ELSTER Receiver Adapter

This adapter enables an SAP BTP tenant to send a tax document to the ELSTER server.

Note
In the following cases certain features might not be available for your current integration flow:

- You are using a runtime profile other than the one expected. See: Runtime Profiles.
- A feature for a particular adapter or step was released after you created the corresponding shape in your integration flow.

  To use the latest version of a flow step or adapter – edit your integration flow, delete the flow step or adapter, add the step or adapter, and configure the same. Finally, redeploy the integration flow. See: Updating your Existing Integration Flow.

Note

This adapter exchanges data with a remote component that might be outside the scope of SAP. Make sure that the data exchange complies with your company's policies.

ELSTER (acronym for the German term *Elektronische Steuererklärung*) is used by the German fiscal management to process tax declarations exchanged over the Internet.

To enable a client to send tax data to German tax authorities, those organizations provide the *ERiC* (*ELSTER Rich Client*) library for sending tax documents. The ELSTER adapter is designed that way that it complies with the requirements of this library and, therefore, enables Cloud Integration to connect as a client to the ELSTER server.

Note

Using this adapter makes only sense in the context of a standard integration scenario (predefined by SAP or an SAP partner) that includes the communication with German tax authorities.

The adapter supports validate and send operations.

The input payload for the ELSTER adapter is supposed to be a complete, valid payload (tax document) including the transfer header. Note that, however, the XML document can have an arbitrary encoding (if this is properly defined in the XML preamble). The adapter ensures that the payload is converted to the encoding the ELSTER server supports (currently *ISO-8859-15*, in future versions this will change to *UTF-8*).

The output payload (sent by Cloud Integration through the ELSTER receiver adapter) will be validated by the ELSTER server.

The inclusion of the transfer header implies that only applications that are registered with the German tax authorities and have a valid vendor ID can actually send messages through the ELSTER adapter.

Note

This software collects personal data according to Article 4, Number 1 and Article 9, Paragraph 1 of the German General Data Protection Regulation (Datenschutzgrundverordnung, DSGVO). In addition to data that is required for the assessment of taxes, this software also collects data related

to the kind of operating system used by the user and transfers it to the fiscal authorities. This information ensures the proper processing of the data and avoids errors in the process.

This data is used by the fiscal authorities according to Article 6, Paragraph 1, Letter e in connection with Paragraph 3, Subparagraph 1, Letter b DSGVO in connection with federal and state tax regulations and exclusively for the purposes mentioned.

Headers

The validate and send operation of the ELSTER receiver adapter sets a header (`SAP_ERiCResponse`) that contains a technical status created by the ERiC library.

The adapter does not read any headers.

Once you have created a receiver channel and selected the Elster Receiver Adapter, you can configure the following attributes. See Overview of Integration Flow Editor.

Select the General tab and provide values in the fields as follows.

General

Parameter	Description
Name	Enter the name of the channel.

Select the Connection tab and provide values in the fields as follows.

Connection

Parameter	Description
Operation	The following operations are supported: • Get Version Gets the versions of the ERiC library provided by the server. The response contains the major, minor, and micro ERiC version (for example, `29.6.2`). • Validate Validates the tax document. Validation of a tax document without sending it only requires the document type (Data Type). Key aliases (Private Key Alias for Encryption and Private Key Alias for Signing) are not required in that case. • Validate and Send Validates the tax document sent to the ELSTER server. In case the server cannot accept the document (maybe it is wrong formatted) or in case the server is down, an error message is provided. In such a case, check the

Parameter	Description
	message processing log and, in case you need more information, the default trace.
Proxy Type	Proxy type to be used to connect to the SFTP server. Choose between the following options: • Internet • Manual This option is only available if Edge has been selected as runtime.
Proxy Host (only available if Manual is selected for Proxy Type)	Enter the name of the proxy host to be used. For example: `proxy.mycompany.com`.
Proxy Port (only available if Manual is selected for Proxy Type)	Enter the proxy port number to be used.
Proxy Credential Name (only available if Manual is selected for Proxy Type)	Enter the referenced credential name used for proxy authentication.
Data Type	Indicates the type of the document provided as payload. Information about the type is required by the ELSTER server to determine the method to be applied by the tax authority. For example, if the value `LStA_2019` is specified, the method *ElsterAnmeldung* can be executed by the server for the year 2019. Other examples are: `DUeAbmelden`, `DUeAnmelden`, `UStVA_2018` or `UStVA_2019`. You can also dynamically configure this parameter with an expression such like `${header.datatype}` or `${property.datatype}` to retrieve the data format dynamically at runtime.

Parameter	Description
Private Key Alias for Encryption	Alias for the key to be used for message encryption Note that X.509 key pair needs to be uploaded to the tenant keystore to set up this scenario. You can also dynamically configure this parameter with an expression such like `${header.encryptionkey}` or `${property.encryptionkey}` to dynamically retrieve its value at runtime.
Private Key Alias for Signing	Alias for the key pair (private part) to be used for message signing. Note that X.509 key pair needs to be uploaded to the tenant keystore Alias for the key pair (private part) to be used for message signing. Note that X.509 key pair needs to be uploaded to the tenant keystore. You can also dynamically configure this parameter with an expression such like `${header.signaturekey}` or `${property.signaturekey}` to dynamically retrieve its value at runtime. You can also dynamically configure this parameter with an expression such like ${header.signaturekey} to dynamically retrieve its value at runtime.