Cloud Single Sign-On and On-Premise Identity Federation with SAP NetWeaver Cloud
White Paper
# TABLE OF CONTENTS

INTRODUCTION ................................................................................................................................. 3
Where we came from .......................................................................................................................... 3
The User’s Dilemma with the Cloud ................................................................................................. 4
The Administrator’s Dilemma with the Cloud ............................................................................... 5

SAML 2.0 AND ID FEDERATION TO THE RESCUE .......................................................................... 5

CONFIGURING CLOUD SSO AND ON-PREMISE IDENTITY FEDERATION ............................................. 5
Sample Enterprise Scenario: xLeave Leave Request Application .................................................. 5
Step 1: Establishing Trust in the corporate IdP to SAP NetWeaver Cloud ..................................... 6
Step 2: Establishing Trust in SAP NetWeaver Cloud to the corporate IdP ..................................... 7
Step 3: Configuring Identity Federation in the corporate IdP ......................................................... 8
Step 4: Configuring Identity Federation in SAP NetWeaver Cloud ............................................. 9

CONCLUSION ..................................................................................................................................... 11

REFERENCES .................................................................................................................................... 11
This whitepaper provides guidance for IT architects and developers about designing and deploying integrated solutions on the SAP NetWeaver Cloud platform that support Single Sign-On and Identity Federation with existing On-Premise Identity Management technology. Based on a sample enterprise scenario, the key concepts and major steps towards implementing the solution are explained.

INTRODUCTION

With the September 13th release [1], the SAP NetWeaver Cloud platform introduced new beta features for Identity (ID) Federation and Single Sign-On (SSO), which became general available for productive usage in December 2012. Before getting into the technology details based on a real-world enterprise scenario, the underlying concepts and common pain-points that are addressed by the new features are explained.

Where we came from

Even before the release in September, SAP NetWeaver Cloud offered a simple and effective way to manage users and protect resources in Web Applications deployed on the platform. With ID Service from SAP, developers are able to outsource the complex tasks of user account lifecycle management and secure authentication to a proven and trusted system in the Cloud [2]. Such systems are usually referred to as Identity Providers (IdP), because they are the authorized system for authenticating users and source obtaining additional information about the user. ID Service from SAP manages the large user base for the SAP Community Network (SCN) and several other SAP external-facing websites such as www.sap.com or the SAP Service Marketplace (SMP). Once logged in to one of those connected websites via ID Service, this central IdP in the Cloud streamlines the user experience by providing SSO across the SAP landscape.

To benefit from ID Service in SAP NetWeaver Cloud-based applications, the developer only needs to add the standard Java EE security tags in the application’s web.xml deployment description that specify the required authentication method and protected resources. The example in Listing 1[3] shows how an application is enabled to use ID Service for authentication and SSO:

```
...
<login-config>
  <auth-method>FORM</auth-method>
</login-config>
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Protected Area</web-resource-name>
    <url-pattern>/</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>Everyone</role-name>
  </auth-constraint>
</security-constraint>
<security-role>
  <description>All SAP NetWeaver Cloud users</description>
  <role-name>Everyone</role-name>
</security-role>
...  
Listing 1 Delegated authentication in web.xml
```

Using either FORM or BASIC as the ID Service-supported authentication mechanisms in the <auth-method> tag, the requested credentials for username and password will be checked by ID Service against the user’s SCN or SMP account. BASIC instructs the Web Browser to perform HTTP Basic Authentication by prompting the user to enter the username and password in a standard login dialog box. The credentials are sent encrypted via SSL/TLS to the application that delegates the actual authentication check to ID Service. For FORM, the application uses the widely adopted standard protocol for Web-based SSO, the XML-based Security Assertion Markup Language (SAML, [4]), which triggers a message flow as shown in Figure 1.
When the user requests a protected resource as specified by the `<url-pattern>` tag(s) in the `web.xml` file, the Web application – or Service Provider (SP) in SAML terminology – redirects the User’s Web Browser to its trusted IdP, which is by default for all SAP NetWeaver Cloud-deployed applications the ID Service from SAP.

This HTTP Redirect sends a SAML Authentication Request message via the User’s Web Browser to the IdP and asks for an authentication statement of the current user.

If the IdP has not yet authenticated the user, it will have to do so before sending back the response to the SAML request. For ID Service being in the role of the IdP, the user will see the login form and has to enter his ID Service credentials (e.g. the SCN username and password).

ID Service sends back a SAML Response via the User’s Web Browser to the Web Application (SP) on SAP NetWeaver Cloud. Upon successful login, the SAML Response includes an authentication statement that confirms that the user on the IdP’s system has logged on successfully at a certain time using a specific mechanism (e.g. password). It is up to the Web application to trust this statement or not. Therefore, a trust relationship to the IdP must be established beforehand. This usually involves the exchange of digital certificates that are used on both sides to verify digital signatures of the messages.

If the user accesses another Web application deployed on SAP NetWeaver Cloud that also uses ID Service for authentication, the above message exchange starts again. However, this time the user is already authenticated at the IdP and does not need to perform step 3 again. Thus, the IdP can immediately send the SAML Response with the authentication statement back to the Web application, and the user is (single) signed-on.

**The User’s Dilemma with the Cloud**

Although the integration with ID Service provides a simple but yet powerful solution for authentication and SSO on the SAP NetWeaver Cloud platform, it comes with some limitations. From the user’s perspective, the prerequisite to successfully authenticate is to have a valid user account in ID Service. For most SAP affiliated developers or administrators this is not an issue – they already have an SCN or SMP user account that they use frequently. However, for the larger number of application end-users, the situation is different. Asking them to add yet another username and password to their long list of user accounts seems to be a bad idea. They expect to sign on to their internal network with their corporate credentials, and then get seamless access to any business application, no matter if it is operated internally by their IT, or if it runs in the Cloud.
The Administrator's Dilemma with the Cloud
As a result of this missing Cloud SSO for employees, new user accounts must be created and maintained in those external systems and platforms. Over time, this leads to inconsistencies between the user's master profile in the corporate user directory and the records in the Cloud. But organizations undergo transformations regularly and employees take over other positions and roles, or leave the company. Without any synchronization mechanism in place, business relevant employee data stored in the Cloud will not get updated. If such profile information, like project-, group- or role memberships, is used to assign permissions in the Cloud applications to authorize business decisions, this lack of consistency can become a serious security and policy issue for an organization. Even worse, if employees quit their job, their Cloud user account remains accessible unless the administrator removes it manually.

SAML 2.0 AND ID FEDERATION TO THE RESCUE
A well-known and proven concept to address these challenges and securely share user profile information across system and network boundaries is ID Federation. With version 2.0 [4], the SAML specifications were enhanced significantly to no longer only address Web SSO, but also to enable ID Federation scenarios. Due to its wide adoption in the industry, many security and identity management products provide support for SAML 2.0. This makes the protocol also the ideal candidate for On-Premise to Cloud SSO and ID Federation.

At its core, the SAML standard specifies an XML-based assertion format that always contains a user's authentication statement, the identity of the IdP that has authenticated the user and issued the assertion with the statement, and, optionally, additional attribute statements about the user's identity. In enterprise scenarios, those attributes usually contain employee or organizational data required by the (Cloud) application. As an initial configuration step in every federation scenario, it is required by both the On-Premise and the Cloud security administrators to specify the attributes of the user account that are exchanged between the IdP and SP across the different administrative domains. This formal contract or Federation Agreement is usually configurable in the respective administration interface of the On-Premise IdP and Cloud SP. For SAP NetWeaver Cloud, the September 13th release introduced such configuration capabilities in the central platform administration tools.

CONFIGURING CLOUD SSO AND ON-PREMISE IDENTITY FEDERATION
A sample enterprise scenario of the fictitious company ITelO is used to explore the process of setting up integrated SSO and identity federation with the corporate network for a business application deployed on the SAP NetWeaver Cloud platform.

Sample Enterprise Scenario: xLeave Leave Request Application
ITelO sells PCs and accessories, and considers Cloud computing as an important strategic direction to improve the alignment between IT and business and to save costs by reducing the up-front expenditure on software and hardware. As a pilot project, ITelO's existing business application to manage employee leave requests, xLeave, was chosen to be the first to run in the Cloud. Since xLeave has been developed with Java EE, migration of the application for the SAP NetWeaver Cloud platform was easy to accomplish. The following security requirements were key criteria in ITelO's vendor selection process for the future Cloud platform of xLeave and other business applications:

- **No additional username and password**: Employees should not need to enter credentials other than the ones they already have for the corporate network to access xLeave in the Cloud
- **Securely share identity data**: Required user profile data in the xLeave application must be securely shared between the corporate user directory and the Cloud platform
- **Assign permissions based on Employee's Role in the Organization**: xLeave, like any other business application, defines roles to manage authorizations:
  - Users assigned to role **Employee** can create and delete their own leave requests
  - Users assigned to role **Manager** can approve or reject leave requests for employees in the organizational unit they are responsible for.
  Those two roles should be assigned to the logged on user in the Cloud based on current group or role memberships in the On-Premise user directory.
ITelO already has SAP NetWeaver Identity Management (IDM) in place to centrally manage and keep all identity data within the enterprise up-to-date. To support ID Federation, SAP NetWeaver IDM includes a SAML 2.0 compliant IdP which runs on the SAP NetWeaver Application Server (AS) Java. Thus, the favorite solution as outlined in Figure 2 uses the SAML standard to integrate the existing On-Premise systems with the Cloud.

Figure 2 ITelO On-Premise Identity Federation Scenario

ITelO followed four major steps to implement the solution for xLeave:
1. Establishing Trust in the corporate IdP to SAP NetWeaver Cloud
2. Establishing Trust in SAP NetWeaver Cloud to the corporate IdP
3. Configuring Identity Federation in the corporate IdP
4. Configuring Identity Federation in SAP NetWeaver Cloud

The following sections describe how those four steps are carried out in ITelO’s enterprise scenario.

Step 1: Establishing Trust in the corporate IdP to SAP NetWeaver Cloud
ITelO’s xLeave application is configured with the FORM method to use the SAML protocol to authenticate users who access a protected resource (URL) as defined in the application’s web.xml file. Instead of using ID Service, xLeave will only accepts ITelO’s corporate IdP as a trustworthy issuer of SAML assertions. ITelO’s Account Administrator can manage the trusted IdPs in the SAP NetWeaver Cloud Account Page, which is the central, Web-based administration tool of the platform.

Trust relationships for IdPs are configured at the Account level. The Account in SAP NetWeaver Cloud separates – similar to a Client in an SAP system – configuration data (e.g. connectivity settings to backend systems) and authorizations. Setting up the trust relationship to an (On-Premise) IdP in an Account is a two-step process: First, the Account Administrator has to configure the SAML settings of the Account’s SP, as shown in Figure 3, which consist of the Account’s (Service) provider name and an asymmetric key pair. The key pair can be generated by the platform which results in a self-signed X.509 certificate, issued to the Account’s provider name. Any SAML Authentication Request (see Figure 1, Step 2) sent by an application of the Account as a result of requesting a protected resource is signed with the private Signing Key of this key pair. In other words, the Account SP key pair is the means to uniquely identify the Account as a trustworthy entity to the outside world.
Consequently, any IdP, that has to accept the SAML Authentication Requests sent by applications of the Account will have to trust the key pair public Signing Key certificate. Adding the SAP NetWeaver Cloud Account as a trusted SP in a corporate On-Premise IdP is a product-specific task. Please refer to the tutorials at [5] for detailed instructions on how to configure the trust for many common on-premise IdP solutions. However, it always comprises the import of the Account’s public Signing Key Certificate into the IdP’s store for trustworthy certificates, so that SAML Authentication Requests can be securely validated and assigned to a known trusted entity. In addition, the URL for sending back the SAML Response and other protocol-specific settings must be configured to successfully establish the trust relationship. Some products can automate this error-prone process by importing a standardized configuration data file based on the so-called SAML2 Metadata format. This XML-based file contains all data required to configure the trust either to a SAML-based SP or IdP, including the Signing Certificate.

For SAP NetWeaver Cloud, the Account Administrator can export a Account’s SAML2 Metadata file by clicking on the Get Metadata link in the Local Provider Settings dialog (see Figure 3). If supported by the corporate IdP product, the Security Administrator can upload this file containing all relevant configuration setting to add the new SP with only a few clicks. shows this step in trust setup for a new Service Provider in the IdP administration interface of SAP NetWeaver IDM.

As a result, a new trusted Service Provider for the Account is created in ITelO’s corporate IdP. Trust has now been established in one direction to accept SAML Authentication Requests from the Cloud. To accept SAML Responses sent back by the corporate IdP, a similar configuration must be applied in the SAP NetWeaver Cloud Account for the IdP as well.

**Step 2: Establishing Trust in SAP NetWeaver Cloud to the corporate IdP**

As already mentioned above, trust relationships to IdPs are centrally managed on the Account-level, which can be accessed via the TRUST tab in the SAP NetWeaver Account Page (see Figure 5). The Cloud
Cloud Single Sign-On and On-Premise Identity Federation with SAP NetWeaver Cloud

Account Administrator can configure more than one IdP per Account, but has to decide which of them will be the active or default IdP used to authenticate users accessing applications in the Account.

Figure 5 Managing Trusted Identity Providers in the Cloud Account

The general settings to configure a SAML2-compliant Trusted Identity Provider are shown in Figure 6. Usually those settings can be provided by the Security Administrator of the On-Premise system. At a minimum, the Name or issuer id that uniquely identifies the IdP, the SSO and Single Logout (SLO) endpoints and bindings, and, most important, the IdP’s Signing Certificate used to verify the signature in the SAML Response, must be known.

Figure 6 Trusted Identity Provider Configuration in the SAP NetWeaver Cloud Account Page

Now that the core trust settings are configured on both sides by ITelO to accept SAML Authentication Requests by the Account’s SP and IdP-issued SAML Responses, the remaining task is to configure ID federation to securely share the required employee profile data for the scenario (see Figure 2)

Step 3: Configuring Identity Federation in the corporate IdP
Starting with the corporate IdP, it is again a product-specific configuration task to instruct the IdP to issue the additional user profile attributes in the SAML Response during a sign-on process. User attributes can usually be configured per trusted SP in the IdP. Figure 7 shows how ID federation in ITelO’s scenario is configured.
For ITelO’s trusted Account/SP, the user profile attributes required by xLeave are mapped to SAML2 Attributes `fname`, `lname`, `orgid` and `empid` in the SAML Response. They are sent via the employee’s Web Browser to the application in the Cloud. Group or role memberships are treated as special authorization attributes in the context of the OP SAML federation configuration. For those attributes, the On-Premise Security Administrator can for example add simple filter rules in SAP NetWeaver IDM so that only selected roles or groups are exposed as SAML Attributes. In ITelO’s federation scenario, only the logged-in employees with assignments to the roles “Employee” or “Manager” in the corporate user directory will get a SAML Attribute issued by the IdP with name `role` and the value set to the assigned role name (see Listing 2).

```xml
... <Attribute Name="role">  
     <AttributeValue xmlns:xs="...">Employee</AttributeValue>  
 </Attribute>  
...  
```

Listing 2 SAML2 Attribute Statement with the employee’s role assignment

As a final step, those attributes in the SAML Response must be mapped in the Cloud to attributes of the logged in user.

**Step 4: Configuring Identity Federation in SAP NetWeaver Cloud**

Similar to the corporate IdP configuration, the employee profile attributes received with the SAML Assertion must be mapped to attributes assigned to the authenticated user or `principal` in the SAP NetWeaver Cloud application. The Account Administrator in the Cloud can configure those mappings for each trusted IdP.

Figure 8 outlines how this is done in ITelO’s case: The incoming SAML Attributes with names `fname`, `lname`, `orgid` and `empid` are mapped to their corresponding principal attributes `firstname`, `lastname`, `orgId` and `userid`. The xLeave application reads the principal attributes using these names. If another application requires similar attributes but uses different names for them, only the mapping configuration will have to change, not the source code of the Cloud application.
Cloud Single Sign-On and On-Premise Identity Federation with SAP NetWeaver Cloud

Figure 8 Cloud Federation Settings

Principal attributes mapped via ID Federation from incoming SAML Responses are accessible in an SAP NetWeaver Cloud-based application using the User Management (UM) API coming with the SAP NetWeaver Cloud Software Development Kit (SDK). Listing 3 shows how xLeave reads the `firstname` attribute from the principal object, which is originally mapped from the `fname` SAML Attribute and which passes the employee's first name from ITelO's corporate user directory via the OP IdP.

```java
import com.sap.security.um.user.User;
import com.sap.security.um.user.UserProvider;
import com.sap.security.um.service.UserManagementAccessor;
...
UserProvider users = UserManagementAccessor.getUserProvider();
User user = users.getUser(request.getUserPrincipal().getName());
String firstname = user.getAttribute("firstname");
...
```

Listing 3 Accessing Principal Attributes in the Cloud Application

The `role` attribute, containing authorization information about the employee's role assignments in the corporate LDAP, is not passed as-is to the principal object. Instead, its value is processed by a set of mapping rules. Based on the results, the logged-in user is assigned to one or more web roles defined in the Cloud application's `web.xml` file. In ITelO's enterprise scenario, two simple mapping rules as shown in Figure 9 are configured for its corporate IdP:

- If the `role` attribute's value in the SAML Response equals "Employee", the user in the Cloud is assigned to xLeave's Employee role
- If the `role` attribute's value in the SAML Response equals "Manager", the user in the Cloud is assigned to xLeave's Manager role
Attribute-based rule mappings do not assign users to single web roles directly. To simplify administration, users are assigned to Groups, which are collections of web roles to manage business-relevant roles on a higher abstraction level. Groups are managed in the Cloud on an Account-level. They must have at least one web role assigned to them, but usually they aggregate web roles across several applications in the Account. As an example, ITelO’s Employees Group could additionally assign the (end-)user roles in a corporate Cloud Portal website or an E-Mail Web client, assuming that those permissions should be given to all employees at ITelO.

Well-defined Groups can help to better manage and oversee access control for all applications in the Cloud. Combined with mapping rules, this concept of federated authorization allows managing role assignments even for large number of users very efficiently. For example, with just one rule, all employees belonging to the “Purchasing” department can be assigned to a Group “Buyers”, which contains the required web roles in a supplier portal.

CONCLUSION

With its support for SSO and ID Federation, the SAP NetWeaver Cloud platform enables customers and partners to seamlessly integrate existing On-Premise identity management infrastructure with applications running in the Cloud, using a non-intrusive and very flexible approach: Without a separate user store and account in the Cloud, employees can single sign-on with their corporate user credentials. All required information in the Cloud about the employee can be passed securely during the sign-on process, based on the proven and standardized security protocol SAML. There is no need to manage additional systems that take care for complex user account synchronization or provisioning between the corporate network and the Cloud. Only the configuration of already existing components on both sides is needed, which simplifies administration and lowers total cost of ownership significantly. Even existing applications can be “federation-enabled” without changing a single line of code.

This whitepaper explained the concepts behind SSO and ID Federation in the SAP NetWeaver Cloud platform, but could only scratch the surface of all configuration details in the setup of ITelO’s sample federation scenario for the xLeave application. For more detailed, hands-on-like tutorials for specific on-premise IdP solutions can be found at [5].

REFERENCES
