SAPinsider

This article appeared in the Apr ▪ May ▪ Jun 2017 issue of *SAPinsider* (www.SAPinsiderOnline.com) and appears here with permission from the publisher, WIS Publishing.

WIS pubs

Gerlinde Zibulski
(gerlinde.zibulski@sap.com) leads the Product Management Team for Security. She has been with SAP for more than 18 years, in the security area since 2001 and as part of her current team since 2009.

Christian Cohrs
(christian.cohrs@sap.com) is Area Product Owner for SAP Single Sign-On and Product Manager for SAP's identity and access management solutions. He has a background in computer science and has worked in various positions at SAP during the last 17 years.

Identity and Access Management in Cloud and Hybrid SAP Landscapes

How to Manage Authentication and Authorization with On-Premise and Cloud Solutions from SAP

"Who am I? And if so, how many?" This not only refers to the title of a popular philosophy book,[1] but it could also describe modern IT landscapes, which involve managing vast numbers of different user identities and their access to your data and applications.

Ensuring appropriate user access to your systems has always been a necessary and difficult task. For your business to function at all, users must have access to your applications and data. Enabling this access can open up a range of regulatory and security risks, however, if it is not properly managed — a task complicated by changing user roles and evolving IT landscapes. These challenges have grown significantly with the advent of technologies such as mobile devices and the cloud, which have increased the complexities of managing user identities and access.

So how do you maintain secure, compliant access permissions for a widening array of user identities across ever more complex landscapes, devices, and technologies? In particular, how do you address this challenge in hybrid environments? Most SAP customers live in a hybrid landscape, with a variety of standard SAP applications as well as custom-developed software running both in the cloud and on premise. How do you provide solid and secure identity and access management for this type of landscape?

This article looks at four solutions — SAP Single Sign-On, SAP Cloud Platform Identity Authentication, SAP Identity Management, and SAP Cloud Platform Identity Provisioning — that provide you with a comprehensive toolkit for managing user identities and authentication in on-premise, cloud, and hybrid environments. You'll learn when it makes sense to use which solution, as well as how to use them together in hybrid environments.

Solutions for User Authentication

User authentication is fundamental to your business — it ensures that the person accessing your application and data is the person who is authorized to do so, and serves as the first line of defense against fraudulent activity. If you can prevent unauthorized users from gaining access to your systems in the first place, you can prevent a costly incident before it ever occurs.

[1] Richard David Precht, *Who Am I? And If So, How Many?* (Spiegel & Grau, 2011).

While user IDs and passwords are the most widely used authentication mechanisms, they are the least secure — hardly a day goes by without a report on insecure passwords, phishing emails, or stolen user data. User IDs and passwords should be used only as a method of last resort, if legacy applications don't accept other authentication tokens, for instance.

Tip: If you must use the user ID and password method, educate your users to create a password based on a passphrase — for example, the passphrase "Finally I have 1 secure password!" is an easy-to-remember passphrase that results in the password Flh1sp! — a password that is complex and not easy to guess.

Although SAP allows user ID and password-based authentication for those who require it (to ensure security in this scenario, passwords are stored as a hash value and communication paths can be encrypted), the recommended approach is to implement strong authentication mechanisms and secure authentication tokens. SAP offers two products that support this recommendation and enable the convenience of single sign-on (SSO): SAP Single Sign-On for on-premise environments and the SAP Cloud Platform Identity Authentication service for the cloud.

SAP Single Sign-On

SAP Single Sign-On — version 3.0, the currently available release, was delivered in July 2016 — is a mature, feature-rich, on-premise SSO product that enables users to authenticate once and gain access to all connected SAP and non-SAP applications.[2] With its ease of implementation and ability to enable SSO to any graphical user interface — whether the standard SAP GUI for Windows, SAP GUI for HTML, or SAP Fiori user interfaces — SAP Single Sign-On is widely used in SAP customer environments and is also used internally by SAP.

To meet varying requirements and preferences, SAP Single Sign-On supports multiple authentication standards, including Security Assertion Markup Language (SAML), the Kerberos protocol, and X.509 certificates. In recent years, organizations have increasingly opted to use SAML due to its support for both web and cloud applications, and its ability to bridge domains and firewalls for identity federation and inter-company SSO. To support those that prefer X.509 certificates but do not have a public key infrastructure (PKI) in place for the issuing of certificates, SAP Single Sign-On enables the generation of short-lived X.509 certificates with a configurable validity (8-10 hours, for example).

To extend its security capabilities, SAP Single Sign-On includes support for both two-factor and multi-factor authentication (see the sidebar "Added Security for Sensitive Applications") as well as RFID-based authentication. If your organization is especially security-aware, SAP Single Sign-On allows you to manage your private keys on a hardware security module (HSM) board. The cryptographic library used for SAP Single Sign-On is FIPS 140-2 certified.[3]

While SAP Single Sign-On is an on-premise product, it can also support cloud landscapes by sending and receiving SAML assertions to and from the cloud.

SAP Cloud Platform Identity Authentication

Introduced in 2014, SAP Cloud Platform Identity Authentication is a service that runs on SAP Cloud Platform and enables simple, secure, cloud-based SSO to both SAP and non-SAP web and cloud applications across any kind of device.[4] It supports SAML, OAuth, and Kerberos as authentication tokens.

SAP Cloud Platform Identity Authentication includes a cloud-based user store that provides centralized storage for user IDs. It includes sign-on to social networks as part of its SSO support, and allows customized branding for a look and feel that is consistent with organizations' branding along with customizable privacy and terms-of-use

[2] For an overview of the latest enhancements delivered with SAP Single Sign-On 3.0, see the article "Secure Single Sign-On Across SAP Landscapes" in the July-September 2016 issue of *SAPinsider* (SAPinsiderOnline.com).

[3] Learn more at https://blogs.sap.com/2015/01/21/sap-s-crypto-kernel-receives-fips-140-2-certificate.

[4] For an introduction to SAP Cloud Platform Identity Authentication, see the article "End-to-End Identity and Access Management in the Cloud" in the October-December 2016 issue of *SAPinsider* (SAPinsiderOnline.com).

policies. It also provides a variety of self-service features, such as self-registration, user-maintained profiles, and password reset functionality.

SAP Cloud Platform Identity Authentication is highly scalable to adapt easily to changing requirements and high availability is ensured by SAP. It works well in a variety of scenarios, including business-to-consumer (B2C), business-to-business (B2B), and business-to-employee (B2E) scenarios.

Similar to SAP Single Sign-On, SAP Cloud Platform Identity Authentication supports multi-factor authentication (see the sidebar "Added Security for Sensitive Applications") as well as risk-based authentication, and since SAML is the technology for web and cloud, you can use this product in hybrid scenarios as well.

When Do I Use Which?

SAP Single Sign-On is ideal for enabling your business users and IT staff to securely access applications and business systems. It is the optimal choice for organizations that want to set up a feature-rich, highly secure SSO solution for their on-premise operations. Since SAP Single Sign-On supports Kerberos and X.509 certificates for authentication, it is also the right choice for organizations that have any systems — even if it's only one — that use the standard SAP GUI for Windows.

SAP Cloud Platform Identity Authentication is the best fit for organizations seeking to provide strong and secure SSO for their cloud-based applications. With its support for a variety of convenient features, such as extensive self-services and self-registration, the reuse of social logins, and branding options, it is especially well suited to B2C scenarios — SAP uses it productively for more than 8.5 million of its SAP Community users.

These two SSO scenarios can also be used together in a hybrid integration scenario.

A Hybrid Integration Example for User Authentication

Let's take a look at an example hybrid scenario that uses SAP Single Sign-On and SAP Cloud Platform Identity Authentication to enable seamless and secure authentication for both on-premise and cloud-based scenarios (see **Figure 1** on the next page).

In the on-premise world, Kerberos/SPNEGO is the most popular technology for enabling SSO, as it is easy to set up and manage. When using Kerberos and SAP Single Sign-On, corporate end users gain access to their SAP applications without manual authentication simply by being logged on to the corporate Microsoft Windows domain. But what happens when a company extends its landscape to the cloud? Cloud-based applications tend to support SAML instead of Kerberos to ensure availability outside of the corporate domain for employees working remotely and for consumers. While SAP Cloud Platform Identity Authentication provides SSO for these cloud-based applications for both employees and consumers, employees working inside the corporate domain face a second authentication screen if, after authenticating to the corporate domain,

Added Security for Sensitive Applications

Both SAP Single Sign-On and SAP Cloud Platform Identity Authentication allow for the integration of additional authentication factors into the logon process. This is a successful and proven way of increasing security in the authentication process for sensitive applications or data — such as the data in your SAP business systems.

A simple way of implementing multi-factor authentication is using SAP Authenticator, an app for your mobile device that provides a time-based one-time password (TOTP) for users to enter when prompted by the application at logon. So, in addition to requiring a regular password (first factor), the user must have a specific mobile device (second factor) that generates a passcode. This type of setup helps provide extra protection for sensitive assets, as a potential hacker must not only determine the password but also have access to a specific physical device. SAP Authenticator can be used with both SAP Single Sign-On and SAP Cloud Platform Identity Authentication.

As an alternative to SAP Authenticator, SAP Single Sign-On also allows you to configure one-time passwords to be sent via email or SMS, or you can use the RADIUS protocol to set up a second authentication factor.

To learn more about multi-factor authentication, see the article "Simple and Secure User Authentication with SAP Single Sign-On 2.0" in the July-September 2015 issue of *SAPinsider* (**SAPinsiderOnline.com**).

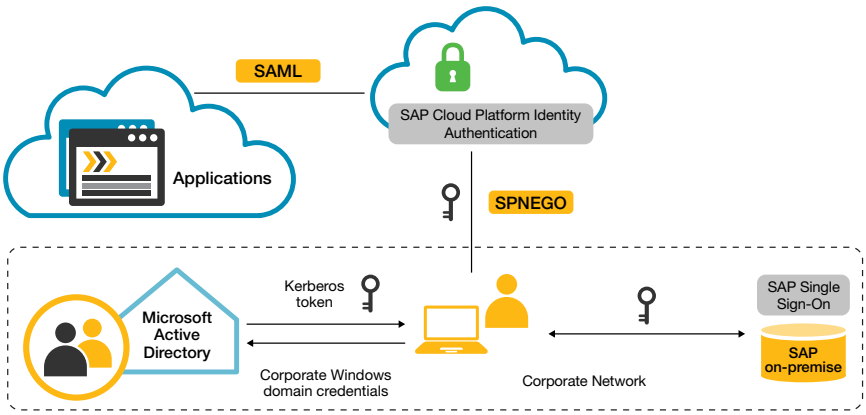

Figure 1 A hybrid scenario that uses both SAP Single Sign-On and SAP Cloud Platform Identity Authentication

they also have to authenticate to the identity provider represented by SAP Cloud Platform Identity Authentication.

So, how do you ensure that employees working inside the corporate domain can access cloud applications as easily as they access their on-premise applications? SAP solutions make this easy by allowing you to integrate the two SSO scenarios. SAP Cloud Platform Identity Authentication allows for Kerberos/SPNEGO authentication — this means that when you configure SAP Cloud Platform Identity Authentication to accept Kerberos tokens as a means of authentication, you ensure that employees inside the corporate domain receive the SAML assertion created by SAP Cloud Platform Identity Authentication seamlessly, without any manual interaction.

From the end-user perspective, this is exactly what they expect, gaining access to business applications in the cloud without any manual authentication. This does not mean that cloud-based business applications are only available for corporate users, however. If SAP Cloud Platform Identity Authentication does not receive a Kerberos token, it will prompt for a user name and password, meaning that consumers also benefit from SSO, since for them the only manual step is authenticating to SAP Cloud Platform Identity Authentication. It is important to note that no changes to the business applications are required. Regardless of whether the initial authentication is based on Kerberos or a manual step, the business applications will always receive the SAML assertion that they expect.

Solutions for Identity Administration

In addition to authenticating identified users, organizations need to manage the user identities and authorizations the authentications are based on. Centralized control over user identities and authorizations is critical in heterogeneous landscapes that include a wide range of systems and technologies, multiple sources of identity data, and changing authorizations and roles.

Managing identities and authorizations separately for each and every system creates redundant, error-prone processes. Organizations can reduce these risks with a centralized administrative infrastructure that covers and automates processes throughout the entire identity life cycle. This centralized approach not only simplifies user management, but also helps fulfill compliance requirements.

SAP offers two products for enabling centralized identity administration: SAP Identity Management for on-premise implementations and the SAP Cloud Platform Identity Provisioning service for cloud-based implementations.

SAP Identity Management

Released in 2007, SAP Identity Management — currently in release 8.0 — is on-premise software that allows organizations, including SAP itself, to centrally administer user identities and their authorizations (such as roles, groups, and privileges) and provision them into SAP and non-SAP systems.[5]

[5] For more on SAP Identity Management 8.0, see the article "Simplify Administration and Extend User Management into the Cloud with SAP Identity Management 8.0" in the April-June 2015 issue of *SAPinsider* (SAPinsiderOnline.com).

Prior to the execution of an access request — such as a request for a new user identity or a role assignment — SAP Identity Management can delegate the request to SAP Access Control for a segregation of duties analysis, risk analysis, and mitigation. Depending on the results, SAP Identity Management provisions the user identities and the roles.

SAP Identity Management includes additional features that help make identity management more efficient. It includes a browser-based self-service password reset function that executes after the user answers a configurable set of security questions, reducing helpdesk calls. It also provides basic reporting functionality for analyzing system access as well as more extended reporting capabilities via integration with SAP Business Warehouse (SAP BW) and SAP Lumira.

SAP Identity Management can extract relevant information from HR systems, including on-premise solutions such as SAP ERP Human Capital Management (SAP ERP HCM) and, via a special connector, SAP SuccessFactors solutions in the cloud. This allows for cleansed and consistent user data, since businesses tend to create, change, and delete identities based on events in the life of an employee. And this identity lifecycle management capability is not limited to HR data in HR systems — SAP Identity Management can also be used to create user identities for business partners or students, for instance.

SAP Cloud Platform Identity Provisioning

For cloud-based identity administration, SAP offers SAP Cloud Platform Identity Provisioning, a new product delivered in September 2016 that is also used internally by SAP to support identity management.[6] Based on SAP Cloud Platform, SAP Cloud Platform Identity Provisioning is a service that allows organizations to administer and provision identities and their roles and authorizations into cloud applications.

SAP Cloud Platform Identity Provisioning currently supports generic provisioning via the System for Cross-domain Identity Management (SCIM) protocol and application-specific provisioning into business applications such as SAP Jam, SAP Hybris Cloud for Customer, and Google G Suite, enabling instant identity and authorization updates across IT landscapes. This both speeds onboarding and increases security.

SAP Cloud Platform Identity Provisioning can also extract user-relevant information from various identity stores — such as those used by SAP's cloud-based HR software, SAP SuccessFactors solutions, and Microsoft Active Directory — enabling rapid implementation. It also includes out-of-the-box integration with SAP Cloud Platform Identity Authentication to rapidly enable SSO across landscapes and devices.

For hybrid scenarios, identities can be received from or pushed to SAP Identity Management or SAP Cloud Integration.

When Do I Use Which?

SAP Identity Management is an ideal user and role provisioning solution for organizations seeking to manage identities and authorizations for their on-premise applications. It provides extensive connectivity to SAP and non-SAP applications and offers compliance functionality through integration with SAP Access Control. While it includes some capabilities for integrating cloud applications, such as a connector for SAP SuccessFactors solutions, its consumption model and architecture target on-premise installations.

Customers that plan to extend their landscape into the cloud should consider SAP Cloud Platform Identity Provisioning. It allows them to reuse existing (cloud or on-premise) identity stores and provision their users along with the corresponding authorizations to cloud-based applications. In addition, SAP plans to significantly enhance this product in the area of cloud connectivity going forward.

SAP Identity Management and SAP Cloud Platform Identity Provisioning can also be used together in hybrid landscapes, where SAP Identity Management covers on-premise applications and SAP Cloud Platform Identity Provisioning covers cloud-based applications. This type of deployment offers the most benefits in a hybrid landscape — customers can take advantage of the sophisticated on-premise functionality of SAP Identity Management, then reuse the user information stored in its identity store for provisioning to their cloud applications. This prevents redundant user maintenance efforts and increases security by relying on a single source of truth for identity data. The built-in

[6] For an introduction to SAP Cloud Platform Identity Provisioning, see the article "End-to-End Identity and Access Management in the Cloud" in the October-December 2016 issue of *SAPinsider* (SAPinsiderOnline.com).

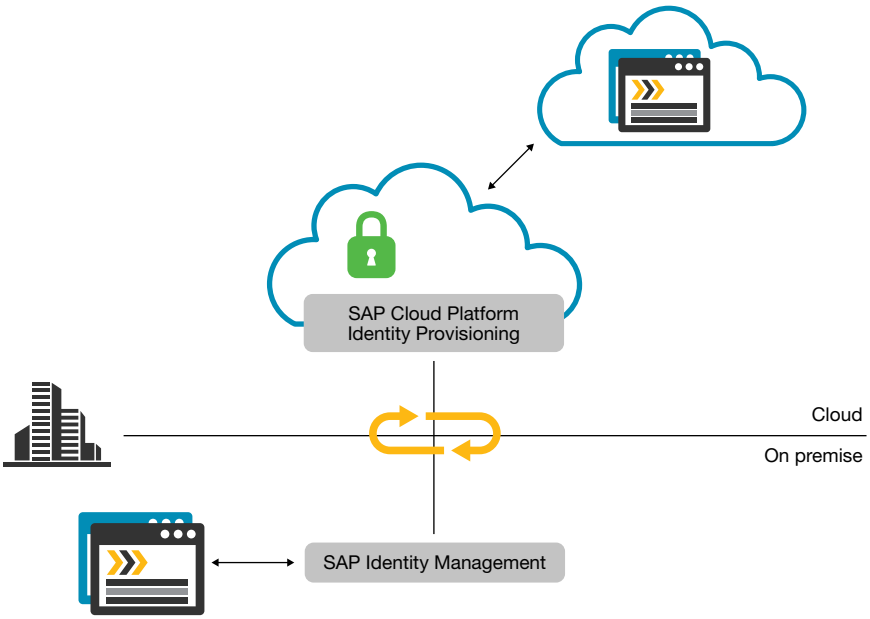

Figure 2 A hybrid scenario that uses both SAP Cloud Platform Identity Provisioning and SAP Identity Management

integration between these two products enables them to seamlessly push/receive identities throughout a heterogeneous landscape.

A Hybrid Integration Example for Identity Administration

Let's take a quick look at a hybrid integration scenario that uses both SAP Cloud Platform Identity Provisioning and SAP Identity Management (see **Figure 2**). We'll assume that you have SAP Identity Management up and running to manage your users on premise and that you have SAP Cloud Platform Identity Provisioning set up for your cloud environment.

First, you must configure a connection from SAP Cloud Platform Identity Provisioning that allows you to read and write to your cloud application. You will also define a mapping between the cloud application entities and the internal data formats of SAP Cloud Platform Identity Provisioning. Then you must configure a dedicated repository in SAP Identity Management for each cloud application that is managed via SAP Cloud Platform Identity Provisioning.

As soon as these two configurations are in place, you can trigger the initial load job for each new repository from SAP Identity Management. This job fetches and stores all cloud application entities, such as technical or account privileges, inside SAP Identity Management. You can now use these entities to provision new users or groups into the cloud applications, or change user assignments.

Summary

To enable safe and secure access to the applications and data your employees, business partners, and consumers need, you must have effective user authentication and identity management in place. The difficulty of accomplishing this task is compounded by IT landscapes that not only encompass a wide assortment of constantly changing user identities and roles, but also heterogeneous systems and technologies.

SAP provides a comprehensive set of solutions that meet the authentication and identity management needs of unique customer landscapes, many of which include a hybrid blend of on-premise and cloud-based solutions. Used in combination, these four solutions — SAP Single Sign-On, SAP Cloud Platform Identity Authentication, SAP Identity Management, and SAP Cloud Platform Identity Provisioning — provide the functionality you need to effectively manage access to your systems and support your journey toward the cloud.

Learn more about user authentication and SSO at **www.sap.com/community/topic/sso.html** and more about identity management at **www.sap.com/community/topic/identity-management.html**. More information about SAP Cloud Platform is available at **https://hcp.sap.com/capabilities/security.html**. ■