JBoss Identity Federation

Developer Guide

1.0.0.alpha1.

by Anil Saldhana

What this Book Covers?

This book aims to help you become familiar with JBoss Identity Federation in order that you can use it to develop your own Federated Identity based services or applications.

Part I 'Getting Started' introduces the federated identity technologies that are provided in this product.

Part II 'Developer Usage' takes a look at the API and Object Model available to you to create applications and services for your needs with Federated Identity.

Part IV 'Resources' provides additional resources.

Part I. Getting Started

Introduction

JBoss Identity Federation allows you to implement SAML v2.0 based services and applications. It also has support for Oasis WS-Trust based applications.

With JBoss Identity Federation, you have the following features.

- SAML v2 and WS-Trust v1.3 Object Model.
- SAML v2 Identity API.
- SAML v2 HTTP/Redirect Binding Support for JBoss and Tomcat.
- SAML v2 HTTP/Redirect Binding Support for JBoss and Tomcat with XML Signature Support.
- WS-Trust Security Token Service (STS).

The SAML v2 specification provides multiple profiles and bindings. In this version of the product, we provide support for web browser based single sign on (SSO) via HTTP/Redirect Binding.

An user/developer is free to implement the other profiles and bindings using the object model provided in this product.

Part II. Developer Usage

Identity API for SAML v2

Note

Use SAML2Request API class for creating SAML request objects.

Use SAML2Response API class for creating SAML response objects.

The following examples displays usage of the API provided in the Identity Federation product.

The SAML2Request API class can be used to create SAML2 requests and convert it into XML and back using the marshall or unmarshall methods.

```
import org.jboss.identity.federation.api.saml.v2.request.SAML2Request;
import org.jboss.identity.federation.saml.v2.protocol.LogoutRequestType;

SAML2Request saml2Request = new SAML2Request();

//We will create an AuthnRequest
AuthnRequestType authnRequest = request.createAuthnRequestType(
  id, "http://sp", "http://idp", "http://sp");

//Now marshall the request into a byte array based output stream
ByteArrayOutputStream baos = new ByteArrayOutputStream();
request.marshall(authnRequest, baos);
request.marshall(authnRequest, System.out); //To Console

//Assume that we have an inputstream where we get the SAML feed
InputStream is = new ByteArrayInputStream(baos.toCharArray());
authnRequest = saml2Request.unmarshall(is);

//We will create a log out request
LogoutRequestType lrt = saml2Request.createLogoutRequest("http://idp");
```

SAML2Response API class can be used to create SAML2 response objects as well as marshall and unmarshall to xml and back.

```
import org.jboss.identity.federation.api.saml.v2.request.SAML2Response;
```

```
SAML2Response saml2Response = new SAML2Response();
saml2Response.createTimedConditions(assertion, this.assertionValidity)

//IssuerInfoHolder is a class for information on the Issuer of SAML Assertions
IssuerInfoHolder issuerHolder = new IssuerInfoHolder("http://idp");
issuerHolder.setStatusCode(JBossSAMLURIConstants.STATUS_SUCCESS.get());

//IDPInfoHolder is a class for information on the Identity Provider
IDPInfoHolder idp = new IDPInfoHolder();
idp.setNameIDFormatValue(IDGenerator.create());

//SPInfoHolder is a class for information on the Service Provider

ResponseType rt = JBossSAMLAuthnResponseFactory.createResponseType(
    "response111",
    new SPInfoHolder(), idp, issuerHolder);

ByteArrayOutputStream baos = new ByteArrayOutputStream();
saml2Response.marshall(rt, baos);
```

JAXB2 Based Object Model for SAML and WS-Trust

JBoss Identity Federation contains an object model for SAMLv2 and WS-Trust v1.3 applications. The object model is very useful for developers who want to build advanced applications that are not fully supported by the Identity API from the previous section.

Object Model for SAML v2

org.jboss.identity.federation.saml.v2 is the package that contains the object model.

Object Model for WS-Trust v1.3

org.jboss.identity.federation.ws.trust is the package that contains the object model.

Part III. Resources

Resources on the Web

JBossIdentity Project Page [http://www.jboss.org/jbossidentity]

JBoss Identity Design Forum [http://www.jboss.com/index.html?module=bb&c=32]