Troubleshooting – Recipient in SubjectConfirmationData is invalid

Author : Tobias Hofmann

Date : May 6, 2020

Scenario

A user authenticated against the SAML 2.0 IdP. The OAuth client is sending the SAML 2.0 Response containing the user assertions to the NetWeaver ABAP system. An error of type invalid grant is returned.

Error message:

```
{     "error": "invalid_grant",     "error_description": "Provided authorizati
on grant is invalid. Exception was Attribute 'Recipient' of element 'SubjectCo
nfirmationData' is invalid. For more information, consult the kernel traces or
 the OAuth 2.0 trouble shooting SAP note 1688545" }
```

Root cause

The OAuth client is sending the SAML Response to the OAuth token service for validation. The SAML Response is configured for a different SAML endpoint in the ABAP system. Therefore the request is denied.

Solution

Configure Keycloak to send the SAML Response to the NW ABBAP OAuth token service. Open the Keycloak administrator console and go to the SAML configuration for the NetWeaver client. Expand the section for Fine Grain SAML Endpoint Configuration.

Here the endpoint is configured to the standard value for SAML in NW ABAP: /sap/saml2/sp/acs/.

https://vhcalnplci:44300/sap/saml2/sp/acs/001

This must be changed to the OAuth token endpoint:

https://vhcalnplci:44300/sap/bc/sec/oauth2/token

Additionally, you can configure the list of valid redirect URIs. By default, these are set to the standard SAML values of NW ABAP as a service provider.

https://vhcalnplci:44300/sap/saml2/sp/acs/001

In a test/POC environment, these can be set to match all URIs.

Set it to /*