Security

SAP Cloud Platform Authentication: Identity Authentication Service
# Table of Contents

Table of Contents .................................................................................................................. 2  

OVERVIEW ............................................................................................................................... 3  

AUTHENTICATION IMPLEMENTATION .................................................................................. 4  
  Technical Scenario ................................................................................................................. 4  
  SAP Identity Authentication Solution ..................................................................................... 4  
  Value Proposition ............................................................................................................... 4  
  Reference Solution Diagram ............................................................................................... 6  
  Reference Solution Components ......................................................................................... 7  
    SAP Cloud Platform Components for Licensing Considerations ..................................... 7  
    Other Components Required in this Use Case ................................................................. 7  
  High Level Implementation Steps ....................................................................................... 8  

SUMMARY ............................................................................................................................... 9  
  Follow SAP ......................................................................................................................... 9
OVERVIEW

SAP Cloud Platform is an essential part of SAP’s digital strategy. It is the platform for our customers’ and partners’ transformation journey toward digital business models. This open platform as a service (PaaS) provides database services including a unique in-memory database and application services. It is the proven cloud platform that enables you to rapidly develop new applications or extend existing ones, all in the cloud.

User authentication is the method of determining whether someone is who they say they are. There are several ways of authenticating users in the SAP Cloud Platform. In this scenario we will look at authentication using the SAP Cloud Platform Identity Authentication service.

SAP Cloud Platform Identity Authentication service is a cloud solution for identity lifecycle management for SAP Cloud Platform applications, and optionally for on-premise applications. It provides services for authentication, single sign-on, and on-premise integration as well as self-services such as registration and password reset for employees, customer partners, and consumers. For administrators, Identity Authentication provides features for user lifecycle management and application configuration.

SAP Cloud Platform offers many methods of authentication to verify and validate the identities of application users, so it is important to understand some of the authentication types. The most common type of authentication between the user and cloud base application is form-based or SAML2.

Authentication Types:

- **FORM or SAML2** - Form-based authentication implemented over the Security Assertion Markup Language (SAML) 2.0 protocol. Authentication is delegated to SAP ID Service or custom identity provider.
- **BASIC** - HTTP Basic authentication delegated to SAP ID service or an on-premise SAP NetWeaver AS Java system. Web browsers prompt users to enter a user name and password. By default, SAP ID Service is used.
- **CERT** - Used for authentication only with client certificate.
- **BASICCERT** - Used for authentication either with client certificate or with user name and password.
- **OAUTH** - Authentication according to the OAuth 2.0 protocol with an access token.
AUTHENTICATION IMPLEMENTATION

Technical Scenario

For almost all applications a business runs, there is a need to verify (authenticate) who the user of that application is. On the SAP Cloud Platform, one of the ways to do that is have the application use the Identity Authentication service as an identity provider (IdP) to authenticate application users.

SAP Identity Authentication Solution

In this setup, SAP Cloud Platform acts as a service provider, and SAP Cloud Platform Identity Authentication service acts as an identity provider (IdP). For the integration, you must set the trust on both sides. Because of the trust setting, when you have deployed an application to SAP Cloud Platform that has protected resources and requires SAML authentication, the user is redirected to the logon page of SAP Cloud Platform Identity Authentication service to provide credentials.

Once setting Identity Authentication as a trusted application identity provider for SAP Cloud Platform all the services in the SAP Cloud Platform are authenticated via Identity Authentication. To set up the trust to your corporate identity provider you need to make configuration changes in the administration cockpit of SAP Cloud Platform and in your Identity Authentication service administration cockpit. The trust configuration for application identity provider made in the SAP Cloud Platform administration cockpit does not affect the authentication for the cockpit itself; this is carried out by default by the SAP ID Service, or can be separately configured to use a different identity provider as the platform identity provider if desired.

When developing application for the SAP Cloud platform it is up to the application developers to implement the authentication process in their application code by selecting the authentication method. For this solution the method would be form-based/SAML2.

Value Proposition

Having a standardized method of authentication means that you only have to do the system authentication configuration once. All application programs can use the same already developed APIs for implementing authentication. SAML is a standardized format designed to interoperate with any system independent how it is implemented.

Because of the standardization it also provides a common user experience. It includes the look and feel of the logon screens but also allows for SAML’s ability for users to securely access multiple applications with a single set of credentials entered only once.

Security is of utmost importance when it comes to enterprise applications especially in the cloud. The IdP is used to provide a single point of authentication. SAML is used to assert the identity to others. This means that applications do not have to keep identities, which in turn ensures that there are fewer places for identities to be breached or stolen.

Because the IdP is cloud based, the software is always kept up-to-date. Many companies do not have the time or people to make the necessary updates in a timely fashion. This just increases the
possibility that hackers will exploit vulnerabilities in the system that have not been patched.

With SAP Cloud Platform Identity Authentication service, there are many benefits of using this as default identity provider for SAP Cloud Platform.

- Authentication with user name and password - Users can log on to applications with their user name and password.
- Single sign-on to applications on SAP Cloud Platform - Users can access multiple cloud applications in the current session by authenticating just once in the Identity Authentication service.
- Social sign-in to applications on SAP Cloud Platform - Users can link their Identity Authentication account with a social network account. That way users can be authenticated through a social identity provider.
- Customized branding - Administrators can configure branding styles for UI elements, emails, and error pages so that they comply with the company’s branding requirements.
- Customized privacy policy and terms of use management - Administrators can add customized terms of use and privacy policies, which users have to accept before registering. They are shown on the registration and upgrade forms.
- Customer security policy - Administrators can select a password policy from a list in accordance with the security requirements and the rules for resetting passwords.
- Dedicated customer tenant - Customers are provided with guaranteed availability and specific configuration of their tenants.
- User import functionality - Administrators can import new users into Identity Authentication or can update data for existing users.
- User export functionality - Administrators can download information about existing users in the current tenant.
- Detailed change logs - Administrators have access to information about the history of operations by tenant administrators.
- User management - Administrators can manage the users in the tenant.
- Administrator management - Administrators can add new administrators and edit administrator authorizations.
- User groups - Administrators can create and delete user groups and assign and unassign users.
- Corporate user store - SAP Cloud Platform Identity Authentication service can be configured to use a corporate user store in addition to its own user store.
- Kerberos authentication - Administrators configure Kerberos authentication to allow users to log on without a username and password when they are in the corporate network.
- Risk-based authentication - Administrators define rules for authentication in accordance with the risk
- Self-services - Users can use services to maintain or update their user profiles and to log on to applications.
Reference Solution Diagram

SAP Cloud Platform is the extension platform for SAP. It enables developers to develop applications securely, thus implementing additional workflows or modules on top of the existing solution they already have.

SAP Cloud Platform supports application scenarios for consumers (B2C), for partners (B2B), and for employees (B2E). The solution provided in this blueprint is available for all three scenarios. All types of users will be asked to authenticate.

The following diagram of the solution illustrates a basic architectural pattern implementing authentication using the SAP Cloud Platform Identity Authentication service.

Employee opens the app and requests service access
1. Service request redirected to IDP for authentication
2. User challenged for credentials
3. The user provides credentials
4. SAP Cloud Platform Identity Authentication performs authentication against the Identity Authentication service and if valid issues a SAML assertion
5. The request return to the service on the cloud platform with the SAML assertion (Authentication is completed at this point)

Note: The on-premise systems and the other cloud systems are depicted above for completeness of the overall landscape picture. In the case of authentication using the SAP Cloud Platform Identity Authentication service, the user identity has been established on the cloud platform. The next steps of authorization (determining what a user has access to) and single sign-on (accessing other system resources without authenticating again) will be covered in other blueprints.
Reference Solution Components

SAP Cloud Platform Components for Licensing Considerations

Please note that the following Bill of Material is for reference purposes only. The following table is only an example of the SAP Cloud Platform services and components required for this use case. Please consult your SAP Account Executive regarding your specific licensing needs.

<table>
<thead>
<tr>
<th>SALES ITEM</th>
<th>FUNCTION</th>
<th>LICENSING METRICS</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Cloud Platform Identity Authentication service</td>
<td>Secure authentication and single sign-on for users in the cloud</td>
<td>Logon blocks of 100/month</td>
<td>3,000 logons</td>
</tr>
</tbody>
</table>

Customers can use the [SAP Cloud Platform pricing estimator](#) to calculate the required investment for a particular project. Scale up or down on services as required.

Members and partners of SAP PartnerEdge\(^1\) can evaluate the development of an application for this use case – most development licensing is covered by the packs offered by SAP’s partner licensing services. Click [here](#) for details.

**Estimating the number of logons per month for SAP Cloud Platform Identity Authentication service:**

Project leads generally assume that users will authenticate with their identity provider once a day. Therefore, we can estimate the number of logons = 100 users * 30 logons/month/user = 3,000 logons/month

**Other Components Required in this Use Case**

The following list describes other components needed to implement this scenario and the role they play in the overall solution

<table>
<thead>
<tr>
<th>COMPONENTS</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity</td>
<td>To securely access remote services that run on the internet or on-premise.</td>
</tr>
<tr>
<td>Generic SAP Cloud Platform Service</td>
<td>To keep the blueprint simplified a generic icon is used since any SAP Cloud Platform services requiring authentication will act the same way.</td>
</tr>
<tr>
<td>Cloud Connector</td>
<td>Serves as the link between on-demand applications in SAP Cloud Platform and existing on-premise systems.</td>
</tr>
</tbody>
</table>

\(^1\) Excluding open ecosystem and basic
High Level Implementation Steps

This is an overview of the steps needed to implement this blueprint:

1. Get IdP (SAP Cloud Platform Identity Authentication service) metadata – this contains information about the IdP URL, certificate, etc.
2. Bind IdP to service provider of the SAP Cloud Platform subaccount – this will configure the SAP Cloud Platform to use IdP for authentication.
3. Get service provider of the SAP Cloud Platform subaccount metadata – this contains information about the SP URL, certificate, etc.
4. Bind SP to IdP – this configuration will allow the SAP Cloud Platform to use the IdP for authentication.
5. Configured IdP SAML attributes – There are attributes that the IdP should pass in the SAML token to help identify the identity of the user.
   a. “NameID” – This value help identifies the user ID that the SAP Cloud Platform may use. (In Cloud Foundry it is Name ID Attribute)
   b. Group – This value is recommended to help with identity federation during role assignment in SAP Cloud Platform. The Groups field is required for Cloud Foundry.

More Information on Identity Authentication Service:

This blueprint highlights important considerations companies need to analyze when implementing authentication for cloud platform applications. It only provides a high-level overview of the process. It is recommended to review further information to help you implement your authentication design and develop applications using a cloud based IdP. The following resources are a starting point:

- SAP Cloud Platform Identity Authentication Service – Online documentation includes an overview of the offering as well as details on how to implement and configure the service.
- Enabling Authentication for Java applications – Online documentation for how to do authentication in your Java applications.
- Configuring SAML 2.0 Authentication for SAP HANA applications – Online documentation for how to perform authentication in your SAP HANA applications.
- Authentication for HTML5 applications – Online documentation for how to do authentication in your HTML5 applications.
SUMMARY

This blueprint provides common information, guidance, and direction for implementing the SAP Cloud Platform Identity Authentication service as the identity provider for applications on the SAP Cloud Platform. It will allow you to use a common source of identities for all your cloud-based applications. It provides a standard, internationally adopted method for authentication using SAML assertions.

Submit Feedback:
Help improve SAP Cloud Platform Security Guides.

- Go to the SAP Cloud Platform Enablement Assets influence session
  http://influence.sap.com/sapcp-enablement-assets
- Click on Submit Improvement to send your feedback or report an error

For more information, please visit SAP Cloud Platform Scenarios

Follow SAP

www.sap.com/contactsap

© 2018 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, any related presentation, and SAP SE or its affiliated company’s strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/corporate-en/legal/copyright/index.epx for additional trademark information