Third-Party Gateway Plug-in Support in the WebSphere Everyplace Server

December 2001

Chung Nguyen

Third-Party Gateway Plug-in Support in the WebSphere Everyplace Server

Chung Nguyen
Pervasive Computing Division

Introduction

WebSphere® Everyplace™ Server, Service Provider Offering for Multiplatforms (WebSphere Everyplace Server) extends e-business to pervasive devices while reducing risk, time-to-market, and integration challenges. It combines all the necessary middleware infrastructure and e-business tools into one integrated, performance-tuned, and comprehensive solution that enables customers to rapidly deploy, connect, adapt, manage, transform, and scale today's Web applications and legacy data into tomorrow's pervasive applications. WebSphere Everyplace Server expands e-business opportunity into the world of mobile e-commerce by protecting current IT investments. One such feature of WebSphere Everyplace Server supports integration with existing third-party gateways, which are vendor gateways other than the IBM Everyplace Wireless Gateway, and ensures interoperability with networks, devices, and applications through adherence of industry standards.

This paper focuses on the design and operation of the authentication plug-in module that allows the use of third-party gateways with WebSphere Everyplace Server. This paper will give the reader a better understanding of the authentication plug-in and how it provides a comprehensive wireless solution. In the following sections, the paper details a user request from a third-party gateway and shows how the authentication plug-in handles the request to ensure interoperability with WebSphere Everyplace Server. Considerations for performance optimization are also discussed in this paper. The information in this paper pertains to a number of WebSphere Everyplace Server components, including WebSphere Edge Server Caching Proxy, also known as Web Traffic Express, WebSEAL-Lite (Authentication Server), Everyplace Active Session Table (AST) server, and IBM® SecureWay® Directory. This paper does not cover product availability and pricing models; for more details on pricing and availability, please contact your IBM representatives or the IBM Pervasive Computing website.

Some important terms and acronyms used in this paper are listed below:

- **WebSEAL-Lite**: WebSEAL-Lite is the core of WebSphere Everyplace Server security functionality. 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 Wireless Gateway. Hence, WebSEAL-Lite enables WebSphere Everyplace Server to use gateways other than Everyplace Wireless Gateway and provides user and device authentication capabilities that enable a device-independent single sign-on.

- **Web Traffic Express**: WebSphere Edge Server Caching Proxy, also referred to as Web Traffic Express, retrieves Internet data for multiple clients and acts as a caching server and content filter, providing the functionality of a proxy server for protocols such as HTTP, FTP, etc.
- **SecureWay Directory**: SecureWay Directory is a central Lightweight Directory Access Protocol Directory (LDAP) database. It contains information related to users, devices, and networks in addition to system configuration information.
- **Active Session Table (AST)**: Active Session Table records user information in a Tivoli® Personalized Services Manager (TPSM) database. The set of user information in the session table entry corresponds to the authenticated user and sends an acknowledgement of the active session to WebSEAL-LITE.

For more details on the WES components, please refer to the following Redbooks:

- *An Introduction to IBM WebSphere Everyplace Suite version 1.1 Accessing Web and Enterprise Applications, SG24-5995-00*
- *Extending e-business to Pervasive Computing Devices Using IBM WebSphere Everyplace Suite version 1.1.2, SG24-5996-00*
- *Using LDAP for Directory Integration A look at IBM SecureWay Directory, Active Directory and Domino, SG24-6163-00*
- *IBM WebSphere Performance Pack: Caching and Filtering with IBM Web Traffic Express, SG24-5859-00*

WebSEAL-Lite Authentication Overview

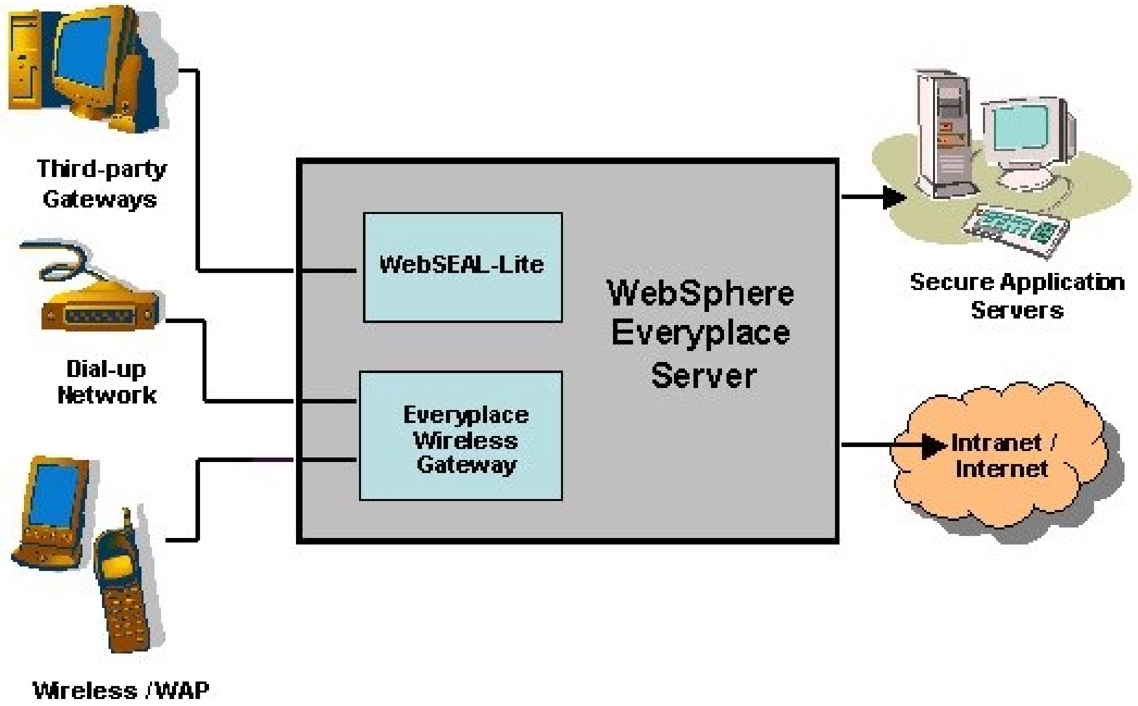
Third-party Gateways
Dial-up Network
Wireless /WAP
WebSEAL-Lite
Everyplace Wireless Gateway
WebSphere Everyplace Server
Secure Application Servers
Intranet / Internet

Figure 1 – Points of entry to the IBM WebSphere Everyplace Server

WebSphere Everyplace Server is designed and implemented to allow centralized user authentications from various points of entry into the WebSphere Everyplace Server domain (see Figure 1). WebSphere Everyplace Server authentication employs several industry standards to maintain confidentiality. Everyplace Wireless Gateway and WebSEAL-Lite perform the user authentication function within the WebSphere Everyplace Server environment. For user requests coming from third-party gateways, WebSEAL-Lite is positioned as the first entry point for all HTTP traffic and uses the HTTP basic authentication process to authenticate the user's credentials. Therefore, third-party gateways that act as a proxy for the client must support HTTP in order for WebSEAL-Lite to carry out the authentication process. The WebSphere Everyplace Server authentication process begins with a validation of the user's credentials embedded in the HTTP header. User credentials and profiles are stored in a centralized repository, which consists of an Active Session Table (AST) database and a SecureWay Directory database (LDAP). To ensure that all user requests from third-party gateways are authenticated and tagged with the active session key, WebSEAL-Lite invokes a corresponding authentication plug-in.

Authentication Plug-in Overview

The authentication plug-in is a gateway-specific module that functions as a bridge between a third-party gateway and WebSphere Everyplace Server. In a multithreaded environment, such as the WebSphere Everyplace Server environment, this authentication plug-in is thread-safe and runs as part of the same process and thread as WebSEAL-Lite. Furthermore, the plug-in has access to the HTTP headers, the URL, the query string, and other information about the current request through the same Caching Proxy plug-in APIs as WebSEAL-Lite.

For user requests coming from third-party gateways, WebSEAL-Lite is positioned as the first entry point for all HTTP traffic and uses the HTTP basic authentication process to authenticate the user's credentials. When WebSEAL-Lite invokes the authentication plug-in, it returns a client user ID revealing who initiated the HTTP request coming through the gateway. WebSEAL-Lite then inspects the HTTP header and looks for the user's credentials. Next, it searches the SecureWay Directory database for third-party gateway definitions and the ePerson entry with client ID attributes that match the client ID returned by the plug-in. If a matching ePerson entry is found, WebSEAL-Lite will modify the user's HTTP request header, record the user ID, organizational unit attributes, and other header information in a local database, which can be accessed by the AST server. Session ID, user ID, device ID, and network information will be inserted into HTTP header as authorization and identification tags. The content and application servers downstream use these pointers to retrieve information from the AST server and LDAP directory to complete the user's requests.

Authentication Plug-in Operations

The synergy of the authentication plug-in process for third-party gateways in the WebSphere Everyplace Server environment is depicted in Figure 2. The figure shows the authentication process conducted by WebSEAL-Lite and the authentication plug-in in conjunction with other WebSphere Everyplace Server components to authenticate an enrolled user from a third-party gateway. In the WebSphere Everyplace Server environment, Tivoli Personalized Services Manager Subscription Enrollment or Customer Care services handles the user enrollment.

1. **Third-party gateway receives a WAP request destined for WebSphere Everyplace Server.**

   This scenario assumes that a user who is already enrolled in the WebSphere Everyplace Server domain is trying to access the services hosted by WebSphere Everyplace Server via another vendor gateway. First, when receiving a user request from a WAP device, the vendor gateway will check its own database to authenticate the user's credential. If the user's credential is not authenticated by the gateway, an HTTP error code 401 is returned to the client indicating a failed authorization.

2. **WebSEAL-Lite receives the user's HTTP request**

   After validating the user, the third-party gateway inserts WebSphere Everyplace Server headers and forwards the request to WebSEAL-Lite using an HTTP protocol. The client ID attribute is configurable and is contained in the third-party gateway definition defined in the SecureWay Directory database. The HTTP request header at this juncture has the form:

HTTP req + UserAgent + Network + User

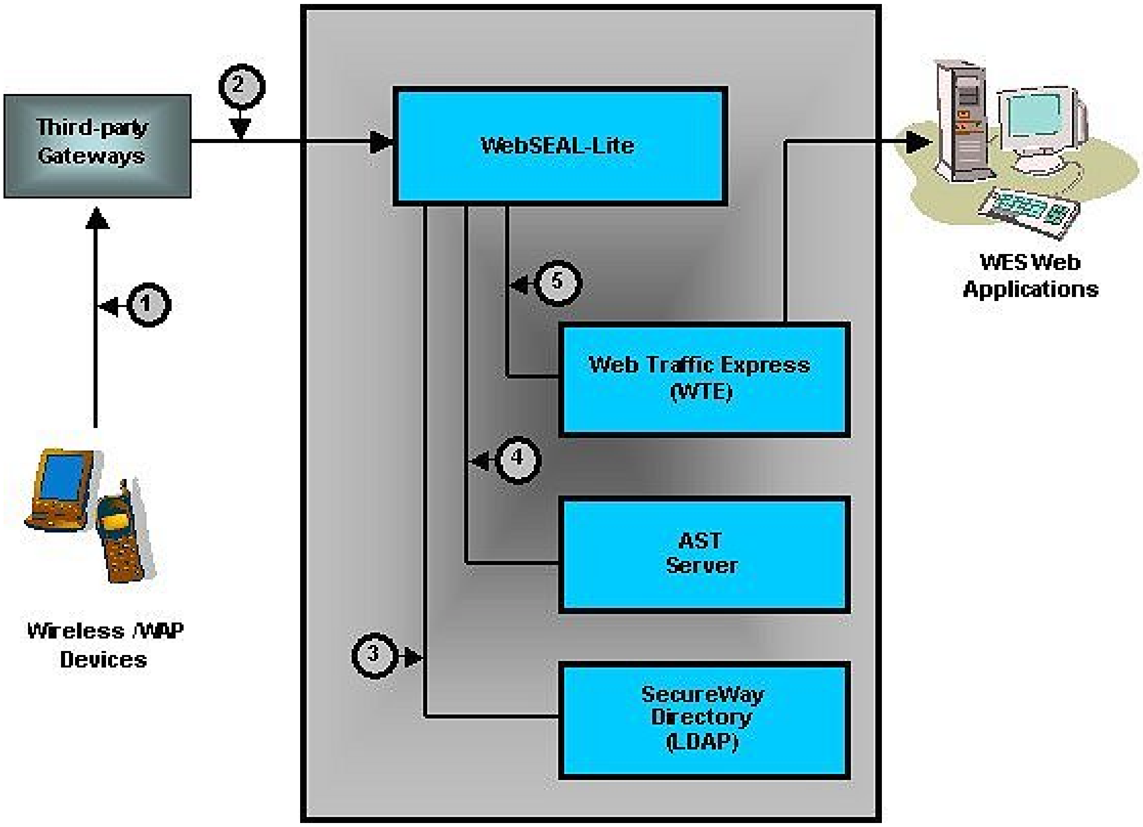

Figure 2 – Synergy of an authentication process for a user request coming from a third-party gateway

3. Authentication plug-in inspects the HTTP header and returns the client ID information to WebSEAL-Lite

After receiving the request, WebSEAL-Lite accesses the SecureWay Directory database for the definition of the third-party gateway (e.g., *cn=thirdpartygateway* under the System Applications portion *sys=SDP* of the database) to determine if the gateway is considered a "trusted" gateway. If the third-party gateway's definition does not exist in the database, WebSEAL-Lite returns a 401 HTTP code error to the client browser, indicating failed authentication. Otherwise, it invokes the authentication plug-in to inspect the user HTTP request header. The HTTP request header now has the form:

```
HTTP req + UserAgent + Network + User + Client ID
```

The plug-in parses through the HTTP header string and looks for the client ID attributes. The client ID attributes can be a user ID string or an MSISDN string. The client ID is then used by WebSEAL-Lite to search the *cn=users* portion of SecureWay Directory for the ePerson entry whose client ID attribute matches the client ID returned by the plug-in.

4. AST formulates an active session key for insertion in the HTTP header

If there is a match from the SecureWay Directory database search for a client ID, an authorization key is returned to WebSEAL-Lite. The authentication plug-in, which also has access to Web Traffic Express, will provide WebSEAL-Lite with information regarding the current user HTTP request header, such as the URL, client ID, query string, network type, and device type. This user request information will be verified once more with the Active Session Table server database to determine whether the user already has an active session. Then, WebSEAL-Lite places a session header in each HTTP request to correlate the identified user, device type, and network type with an active session and associate each individual HTTP request with an appropriate authentication session.

If it is the first request from the user, i.e., no active session key exists, WebSEAL-Lite uses the user ID and organizational unit attributes in the SecureWay Directory database to construct the session ID and the authorized client ID. The session ID is a string generated when an AST entry is written to uniquely identify and differentiate an active session. The formats for the session ID and client ID are:

Session ID:	X-IBM-PVC-Session
Client ID:	X-IBM-PVC-Client-id

This session information will be used to create a new AST session record in the AST database for this request. Then, the new AST session key is inserted into the HTTP request header for web servers downstream. The inserted AST key has the form:

```
Inserted AST key = [session ID, client ID, device, network]
```

If there is an existing AST session that corresponds to the user ID, WebSEAL-Lite will update the record in the active session database for the time of the last visit.

5. WebSEAL-Lite populates remaining WebSphere Everyplace Server headers

Once WebSEAL-Lite receives a return code and the session key (either new or updated) from the AST server indicating that the authentication is approved, it will populate the final form of the HTTP request header and direct it to the Web application servers to fulfill the request. The fully authenticated HTTP header now has the form:

HTTP req + User-Agent + Network + Device + User + Authorization + Session ID

In most cases, WebSEAL-Lite retrieves responses from the Web Traffic Express server and sends the responses back to the client. However, if the user request is destined for a third-party service on the Internet, WebSEAL-Lite will remove authorization headers from the request prior to forwarding it to third-party web servers.

Performance Considerations

Since every user request that comes through a third-party gateway calls the authentication plug-in, it is important that the plug-in works efficiently and avoids lengthy operations. One of the plug-in's most expensive operations is the SecureWay Directory database search for the ePerson entry with a client ID attribute that matches the one returned from the plug-in. The cost of this operation becomes significant when searching an LDAP database with a large number of entries. However, the performance of this search operation can be improved by creating a database index, preferably a DB2 index, which represents the relationship between the SecureWay Directory's ePerson entries and the client ID attributes. Third-party gateway requests that require a SecureWay Directory database search use the index as a lookup table; hence, the overall performance improves significantly.

Authentication Plug-in Installations

Beginning with WebSphere Everyplace Server version 1.1, IBM provides interoperability support for a number of third-party gateways. In the current WebSphere Everyplace Server 2.1.1 release, WebSphere Everyplace Server customers can select and download an appropriate authentication plug-in module for their existing wireless/WAP gateway from a list of supported third-party gateways at the IBM Pervasive Computing website:

http://www6.software.ibm.com/dl/everyplace/gateway-p

Prerequisites and instructions for installing each gateway specific plug-in are also found in the Readme file included in the plug-in package.

Conclusions

With the authentication plug-in feature in WebSphere Everyplace Server environment, support for single sign on, centralized authorization, and secured authentication methods are enabled. This plug-in's capability provides a seamless interoperability between third-party gateways and the WebSphere Everyplace Server environment to ensure all functions within the WebSphere domain can be accessed by defined user privilege. Moreover, this feature offers a quick and robust integration of WebSphere Everyplace Server components with other wireless applications and an industry-standard infrastructure to protect the customers' existing e-business investment and provide them the most flexibility for extending their applications out to mobile users.

Glossary

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

Dial-up Network
Dial-up traffic from the open internet.

Device Type
The device type is queried from the HTTP header and used as a key to look up a device profile in LDAP. The device profile is extracted from LDAP at initialization time.

ISDN
Integrated Services Digital Network is a network that supports both digital telephone networks and Global System for Mobile Communication (GSM) networks.

Network Type
The network type is queried from the HTTP header and used as a key to look up a network profile in LDAP. The network profile is extracted from LDAP at initialization time.

MSISDN
Mobile Subscriber ISDN (MSISDN) number is the dialable number that callers use to reach a mobile subscriber. Some phones can support multiple MSISDNs - for example, a U.S. based MSISDN and a Canadian based MSISDN. Callers dialing either number will reach the subscriber.

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.

Third-party Wireless Gateway
Third-party wireless gateways or vendor gateways are any wireless/WAP gateways other than the IBM Everyplace Wireless Gateway (EWG).

Tivoli Personalized Services Manager (TPSM)
TPSM provides a comprehensive set of management services to the solution, including content personalization, subscriber enrollment, customer care and customer self-care.

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.

Wireless Access Protocol (WAP)
An open industry standard for mobile internet access. WAP allows mobile users with wireless devices to easily and instantly access and interact with information and services.

About the Author

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 the 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.