SAPinsider

This article appeared in the Jan ▪ Feb ▪ Mar 2012 issue of *SAPinsider* (http://sapinsider.wispubs.com) and appears here with permission from the publisher, WIS Publishing.

WIS PUBLISHING

Enable **Secure** Single Sign-On in the **Cloud**

The New ID Service from SAP Makes It Possible

by Marko Sommer and Stephan Zlatarev, SAP AG

Cloud computing is becoming a must-have for companies looking to stay relevant; if you aren't already integrating on-demand solutions into your end-to-end business processes, it's likely only a matter of time before you do. On-demand solutions offer a range of cost-effective benefits, including the ability to access functionality as needed, without requiring an additional IT infrastructure and staff resources. They also enable companies to respond quickly and flexibly to changing business needs (see sidebar on the next page).

However, the cloud also brings with it new challenges, not the least of which is managing user access and information in landscapes that include on-demand applications. While users have come to expect consistent user management and single sign-on capabilities for authenticating, securing, and integrating applications into their end-to-end processes, on-demand solutions have remained as separate entities that require separate user maintenance — until now.

SAP is answering this challenge with a new ID service that enables single sign-on across the SAP landscape, as well as centralized user information management — taking a fragmented process and turning it into a streamlined user experience. The ID service from SAP, an on-demand deployment, bridges the gap between customers' on-premise applications, SAP on-demand applications, and third-party on-demand applications by verifying user identities, granting authentication, and enabling secure single sign-on across the landscape.

Introducing the ID Service from SAP

SAP's ID service, which will be available in Q2 of 2012, covers the processes for managing identities and their life cycles within the SAP cloud. With this ID service, users will be able to set up one SAP identity and leverage single sign-on when browsing SAP websites, using SAP on-demand systems, or accessing third-party on-demand applications. **Figure 1** on the next page shows how SAP's ID service integrates into SAP's on-demand landscape.

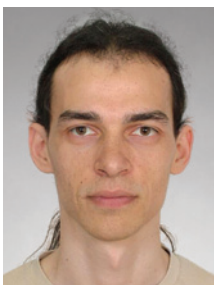
SAP's ID service saves time and resources by enabling users to update their profiles only once and requiring just one password to log on to SAP's various on-demand systems. In fact, SAP itself is already benefiting from the ID service. The SAP cloud administration teams, for example, have realized reduced TCO for SAP's on-demand offerings because one central system is handling the registration, authentication, and provisioning of user data. SAP's IT hosting team also uses the ID service for authentication purposes in conjunction with SAP NetWeaver Identity (ID) Management to administer and provision user data for employees, partners, and customers to the various systems.

ID Service Features and Functions

The ID service contains a range of features and functions to meet the needs of SAP customers. These include:

- A central store for identities related to all on-demand applications
- Single sign-on between SAP on-demand applications and integration with third-party on-demand applications
- Central management of identity information (including user information, such as name, descriptor, email address, customer relation, passwords, etc.)

Marko Sommer (marko.sommer@sap.com) is Project Manager for SAP ID Service at SAP AG. Marko joined SAP in 1998, and held various positions in the Industry Development for Healthcare and Insurance group before joining the SAP TIP Core Identity Management and Platform Security team in February 2011.



Stephan Zlatarev (stephan.zlatarev@sap.com) is Area Product Owner on the SAP TIP Core Identity Management and Platform Security product team. Since 2010, he has been the product owner of SAP ID Service, which aims to enable SAP cloud solutions and integration scenarios with single sign-on.

- Synchronization of user accounts to and from on-demand target systems
- Runtime functionality for user authentication, single sign-on, and trust management

The ID service acts as an identity provider (IdP) that verifies and authorizes users when they sign in by issuing security tokens. SAP uses the ID service as an IdP for its external-facing websites, such as **www.sap.com** and the SAP Developer Network (SDN), as well as for its business applications based on SAP NetWeaver, SAP Business ByDesign, and the Java platform. The ID service also supports the Security Assertion Markup Language (SAML) 2.0 standard, an XML-based authentication protocol used to issue security tokens.

The Rise of On-Demand Cloud Solutions

As companies continue to integrate on-demand solutions with their existing on-premise applications, SAP continues to invest in its on-demand portfolio of software-as-a-service (SaaS) and platform-as-a-service (PaaS) offerings.

For example, SAP Business ByDesign — an integrated, cloud-based suite for managing financials, human resources, sales, procurement, customer service, and supply chain processes — has become an established and successful on-demand solution for small and medium-sized enterprises. Line-of-business on-demand solutions are also currently available as add-ons to SAP Business ByDesign; these include solutions for sales, sourcing, contracts, and supplier management. SAP is building more of these add-ons, like travel on-demand, for instance, which is planned for release in 2012.

SAP also offers Java applications for on-demand analytics — these include solutions like SAP Carbon Impact OnDemand, which helps companies assess and report on their carbon footprints — and for collaborative applications like SAP StreamWork, an online collaborative environment for sharing data and making decisions. SAP is also developing a new, PaaS-based Java technology stack, due for release in 2012, which will enable SAP, partners, and customers to develop a whole new family of cloud-based applications that leverage open standards and allow collaboration with the greater Java community.

The ID service from SAP enables single sign-on across the SAP landscape, as well as centralized user information management — taking a fragmented login process and turning it into a streamlined user experience.

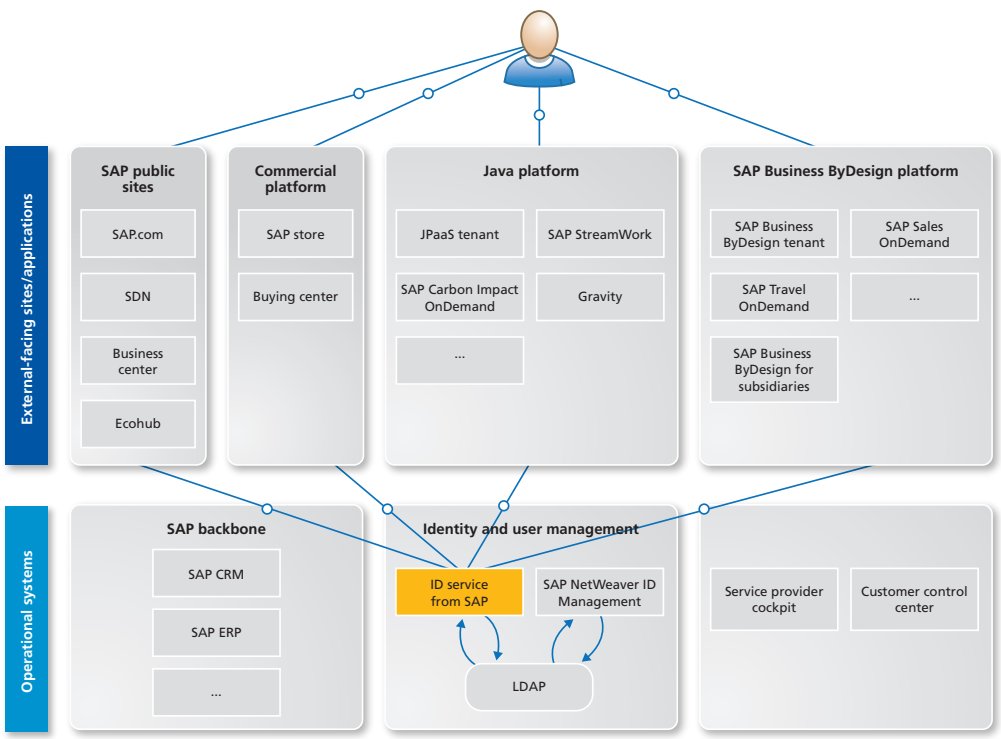


FIGURE 1 ▶ The ID service integrated into SAP's on-demand landscape

Let's take a closer look at how the service works and at the data model the service uses to store information.

How It Works

When a user requests a resource from a service provider — for example, if the user wants to create a travel booking in an on-demand travel system — the web browser redirects the request to SAP's ID service. As the central component for authentication, SAP's ID service checks whether it already has an active session for the user.

If an active session does exist — that is, if the user has already authenticated with any of SAP's on-demand applications that connect to SAP's ID service — the ID service responds with a SAML assertion. The user's web browser again redirects the request to the target resource at the service provider and includes the SAML assertion in the request. The service provider then grants access and responds with the requested resource.

If an active user session does not yet exist, the ID service checks for valid credentials (like an X.509 certificate) or requests authentication via a username and password. If valid credentials are provided, the ID service issues a SAML assertion and a user session is established on the IdP.

The ID Service Data Model

To be able to seamlessly authenticate users, SAP's ID service maintains user information, such as a unique identifier, credentials, contact information, and more. There are three sources of user information for different contexts, each of which has different information requirements and interacts with the ID service in different ways:

- **Person:** Any individual can use SAP on-demand solutions. Use of SAP on-demand solutions is based on an individual terms-of-use agreement; a person is responsible for maintaining his or her user identity (which includes the user name, credentials, and contact information) with the ID service. One example of a person using an SAP on-demand solution is through the SAP Community Network, which is accessible after a person self-registers.
- **Company:** A company can be registered with SAP as a customer or a partner, and can grant its employees, customers, or partners access to SAP on-demand solutions based on the company's contract with SAP. The company is responsible for maintaining its members' company-specific user information with the ID service.
- **Service provider:** The service provider is the provider or platform of one or more SAP on-demand solutions that share the same user management and session management. A service provider may require, for example, that terms of use shared by a group of service providers be accepted and stored centrally, or it may require that the ID service identify end users in a certain way (via user mapping, for example). With the ID service from SAP, service providers can maintain service provider-specific user information in a central store.

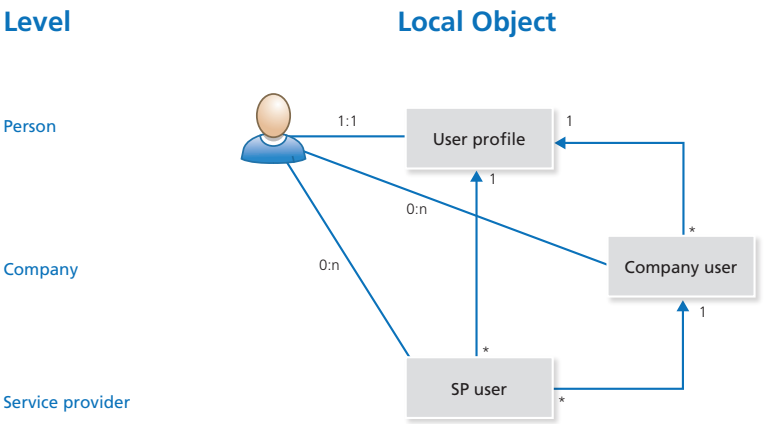


FIGURE 2 ▲ Logical data model for identities in the ID service

Figure 2 shows how the different levels of user information are reflected in SAP's ID service data model.

Summary and Outlook

On-demand is in demand, and the ID service from SAP answers the challenges of integrating on-demand solutions into your SAP landscape. It ensures that customers can establish single sign-on for their end-to-end processes and integrate their on-premise and on-demand applications — so that users are not required to enter additional credentials when navigating from on-premise to on-demand applications. The service provides mature functionality for managing profiles and is an integral part of SAP's on-demand portfolio.

In the future, SAP plans to enhance the ID service to support single sign-on from on-premise to on-demand via IdP proxy, customer-oriented monitoring scenarios for the SAP cloud user base, web service security, and integration with Google accounts. ■