COLUMN

Security Strategies

SAPinsider

This article appeared in the Jul ▪ Aug ▪ Sep 2011 issue of *SAPinsider* (http://sapinsider.wispubs.com) and appears here with permission from the publisher, WIS Publishing.

WIS PUBLISHING

Eliminate **Password Chaos** While Ensuring System **Security**

SAP Offers Enhanced SSO Functionality with SAP NetWeaver Single Sign-On

by Jonathan Cooper and Frane Milicevic, SAP

Jonathan Cooper (jonathan.cooper@sap.com) joined SAP in 2011. As Product Owner, he is responsible for the Enterprise Single Sign-On functionality. Previously, Jonathan worked for SECUDE as a Technical Editor and Product Manager.

Frane Milicevic (frane.milicevic@sap.com) joined SAP in February 2011. As Product Owner, he is responsible for SAP's Secure Login functionality. Previously, Frane worked for SECUDE as Senior Security Consultant and Product Manager.

See if this scenario sounds familiar: In the course of your workday, just to perform your everyday business tasks, you must log in to several different systems, entering a password each time. Since you're required to change these passwords frequently and create lengthy, difficult combinations to increase security, you might find yourself logging in to an infrequently used application and being unable to remember that specific password. This creates a delay as you submit a ticket to your help desk and wait for a response.

Or say you're an IT administrator working at your company's help desk. How many requests do you get that have to do with forgotten passwords? And can't you think of a million more valuable things you could be doing with your time?

Companies looking to eliminate this password chaos should consider single sign-on (SSO) functionality. With SSO solutions, users need to authenticate only once; all subsequent authentication processes are handled in the background without prompting users for additional passwords.

However, for several reasons, some companies still have not embraced SSO. Some believe that having only one password and entry point for all applications and data might weaken their security. In reality, though, users who are tired of forgetting and resetting their passwords often choose the same password for each application, only changing one character when they have to change passwords. Or, they write them down or store them as plain text on easy-to-access mediums like word processing documents or sticky notes.

Accordingly, eliminating the need for passwords in business applications actually means getting rid of a number of processes that are costly and have inherent security risks. For example, without passwords, companies can bypass the dangers of password phishing.

Another reason companies aren't yet using SSO is that implementing it simply isn't a high enough priority; they wonder if the ROI of SSO makes up for the time required to implement it. We would argue that the time spent implementing SSO pays for itself through improved productivity from users who can focus on their work, undistracted by the process of inventing and changing passwords, calling the help desk, or constantly being prompted with new login screens. The help desk, which will no longer have to deal with daily password requests, will also be able to focus on more valuable work.

In addition to these key benefits, the argument in favor of SSO has become even stronger with new security functionality that is now available within SAP NetWeaver Single Sign-On.

SAP NetWeaver Single Sign-On: Features and Functionality

There are two options when implementing SSO:

- **Using security tokens that contain a user's identity and are accepted by the applications.**

Key Concept: SAP NetWeaver Single Sign-On

As a result of SAP's acquisition of SECUDE, SAP received SECUDE's Secure Login and Enterprise Single Sign-On solutions and integrated these into SAP NetWeaver Single Sign-On.

This is enabled through Kerberos, browser-based cookies, client certificates, or Security Assertion Markup Language (SAML) tokens.

- **Using passwords to enter business applications.** In this case, the SSO software automatically enters the user credentials into the password prompts or dialog boxes.

SAP has supported the first option for a long time, with SAP logon tickets, Kerberos, and SAML. Now, with SAP NetWeaver Single Sign-On, SAP has greatly strengthened its support for both options. Let's take a closer look at two major new capabilities now available within the SAP NetWeaver Single Sign-On toolbox.

Secure Login

At the core of the new SAP NetWeaver Single Sign-On solution is SAP's new **Secure Login** component (see **Figure 1**), which enables identity authentication through client certificates (security tokens) across both SAP and non-SAP applications. (In the past, customers needed to turn to SAP partners to support authentication through client certificates.)

A major benefit of using X.509 client certificates is that so many applications support this method; it is a stable and widely accepted standard (which translates into lower TCO). Furthermore, this method provides more security than passwords do, protecting the user from accidentally giving away or losing any private credentials. On top of that, Secure Login provides customers with a lean, easy-to-use instance that issues client certificates to users when they need them.

Using Secure Login

If your company chooses to use Secure Login, users will first have to authenticate against the Secure Login SSO infrastructure. This initial authentication needs to happen only once, as long as users do not log out or shut down their computer. For this initial authentication, Secure Login supports:

- **Reuse of Windows credentials, which are stored in an Active Directory.** This process happens in transparent mode, so users do not have to type in their credentials again; rather, they receive the client certificate as soon as they log in to Windows. (Note: This feature will be available in support package 1, planned for October 2011.)
- **Radius protocols.** Third-party solutions that are based on Radius can use a one-time password to enable SSO.
- **User credentials.** Stored in the LDAP directory or in the ABAP application server (user database), these credentials can be used to provide X.509 user certificates.
- **Public-key infrastructure (PKI) integration.** If your company already uses a PKI, Secure Login supports SSO through users' smart cards. Note that companies running Secure Login do

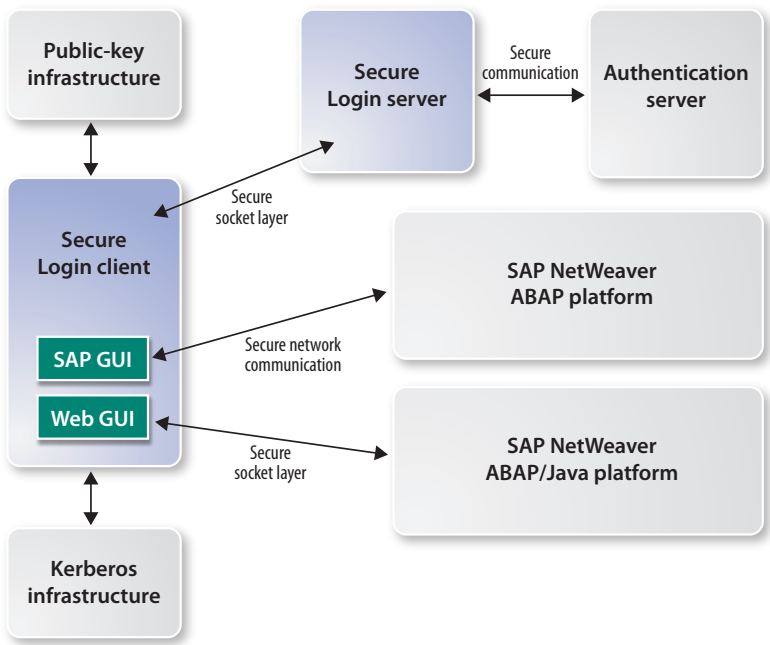

FIGURE 1 ▼ SSO in SAP GUI with Secure Login

SAP's Classic SSO Technologies Are Here to Stay

SAP has supported SSO through logon tickets and SAML* and will continue to do so to enable web-based SSO scenarios.

In addition, SAP will continue to support the Kerberos open standard method of SSO. SAP applications that support Kerberos for authentication include SAP NetWeaver Portal. Users that work in a Windows domain with Kerberos enabled will still be able to log in to the portal using Kerberos without an external SSO solution.

* For more information, see "Taking SSO to the Next Level" by Dimitar Mihaylov and Yonko Yonchev in the July-September 2010 issue of *SAPinsider* (sapinsider.wispubs.com), as well as "How to Future-Proof the Security of Your System Infrastructure in a Service-Enabled World" by Yonko Yonchev in the July-September 2008 issue.

not need a PKI; it's simply possible to integrate Secure Login into it.

To implement the Secure Login component, administrators need to configure the server only once to accept the user's credentials. Administrators will also need to configure any applications to use the client certificate for authentication. In particular, they'll need to make sure the mapping between certificates and users is maintained. The integration between SAP NetWeaver Identity Management (SAP NetWeaver ID Management) and SAP NetWeaver Single Sign-On components will help foster this process.

Once everything is set up, and after the initial user authentication, the Secure Login server will issue a client certificate that is pushed into the Windows Certificate Store and the SAP GUI Personal Security Environment for secure network communication. The client certificate acts as the secure SSO token that authenticates against all applications.

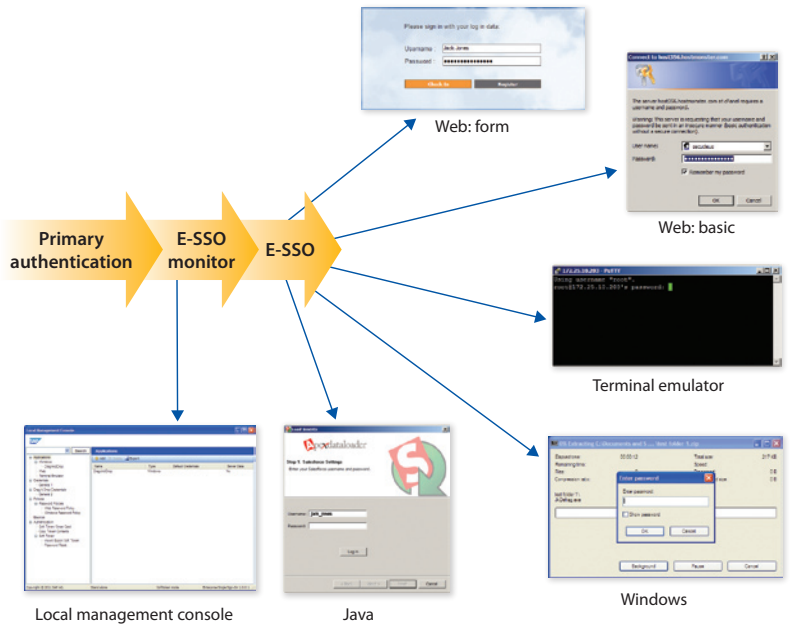

FIGURE 2 ▲ SSO through E-SSO; users need only authenticate their identity once, then E-SSO will perpetuate that authentication through other applications

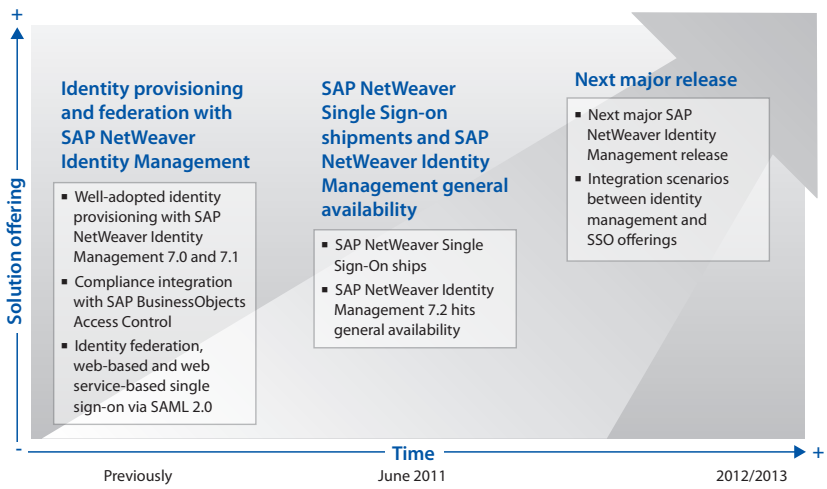

FIGURE 3 ▲ Plans for upcoming SAP NetWeaver SSO functionality

Enterprise Single Sign-On

SAP NetWeaver Single Sign-On will also support SSO to legacy applications (after the user undergoes initial authentication, of course). This is done through the **Enterprise Single Sign-On** (E-SSO) component (see **Figure 2**).

This method of SSO is especially useful for a wide variety of applications, such as Skype, webmail, and WinRAR, which do not support client certificate-based authentication. E-SSO works, for example, with Windows applications, terminal emulators, Java applications, and websites/web-based applications.

Using E-SSO

Once E-SSO is installed, users can set up the SSO mechanism on their own. E-SSO will automatically prompt the user — via a credential registration wizard — to enter credentials for an application or website for safe storage in the solution's soft token or smart card framework.

After this initial phase, E-SSO takes over authentication to the respective applications, without requiring any further user interaction. All credentials that have been accumulated will be stored securely within the E-SSO framework; in addition, the solution can automatically change the user passwords into randomly generated, more complex passwords to bolster security.

Continuing the Evolution of SSO

SAP will continue to enhance its SSO offerings. With the next releases of SSO functionality (see **Figure 3**), we hope to make our SSO solutions even easier to deploy and run, and to extend their reach to allow SSO to work with more enterprise applications out of the box.

For more information, visit **www.sdn.sap.com** → Security and Identity Management → SAP NetWeaver Single Sign-On. ■

Copyright