Single Sign-on Support with WebSEAL-Lite in WebSphere Everyplace Server

March 2002

Samuel R. Barahona-Rodriguez, IBM Pervasive Computing, Austin, Texas

Ronnie Jones, IBM Pervasive Computing, Raleigh, North Carolina

Chung T. Nguyen, IBM Pervasive Computing, Austin, Texas

Single Sign-on Support with WebSEAL-Lite in WebSphere Everyplace Server

Introduction

As enterprise systems expand to support the growth of e-business processes, users and system administrators are challenged with increasingly complicated interfaces to accomplish their job functions and secure business transactions in today's Web environment. Users frequently have to undergo many authentication processes as they sign on to multiple systems, necessitating an equivalent number of credential inquiry dialogues, each of which may involve different usernames and authentication information. System administrators are also faced with managing user accounts in each of the multiple systems to be accessed while maintaining the integrity of security policies. To this end, the concept of single sign-on (SSO) promises many security enhancements by automating access to all authorized web services and enterprise-wide applications through a single login. This powerful solution eliminates the need for a user to remember multiple sign on processes, user IDs, or passwords. Furthermore, it reduces the time network administrators spend on password management and improves productivity as well as profitability by providing users and customers with instant access to their own personalized resources.

In WebSphere® Everyplace™ Server, Service Provider Offering for Multiplatforms (WebSphere Everyplace Server), the single sign-on feature can be implemented with WebSEAL-Lite, an authentication and authorization plugin for WebSphere Edge Server Caching Proxy, also known as Web Traffic Express . WebSEAL-Lite is the central point of user authentication for the WebSphere Everyplace Server domain. One of the many features of WebSEAL-Lite is its single sign-on capability, which allows a user to log on to all services within the WebSphere Everyplace Server infrastructure without being challenged again. With this feature, user authentication only needs to be done once to access services requiring a user ID and password within the WebSphere Everyplace Server domain. Authentication is still needed for services outside the WebSphere Everyplace Server domain. The next section addresses the implementation of SSO in the WebSphere Everyplace Server environment.

Single Sign-On Implementation with WebSEAL-Lite

There are many possible ways to configure an SSO environment. The selection of a method should depend on the particular environment configurations, the characteristics and features of the servers involved,and the security requirements. In this section, we will outline the implementation steps to enable single sign-on functionality in the WebSphere Everyplace Server environment.

WebSphere Everyplace Server uses a Lightweight Third Party Authentication (LTPA) authentication mechanism for enabling SSO in its environment. If additional servers involved in the SSO solution also support the LTPA cookie, this approach is the most favorable to follow. In this scenario, we assume that our back-end server does not support LTPA cookies. Furthermore, we do not include Policy Director in our environment, and the underlying WebSphere Everyplace Server environment authenticates the user's credentials using WebSEAL-Lite only. The Secure Socket Layer (SSL) and X.509 certificates are used to enable secure connections between our browser and the WebSphere Everyplace Server environment and between the WebSphere Everyplace Server environment and the back-end server.

Our environment uses client-side certificates for user authentication on WebSEAL-Lite. Other authentication mechanisms, such as basic authentication, do exist, but certificates are more secure and safer, especially over untrusted networks.

The WebSEAL-Lite SSO mechanism is realizable through the use of a smart junction. A smart junction is a physical connection between a WebSEAL-Lite server and an application server. When properly configured, WebSEAL-Lite can protect both its own resources and the resources on the junctioned server. To create a WebSEAL-Lite junction, an alias IP address has to be defined for the WebSEAL-Lite/Web Traffic Express machine. All requests made from the browser to the alias will be routed to the WebSEAL-Lite/Web Traffic Express machine and then redirected through the WebSEAL-Lite junction to the back-end server.

The flow of a single sign-on mechanism under this environment is as follows (Fig. 1):

1. Using a client-side certificate, the user sends a request for a service to WebSEAL-Lite through an SSL connection.
2. WebSEAL-Lite verifies the certificate.
3. The certificate subject name is mapped to a user on IBM® SecureWay® Directory (LDAP) via the ePerson entry attribute specified on the `ldap_attribname_certdn` setting on the `ibmwesas.conf` file.
4. Once the user is authenticated, the request is redirected using a WebSEAL-Lite junction to the back-end server.
5. The junction starts a new SSL connection, between Web Traffic Express and the back-end server.
6. The back-end server maps the request to a user in its user database and creates a session.

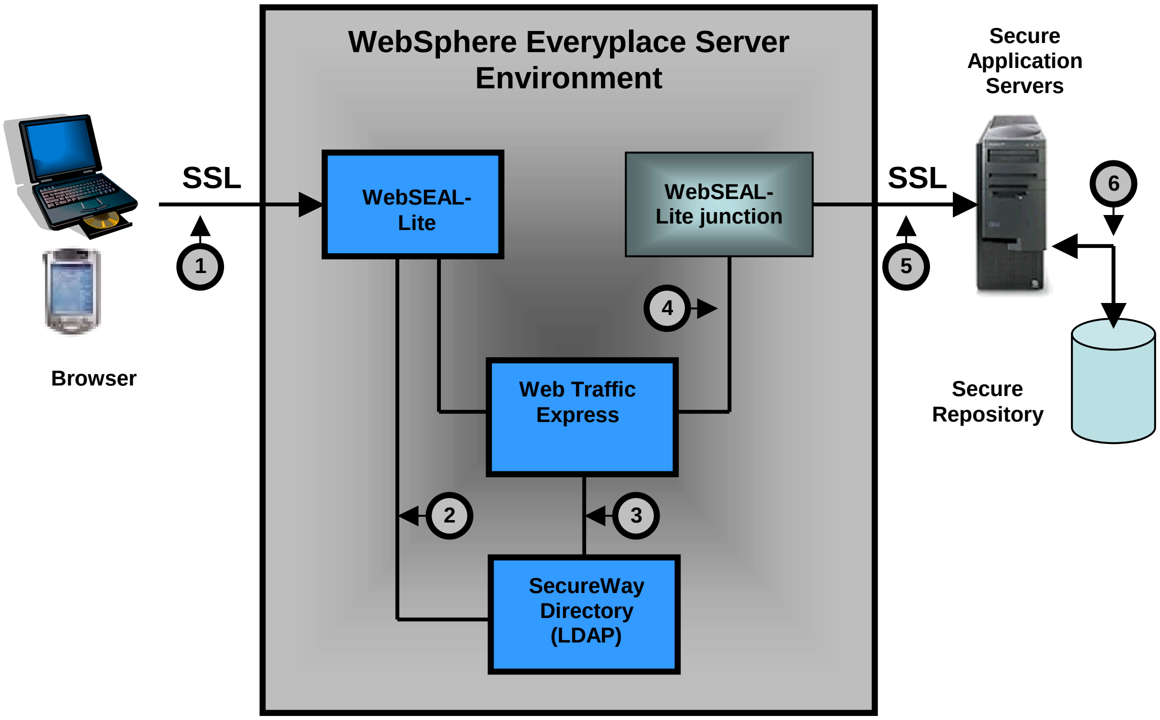
WebSphere Everyplace Server Environment
Secure Application Servers
SSL
WebSEAL-Lite
WebSEAL-Lite junction
SSL
6
1
5
4
Browser
Web Traffic Express
Secure Repository
2
3
SecureWay Directory (LDAP)

Fig. 1 – WebSEAL-Lite Single Sign-On Operational Flow

The back-end server should be configured to use SSL and to behave in one of the following ways:

a. The back-end server allows the WebSEAL-Lite/Web Traffic Express server to perform authentication. The back-end server maps the user making the request to a user in its database and starts a session but it does not perform any further authentication. The http headers that come with the request, for example, the X-IBM-PVC-User header, are used to perform the required mapping.

or

b. The back-end server performs authentication using an authentication header that includes UserID and Password. In this case, Web Traffic Express has to be configured to forward the authentication header to the back-end server.

Since the security configurations on web application servers are vendor specific, a back-end server may require a different security configuration setting. For the purpose of this scenario, we assume that the back-end server will trust the WebSEAL-Lite for authentication and that it will map the user on the X-IBM-PVC-User header to a user in its database.

Setting up single sign-on in a WebSphere Everyplace Server environment

This section includes specific steps to enable the single sign-on function in the WebSphere Everyplace Server environment. The prerequisites for this implementation are as follows:

- WebSphere Everyplace Server installed on an IBM AIX® version 4.3.3 platform.
- WebSphere Everyplace Server version 2.1.1 or later

1. **Configure an alias on the WebSEAL-Lite machine**
   You must have a separate IP address available to configure an alias. The machine on which the browser is running must be able to resolve this IP address.

   a. From a command prompt on the WebSEAL-Lite machine, type `smitty`
   b. Select the appropriate option and press ENTER to expand the following menus:

      ➢ `Communications Applications and Services`
      ➢ `TCP/IP`
      ➢ `IPV6 Configuration`
      ➢ `IPV6 Network Interfaces`
      ➢ `Configure Aliases`
      ➢ `Add an IPV4 Network Alias`

   c. Enter the IP address and network mask on their respective fields. For this scenario, the alias is "`alias.ibm.com`".

2. **On the WebSEAL-Lite machine, create a Key Ring file and Key Ring Stash file using IKEYMAN**

   a. From a command prompt, type `ikeyman`
   b. From the pull-down menu, select **Key Database File -> new**
   c. Select a name and location for your Key Ring File and click **OK**. For this scenario, the Key Ring File is `/etc/cert/key.kdb`.
   d. Type a password, and check the **Stash the password to a file** option. Click **OK** to save these changes.

3. **On the back-end server, export a personal certificate into a PKCS12 file**

   Consult your back-end server documentation for instructions.

4. **Import the back-end server personal certificate into your WebSEAL-Lite machine using IKEYMAN**

a. From a command prompt, type `ikeyman`

b. From the pull-down menu, select **Key Database File -> open**

e. Browse for the Key Ring File created on step 2 and open it. For this example, open `/etc/cert/key.kdb`.

c. On the **Key database content** pull-down menu, select **Personal Certificates**. Click **`Import`** to import this certificate.

d. Browse for the PKCS12 file created during step 3, and click **OK** to complete the import process.

5. If the IBM HTTP Server is running on the WebSEAL-Lite machine, make sure it is not listening to the SSL port 443

a. Open the `/usr/HTTPServer/conf/httpd.conf` file.

b. If you find the line `Listen 443`, comment it out.

c. Restart the http server by issuing `apachectl stop` and `apachectl start` commands.

6. On the WebSEAL-Lite machine, edit the `ibmproxy.conf` file to enable SSL

a. Open the `/etc/ibmproxy.conf` file

b. Change the value of the SSLEnable directive to ON.

c. Set the KeyRing and KeyRingStash directives to point to the files created in step 2:

- KeyRing `/etc/cert/key.kdb`
- KeyRingStash `/etc/cert/key.sth`

7. On the WebSEAL-Lite machine, create a remote junction in the `osdef.conf` file

Using the alias created for the WebSEAL-Lite machine in step 1, create a junction that points to the back-end server on port 443. The junction will be called `ssojunction`.

a. Add the following lines to the `/opt/pdweb-lite/etc/osdef.conf` file:

```
[Remote: /WebSEAL-Lite/reverse/alias.ibm.com]

domains = alias.ibm.com alias.ibm.com:443 alias.ibm.com:8081
login_method = certificate
require_ssl = yes
require_ssl_errorfile = /opt/pdweb-lite/samples/require_ssl.htmls
require_cert_errorfile =/opt/pdweb-lite/samples/require_cert.htmls

[Junction: /WebSEAL-Lite/reverse/alias.ibm.com:/ssojunction=https//<back-
   end webserver>:/443/]

require_ssl = yes
require_ssl_errorfile = /opt/pdweb-lite/samples/require_ssl.htmls
require_cert_errorfile =/opt/pdweb-lite/samples/require_cert.htmls
```

9. Create a client side certificate (for example, from http://www.thawte.com or http://www.verisign.com) and install it on your browser.

10. On the WebSEAL-Lite machine, add the SSLCertificate directive to the `ibmproxy.conf` file

a. Open the `ibmproxy.conf` file

b. Add the following line:

```
SSLCertificate alias.ibm.com SSCertLabel ClientAuthRequired
```

where *alias.ibm*.com is the alias defined in step 1, and *`SSCertLabel`* is the label name of the certificate imported from the back-end server in step 4.

11. **Edit the client certificate attribute**

    Since a client certificate is set for `login_method`, the attribute `ibm-CertificateSubjectAndIssuer` is used to store the DN of the client certificate. To edit this field, the `ibm-CertificateForDN` auxiliary class has to be added to the LDAP user entry.

    a. Launch Directory Management Tool on the WebSEAL-Lite machine.
    b. Highlight the user entry under the cn=users container. For example, uid=george.
    c. Click on **Add Auxiliary class**.
    d. Select the **ibm-CertificateForDN** object class.
    e. Click **OK** until you return to the main Directory Management Tool window.

12. **On the WebSEAL-Lite machine, set up the `ldap_attribname_certdn` WebSEAL-Lite attribute**

    a. Open the `/opt/pdweb-lite/etc/ibmwesas.conf` file.
    b. Modify the following line:

    ```
    Ldap_attribname_certdn  ibm-CertificateSubjectAndIssuer
    ```

13. **Modify the LDAP ePerson entries to contain certificate information**

    a. Using the Directory Management Tool on the WebSEAL-Lite machine, open the ePerson entry of the user you want to modify.
    b. Select the **Other** window.
    c. In the **ibm-CertificateSubjectAndIssuer** field, add the certificate subject name. For example, using certificates from http://www.thawte.com , you would enter `MAIL=`*`user@ibm.com`*`,CN=Thawte Freemail Member where `*`user@ibm.com`*` is the appropriate e-mail address`.
    d. Click **OK** until you return to the main Directory Management Tool window.

14. **Restart WebSEAL-Lite and Web Traffic Express**

15. **Retrieve a document from the back-end server**
    The sample URL below requires that `sample.html` exists on the back-end web server.

Open http://*alias.ibm.com*:*8081*/ssojunction/sample.html where *alias.ibm.com* is the alias defined in step 1, and *8081* is the port number used by Web Traffic Express. If Web Traffic Express uses port 80, no port number is required in the URL.

Conclusions

In a WebSphere Everyplace Server environment, the single sign-on function reduces the cost of user ID and password management, increases user productivity and efficiency, and maintains the integrity of network resources and system security protection. In addition, since enabling single sign-on requires no additional hardware or software and is fully compliant with open industry standards, it allows enterprise organizations to leverage their current systems and resources and receive a quick return on this investment.

Glossary

ePerson

An entry in the LDAP database that contains user profiles and information

Secure Socket Layer (SSL)

This security technology, also called the IEFT standard Transport Layer Security (TLS), uses data encryption, message digest, digital certificate, etc., to achieve multiple security objectives, such as confidentiality, authentication, and data integrity.

SecureWay LDAP

The IBM SecureWay Directory is a central Lightweight Directory Access Protocol Directory (LDAP) database. It contains information related to users, devices, and networks in addition to the system configuration information.

Session ID

The session ID uniquely identifies an active session. An active session corresponds to an authenticated user. The session ID is attached to the Authentication Server session header.

User-Agent

User-Agent is a field in the HTTP header that defines the user ID and password for authentication.

User ID

The client device passes user identification to the Authentication Server when prompted for basic authentication. The Authentication Server queries the User ID information in the HTTP header.

WebSEAL-Lite

WebSEAL-Lite is the core of security functionality in WebSphere Everyplace Server. It is the central point of user authentication and authorization for the WebSphere Everyplace Server domain. WebSEAL-Lite is also the point of entry to the WebSphere Everyplace Server domain for devices that do not connect through IBM Everyplace™ Wireless Gateway. Hence, it enables WebSphere Everyplace Server to use third-party gateways and provides user and device authentication capabilities that enable a single, device-independent, user sign-on.

Web Traffic Express (WTE)

Web Traffic Express is also referred to as WebSphere Edge Server. It provides the functionality of a proxy server for various protocols, such as HTTP, FTP, etc.

About the Authors

Samuel R. Barahona-Rodriguez (samuelr@us.ibm.com) is a Software Engineer for IBM in Austin, Texas, working on the Pervasive Computing Division team. As a developer, he has worked to enable IBM partnerships with WebSphere Everyplace Server. He has also worked on the development of Java technologies.

Ronnie A. Jones (rajones@us.ibm.com) is a Software Engineer for IBM in Research Triangle Park, North Carolina, working on the Pervasive Computing Division team. He has worked as the technical lead for WebSphere Everyplace Server Test.

Chung Nguyen (nguyencj@us.ibm.com) is an Advisory Software Engineer for IBM in Austin, Texas, working on the Pervasive Computing Division team. He has engaged in both development and architectural design with several key IBM business partners to enable their products to work with WebSphere Everyplace Server. He has authored several papers and patents on Java technology and signal recognition methods. His interests include wireless technology, voice recognition, neural networks, and artificial intelligence.

All statements regarding IBM future direction or intent are subject to change without notice and represent goals and objectives only.