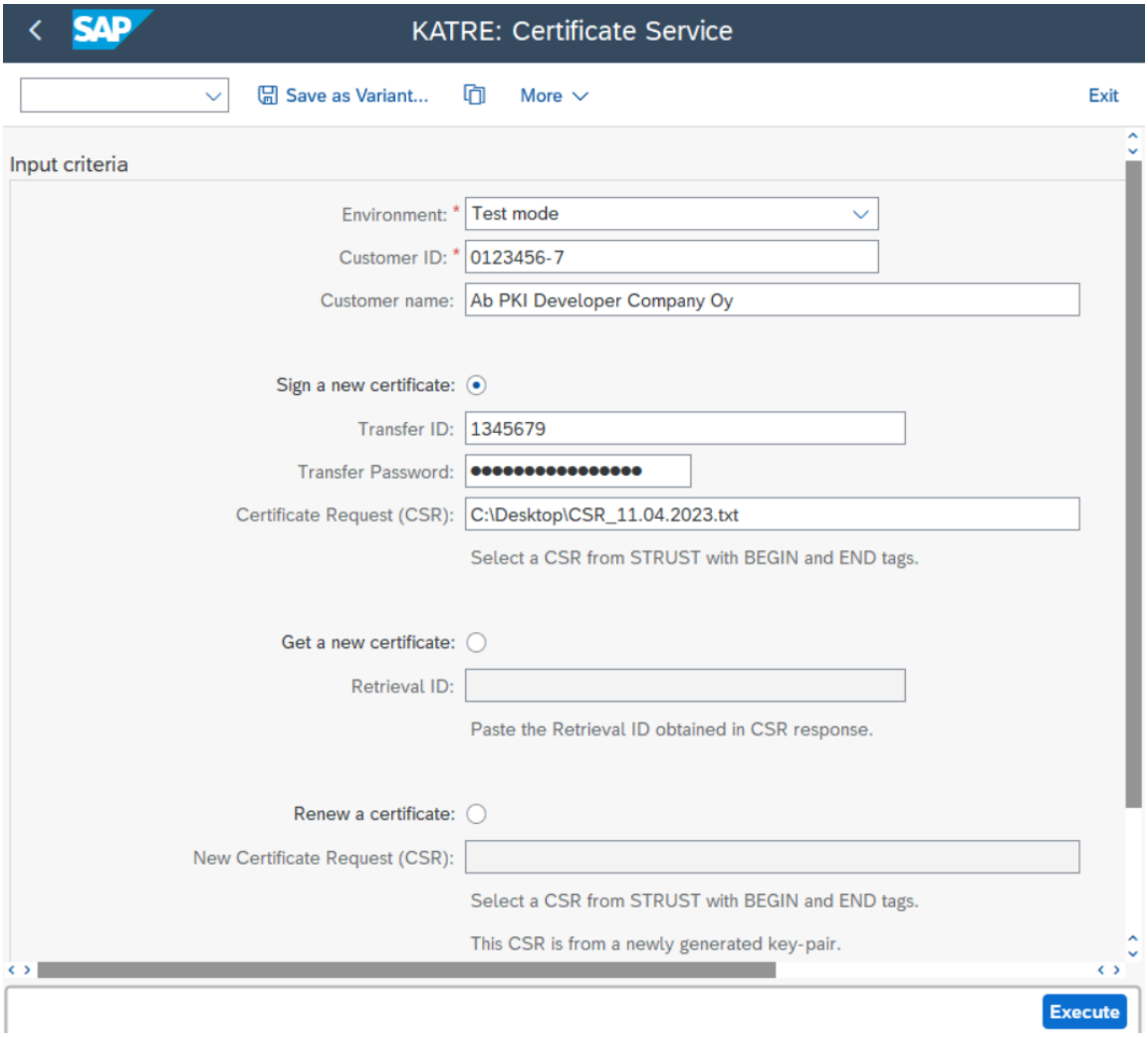
The Certificate Service report HFIIRCERT (transaction PC00_M44_IR_CERT) can be used for obtaining a new certificate or renewing an existing one.

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

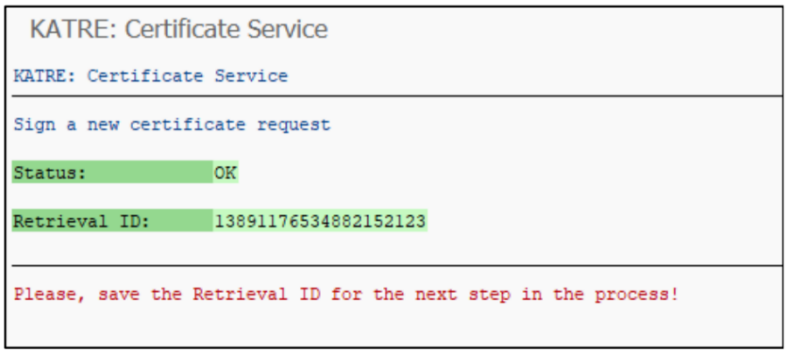
1. Open the transaction PC00_M44_IR_CERT.
2. Fill the selection screen with your data and select the first radio button *Sign a new certificate*
3. Press F4 to select a *Certificate Request (CSR)* saved from the CI.

Example

This is an example of how you can call the 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!

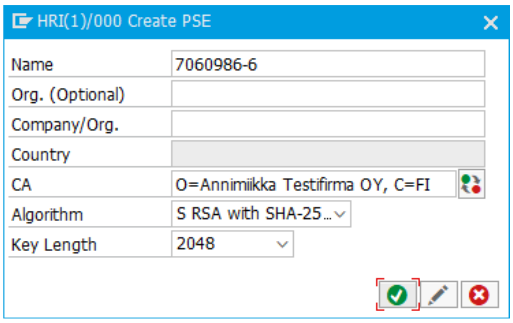
9. Copy the whole certificate (without the BEGIN/END sections) to your clipboard.
10. Paste the certificate into a text editor (e.g. Notepad) and save as *certificate_response.p7b*
11. In CI, in Overview section, Manage Security, tile Keystore, click on the action button of certificate created in the first step in section 5.1.
12. Select Update Signing Response and chose the certificate file saved from the Certificate Service report.

> **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.

5.2 Creating new certificate in STRUST

5.2.1 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**



5.2.2 Creating Trust Centers in STRUST database

1. Open the transaction STRUST in the Change mode.
2. In the upper menu, click Certificate → Database.
3. Create 3 new entries for certificates (downloaded in the next chapter). You need to use a customer-specific namespace Y* or Z*.

   Example

   For example, the entries can look like this:

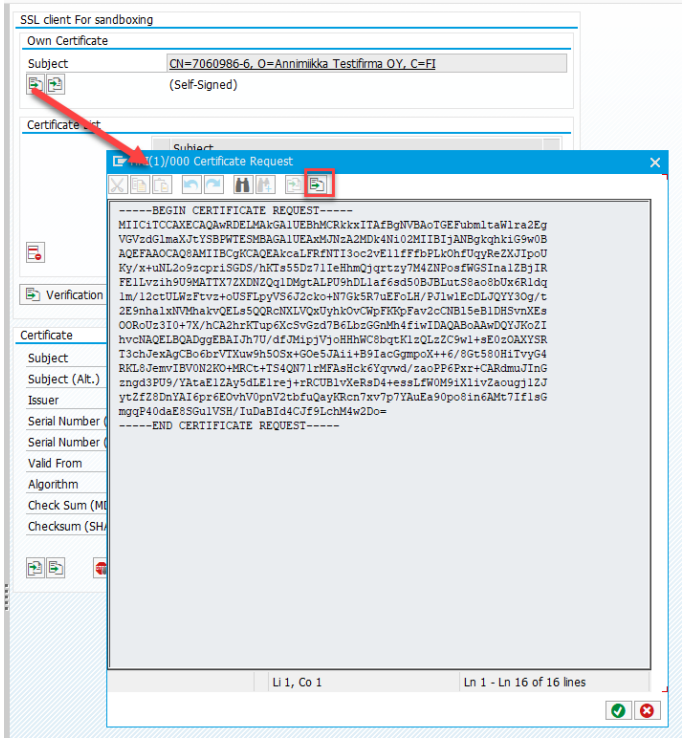
   - ZKATRE1 CA KATRE: VerohallintoRootTestCAv1.cacert.crt
   - ZKATRE2 SERV KATRE: VerohallintoIntermediateTestCAv1.cacert.crt
   - ZKATRE3 SERV KATRE: DataProvidersTestIssuingCAv1.cacert.crt

   Caution

   Please, note that the certificates for the Productive system may be different.

5.2.3 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.



5.2.4 Exporting IR certificate chain to STRUST database

1. Open the Incomes Register's website (currently only in Finnish)

   https://www.vero.fi/tietoa-verohallinnosta/kehittaja/varmennepalvelu/dokumentaatio/

2. Download the ZIP file with required certificates:
   For testing: DataProvidersTestIssuingCAv1-chain.cacert.zip
   For production: DataProvidersIssuingCAv1-chain.cacert.zip

3. Save the 3 certificates from the ZIP file to your local machine.
4. Open the transaction STRUST in the Change mode.
5. For each of those 3 certificates, perform the following steps.
6. In the upper menu, click Certificate → Import. Select a file with the certificate from your machine.
7. In the upper menu, click Certificate → Export. Select the Database tab and then select the Trust Center relevant for that certificate. Provide some Description.

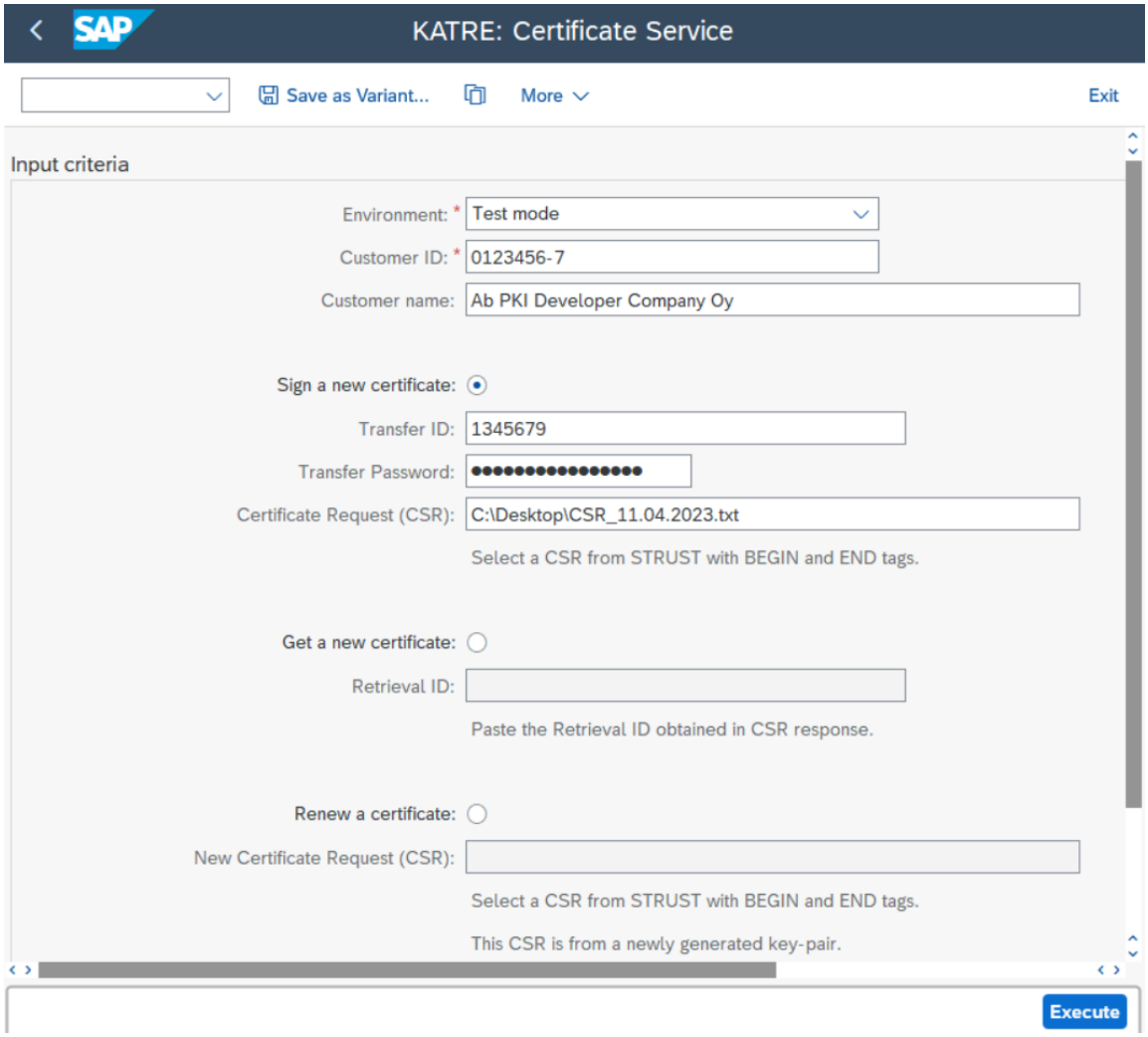
5.2.5 Certificate Service report

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 radio button *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 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

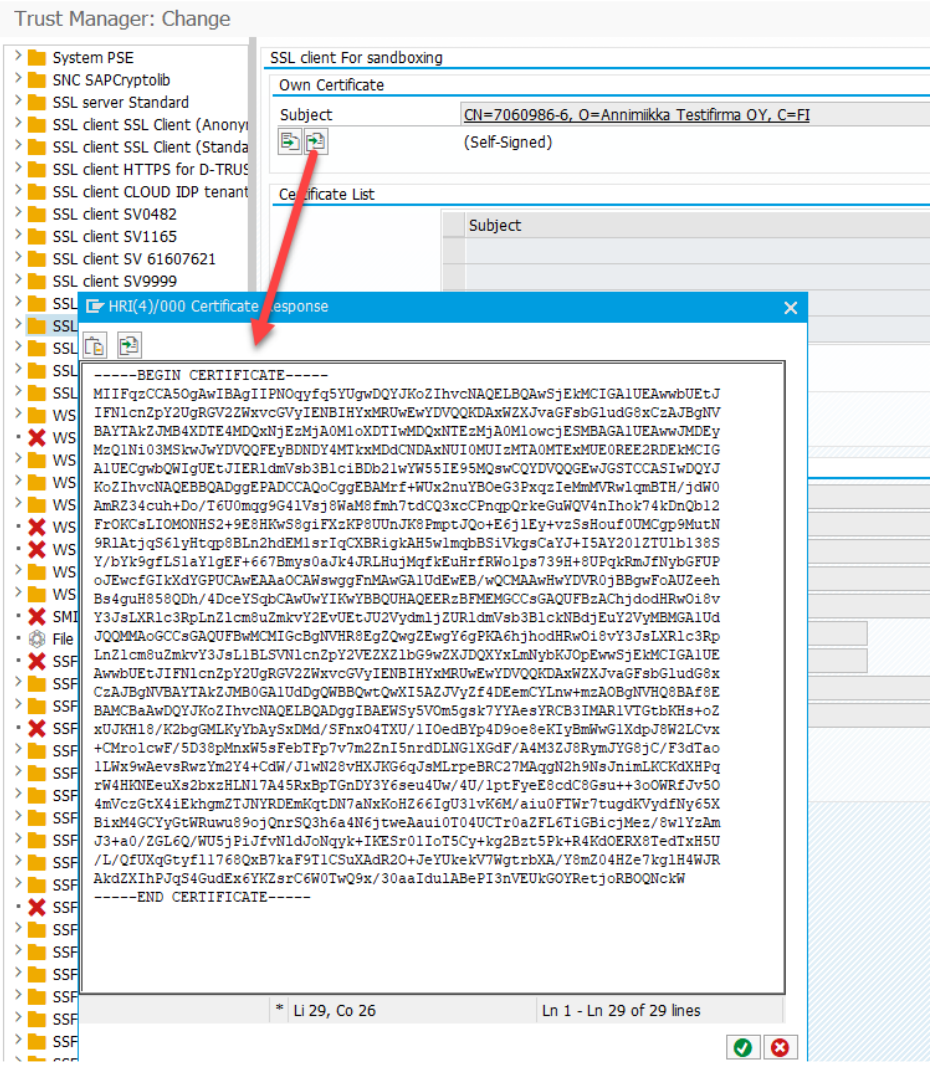
If an error in the process occurs, it is displayed on the screen. Please, check the configuration and try again.

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.
14. If your system is of version >= SAP_BASIS 750, you can export the created credentials directly from STRUST transaction. Select export under PSE menu item and save file in the .p12 format. For export on lower system versions, follow steps in section 5.2.6.

> **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.

5.2.6 Exporting certificate to PKCS#12

Follow this section if you are unable to download the certificate directly from STRUST. To be able to upload the obtained certificate to the *SAP Cloud 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:

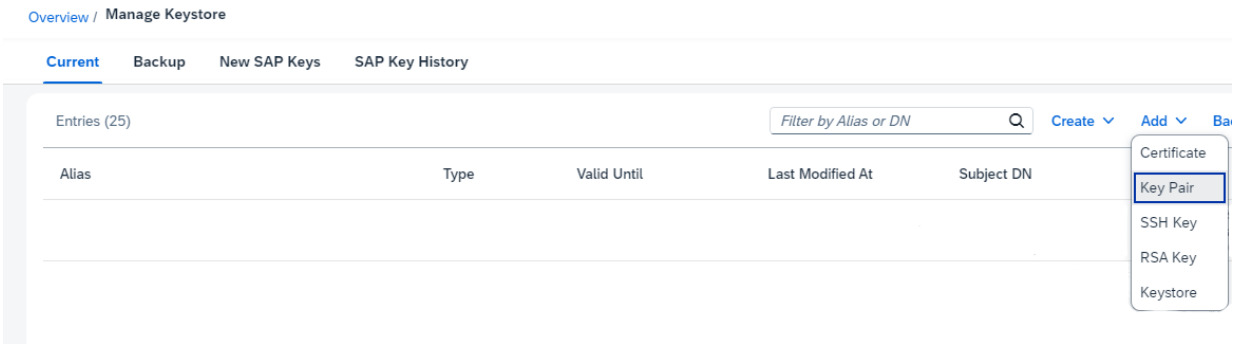
sapgenpse export_p12 [options] -p <pse_file> <filename>.p12

```
C:\Users\                                    H\SAPCRYPTOLIB>sapgenpse.exe export_p12 -v -p STRUST.pse CERTIFICATE.p12
Trying to open PSE STRUST.pse
 Opening PSE "C:\Users\       \AppData\Local\sec\STRUST.pse"...
 No SSO credentials found for this PSE.
 PSE (v2) open ok.
PSE "C:\Users\       \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 CI.

5.2.7 Uploading Key Pair to Keystore

1. In the CI, open the *Overview/Monitor* 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*.
6. Now you have a Key Pair deployed in the CI 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.

6 Switching the WS functionality on

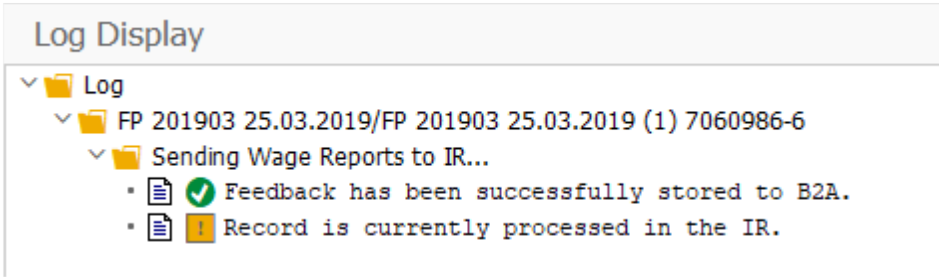
The change the functionality in the B2A Manager from the manual Download/Upload mode to the automatic WS-based, you need to perform the following steps:

1. Open the transaction *PE03*.
2. Enter the feature name 44KWS and press *Change*.
3. Select the only node in the decision tree and the *Change Nodes* button.
4. Set the value of the node to "X" - this switches ON the WS functionality.
5. *Save* and *activate*.

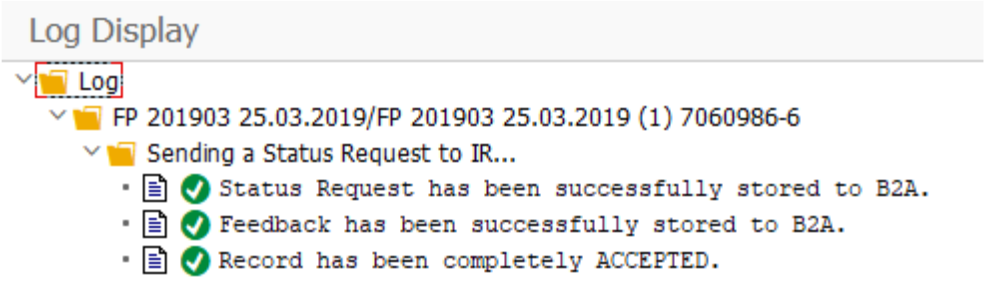
7 Process in the B2A Manager

The process of the KATRE reporting is basically the same, all the announcements are stored in the B2A Manager. With this new WS-based functionality, the process in the B2A Manager now looks like this:

1. Select one or more entries in the displayed ALV in the B2A Manager.
2. Click the *Execute* button to send the data to the IR.
3. The processing log is displayed saying that the Record is currently being processed in the IR.



4. Then after some processing time (depends on how fast is the IR's processing), you have to click the *Execute* button again to ask for a Status Response.
5. Again, the processing log is displayed.



6. The processing in the B2A Manager should be complete → check the Viewer for final data report (HFIIRVFWR) for detailed analysis of the messages (if rejected for instance).

> **Note**
>
> Sometimes, after you click the Execute button for the second time, the processing log displays the message, that the Record is still being processed in the IR. This means that you have to wait for a little longer and repeat the Execute action until you successfully receive a Status Response.

www.sap.com/contactsap

Material Number: