How to authenticate application users using SAML

Applicable Releases:
SAP Mobile Platform 3.0 SP6

Version 1.0 - April 2015

Document History

<table>
<thead>
<tr>
<th>Document Version</th>
<th>Authored By</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Technology RIG</td>
<td>First release of this guide</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

1. **Scenario** ........................................................................................................................................... 4  
2. **Background** ....................................................................................................................................... 4  
3. **Prerequisites for the Exercise** ........................................................................................................... 4  
4. **Step-by-Step Procedure** ................................................................................................................... 5  
   4.1  *Configure SMP “Local Service Provider” (SP)* ............................................................................... 5  
   4.2  *Upload the SP metadata & obtain the IdP metadata* ....................................................................... 8  
   4.3  *Configure SMP “Trusted Identity Provider” (IdP)* ......................................................................... 10  
   4.4  *Create a new authentication provider profile for application user* ........................................... 11  
5. **Appendix** ......................................................................................................................................... 18  
   5.1  *Enable more logging* ..................................................................................................................... 18
1. SCENARIO

In this document we will go through the process of configuring SMP to use SAML2 provider for authentication. We will start out with an existing SMP (Service Provider) system and an existing Identify Provider (IdP) system then perform the linkup between the 2 systems.

Finally, we will test the new authentication process for the user.

2. BACKGROUND

A security profile verifies the identities of application users and administrators who request access via one or more configured authentication providers. SAP Mobile Platform Server supports a variety of built-in authentication providers that authenticate users. Administrators create a security profile and assign one or more providers to it using Management Cockpit. Here is a list of authentication providers that you can use within SMP:

- No Authentication Challenge Provider
- System Login (Admin Only) Provider
- Populate JAAS Subject From Client Provider
- X.509 User Certificate Provider
- **SAML2 Provider**
- Principal Propagation Single Sign-On Provider
- HTTP/HTTPS Authentication Provider
- Kerberos Single Sign-On Provider
- Directory Service (LDAP/AD) Provider

The provider that we will be using for this exercise is SAML2 Provider. When you use the Security Assertion Markup Language 2.0 (SAML2) protocol in SAP Mobile Platform, you define a local service provider to determine authorizations based on information from a trusted identity provider. The trusted identity provider maintains its own database of users and their SAML2 attributes. When a user requests access to a resource, the service provider retrieves a SAML2 assertion from the identity provider. The service provider then reads the user name from the subject or one of the attributes in the SAML2 assertion to determine whether to grant the user access to the resource.

3. PREREQUISITES FOR THE EXERCISE

The prerequisites for this will vary but we will list what we will be using during this exercise.

- SAP Mobile Platform 3.0 – This guide will assume you have this installed and running. We are using SMP 3.0 SP6 for this exercise. Ensure you that you can start & stop the application on demand here since we will be doing this as part of the exercise. At the same time, you would need access to the file system of this OS since we will be updating some configuration file.
- Identity Provider (IdP) – this guide will assume you have access to this and have the ability to perform certain configuration within this provider. For this exercise, we will be using the SAP Cloud Identity Service.
- Web Browser – For this exercise, we will be using Chrome. You can use any other web browser.
- REST Client – Since we are Chrome, we will be using “Postman – REST Client” which mean you would need a Google account. To get the Postman client go to the Chrome store at https://chrome.google.com/webstore/category/apps?utm_source=chrome-ntp-icon and search for the postman rest client
4. **STEP-BY-STEP PROCEDURE**

This is the overall sequence of steps in the Exercise:

1. Configure SMP “Local Service Provider” (SP)
2. Upload the SP metadata & obtain the IdP metadata
3. Configure SMP “Trusted Identity Provider” (IdP)
4. Create a new authentication provider profile for application user

4.1 **Configure SMP “Local Service Provider” (SP)**

For this part of the exercise, we will be using the all the functionality that is provided by SMP to perform the configuration.

1. Login to SMP Admin Cockpit using the default account “smpAdmin” and the password that was set during the installation.

   **Note:** You may get a warning about the site certificate since it is a self-signed cert. You can just continue with the page.

2. Click on “SETTINGS” tab and “SYSTEM” tab

3. Change the year on the SAML self-signed certificate instead of the default (one year).

4. Click on the “SETTINGS” tab and “SAML” tab

5. Provider the information that is needed here

   a. “Local Provider Name” – A unique name that identifies this local service provider within all the trusted identity providers you plan to use. To ensure uniqueness, you might use a name you are certain that no one else has registered, such as DN::mysmp1. This name appears in the
trusted identity provider to represent this SAP Mobile Platform installation. Maximum length is 256 characters.

b. “Base URL” – For a single SAP Mobile Platform installation where clients connect directly to SAP Mobile Platform, you can use the fixed IP address or host name of your SAP Mobile Platform Server for the value – for example, https://198.164.10.18:8081. To test with SAP Mobile Platform SDK clients, this must be an HTTPS URL. If you are testing locally with something like a REST client, HTTP works. For an SAP Mobile Platform cluster, or when clients are connecting from the Internet, you will have a load-balancer/reverse-proxy between the client and SAP Mobile Platform. In this case enter the URL of the load balancer or of the reverse-proxy.

c. “Signing key” – we will leave this blank for now

d. “Signing Certificate” – we will leave this blank for now

6. Click on “Generate Key Pair” – this will generate a self-signed certificate
### Local Service Provider

<table>
<thead>
<tr>
<th>Local Provider Name</th>
<th>Base URL</th>
<th>Signing Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>DN: mysp1</td>
<td><a href="https://10.173.0.128.8081">https://10.173.0.128.8081</a></td>
<td>MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgE/AACgBALuolItTQuoF8AbzdqKoDMrcr001 uuduos2MQHWNrtninqT8ljiyfoM/cHTh2YF1Pi/oR6y9x5eue+gLpWiacXeTh3Z+S0w4AyUF2pUkholsyYMu1zZ4TQeFwLGKoW5hUb9TyCRI+J5GaroU3Xsd3f65NMFTaupLtiGlN6BancvAmVA4AFO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MIIB/DCCAuWwNgAWEIAgIEwXzHt7ANBkgqkhiGi9w0BAQUF/ADAxwMQ8wDQYDVQQKEwZT0VAgU0JxETAFBhNVbaCTCFehb6xkb3JmMGswCCyDVQGGeWJERTAcFw0xNTA0MJ1yMfNMD1NDFaFw0xNjA0M1AyMDM1NDFAFExDzANB/nNVBAoBTNhUncERTTRFMA8GA1UEFwMV25mGRvcm</td>
</tr>
</tbody>
</table>

**Info:** The content of the “Signing Certificate” can be placed into a text file with an extension of “.cer” and you would see the certificate information.

**Certificate Information**

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

**Issued to:** SAP SE

**Issued by:** SAP SE

**Valid from** 4/20/2015 to 4/20/2016

7. Download the metadata file for this Local Service Provider by click on the “Get Metadata”
8. You will get an xml file with the content you have just configured.

9. Click “Save” button

4.2 Upload the SP metadata & obtain the IdP metadata

NOTE: For this part of the exercise, we will be using an SAP Cloud Identity Service. Your identity provider administration will be different and have a different interface. Use these steps for reference to the things that have to be don on the identity provider side.

1. Login into IdP console for configuration & create an Applications. We will sticking with the basic so we will default most of the value.

2. Open the SAML 2.0 Configuration panel and browse to the SMP “Local SP” metadata file. This will automatically populate all the necessary fields on this panel.
3. Click on the “Save” button

4. On the administration console home page, navigate to “Tenant Settings”.

5. Select the tenant then download the IdP metadata file and again this would depend on the IdP software that you are using.
6. You will get an xml file with the content for the IdP.

4.3 Configure SMP “Trusted Identity Provider” (IdP)

1. Login to SMP Admin Cockpit using the default account “smpAdmin” and the password that was set during the installation.

2. Click on the “SETTINGS” tab and “SAML” tab

3. Click on “Trusted Identity Provider” and click on “New”

4. Browse to the IdP metadata file & click on “Save”. All the values populate from the metadata file.
5. Result

Note: You will need the IdP “Name” for next part of the exercise.

4.4 Create a new authentication provider profile for application user

1. Login to SMP Admin Cockpit using the default account “smpAdmin” and the password that was set during the installation.

2. Click on the “SETTINGS” tab and under “Security Profiles”

3. Click on “New” and enter a profile name
4. Click on the “Add” button & input the provider information about IdP.

```
Add Authentication Provider - SAML2
```

```
*Control Flag: optional
Provider Description
*Identity Provider Name: mobilesecure.accounts400.ondemand.com
```

**Note:** The “Identity Provider Name” should be the name that you performed earlier.

5. Click “Save” to store the new authentication provider & “Save” again to store the new security profile properties

6. The end result should be something like this.

```
SECURITY PROFILE PROPERTIES
*Name: SAML_ondemand

Check Impersonation

AUTHENTICATION PROVIDERS FOR SAML_ONDemand
```

7. Click on the “APPLICATIONS” tab

8. Click on “New” button and input a meaningful name then click “Save”
9. On a newly open window, input the value for the “Endpoint”:
   http://services.odata.org/V2/Northwind/Northwind.svc/
   NOTE: This is a general OData service provided on the internet. Your SMP system will need to have
   internet access to reach this service.

10. Under the “SSO Mechanisms”, leave this empty since the endpoint is not using any authentication
    method.

    **Note:** In order to authenticate with the backend using SSO mechanisms with SAML then the only
    support method is X.509

11. Click on the “AUTHENTICATION” tab and select SAML security profile that was created earlier for the
    “Profile Name”

    ![APPLICATION](myApp)
    ![SECURITY PROFILE](OVERVIEW BACK END AUTHENTICATION CLIENT POLICY PUSH CLI)
    ![AUTHENTICATION PROVIDERS FOR SAML_ONDEMAND](Type Description)

12. Click “Save”

13. Now we can test the SAML user with this configured backend application by using a REST client.

14. Start “Chrome” & input the following into the URL address bar: chrome://apps/
Note: Assumed you have installed the REST client app. If not then go to the prerequisite section to get the URL to install the app.

15. Launch the “Postman....” App

16. Input URL for the “Normal” tab:
   http://10.173.0.128:8080/odata/applications/latest/myApp/Connections

   **Note:** change the address to fit your environment & change the app name accordingly if you did not follow this exercise exactly

17. Change the method to “POST”

18. Click on “Headers”

19. Add another header type “Content-Type = application/xml”
20. Switch to “raw” view & input the following XML

```xml
<?xml version="1.0" encoding="UTF-8"?>
<entry xmlns="http://www.w3.org/2005/Atom"
  <category term="applications.Connection"
  <content type="application/xml">
    <m:properties>
      <d:DeviceType>Windows</d:DeviceType>
    </m:properties>
  </content>
</entry>
```

**Note:** You can change the device type to Android, iPhone, iPad, etc.

21. Click the “Send” button and you should see similar to this after switch to the “Preview” mode.

22. Provide logon information and click “Log On”

23. Since we are using the REST client and it does not handle the redirect correctly. You may get an error message something similar to this.
24. You would need to restart the “REST” Client and perform the post again with the data above. This time the application should not force the IdP authentication screen again since you already have the token.

25. You will see something similar to the screen below.

26. If you login into SMP Admin Cockpit and verify that the registration has taken place correctly within SMP.
<table>
<thead>
<tr>
<th>Registration ID</th>
<th>Application ID</th>
<th>Device Type</th>
<th>User Name</th>
<th>Registration Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>34d0106e-a124-43ae-9e4e-74e65d24d79f</td>
<td>myApp</td>
<td>Windows</td>
<td>None</td>
<td>Apr 21, 2015 16:41:19 UTC</td>
</tr>
</tbody>
</table>
5. APPENDIX

5.1 Enable more logging

1. In the SMP Admin Cockpit, click on “LOGS” tab and “SETTINGS”

   ![Server Log Configuration]

2. Select the “Log Level” to be debug & select “Trace” to enable

   ![Server Log Configuration]

   Note: Notice that we only enable the debug option for the “Security” component.

3. Save the setting
4. You can view the trace using the SMP Admin Cockpit by clicking on “LOG FILES”

<table>
<thead>
<tr>
<th>Log File Name</th>
<th>Date Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>MO-AF7F33B7E-smp-server.log</td>
<td>13/04/2015 05:47:00 PM</td>
</tr>
</tbody>
</table>