Single Sign on using SAML with IBM DataPower (XML Appliance)

IBM DataPower

IBM DataPower is an XML appliance providing generic XML and XML security processing.

Checking SAP Notes

SAML Sender-vouches is supported with releases AS ABAP 7.00 (SP 15) and higher. Please ensure the following SAP notes have been applied:

**AS ABAP 7.00:**
- SAP Notes: 1176558, 1325457
- Kernel Patch level: 207

**AS ABAP 7.01:**
- Support Package SP5
- Kernel patch level: 74

**AS ABAP 7.10:**
- SAP Notes 1170238, 1325457
- Kernel patch level: 150

Configure the provider

The ws provider needs to be configured to SAML Sender-Vouches authentication. To create such a configuration, follow the instructions.

Configure Trust between DataPower and SAP WebAS ABAP

A key must be generated on DataPower and exported into the SAP system to establish the trust. While many tools may be used to create such a key, recommended solution is to use the DataPower crypto toolkit as this also installs the keys into DataPower.

Any SAML assertion created by DataPower needs to be trusted by the SAP system and be mapped to an SAP user. Please follow the instructions from section Configure Trust for SAML SenderVouches authentication (ABAP) using the following information:

- SAML Issuer: <as defined in DataPower>
- SAML Name Identifier: (empty, not used)
- Subject of the X.509 certificate used for the message signature (from the example): CN=DataPower OU=NW SIM, O=NW, L=Walldorf, SP=Baden Wuerttemberg, C=DE

WSDL Files

SAP systems can generate different flavors of WSDL files. The WSDL files expected by DataPower must not contain WS-Policy. By default the 7.00 ABAP systems generate a WSDL with WS-Policy. To generate a WSDL without Policy, change the WSDL URL by replacing `ws_policy` with `standard`, i.e.


DataPower Configuration

1. Set the AAA Policy to authentication and authorize steps
2. Set post processing "Generate SAML Assertion" and set:
   1. SAML Version 1.1
   2. SAML Issuer (as used for the user mapping)
   3. Assertion validity: 300
   4. SAML Message Signing Key: none
5. SAML Message Signing Certificate: none
6. SAML Message Signing Algorithm: rsa
7. SAML Signing Digest Algorithm: sha1
8. Wrap SAML Assertion in a WS-Security Header: on

3. Add an STR-Transform as XSLT transform
4. Configure certificate to be send

Expected SOAP messages

See Single Sign on using SAML Sender Vouches example