SAP HR Integration with ELSTER ERiC for Germany

HR Tax Integration for Germany (SAP HR Tax Integration for Germany (LStA, LStB, ELStAM)

SAP Cloud Platform Integration Configuration

THE BEST RUN SAP®

TABLE OF CONTENTS

1. OVERVIEW AND PREREQUISITES

This integration package enables you to transfer German tax-specific notifications to the authority. The following notifications are supported: LStA, LStB, and ELStAM.

For the transfer, the integration package applies specific requirements for message security, which are set by the German authorities. Therefore, the integration package uses the mandatory ERiC Libraries. The functionality is valid for German customers only. On-Premise System (ERP) and Employee Central Payroll (ECP): Minimum Release 6.00

Before you start with the activities described in this document, ensure that the following prerequisites are met:

1.1 Configure SAP CLOUD PLATFORM INTEGRATION

1.1.1 Initial Configuration of the Cloud Integration Tenant

SAP CLOUD PLATFORM INTEGRATION (CPI) test and productive tenants are live and users in the tenants have sufficient rights and privileges to copy the integration package and to configure and deploy the integration flow. To deploy the security content, role 'AuthGroup.Administrator' is required.

Set up and configure the Cloud Platform Integration tenant as described in the *Get Started* documentation for SAP Cloud Platform Integration. https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/e7b1eaa2246641b3a6188233cf219ab8.html

For the subsequent configuration of HR (On Premise + ECP), note down the URL of the tenant (the TMN URL you received when the tenant was provisioned).

1.1.2 ELSTER certificates for SAP Cloud Integration

To exchange data with the authority, you need one or more certificates from the authority. These certificates can be obtained from the ELSTER Online-Portal. If you already use the data exchange with the authority and you want to switch communication from middleware Business Connector (BC) or PI/PO to CPI, you must use the existing certificates.

The ELSTER certificates are files in PFX format (<filename>.pfx) and are password-protected.

For subsequent configuration, make sure that the certificate file and password are available.

2 SETUP STEPS IN SAP CLOUD PLATFORM INTEGRATION

2.1 Copy Published Package 'SAP HR Integration with ELSTER ERiC for Germany' to your Package

Go to the 'Discover' chapter of your tenant and find the package 'SAP HR Integration with ELSTER ERiC for Germany:

Click on package name, then click ‘Copy’ in the upper left corner.

Note: the package version on the screenshot may differ from the current one.

2.2 Configure Integration Flow for HR Data

These steps are optional. Steps 2.2 and 2.2.1 are only necessary if the package is copied more than once or if it was not possible to use the default URL for the connection between HR (on Premise or ECP).

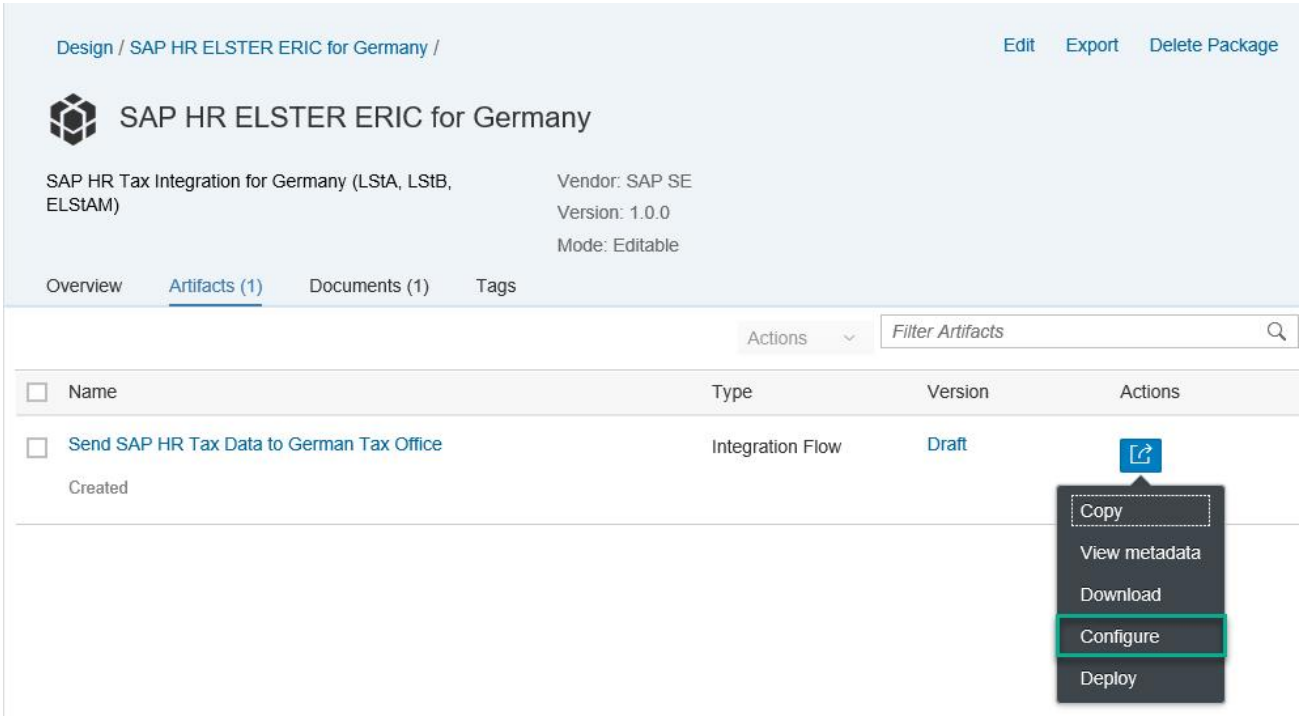

Figure 1. ELSTER integration package "Artifacts" tab

2.2.1 Configure Sender Tab

Address: Update the connection address to a name that allows you to differentiate between different packages (for example**,** /ELSTER_HTTP_Sender_1). As previously mentioned, you should only change this default value if absolutely necessary.

User Role: If you want to use a specific role for the ELSTER Integration Flow you can select a user role different from ESBMessaging.send. This role must be created in Cloud Platform Cockpit. You should only change this default value if absolutely necessary.

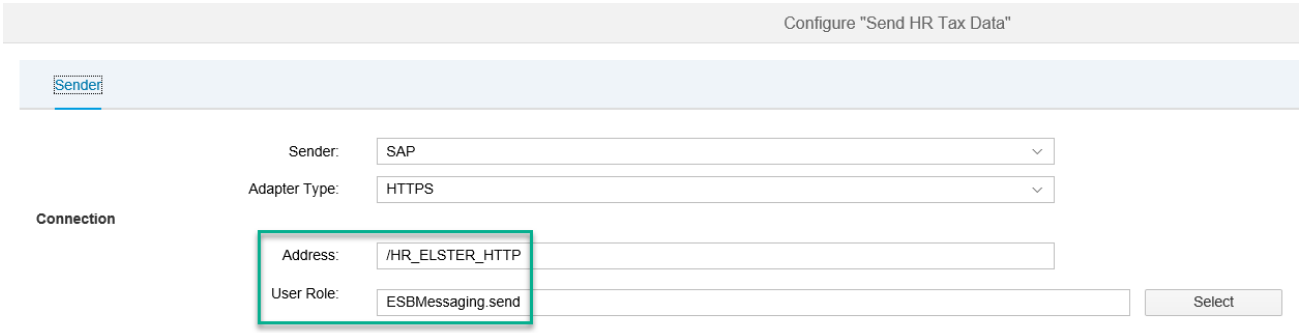

Figure 2. "Send SAP HR Tax Data to German Tax Office" iFlow - Sender adapter properties

3. DEPLOY CERTIFICATES FOR SAP CLOUD INTEGRATION

The certificates for the data exchange with the authority are stored in the CPI Keystore. Therefore, add certificate <filename>.pfx provided from the authority to the CPI Keystore.

1. Navigate to the keystore. Overview -> Manage Security -> Keystore

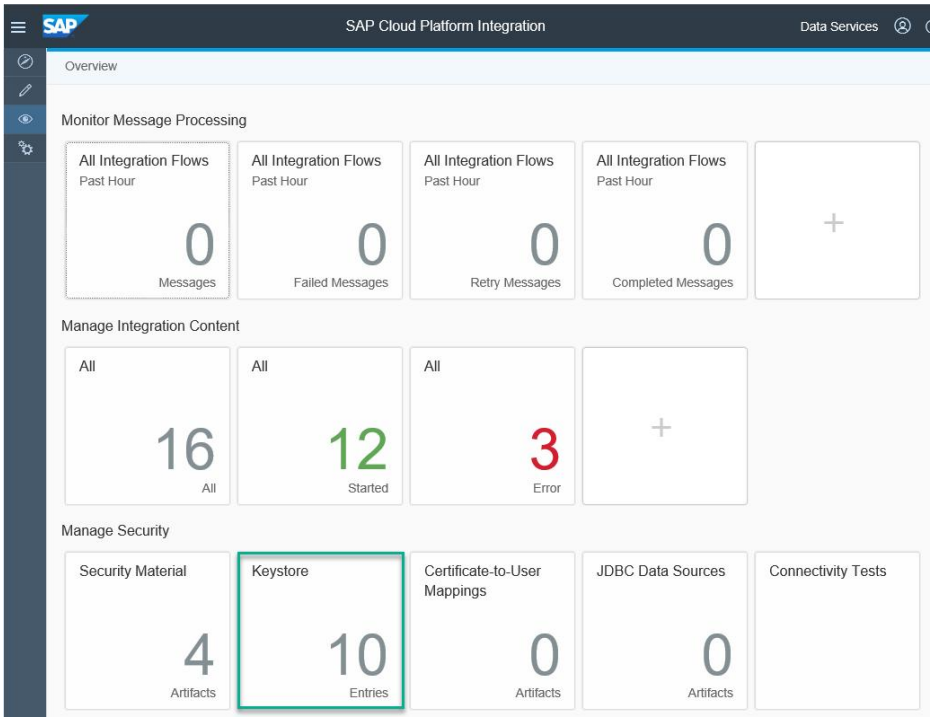

Figure 3. Monitor Keystore

2. Add the PFX-file with the certificate to the keystore. Choose Add -> Keystore

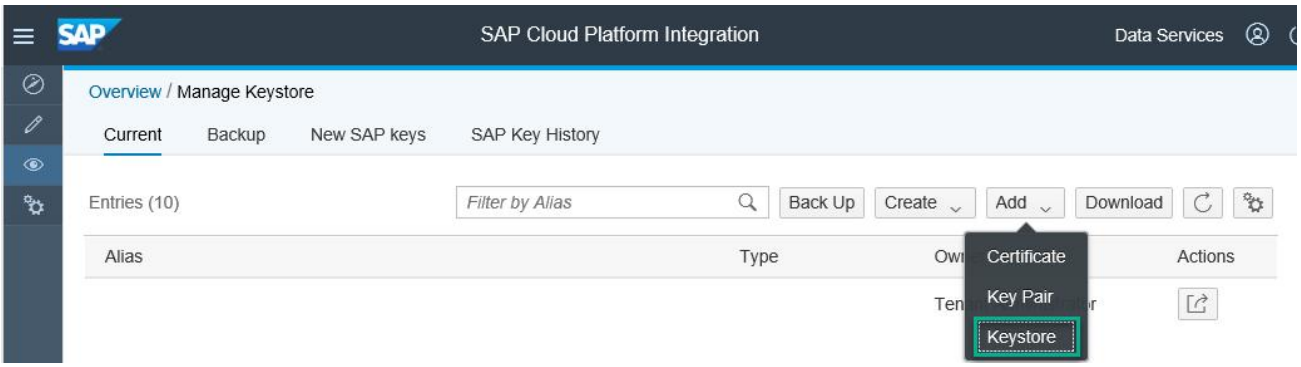

Figure 4. Add PFX-File to the keystore

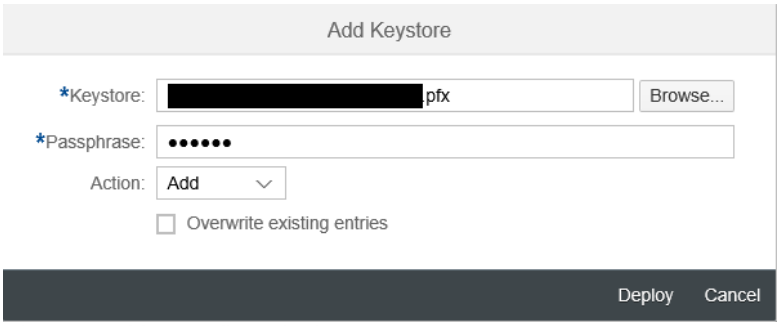

Figure 5. Add PFX-File to the keystore

After adding the PFX-file to the CPI Keystore, you will find two new entries in the certificate list of the keystore. The new entries are called *encyptionkey* and *signaturekey.*

3. Rename the new entries
One of the certificates in the PFX-file is for the encryption and one is for the signature.

Rename entry *encryptionkey* to *elster_hcm_ag_enc* and entry *signaturekey* to *elster_hcm_ag_sig.*

Remarks:

- The suffix _enc and _sig are obligatory and cannot be changed.
- If you use a name other than *elster_hcm_ag<suffix>,* you must customize this value in the corresponding HR system.

- The value *elster_hcm_ag* is the default value set in the HR system. If CPI is used for different companies with different certificates, avoid entries with elster_hcm_ag<suffix>. Otherwise a HR system with incomplete Customizing could send and request data belonging to a different customer from the authority.

For more information about certificate deployment in SAP Cloud Platform Integration, see SAP Note 2469460 “Key-store management in SAP Cloud Platform Integration for process services”.

3.1 CPI - Using Multiple Certificates for Different Companies

If it is necessary to use different certificates for multiple companies, you must upload these pfx-files to the CPI keystore. Make sure that you rename each of the two different keys with suffix *_enc* and *_sig*. Avoid entries with the default name elster_hcm_ag<suffix>.

Example:

Company ABC (DE010001)	**Company XYZ (DE020001)**
elster_hcm_ag_DE010001_enc	elster_hcm_ ag_DE020001_enc
elster_hcm_ag_DE010001_sic	elster_hcm_ ag_DE020001_sic

In the corresponding Customizing in the HR system, the name of the keystore entry has to be maintained in supapplication LSTK. Details are given in step HR - *Using Multiple Certificates for Different Companies.*

4. SETUP OF THE HR PAYROLL SYSTEM

In the HR (on Premise or ECP) system, you need to configure the HTTPS connection to the CPI solution and some additional Customizing tables.

4.1 Set up HTTPS Connection to CPI System

To set up the HTTPS connection, you need the URL of the tenant (the TMN URL you received when the tenant was provisioned). You can also find the URL in the CPI Overview -> Manage Integration Content by clicking on the Integration Content.

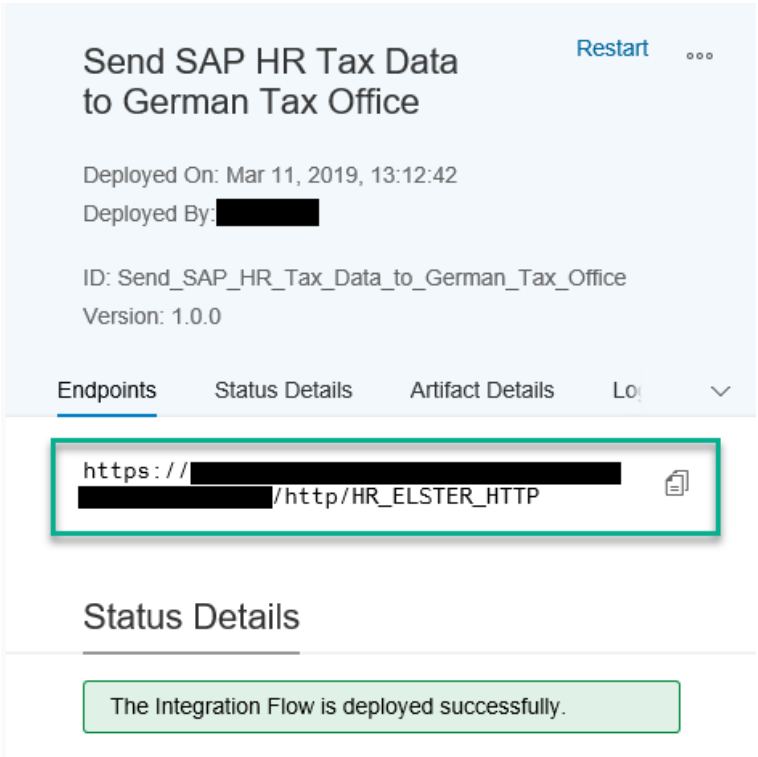

Figure 6. Manage Integration Content - Details Send SAP HR Tax Data to German Tax Office

To setup a secure HTTPS connection between the application system (HR/FI) and the Cloud Integration tenant, add the load balancer root certificate to the HR/FI trust store. Further details are available in *blog How to setup secure http inbound connection with client certificates.* https://blogs.sap.com/2017/06/05/cloud-integration-how-to-setup-secure-http-inbound-connection-with-client-certificates/

1. Start transaction SM59.
2. To create a new connection, select Edit-> Create.
3. For the RFC destination, enter value *HR_DE_ELSTER* (or if necessary another value) for the connection name. (If you use the default name *HR_DE_ELSTER,* no additional Customizing for constant RFCDE is required in later steps.)
4. Set connection type *G* (http connection to external serv).
5. Enter *ELSTER HTTPS – CPI connection* in the *Description* field.
6. On the *Technical Settings* tab, enter the following values:
    a. *Target Host:* < IFLMAP URL for the CPI tenant>
    Note: Make sure that you don't enter https:// in the field *Target Host*
    Example: 1234567890-iflmap.hcisbp.eu3.hana.ondemand.com
    b. *Service No.*: 443
    c. *Path Prefix:* /http/HR_ELSTER_HTTP
    d. *http Proxy Options <Enter own proxy values>*
    HR ECP-Customers: No entries are necessary. The proxy settings are preconfigured by SAP in the global proxy settings.

Example:

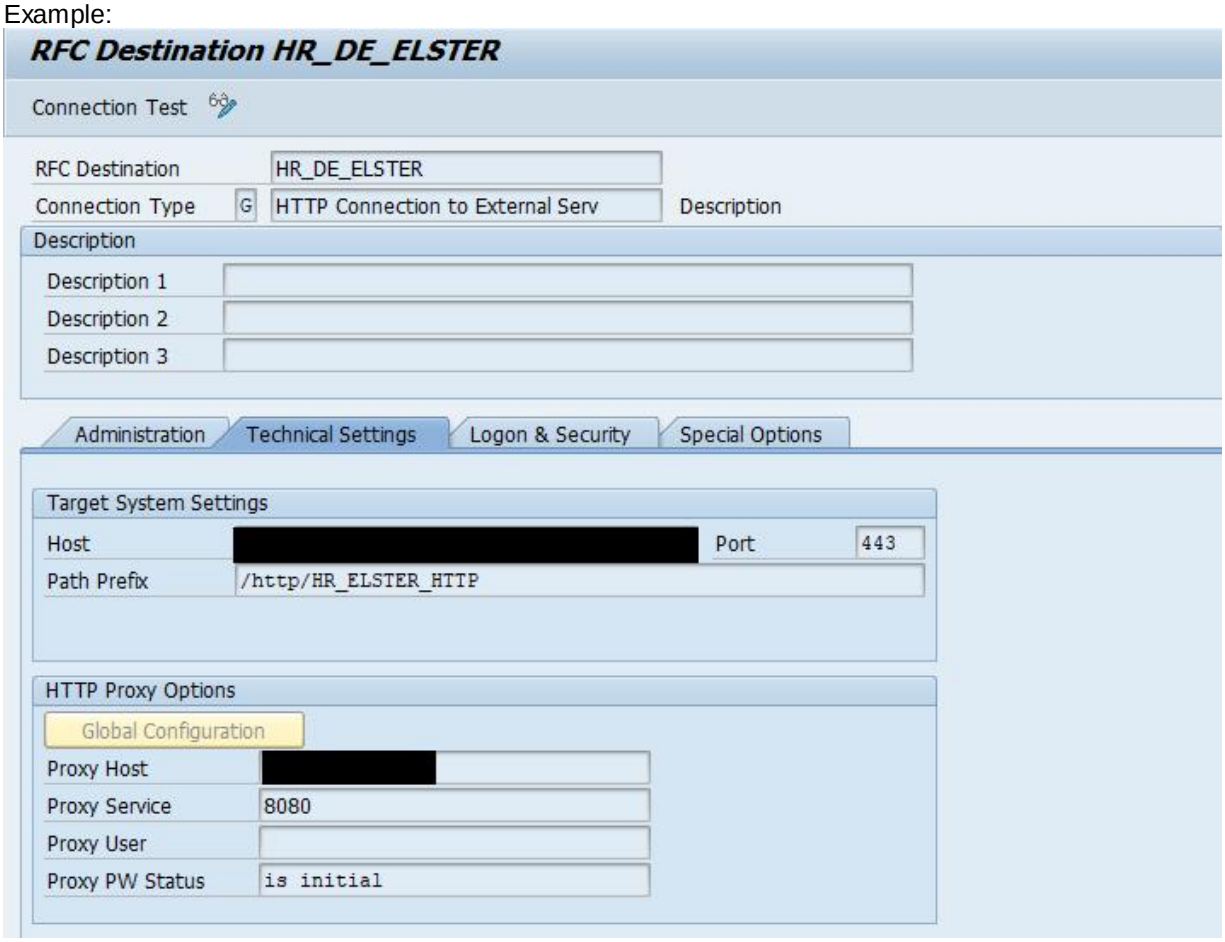

Figure 7. Transaction SM59 - Customizing HTTPS Connection

7. Logon & Security tab

There are two options for setting up the authentication: basic authentication or client certificate-based authentication. The more secure option is to use client certificates.

Basic Authentication

· Create a user in Cloud Integration and assign the ESBMessaging.send role. More information can be found in the documentation in chapter *Defining Permissions for senders to Process Messages on the Runtime Node*. https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/24585cc503334e6c917ef383efb5558a.html?q=ESBMessaging.send

In the Logon & Security tab enter:

a. Logon with user: Choose *Basic Authentication* and enter a valid user and password for logging on to CPI

b. Logon with ticket: Select *Do Not Send Logon Ticket*

c. Security options: Select SSL *Active* and SSL Certificate *Default SSL Client (Standard)*

Example

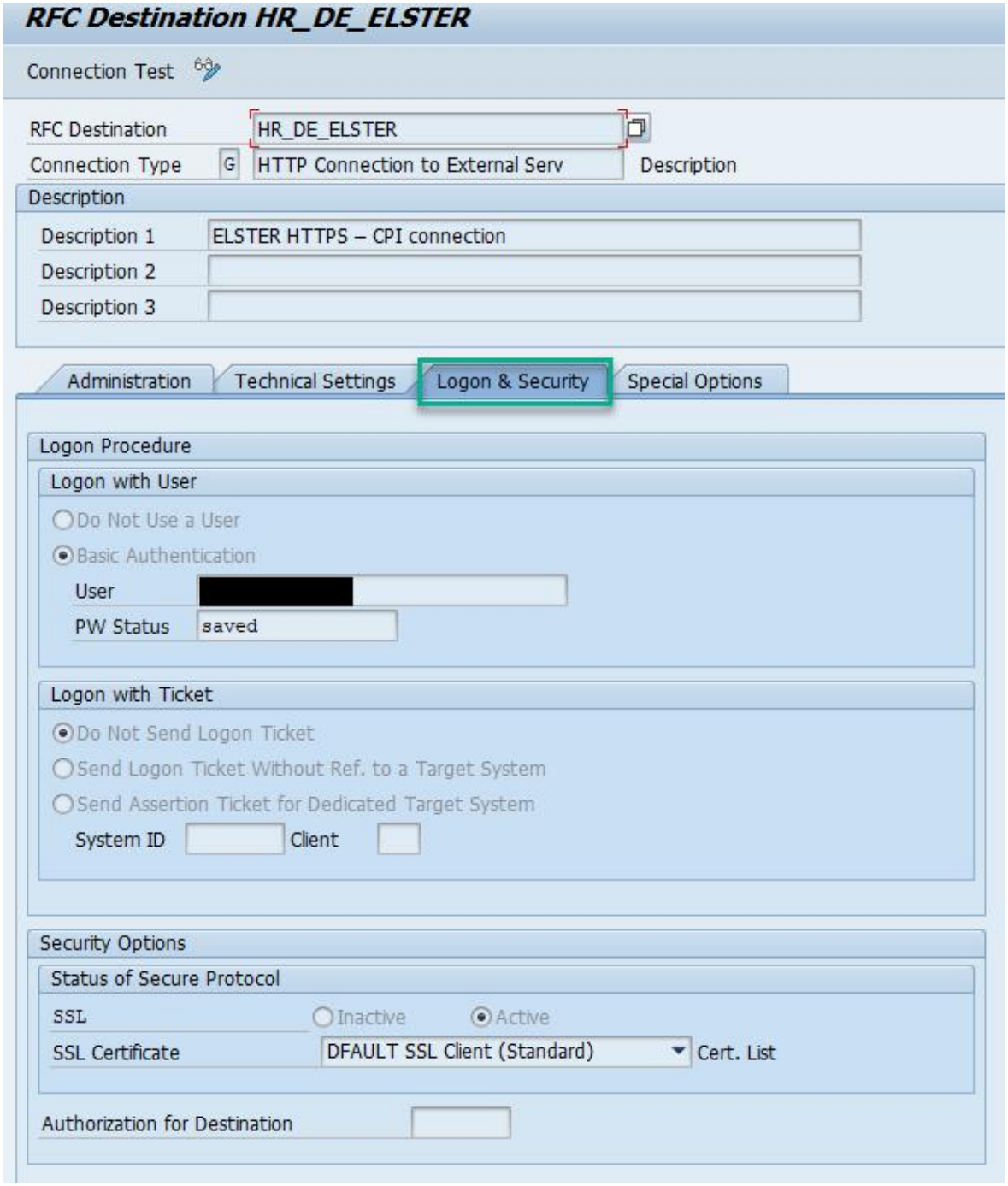

Figure 8. Transaction SM59 - Customizing HTTPS Connection

Client certificate-based authentication

- Set up the client certificate in the HR/FI system and upload to Cloud Integration in the certificate-to-user mapping as described in the blog *How to setup secure http inbound connection with client certificates*. https://blogs.sap.com/2017/06/05/cloud-integration-how-to-setup-secure-http-inbound-connection-with-client-certificates/

4. 2 Customizing V_T50BK

4.2.1 Constant USEXI

Use constant USEXI to enable the usage of CPI ERiC for communication with the authority. For all three tax types, constant USEXI must be set to value *CPIERIC*.

Area	Document Type	Constant	From	To	Value
ST	LSTA	USEXI	01.01.1800	31.12.9999	CPIERIC
ST	LSTB	USEXI	01.01.1800	31.12.9999	CPIERIC
ST	E2AE	USEXI	01.01.1800	31.12.9999	CPIERIC

Example:

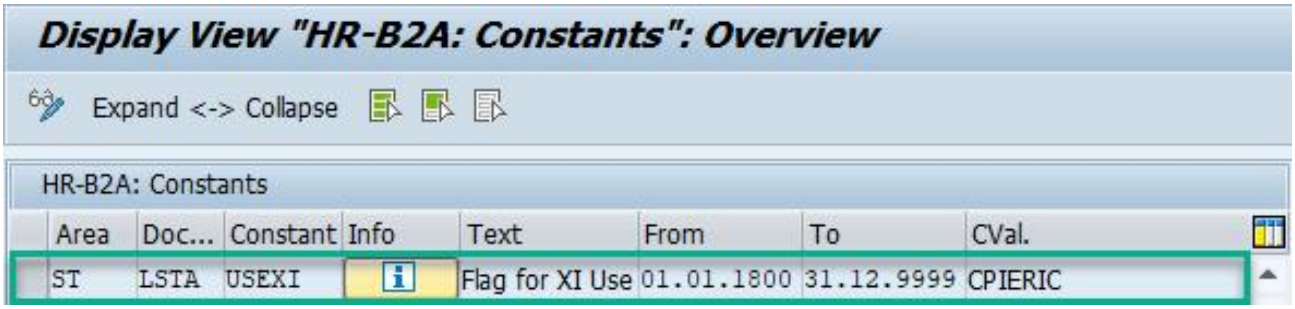

Figure 9. View V_T50BK

4.2.2 Constant RFCDE

Use constant RFCDE to set the HTTPS connection, which is used to connect to the CPI system. If there is no value provided for the constant, the system uses HR_DE_ELSTER for the connection. To use a connection different to HR_DE_ELSTER, set the connection name as the constant value for RFCDE. In this case, constant RFCDE must be set for all three tax types.

Area	Document Type	Constant	From	To	Value
ST	LSTA	RFCDE	01.01.1800	31.12.9999	
ST	LSTB	RFCDE	01.01.1800	31.12.9999	
ST	E2AE	RFCDE	01.01.1800	31.12.9999	

Example:

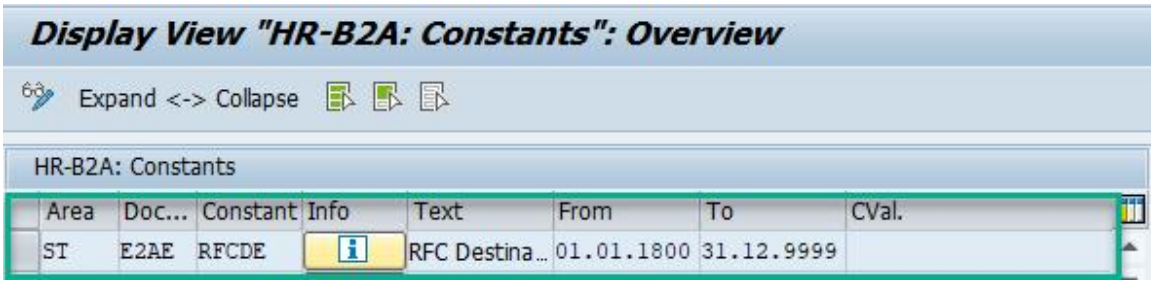

Figure 10. View V_T50BK

In this case (no constant value provided), the system uses HR_DE_ELSTER to connect to the CPI system.

4.3 HR - Using Multiple Certificates for Different Companies

The tax authority provides the employer with a certificate. Technically you do not have to use more than one certificate to exchange data from one HR system (On Premise or ECP) with the tax authority. In the HR system, you can define one company as the data provider. The tax authority has issued the certificate for this data provider. The data provider is defined in subapplication LSTD *Employment Tax Statement - Data Provider* in View V_T596M.

If only one data provider is used, it is sufficient to upload the corresponding certificate with alias elster_hcm_ag<suffic> to the CPI certificate store. As elster_hcm_ag is the default name for the certificate, no further Customizing for the certificate is necessary in the HR system.

If different certificates should be used for different data providers (companies), the following Customizing steps are necessary:

1. Ensure that the different data providers are defined in subapplication LSTD.
2. Upload the different company certificate with different aliases (for example, elster_hcm_ag_DE010001<suffic>, elster_hcm_ag_DE020001<suffic>) to the certificate store.
3. Maintain the different aliases in subapplication LSTK, View V_T596M.

Example:

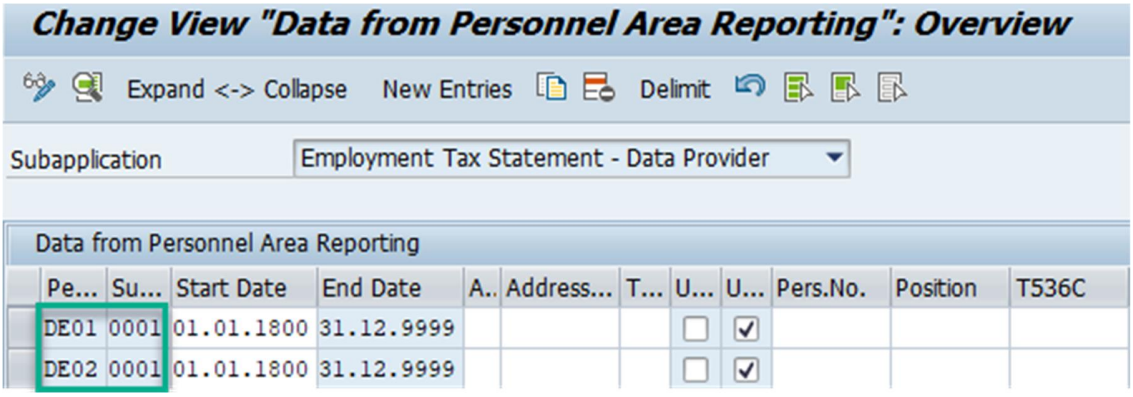

Figure 11. Customizing subapplication LSTK

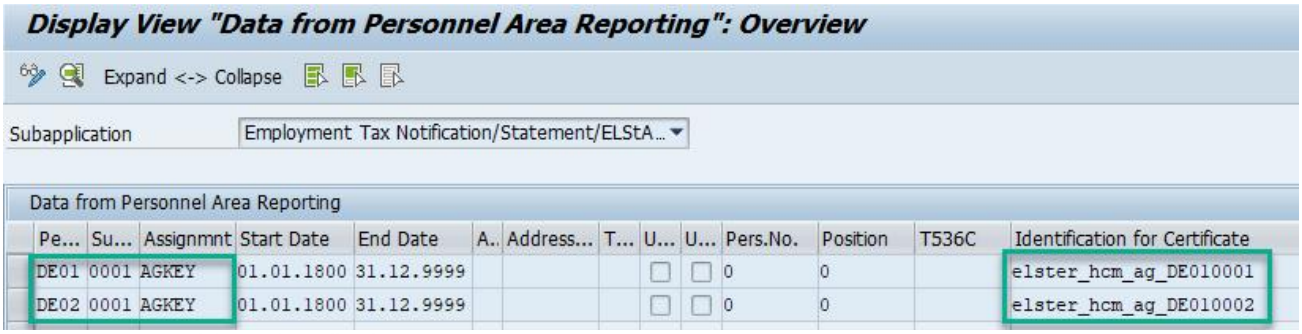

Figure 12. Customizing subapplication LSTK

5. TESTING

For testing, use program Test Report for Communication ETNotif./ETStmt/ELStAM (RPUTX7D0).

1. Go to transaction SA38 or SE38.
2. Enter the report name RPUTX7D0 and choose the Execute (F8) button.
3. On the selection screen, you can choose the tax type you want to test. Make sure that you test all three tax types. There are also additional fields on the selection screen. These fields are optional and may only be used for specific tests.
4. Start the report. The report sends XML test data to the authority and also checks if the authority receives this data.

6. EXTERNAL INFORMATION AND LINKS

Overview: Cloud Integration - Usage of the ELSTER Adapter

www.sap.com/contactsap

THE BEST RUN SAP®