SAPinsider

This article appeared in the Jul • Aug • Sep 2012 issue of *SAPinsider* (http://sapinsider.wispubs.com) and appears here with permission from the publisher, WIS Publishing.

WIS pubs

Take Advantage of Cross-Platform, Cross-Device Access While **Keeping Your Data Secure** with SAP NetWeaver Gateway

by André Fischer and Genady Podgaetsky, SAP AG

Making your SAP systems available through the platforms and devices in which your users already spend their time is a boon to business growth — however, it also presents the challenge of ensuring secure, seamless access to your data. To help, SAP offers SAP NetWeaver Gateway, a development framework that allows you to expand the reach of your SAP software across a wide range of devices and platforms, including mobile, collaborative, and social media environments, and to do so with speed, ease, and at a low cost.

Based on market standards,[1] SAP NetWeaver Gateway allows non-SAP developers to use the development tool of their choice to quickly create and deploy rich applications that connect users, via services, to SAP back-end software. SAP NetWeaver Gateway also secures network communications to help keep data protected and works with several types of authentication mechanisms, including those that enable single sign-on (SSO), to create a more seamless user experience. In this article, we'll provide you with an overview of how SAP NetWeaver Gateway security works, and the options available for authentication and SSO.[2]

Understanding SAP NetWeaver Gateway Security

Network communications and user authorizations are critical to maintaining control over your data. Fortunately, SAP NetWeaver Gateway supports the infrastructure you already have in place for network security and user authorizations, so you don't have to reinvent the wheel.

Network and Communication Security

Instead of using proprietary protocols, the communication between SAP NetWeaver Gateway and the consumer (the browser-based or cloud application, mobile device, etc.) is based on the OData Protocol. This is an HTTP-based protocol in which the interaction between the client and the SAP NetWeaver Gateway server resembles how an end user would browse web pages. The communication is facilitated via the Internet Communication Manager (ICM) process of SAP NetWeaver Application Server, using handlers in the Internet Communication Framework (ICF).

This means that SAP NetWeaver Gateway supports the same authentication options offered by the underlying SAP NetWeaver Application Server ABAP runtime. The communication exchange can be easily encrypted using HTTPS and secured using a reverse proxy, such as the SAP Web Dispatcher, which provides protection on the protocol level.

Communication between SAP NetWeaver Gateway's server and the SAP Business Suite back-end system is based on SAP remote function calls (RFCs). The trusting/trusted system relationship established by the RFC connection enables SSO between the server and the back-end systems. The SAP NetWeaver Gateway infrastructure also includes token-based CSRF (Cross-Site Request Forgery) protection, which checks all

[1] This includes the Open Data Protocol (OData), which was recently submitted to OASIS for standardization.

[2] See "SAP NetWeaver Gateway Extends the Reach of SAP Business Applications" by Adi Kavaler in the July-September 2011 issue of *SAPinsider* (sapinsider.wispubs.com).

André Fischer (andre.fischer@sap.com) is a Product Manager for SAP NetWeaver Gateway who joined SAP in 2004. André often speaks at SAP TechEd and has published numerous articles and blogs about SAP security-related topics.

Genady Podgaetsky (genady.podgaetsky@sap.com) is a Security Expert for SAP NetWeaver Gateway and Duet Enterprise products. Genady has been with SAP since 2005 and has 16 years of experience in the computer industry.

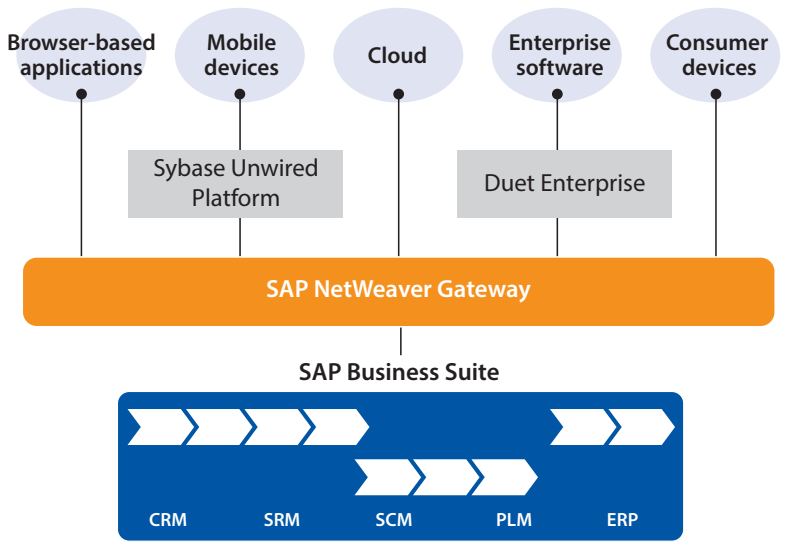
modifying requests from a user's browser to the SAP NetWeaver Gateway server for a valid CSRF token. In addition, virus scanning can be performed on incoming update and create requests for SAP NetWeaver Gateway services that are used to upload documents to the back-end SAP Business Suite system.

Note: To enable a trusted RFC connection between the SAP NetWeaver Gateway system and back-end systems, you must ensure that the usernames are identical in both.

SAP NetWeaver Gateway at a Glance

SAP NetWeaver Gateway is an add-on to the ABAP technology platform that can be deployed either on a separate server or locally on an SAP Business Suite system. SAP NetWeaver Gateway also integrates with Sybase Unwired Platform and Duet Enterprise.

As shown in the figure below, SAP NetWeaver Gateway forms a bridge among various consumer channels (mobile and non-mobile clients, such as browser-based applications, smartphones, tablets, the cloud, and enterprise software) and the business layer of an existing SAP solution landscape. Through SAP NetWeaver Gateway, SAP Business Suite data can be exposed by services that support the Open Data Protocol (OData) , which is a simple HTTP-based protocol for accessing data that is commonly used by mobile applications and HTML5 web applications.



▲ SAP NetWeaver Gateway connects devices, environments, and platforms to SAP software solutions

User Management and Authorizations

Since you can deploy SAP NetWeaver Gateway as an add-on to the ABAP runtime of SAP NetWeaver Application Server, SAP NetWeaver Gateway is able to leverage the user management and authorization concepts that are currently in place in your back-end SAP systems so you don't have to maintain a separate configuration for SAP NetWeaver Gateway authorizations and user management.

It is also possible to define ABAP authorization roles in the SAP NetWeaver Gateway system to control access to SAP NetWeaver Gateway services using a "white list" approach. This means only users assigned to a predefined role in the SAP NetWeaver Gateway system can access the services. With this approach, even if user access is granted at the service level, the SAP user authorizations are checked in the back-end system against the assigned ABAP authorizations.

Some SAP customers may choose to run SAP NetWeaver Gateway on a separate SAP NetWeaver Application Server to protect their SAP back-end systems from malicious requests coming from the outside. In scenarios like this, SAP NetWeaver Gateway can be easily connected to an existing central user administration or identity management system landscape for user/role synchronization.

Now that you understand how user management and network communication is secured with SAP NetWeaver Gateway, let's review the options available for authentication.

Authentication Options with SAP NetWeaver Gateway

There are different methods for implementing authentication with SAP NetWeaver Gateway, depending on the scenario in which you want to use it. For example, to ensure the security of your back-end data, a web application that is external to your SAP landscape requires a different type of authentication to SAP NetWeaver Gateway than a native client-side or desktop application that resides within your system landscape.

To meet the needs of different scenarios, SAP NetWeaver Gateway supports several authentication options, including options that enable SSO.

Browser-Based SAML 2.0 Authentication

Security Assertion Markup Language (SAML), currently in version 2.0, is an XML-based open standard that allows you to enable SSO with SAP NetWeaver Gateway using the authentication options you already have in place. A typical SAML setup includes an identity provider (IdP) from solutions (such as SAP NetWeaver Single Sign-On[3] or Microsoft Active Directory Federation Services) that create SAML assertions and a service provider (such as SAP NetWeaver Gateway) that receives the SAML assertions. The consumer can authenticate to the IdP using one of the authentication options supported by the IdP, receive a SAML assertion, and forward it to SAP NetWeaver Gateway to enable login.

Browser-based SAML 2.0 authentication does not require deployment of client certificates, making it an ideal authentication option for web-based SSO access — users in such scenarios cannot be expected to install software or certificates in their environments. You can also use browser-based SAML 2.0 authentication in intranet scenarios by leveraging Integrated Windows Authentication to authenticate the IdP and achieve SSO.

X.509 Client Certificate Authentication

X.509 client certificates are widely accepted and supported as the standard for identity authentication. In this method, a digital certificate with the user's public key is sent to the server, which then validates the certificate and allows login. X.509 client certificates usually require a public key infrastructure (PKI) to handle the certificates. Customers that do not have a PKI in place can use SAP NetWeaver Single Sign-On, which creates short-lived certificates in the user's certificate store to enable SSO to SAP NetWeaver Gateway.

Note that, when using SAP NetWeaver Single Sign-On, users have to be authenticated against the SSO infrastructure of the secure login component. This authentication can be performed seamlessly by reusing the user's Windows login credentials. The secure login server issues a client certificate that it pushes to the Windows Certificate Store; this certificate can then be used for SSO to SAP NetWeaver Gateway.

[3] SAP NetWeaver Single Sign-On allows users to assign identity credentials that support single sign-on mechanisms. The solution is not, however, a panacea to all single sign-on needs; rather it enables a variety of authentication scenarios.

SAP Logon Tickets

When using logon tickets for authentication, a user's ticket is stored as a non-persistent cookie in the user's web browser. This cookie contains the username; therefore to ensure security, we recommend that you protect the web client's cookie cache and employ transport layer security mechanisms, such as secure socket layer (SSL).

Basic Authentication

Basic authentication is the simplest form of authentication. In this case, the consumer application simply provides a user name and password when making a request to SAP NetWeaver Gateway. Using basic authentication is generally not recommended for authentication to SAP NetWeaver Gateway, since it does not support SSO, and requires the consuming application to provide secure storage for the login credentials and handle initial and expired passwords.

This option is also risky because users can be locked out due to distributed denial-of-service (DDoS) attacks. Basic authentication is a valid option in a business-to-consumer scenario in which a web server connects to SAP NetWeaver Gateway on behalf of all service users. In this scenario, the user's credentials would be known only to the calling web server rather than to the end users.

So when does it make sense to use which authentication option with SAP NetWeaver Gateway? Let's take a look.

Choosing the Right Option for Authentication

Choosing the appropriate authentication option for your company depends on your particular SAP NetWeaver Gateway scenario. **Figure 1** on the next page summarizes which authentication

SSO offers an array of benefits in an environment that uses SAP NetWeaver Gateway. A user only needs to remember a single set of credentials, regardless of the UI, which helps increase productivity. SSO also means that all authentication-related information is centralized on a single security service provider, which helps enterprise administrators enforce a consistent authentication policy throughout the identity management process.

Consumer	Basic authentication	SAP logon tickets	X.509 client certificate authentication	Browser-based SAML 2.0 authentication
Web application (HTML5/ Silverlight/Flex)	●	● *(When published via SAP NetWeaver Portal)*	●	●
Desktop application (.NET/Java)	●	●	●	●
Mobile application	●	●	● *(When running on Sybase Unwired Platform)*	● *(When not running on Sybase Unwired Platform)*

FIGURE 1 ▲ Authentication options in SAP NetWeaver Gateway (recommended options are shaded in green)

options SAP NetWeaver Gateway supports, and which are recommended (shaded in green), for some of the most common scenarios.

Web Applications

In this scenario, the consumer is any client-side web application that is based on HTML5, Silverlight, or Flex, and accesses the service that exposes the back-end SAP data on the SAP NetWeaver Gateway server directly from the user's browser. Since the application runs in the browser, it can leverage the authentication options that are available for browser-based access out of the box (basic authentication, X.509 client certificate authentication, and browser-based SAML 2.0 authentication).

While all of the authentication options are supported in this scenario, the recommended option for SSO with SAP NetWeaver Gateway in this case is browser-based SAML 2.0 authentication. In contrast to X.509 client certificate authentication, no certificates need to be distributed to the user environment by a PKI or other software solution, and unlike basic authentication, there is no risk of users being locked out due to a DDoS attack.

SAML 2.0 is also suitable for kiosk scenarios because it can use various authentication options simultaneously. For example, SAML can use an IdP (such as Microsoft Active Directory Federation Services or SAP NetWeaver SSO) and leverage the user's Windows domain username and password to enable smoother SSO. SAP logon tickets are the method of choice if the web application is published via SAP NetWeaver Portal.

Desktop Applications

Client-side desktop applications typically run on an employee's desktop in the company intranet, and development platforms can include, among others, .NET and Java. The most logical approach to achieving SSO in a client-side environment is to leverage the initial authentication when a user logs on to the corporate network, because the user only has to remember one password. In most cases, this will be Windows domain user authentication, which uses Kerberos. SAP NetWeaver Gateway currently does not support Kerberos-based authentication out of the box (future releases could change that; see sidebar), but the user can acquire tokens from the initial authentication that SAP NetWeaver Gateway accepts for login.

You can choose browser-based SAML 2.0 authentication if the IdP supports Kerberos-based authentication, which is the case for SAP NetWeaver Single Sign-On and Microsoft Active Directory Federation Services. Strictly speaking, however, browser-based SAML 2.0 authentication is supported only for applications that run inside a browser and perform redirects, handle cookies, and manage security sessions. To use browser-based SAML 2.0 authentication, the client code for the desktop application needs to ensure that it behaves like a browser when handling HTTP redirects, managing forms, and processing cookies. With the upcoming support of OAuth (see sidebar), this will no longer be necessary.

From a developer's perspective, it is more straightforward to use X.509. However the use of X.509 requires that certificates be rolled out using either a PKI infrastructure or the secure login component of SAP NetWeaver Single Sign-On if there is no PKI in place.

Mobile Applications

Managing the vast array of mobile devices and applications throughout an enterprise is a challenge. But mobile enterprise application platforms, such as Sybase Unwired Platform, make it easy to quickly develop and deploy mobile solutions across the mobile workforce.

With Sybase Unwired Platform, which is leveraged by new mobile applications such as SAP

Authentication Support for the Cloud, Social Networks, and Intranet: OAuth 2.0 and Kerberos (SPNego)

While cloud-based solutions and social networking applications have opened up a new world of opportunity, they also bring a host of new challenges and requirements when it comes to authentication. To simplify authentication support for the cloud, social network, and intranet integration, SAP is currently looking into supporting two additional authentication options for SAP NetWeaver Application Server ABAP: OAuth 2.0 and Kerberos (SPNego). Depending on the underlying SAP NetWeaver Application Server release, SAP NetWeaver Gateway would also support these options.

OAuth 2.0

OAuth is an open standard for authorization that allows access to information without sharing access permissions. Supporting the OAuth 2.0 protocol is especially beneficial for web, cloud-based, and social network scenarios.

For example, with OAuth, if an employee launches an HTML5-based application from a browser, the application can perform service calls on behalf of the authenticated user. OAuth makes it possible to fulfill corporate security policies that usually require restricted user permissions in the business application for inbound calls from the Internet or a public cloud provider. With SAML-based authentication, the same token can be used to call a service that lists all employees and to perform changes in the back-end system when another service is called, provided the user has the appropriate authorizations. With the OAuth-based approach, the client is granted access only to a certain list of services based on approved access lists (called scopes).

Kerberos (SPNego)

For intranet scenarios, SAP plans to enable authentication on SAP NetWeaver Application Server ABAP by using the Kerberos protocol (via SPNego, which extends Kerberos to web applications through HTTP). The Kerberos library will be available as part of SAP NetWeaver Single Sign-On, which must be licensed by the customer.

With Kerberos, the user logs on to the domain controller of the Windows domain at the beginning of the working day and is issued a Kerberos ticket. The user is then able to access OData services provided by SAP NetWeaver Gateway using SSO based on this ticket.

Mobile Sales and SAP Mobile Service, a relay server manages requests from mobile devices to Sybase Unwired Platform 2.1 server. This communication is HTTP-based with message-based encryption.

The recommended SSO authentication option for mobile devices running on Sybase Unwired Platform is to use X.509 client certificates, which require an existing PKI infrastructure for certificate distribution or using the SAP Afaria mobile device management solution for this purpose. With this approach, Sybase Unwired Platform 2.1 server establishes an HTTPS connection to SAP NetWeaver Gateway with client certificate forwarding in the HTTP header.

If certificates cannot be used — if no PKI is in place, for example — SAP NetWeaver Portal can be used as an external authentication provider. In this case, the developer configures SAP NetWeaver Gateway to trust the SAP logon tickets that SAP NetWeaver Portal issues based on the user's portal credentials.

If the mobile applications are not using a mobile enterprise application platform such as Sybase Unwired Platform, browser-based SAML 2.0 authentication is the recommended option because it does not require any additional deployments, such as certificates, on the user's device. As in the case of desktop applications, the client code for mobile applications that want to leverage the SAML 2.0 browser protocol would need to ensure that the application acts like a browser when handling HTTP redirects, managing forms, and processing cookies (in contrast, Sybase Unwired Platform supports SSO out of the box).

Summary

SAP NetWeaver Gateway is paving the way for your SAP software to reach users anytime, anywhere, on any device. Such an expansive reach requires a comprehensive approach to security and user access. This article touched on the basics of network authentication with SAP NetWeaver Gateway to help you start formulating an approach that will work for you. With an informed understanding of these concepts and knowledge of which authentication options are best suited for the most common scenarios, you are already well on your way. ■