# [DEPRECATED]

# ELSTER - HR Tax Integration for Germany

SAP Cloud Platform Integration Configuration

THE BEST RUN SAP

# TABLE OF CONTENTS

# 1 PREREQUISITES

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 Set up Tenants

SAP CLOUD PLATFORM INTEGRATION 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, the required role is ‘AuthGroup.Administrator’. For the subsequent configuration of ECP, note down the URL of the tenant (it is the TMN URL which you received when the tenant was provisioned).

### 1.1.2 Deploy Certificates for SAP CLOUD INTEGRATION

To establish a connection between the SAP Cloud Integration and Tax Agency servers, you must obtain several certificates, and then deploy these to the SAP Cloud Platform Integration tenant. 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”.

# 2 SETUP STEPS IN SAP CLOUD PLATFORM INTEGRATION

## 2.1 Copy Published Package ‘ELSTER Integration for Germany’ into Your Package

Go to the ‘Discover’ chapter of your tenant and find the package ‘ELSTER Integration 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.

If your usage scenario requires more than one company code data to be submitted to the tax agency, copy the data more than once. In this case, you will see the warning ‘Could not copy package, as its already exists…’:

Click on the ‘Create copy’ button; new dialog window ‘Provide suffix’ will appear, it is recommended to provide suffix corresponding to the company code or company name:

## 2.2 Configure Integration Flow for HCM Data

**Note:** This step must be repeated for every package that was copied as described in chapter

**1)** Go to the integration package that was copied from the original ‘ELSTER Integration for Germany’.

**2)** Click on the Artifacts tab.

**3)** Click on action button that corresponds to integration flow ‘Send ELSTER HCM Data‘.

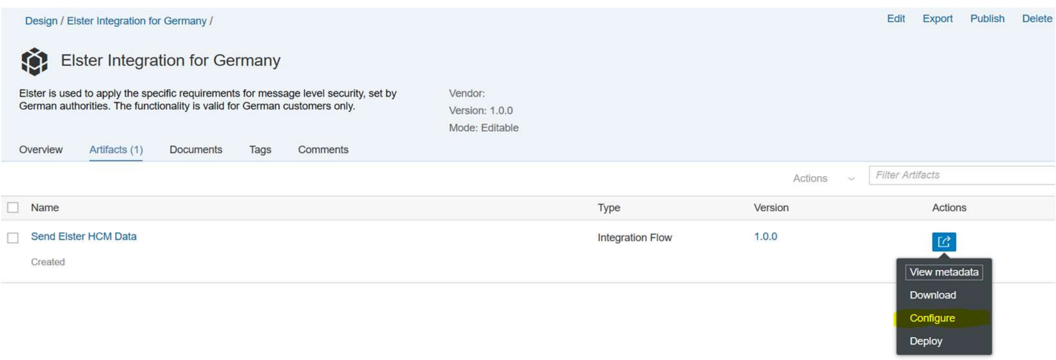



*Figure 1. ELSTER integration package “Artifacts” tab.*

**Note:** the version of the integration on the screenshot may differ from the current one.

4) Choose Configure and maintain the following configuration the parameters as described below.

### 2.2.1 Configure Sender Tab

• Update the connection address to a name that can be linked easily to the company code that uses it (e.g. /ELSTER_HTTP_Sender)

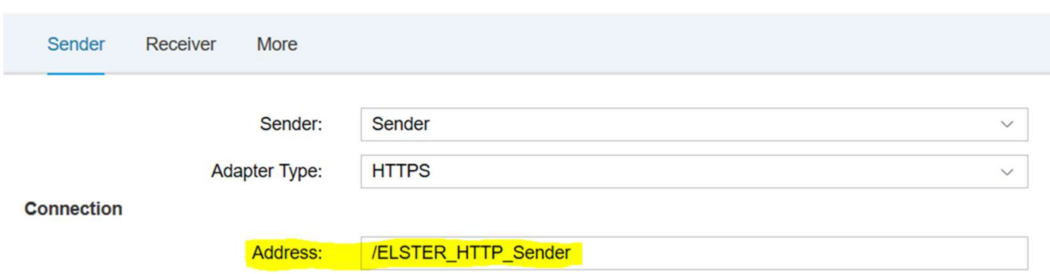



*Figure 2. "Send ELSTER HCM Data" iFlow - Sender adapter properties*

• Select the required authorization (User Role or Client Certificate) that has been configured for the connection between your ERP system and the tenant:

**a.** For the User Role authorization, please select relevant user role (e.g. ESBMessaging.send)


*Figure 3. Authorization properties - "User Role"*

**b.** For the Client Certificate authorization, please provide certificate credentials


*Figure 4. Authorization properties - "Client Certificate"*

## 2.1.2 Configure Receiver Tab

- Update the connection address to be used. By default the message header „ELSTER URL“ is used. If not modified, by default this header stands for „http://datenannahme1.elster.de/Elster2/EMS“

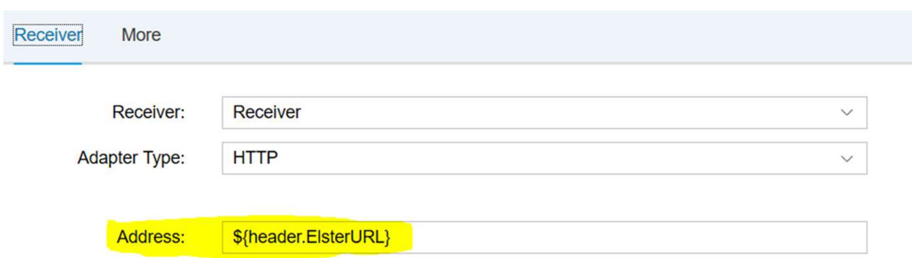



*Figure 5. "Send ELSTER HCM Data" iFlow - Receiver adapter properties*

- Select The required Authorization (None, Basic for Client Certificates)

  **a.** For the **“*Client Certificate*”** option, please provide the certificate alias (Figure 6.)


*Figure 6. Authentication properties - "Client Certificate"*

**b.** For **“*Basic*”** authentication, please provide the credential name. (Figure 7.)


*Figure 7. Authentication properties - "Basic"*

**c.** Use **“*None*”**, if no authentication is required.

## 2.2.3 Configure “More” Tab

**Note:** the layout under this menu tab may differ from the screenshot provided

In this tab you can find the following properties:

- ***ELSTER URL***: This is the URL that will be used by the receiver adapter (if the address is configured as “${header.ElsterURL}”.
- ***OwnCertificates***: The alias of the private key, used for data signing and decryption.
- ***PartnerCertificates***: The alias of the certificate used for data sent/received from ELSTER authorities to be encrypted.

***Note:** The default values of this properties can be found in “Figure 8”.*

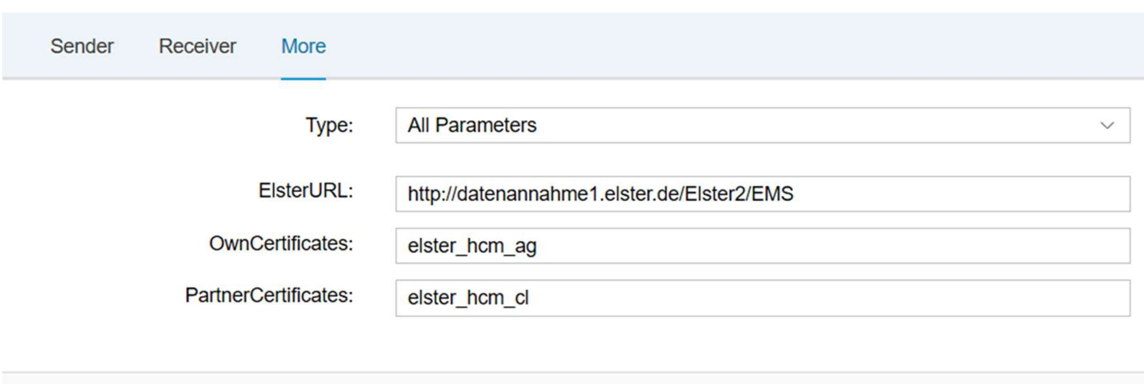



*Figure 8. "Send ELSTER HCM Data" iFlow - "More" tab*

## 2.3 Using payload data to dynamically setup the properties.

This iFlow can work with two types of payloads. The first one is the standard ELSTER payload. The second one follows the structure described in “Figure 9”:

```
<SAP>
    <DATTYPE> {Payload type} </DATTYPE>
    <URL> {URL to the German authorities} </URL>
    <CERTSTORE>
        <CERT_AG> {certificate alias} </CERT_AG>
        <CERT_CL> {certificate alias} </CERT_CL>
    </CERTSTORE>
    <TRACE> {DEUG, INFO, etc.} </TRACE>
    <ELSTER> {Base64 encoded ELSTER payload} </ELSTER>
</SAP>
```

*Figure 9. XML Format of the payload.*

The table below show the relation between the payload properties and the iFlow properties:

| Payload Property | iFlow property | Default Value | Description |
|---|---|---|---|
| DATTYPE | N/A | Not used yet | Not used yet |
| URL | ElsterURL | http://datenannahme1.elster.de/Elster2/EMS | The URL to the German authorities |
| CERT_AG | OwnCertificates | elster_hcm_ag | The alias of the private key, used for data signing and decryption. |
| CERT_CL | PartnerCertificates | elster_hcm_cl | The alias of the certificate used for data sent/received from ELSTER authorities to be encrypted. |
| TRACE | N/A | Not used yet | Not used yet |
| ELSTER | N/A | N/A | The payload itself |

# 4. Setup of the Employee Central Payroll System

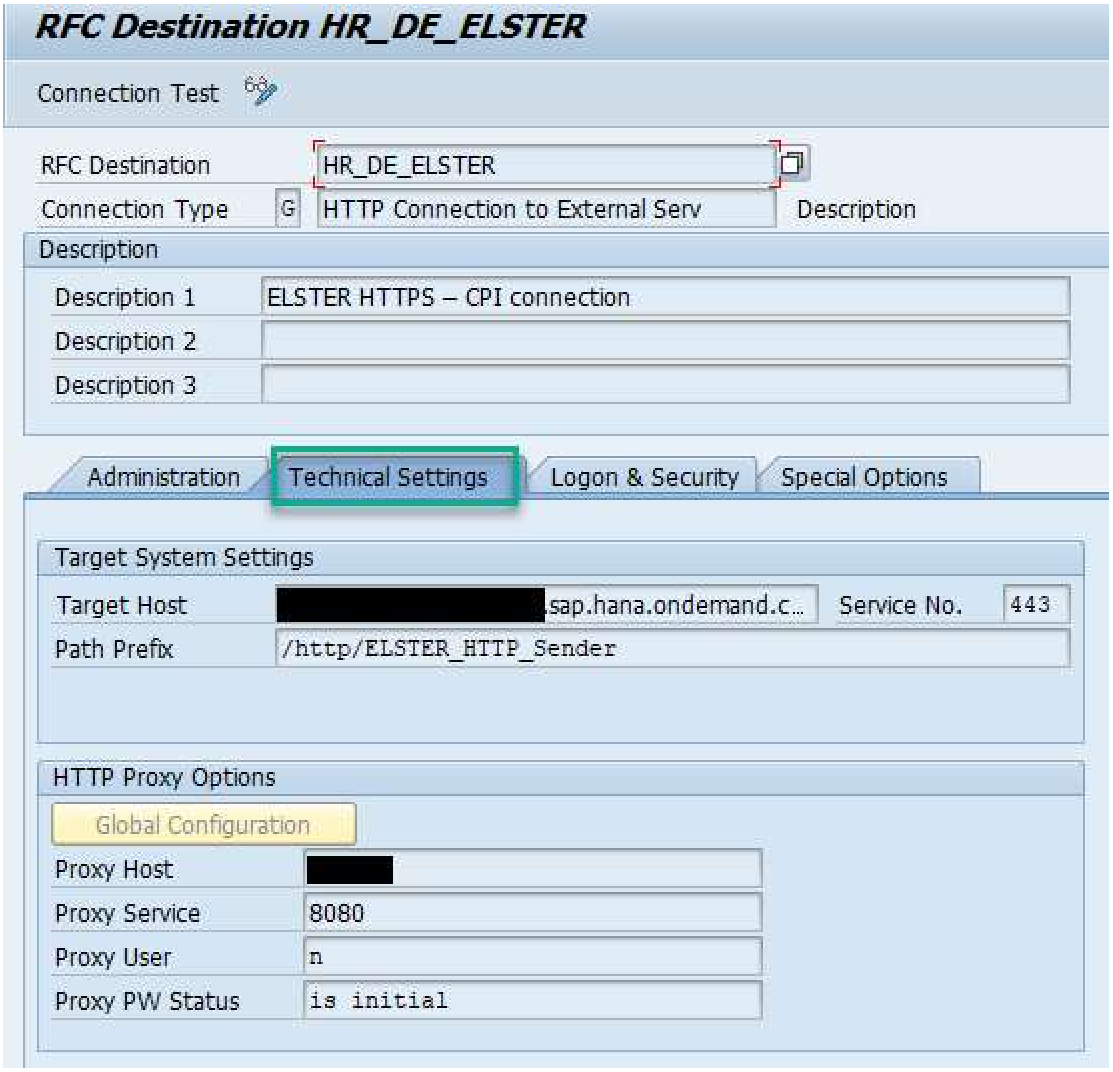
In the ECP system, you need to configure the HTTPS-connection to the CPI solution and some additional Customizing tables.

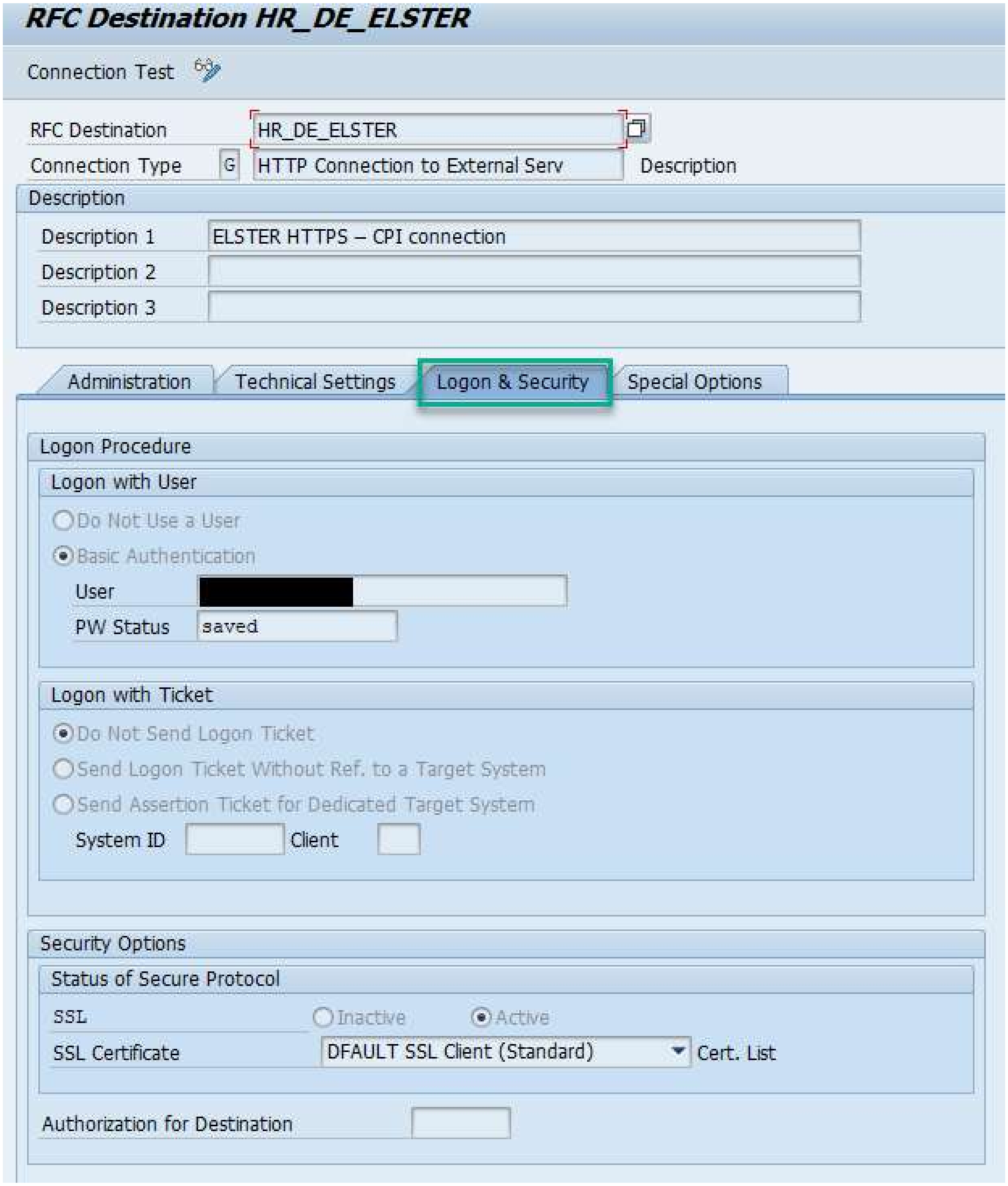
## 4.1. Set up HTTPS Connection to CPI System

To set up the HTTPS connection, you need the URL of the tenant (it is the TMN URL which you received when the tenant was provisioned).

1. Start transaction SM59.
2. To create a new connection, select Edit-> Create.
3. For the RFC destination, enter the 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:* <TMN URL for the CPI tenant>
    b. *Service No.*: 443
    c. *Path Prefix:* /http/ELSTER_HTTP_Sender
    d. *http Proxy Options <Enter own proxy values>*
7. On the Logon & Security tab, enter the following values:
    a. *Logon with User*: Choose *Basic Authentication* and enter a valid User and PW for logon 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:


RFC Destination HR_DE_ELSTER
Connection Test
RFC Destination
HR_DE_ELSTER
Connection Type
G
HTTP Connection to External Serv
Description
Description
Description 1
ELSTER HTTPS – CPI connection
Description 2
Description 3
Administration
Technical Settings
Logon & Security
Special Options
Target System Settings
Target Host
[redacted].sap.hana.ondemand.c...
Service No.
443
Path Prefix
/http/ELSTER_HTTP_Sender
HTTP Proxy Options
Global Configuration
Proxy Host
[redacted]
Proxy Service
8080
Proxy User
n
Proxy PW Status
is initial


RFC Destination HR_DE_ELSTER
Connection Test
RFC Destination
HR_DE_ELSTER
Connection Type
G
HTTP Connection to External Serv
Description
Description
Description 1
ELSTER HTTPS – CPI connection
Description 2
Description 3
Administration
Technical Settings
Logon & Security
Special Options
Logon Procedure
Logon with User
Do Not Use a User
Basic Authentication
User
[redacted]
PW Status
saved
Logon with Ticket
Do Not Send Logon Ticket
Send Logon Ticket Without Ref. to a Target System
Send Assertion Ticket for Dedicated Target System
System ID
Client
Security Options
Status of Secure Protocol
SSL
Inactive
Active
SSL Certificate
DFAULT SSL Client (Standard)
Cert. List
Authorization for Destination

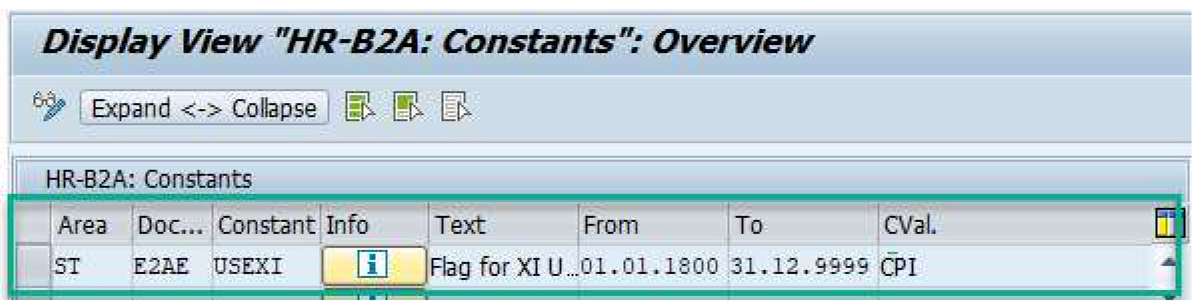
## 4.2. Customizing V_T50BK

### 4.2.1. Constant USEXI

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

| Area | Document Type | Constant | From | To | Value |
|---|---|---|---|---|---|
| ST | LSTA | USEXI | 01.01.1800 | 31.12.9999 | CPI |
| ST | LSTB | USEXI | 01.01.1800 | 31.12.9999 | CPI |
| ST | E2AE | USEXI | 01.01.1800 | 31.12.9999 | CPI |

Example:



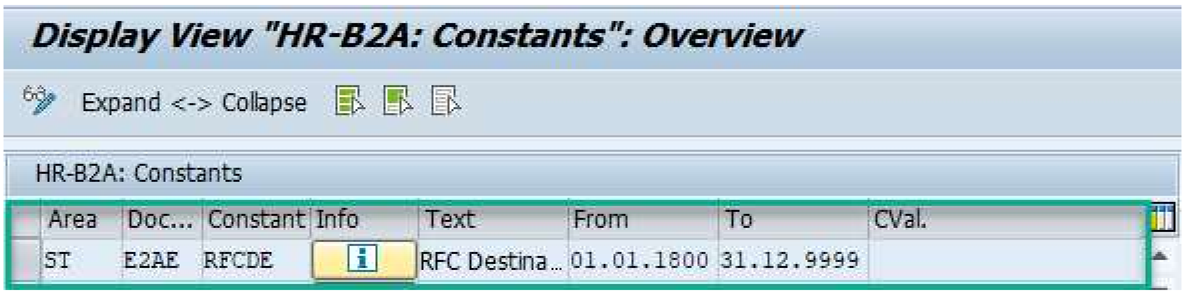

### 4.2.2. Constant RFCDE

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:




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

## 4.3. Using Multiple Certificates for Different Companies

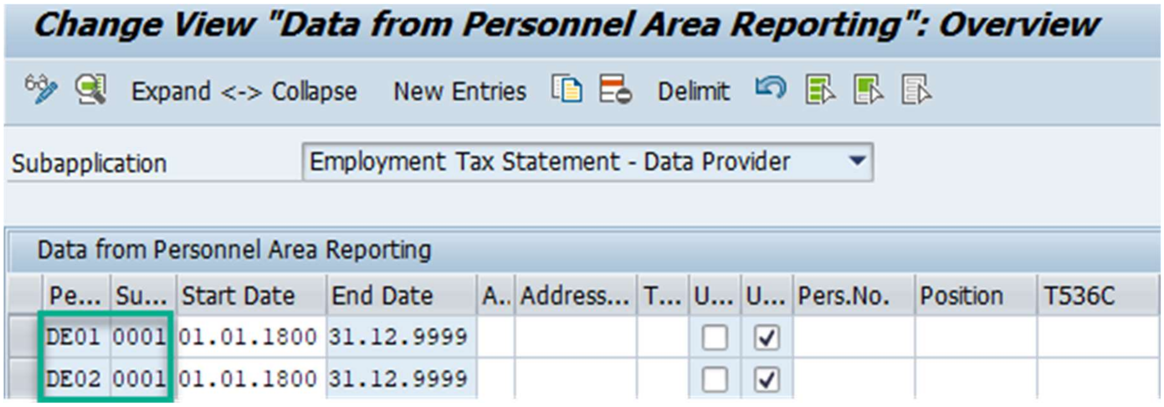
The tax authority provides the employer with a certificate. Technically you do not have to use more than one certificate to exchange data from one ECP system with the tax authority. In the ECP system, you can define one company as the data provider. The tax authority has issued the certificate for this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

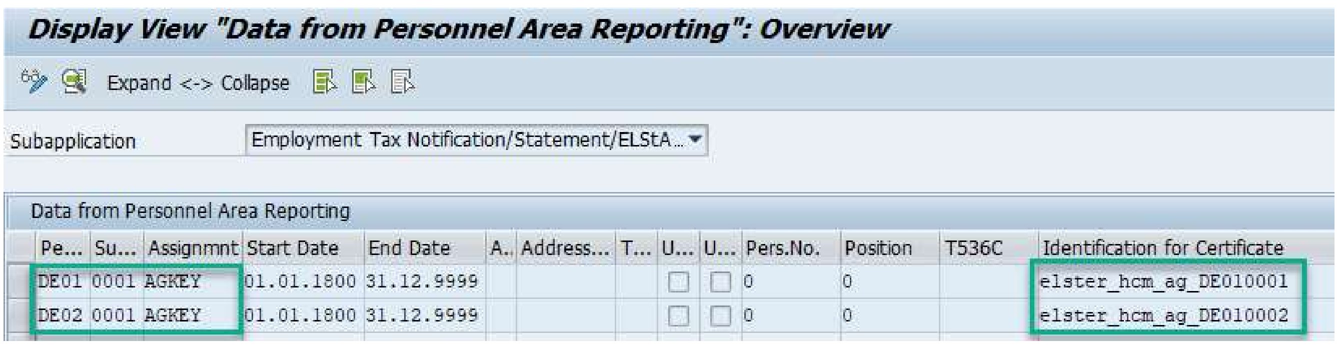
If only one data provider is used, it is sufficient to upload the corresponding certificate with alias elster_hcm_ag in the CPI certificate store. As elster_hcm_ag is the default name for the certificate, no further Customizing for the certificate is necessary in the ECP system.

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, elster_hcm_ag_DE020001) to the certificate store
3. Maintain the different aliases in subapplication LSTK, View V_T596M

Example:




## 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 be used only 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

ELSTER Integration

Troubleshooting process for ELSTER related PI scenarios

**www.sap.com/contactsap**



THE BEST RUN SAP®