How to Future-Proof the Security of Your System Infrastructure in a Service-Enabled World

Apply Tried and True SSO Concepts

Using single sign-on (SSO) to securely authenticate users and ensure security is not a new practice; numerous established SSO solutions offer the means to standardize access management infrastructures and promote user productivity while protecting invaluable enterprise resources. For years, companies implementing SSO have had a wide array of options to help them get the job done — including X.509 client certificates and Public Key Infrastructures (PKIs), Kerberos, Security Assertion Markup Language-based methods, SSO tickets (a solution specific to SAP environments), and even biometric authentication via custom-developed solutions.

To date, there’s been a strong emphasis on deploying these SSO solutions to secure access to enterprise resources delivered through application servers directly to the user’s desktop — such as those accessed through a Web browser or SAP GUI. But now, with the next evolutionary stage of enterprise IT architectures — including service enablement for applications and service-oriented architecture (SOA) — enterprise architects and administrators face a wider array of options for delivering enterprise application content to users, be it as a service to be used by another service, or as a service directly consumed and used by applications designed to deliver a richer end-user experience. Both cases share the service-enabled interactions with enterprise application providers (with SAP ERP or SAP NetWeaver Process Integration servers, for example). Service-enabled applications, however, do not carry embedded information about the user interface (UI) — they promote system-to-system interactions, allowing end users to choose the UI they find most comfortable to work with.

For security and user authentication, this has important implications: The UI components — through which a user directly provides a private security token as proof of identity — are left out of the security picture. As a result, administrators in service scenarios must resort to using trusted systems as intermediaries to relay user identity information and enable secure access to protected service provider content.

With these growing challenges, IT managers and security administrators will be happy to learn that the tried and true SSO concepts are still go-to solutions to authenticate and authorize user access — even across a more flexible and open service-based enterprise software application environment.

**Why SOA Landscapes Bring New Challenges to SSO Mechanisms**

In end-to-end, UI-to-service-provider scenarios common in SOA environments, the traditional concept of user authentication and SSO includes two distinct stages (see Figure 1):

- **Initial user authentication**, the stage in which a user directly shows proof of identity from his or her desktop application — via SSO, for example, or by entering a user ID and password.
• **User identity propagation**, the stage in which the identity that the user establishes in the initial authentication is used to access service-enabled enterprise applications via service intermediaries or application layers that the user doesn’t interact with directly.

Although seamless to the end user, these two stages function more or less independently — and the common link between them is the user’s identity. To establish this link, which is usually represented by the user’s logon ID, the participants in the end-to-end authentication process must share user identity information, either through a shared user store or through a common identity management product — like SAP NetWeaver Identity Management, for example.

Another important requirement for keeping this link intact at system run time is being able to securely forward the user’s identity information. Propagating a user’s identity across system boundaries through a service call is not particularly difficult — but propagating it securely, without hampering productivity does pose a challenge. Without properly secured user identity propagation, though, you’d be introducing risk: Malicious users can easily bypass accountability requirements for accessing service resources by intercepting service requests and later impersonating legitimate users to call the service.

What is needed, then, is a balance between security and service availability. To this end, users can look to familiar functionality available with SSO to enable identity propagation and let users access service-enabled enterprise resources after signing in to secured and trusted front-end applications or portal systems. Securing subsequent identity propagation solutions with digital signatures, which are generated and verified with the trusted systems’ key pairs, can provide the necessary security while avoiding limitations that come with trusted systems retrieving and managing end-user keys for every security call.

When administrators use SSO in conjunction with an identity management solution like SAP NetWeaver Identity Management, they can synchronize the user identity information and be certain that it stays consistent. Through user identity propagation, they can also confirm that the end users who signed on at the front-end application indeed accessed information resources under their own permissions — even as they navigate across loosely coupled, service-based enterprise landscapes.

The concept of using SSO in conjunction with security solutions like Kerberos and PKIs to enable initial user authentication at the user desktop (stage 1 in Figure) is well established, and the idea of balancing availability and security to establish a trusted system for direct user interaction is well understood. But let’s take a closer look at the standard SAP solutions that enterprises can use to enable secure user identity propagation in typical, loosely coupled, service-based transactions (stage 2 in Figure).

### Selecting the Right SSO Solution for an SOA Environment

SAP has two solutions to choose from, depending on the scope and goals of your SSO endeavor: SSO tickets and Security Assertion Markup Language (SAML)-based methods.

#### SAP-Specific SSO Tickets

The SAP SSO ticket is an SAP proprietary mechanism that sends a cookie-based SSO token from a service caller to a service provider with the goal of securely transferring user ID information across the interacting systems. Simply put, the sender system creates a digitally signed, cookie-based SSO ticket, and the receiver system verifies its signature and accepts or rejects it for user authentication once the sender system calls a service.

Let’s put this process in the context of our Figure 1 example. During user identity propagation (the second stage), the sender system is the service client — typically a portal or a composite server — and the receiver system is the back-end service provider, an SAP ERP system, for example.

The receiver system verifies the digital signature of this SSO ticket with the sender system’s X.509 public key certificate. Based on this check, the receiver system can securely determine if:

- The ticket was issued by a trustworthy system.

This tells the receiver system that the ticket contents, including the user IDs, are authentic and can reliably be trusted. Note that the receiver can evaluate this SSO ticket only if the sender and receiver have set up a trust relationship — a

---

1 To learn more about **SAP NetWeaver Identity Management**, see “Getting Started with Identity Management” by Keith Grayson in the April-June 2008 issue of **SAP Insider** (www.SAPinsideronline.com). The way in which ID management solutions should factor into your SSO security, however, is beyond the scope of this article.
configuration step that includes an administrator importing the ticket sender’s X.509 system certificate into the receiver's key storage.\textsuperscript{2}

- The ticket is authentic.\textsuperscript{1} This tells the receiver system that the ticket wasn’t modified while it was transmitted. This authenticity is established via cryptographic mechanisms, which verify the digital signature against the sender’s X.509 certificate.

For internal identity propagation security across an SAP landscape, SSO tickets are the SSO method of choice. You likely use this solution in your company now to enable current scenarios, such as RFCs and other SAP NetWeaver communication protocols. For more complex security needs that stretch beyond the SAP space, however, consider using SAML-based SSO methods to secure the user identity propagation.

**New SAML SSO Scenario Supported with SAP NetWeaver**

SAML, an XML framework for exchanging authentication and authorization information in assertions, is an SSO solution developed by the Organization for the Advancement of Structured Information Standards (OASIS).

SAML therefore offers a significant advantage in that it allows for interoperable security across many landscapes — not just SAP ones — allowing secure heterogeneous system integration. SAP relies on SAML to enable another of its major SSO methods that propagates user identity for enterprise services: the Sender-vouches subject confirmation method for WS Security SAML token profiles 1.0.

The Sender-vouches subject confirmation method enables security interoperability for user identity propagation in service-based scenarios with SOAP Web service-based calls across heterogeneous environments (see Figure 2). It is available with SAP NetWeaver 7.1, as well as with support packages 14 and higher for SAP NetWeaver AS ABAP 7.0.

**SSO Tickets vs. SAML SSO Solutions**

SSO tickets, while ubiquitous in SAP landscapes as a means for propagating user identities in service calls, impose limitations stemming from their security configuration. For example, the sender and receiver systems need to share a user store to ensure that the user identity is the same; the ticket validity must be configured; and for confidentiality guarantees, the ticket transfer should be executed over an encrypted connection. Other constraints arise from the fact that the SSO tickets have limited interoperable communication from non-SAP service consumers since such systems are not programmed to issue SSO tickets.

The Sender-vouches subject confirmation method for WSS SAML token profiles overcomes the interoperability constraint with non-SAP service consumers. Still, it does have several similarities with the SSO ticket mechanism. Like SSO tickets, the assertions sent with this scenario contain the user ID, as well as the sender system’s name and digital signature. And while SAML tokens exchange the user information in a technically different XML-based format as compared to SSO tickets, the actual contents are similar.

As with SSO tickets, prerequisites for using SAML tokens include configuring a trust relationship between the service consumer that issues the SAML token and the service provider, and synchronizing the user identities in the different systems through a shared user store or identity management solution.

**User Identity Propagation: The Next Generation**

In addition to the Sender-vouches subject confirmation method for SAML, SAP NetWeaver 7.1 will support an additional SAML solution for user identity propagation: the Holder of Key subject confirmation method. In this method, the SAML assertion issuer, which confirms the user’s identity for the service

---


\textsuperscript{1} By authentic, I mean conforming to fact and therefore worthy of belief.
calls, is decoupled from the consumer and provider systems (see Figure 3).

This decoupling allows administrators to configure a third system as a central point for issuing SAML assertions for service provider calls. This system could be a specialized access and identity management product or a specially configured portal system that can access user identities and issue SAML assertions for those identities. Under this method, the trust association must be set up between the third system (acting as a SAML assertion issuer) and the service provider itself, thus enabling greater scalability of trust management with multiple service providers.

The Holder of Key subject confirmation method allows administrators to move from having to establish point-to-point trust between service sender and receiver systems to more manageable star-like trust relationships, with the SAML assertion issuer as the center. Such centralization will provide advantages in high-volume service scenarios, allowing companies to scale the trust configuration and access management to include enterprise services exposed from external service provider systems.

In addition, because SAML is an industry-standard solution, the SAML assertion issuer role can be taken over by specialized identity and access management products provided by either SAP or partners. This provides the flexibility that companies have been seeking: Administrators can use an already available product with SAML token-issuing capabilities, and they’re not required to switch to an SAP-specific one to implement high-volume enterprise SOA scenarios.

**The Big Picture: Identity Propagation and SSO in Access Management**

Even now, some readers may be asking: Why bother with user identity propagation? One alternative method would be to execute calls to back-end resources under a shared or service user authentication context—an option available with SAP NetWeaver. But when users access critical enterprise information resources via SAP NetWeaver, administrators and managers need to make sure that they can properly control access rights assignments and keep track of what was used—all of which can help fulfill compliance requirements.

Accessing resources under shared service user permissions clearly can’t meet requirements for performing granular authorizations checking or auditing in service scenarios—the same service user is always logged in at the service provider.

In contrast, SSO solutions that enable user identity propagation allow users to access only those service-enabled enterprise resources for which those users were granted permission. Securing this propagation process with digital signatures, generated and verified via trusted system key pairs, provides the necessary security guarantees and doesn’t impose prohibitive limitations for security key retrieval and management.

As business networks increasingly form based on loosely coupled enterprise services, the need for security and accountability is rising in importance, with authenticated user access to enterprise IT resources becoming a major concern. But with SAP-specific SSO tickets to support your current security needs and SAML-based scenarios to support interoperable security configurations, administrators can count on familiar SSO mechanisms to remain a stronghold of their security arsenal for a long time to come.

---

**Additional Resources...**

- **The Administration and Infrastructure 2009 conference** in Orlando, March 25-27, 2009, for sessions on SAP system security and access management (www.sapadmin2009.com)