A technical discussion of a mobile security implementation

March 2002

WebSphere® software

Helping to create a trusted environment to access confidential information from virtually everyplace you are.

By Tom Covalla, Frank Seliger
and Tony Wrobel
IBM Pervasive Computing Division

Contents

Introduction

Increasingly, companies rely on electronic creation, transmission and storage of personal, financial and other confidential information. Giving professionals convenient access to such information starts with enabling the growing numbers of mobile transactions through the use of a new class of intelligent and portable computing devices. Pervasive computing allows workers to take action virtually anywhere anytime. Moving from e-business to pervasive e-business also assumes professionals can access and transfer sensitive information through transmission over the Internet and other public networks. How do you create a pervasive computing environment that provides high security for confidential transactions? How can you be confident—trust—that your data is safe? Security for data communication has been well documented ever since the Internet became popular. Six common security requirements for pervasive e-businesses are:

Authentication. With any communication, you want to know who you are communicating with, and the other party needs to be certain that you are you. Over the Internet, when you communicate with a Web site server, you want to be sure that it is who it claims to be. This is called server authentication. Client authentication is how you establish your identity. The combined authentication of server to client and client to server is called mutual authentication.

Confidentiality. As a synonym of secrecy, confidentiality is defined as the means to protect data communication from eavesdropping. You want knowledge for only those who need to know.

Integrity. You need to verify that data has not been altered in transit by a third party. Integrity helps you prevent forgery, tampering and unauthorized alteration.

Authorization. To avoid improper use of your data and services, you limit what information the user is allowed to see or what actions a user may take. Authorization can minimize the chance of exposing sensitive information to malicious attack or unauthorized alteration.

Nonrepudiation. You need ways to prevent parties in the data transaction from denying their actions after transactions are completed. You can enforce accountability for electronic transactions with nonrepudiation.

> *Privacy.* You expect to give your users ways to control sensitive information that they provide to applications and other system users.

These are the six characteristics normally required by online content and application services which involve data communication. Another important requirement for more secure computing is creation of a boundary for the service domain. This reduces opportunity for attack by hackers from public networks. Firewalls are commonly used to prevent attacks, such as denial of service, packet spoofing (pretending to be the server or the client) and impersonation.

Security matters. When the public Internet is used to convey confidential information, it becomes even more important. And when confidential information is transmitted from highly portable devices, security becomes critical. This white paper addresses security implementation within IBM WebSphere® Everyplace™ Server, Version 2.1. It explains the general security objectives for data communication and the security design of WebSphere Everyplace Server. The paper discusses three types of security implementations within WebSphere Everyplace Server—TCP/IP security, wireless security and IBM MQSeries® Everyplace security. It also explains firewall use with WebSphere Everyplace Server and the overall integrated security design. Everyplace Server can provide a foundation for companies that want to expand business to pervasive e-business with security-rich function. The following major functions of WebSphere Everyplace Server can extend protection and add value to your information assets. And WebSphere Everyplace Server supports selectable installation, which means you can use many of the components independent of others that you may or may not need to install.

Connectivity

WebSphere Everyplace Wireless Gateway. Can provide security-rich wired and wireless connectivity between the information technology (IT) network and the communications network, for example, Global System for Mobile (GSM) communication, code-division multiple access/time-division multiple access (CDMA/TDMA), Internet service data network (ISDN), General Packet Radio Services (GPRS). Everyplace Wireless Gateway also provides connectivity for protocol translation (TCP/IP, Wireless Access Protocol, or WAP) and support for Short Message Service (SMS).

Content adaptation

WebSphere Transcoding Publisher. Allows transformation of arbitrary content into a form that can be presented on a different device from the originally intended device, such as changing HTML content intended for desktop personal computers to Wireless Markup Language (WML) content suitable for the new type of smart phones.

MQSeries Everyplace component. Enables pervasive computing devices to queue messages and transactions, and helps assure transaction completion (once and only once), efficiently and with high security in connected and disconnected end-user scenarios.

Everyplace Synchronization Manager. Enables pervasive computing devices to operate applications offline and synchronize results (e-mail, personal information manager or databases) of the activities with a server database when connectivity is reestablished.

Content delivery

Location-based services. Location services can provide privacy-based access to location information:

- *Locates mobile end users (their longitude/latitude or city/state/country)*
- *Supplies information to applications that deliver personalized content based on the location (for example, a restaurant application can identify the nearest restaurant to your current location)*

Intelligent notification services. Enables end users to be notified when certain events of interest occur (for example, a sports team scores a touchdown). Notifications are delivered through the following SMS messages: WAP *push* messages, e-mail, and/or instant messaging.

Management services

Tivoli® Personalized Services Manager (TPSM). Offers a comprehensive set of management services, including content personalization, enrollment, self-care, customer care, interfaces to external billing systems, reporting, software distribution and update and availability status.

Security-rich features

WebSEAL-Lite capability. Gives user and device authentication with ability to enable a single, device-independent user logon, and pass-through of authentication information to Web application servers. Also WebSEAL-Lite integrates with Tivoli Secureway® Policy Director from IBM for user authorization and access control.

Tivoli Secureway Policy Director. Provides fine-grained access control for user requests to Internet addresses, or URLs. Includes privacy management for user location information.

WebSphere Everyplace client. Permits use of Two-Party Key Distribution Protocol (2PKDP), the security protocol that combines mutual authentication with key distribution using a minimal number of messages. 2PKDP supports encryption and decryption for all signals coming into and going out from WebSphere Everyplace Server, with a choice of either data encryption standard (DES) or RC5 encryption algorithms.

WAP client. Utilizes Wireless Transport Layer Security (WTLS) for communication between a WAP-enabled device and the Everyplace Wireless Gateway.

Firewall support. Support for integrating Tivoli SecureWay Firewall and popular third-party firewalls to protect against unauthorized access and viruses. The firewall component is not included in the WebSphere Everyplace Server package.

Performance optimization

WebSphere Edge Server. Provides highly scalable caching functions on a server to help reduce bandwidth costs and improve response times when processing URLs. In addition, WebSphere Edge Server dynamically monitors and load-balances activity across the set of WebSphere Everyplace Server processors that is deployed in a configuration.

Base (common) services

SecureWay Directory. A central Lightweight Directory Access Protocol (LDAP) directory which contains runtime information about active sessions, users, devices and networks. This database can make it easy for WebSphere Everyplace Server components (and components of any server that is added to the configuration) to access the runtime information, centrally, without having to replicate the data in other repositories. WebSphere Everyplace Server console. Provides a single console for system administrators to perform installation and diagnostic procedures, administrative procedures and system maintenance procedures.

WebSphere Everyplace Server addresses your security requirements

WebSphere Everyplace Server helps create a safe environment to support pervasive e-business. It includes centralized user authentication from limited points of entry. WebSphere Everyplace Server can exploit single sign-on capability for user-friendly implementation of credential-sharing across the services hosted by the suite. WebSphere Everyplace Server relies on a set of industry security standards, such as Transport Layer Security/Secure Socket Layer (TLS/SSL) and Wireless Transport Layer Security (WTLS) to achieve the security objectives for the service domain. WebSphere Everyplace Server uses proxy technology in conjunction with firewalls to define the boundary for the service domain.

Authentication

The user authentication function within WebSphere Everyplace Server is performed by the Everyplace Wireless Gateway component and WebSEAL-Lite capability. The administrator authentication within WebSphere Everyplace Server is component dependent.

WebSphere Everyplace Server employs several industry-standard technologies to perform credentials acquisition and authentication. For credentials acquisition, WebSEAL-Lite uses:

- *The HTTP basic authentication process to authenticate user transmissions coming from the Internet and third-party gateways. For this reason, clients and/or the gateway proxy for the clients must support HTTP.*
- *A custom forms-based login to collect username and password.*
- *SSL X.509 client certificates.*

The WebSphere Everyplace Wireless Gateway component authenticates users from three different types of connections. Each type of user connection uses a different authentication process. Details on these processes appear later in this paper. To perform actual authentication of credentials, WebSEAL-Lite can utilize either Tivoli Secureway Policy Director or LDAP. Everyplace Wireless Gateway can use either LDAP or RADIUS for username and password authentication.

Confidentiality

WebSphere Everyplace Server utilizes a set of industry-standard security technologies to help achieve the goal of confidentiality. Such technologies include SSL and WTLS. In addition, Everyplace Wireless Gateway uses a modified version of Point-to-Point Protocol (PPP) called Wireless Optimized Link Protocol (WLP) to create encrypted tunnels to promote confidentiality for clients with wireless client software applications installed. Security mechanisms provided by the operating system platform, such as Internet Protocol (IP) security, can also be used within WebSphere Everyplace Server.

Authorization

The access control in WebSphere Everyplace Server is implemented using Tivoli SecureWay Policy Director HTTP proxy technology. You can implement finer levels of access control at individual WebSphere Everyplace Server components and application servers by integrating SecureWay Policy Director with the WebSphere Everyplace Server services.

Data integrity

WebSphere Everyplace Server helps to provide data integrity using features, such as message digest and certificates, included in the SSL and WTLS technologies.

Nonrepudiation

Nonrepudiation can be achieved by using digital signature in addition to the security mechanisms employed by WebSphere Everyplace Server, such as TLS/SSL. But, no specific capabilities for nonrepudiation are provided inWebSphere Everyplace Server.

Privacy

WebSphere Everyplace Server enables location-based services, which require dispersing a user's location information to enabled applications. WebSphere Everyplace Server provides mechanisms for individual users to control which applications can see their location information.

Security implementation within WebSphere Everyplace Server

The following sections describe how the components of WebSphere Everyplace Server provide all the functionality to help implement high security.

Single sign-on

Figure 1 shows how WebSphere Everyplace Server allows users to connect to it through either the Everyplace Wireless Gateway component or the WebSEAL-Lite capability. Users from Internet or third-party gateways connect to Everyplace Server only through WebSEAL-Lite. Users may also access WebSphere Everyplace Server using three types of links through Everyplace Wireless Gateway, including:

- *A dial-up connection based on PPP*
- *A wireless client-created connection over wireless or IP networks*
- *A wireless connection based on WAP*

The user authentication can be conducted at points of entry by Everyplace Wireless Gateway and WebSEAL-Lite.

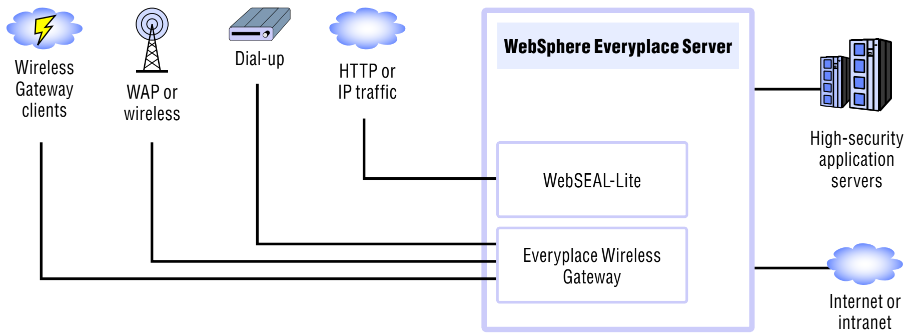

Figure 1. Points of entry to the IBM WebSphere Everyplace Server

WebSphere Everyplace Server is designed to achieve single sign-on (SSO) by authenticating users only once for access to a given service hosted by WebSphere Edge Server. This SSO authentication design is achieved by sharing user session information through a centralized repository, use of HTTP cookies or by way of TLS/SSL session persistence. This centralized repository consists of the active session table (AST) database. As shown in Figure 2, the Everyplace Wireless Gateway component uses a centralized RADIUS server to authenticate users. WebSEAL-Lite uses either SecureWay Policy Director or LDAP to authenticate users if username and password are the credentials being used. They each deposit user active session entries into the AST database to share the user session information.

In addition to credential-sharing across WebSphere Everyplace Server components, SSO relies on coordination between the two authentication agents—the Everyplace Wireless Gateway component and WebSEAL-Lite capability. WebSEAL-Lite is used as the central point for authentication, or it can be set up to trust and acquire authentication information from Everyplace Wireless Gateway. WebSEAL-Lite is the first entry point for all HTTP traffic from the Internet and third-party gateways. The Everyplace Wireless Gateway also routes all HTTP requests to WebSEAL-Lite which is the next nonfirewall hop after Everyplace Wireless Gateway. Users already authenticated by Everyplace Wireless Gateway will not be reauthenticated by WebSEAL-Lite. SSO also implies the ability to supply a token or credentials to back-end application servers that they require. WebSEAL-Lite supports the ability to configure a specific set of authentication tokens for any given back-end server. For example, a lightweight third-party authentication (LTPA) token for SSO can be passed to IBM WebSphere Application Server. A simple username and password or a cookie of a configurable format can be passed to other servers. This capability is depicted in Figure 3.

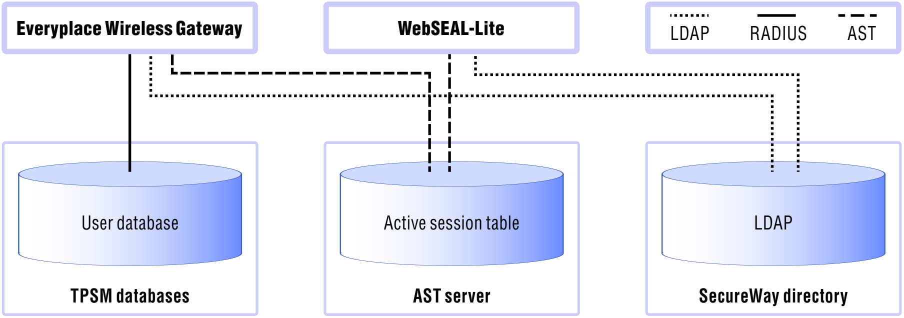

Figure 2. Single sign-on implementation in the WebSphere Everyplace Server

Everyplace Wireless Gateway authentication

Three types of links can be used to access Everyplace Wireless Gateway (PPP, WAP or Everyplace Wireless Client). Users of any of these links are authenticated using appropriate protocols. After authentication, each connection is encrypted using proper encryption provided by these protocols. Devices with Everyplace Wireless Client application software installed can access WebSphere Everyplace Server through Everyplace Wireless Gateway. The client and server authentications are simultaneously completed using Two-Party Key Exchange Protocol included in the Wireless Optimized Link Protocol (WLP).

IBM developed WLP which is particularly useful in a wireless environment where transmissions can potentially be readily intercepted and spoofing is a particular concern. Part of the authenticated logon process includes encrypted distribution of encryption keys, which are dynamically generated and used only for that user's connection session with the gateway. This logon and two-party authentication process, complete with key distribution, can be efficiently achieved through the exchange of four radio network packets. The authentication is an option, and can be enforced on a per-user basis.

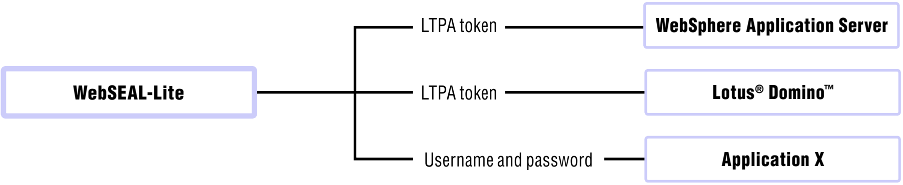

Figure 3. Single sign-on to back-end application servers

WAP clients can access the wireless gateway using WAP. Client authentication is done using the handshake protocol of WTLS. During the handshake process, in addition to negotiating security algorithms and exchanging cipher secrets, the user also enters a user ID and password. Clients are able to use WTLS client certificates to authenticate. In addition, client authentication can also be done using HTTP basic authentication.

Everyplace Wireless Gateway supports cookies on behalf of its WAP clients. It can open SSL connections to destined Web and application servers on behalf of WAP clients if WAP clients request a Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) connection. WAP client connections authenticated by the Everyplace Wireless Gateway component are assigned with the trusted Everyplace Wireless Gateway Internet Protocol (IP) address. When the user is authenticated, the Everyplace Wireless Gateway inserts the trusted IP address into the user's HTTP request header and passes it on to WebSEAL-Lite.

When WebSEAL-Lite receives the HTTP request from Everyplace Wireless Gateway, it inspects the request header and acknowledges the trusted source IP address. WebSEAL-Lite skips the authentication process because the user request is considered to be trusted. It looks up the session information supplied by Everyplace Wireless Gateway (either in the active session table or in the HTTP headers) and creates a session ID. WebSEAL-Lite inserts device and network information in the header. It then passes the HTTP request to the target Web server or application server. WebSEAL-Lite trusts any request because the user who submitted the request has already been authenticated by the Everyplace Wireless Gateway, based on knowledge of which source IP addresses the gateway allocates to its client connections. This method is good for identifying such requests, but as a trusting mechanism it's less secure, because IP addresses can be spoofed. To achieve a more secure trusting mechanism, you should use a high-security communication, such as IP Security, between the Everyplace Wireless Gateway and WebSEAL-Lite nodes.

Everyplace Wireless Gateway also supports two methods to acquire authentication information (user identity) from an external network access server (NAS):

> *Account Lookup.* If the WAP gateway is configured to use account lookup, it sends account resolution requests to an external account lookup program when it requires account verification. The protocol is an HTTP1.1GET request, which allows the requester to specify a single address as a parameter to a servlet or common gateway interface (CGI) script (the lookup program). The lookup program is expected to return a formatted response in plain text containing the account name associated with the lookup address.

Device resolver. If the WAP gateway is configured to use device resolver capability, the gateway also functions as a RADIUS server to which RADIUS records are sent from the NAS that contains a mapping from the source IP address and device identifier (MIN/MSISDN). Everyplace Wireless Gateway can use this mapping when it receives requests from the NAS to know the device ID of the WAP device so that it can insert the ID into the HTTP header. WebSEAL-Lite then maps the device ID to a user identity by lookup in LDAP.

WebSEAL-Lite authentication

WebSEAL-Lite offers three methods for authentication:

- *Username and password. The validation of a user's identity by comparison of a supplied password with a previously stored value.*
- *X.509 client-side certificates. WebSEAL-Lite can access the user's X.509 certificate data and can map from that information to the user's LDAP entry to acquire the user's identity. This mapping is achieved by direct lookup of the LDAP entry using the certificate distinguished name (DN) as a key, or by simply parsing the certificate DN (under control of a configurable template) to extract the WebSphere Everyplace Server username@realm.*
- *No method. No authentication is required to access the designated Web space.*

In addition, within username and password authentication, these credentials can be collected in two ways:

- *HTTP basic authentication. This option is identical to the WebSphere Everyplace Suite, Version 1.1 method.*
- *Custom forms-based login. With a custom form, WebSEAL-Lite is configured to utilize a URL form that contains POST-able fields for the username and password.*

Two different options can be used to achieve the authentication step:

- *Direct comparison with the stored password in the user's LDAP entry. This option applies only when SecureWay Policy Director is not integrated with WebSEAL-Lite.*
- *Calling SecureWay Policy Director authentication (AZN) application program interface (API). SecureWay Policy Director authentication is used when SecureWay Policy Director is also used for authorization. See the section about Authorization for more details.*

Making use of SecureWay Policy Director, the choice of authentication method is generally dependent on the target URL. The choice of credential acquisition method for username and password authentication is also configurable and dependent on the target URL for the request.

Third-party gateways

In addition to direct authentication of user's sessions, WebSEAL-Lite offers the ability to trust requests that are routed through a third-party WAP gateway similar to the way it trusts requests from Everyplace Wireless Gateway. This capability is enabled through a plug-in exit that is specific to the gateway implementation. This mechanism also enables WebSEAL-Lite to identify the user making the request. Several plug-ins are already available and tested for WAP gateways, such as Nokia, Ericsson and Motorola. These are available on the IBM Pervasive Computing Web site at **ibm.com**/pvc.

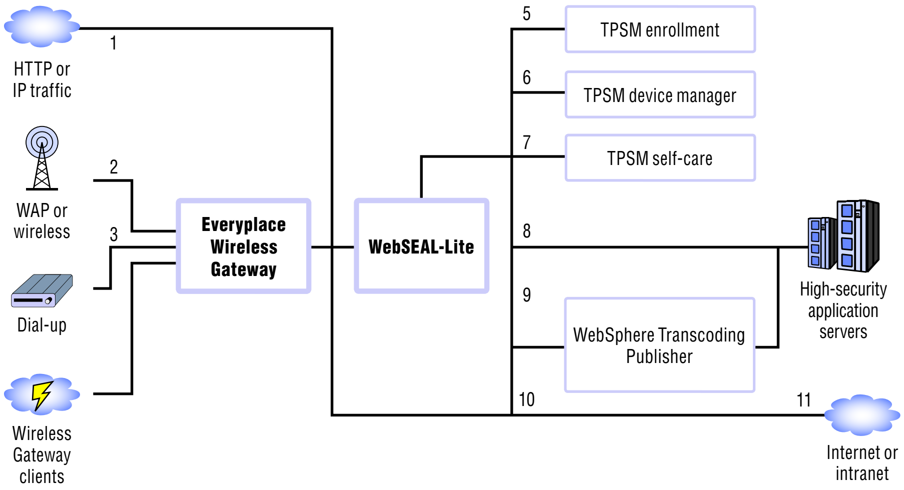

Figure 4. Confidentiality in the WebSphere Everyplace Server environment

Encrypted connections

Confidentiality is achieved by providing encrypted connections between clients and WebSEAL-Lite, and between WebSphere Everyplace Server components. As displayed in Figure 4, the most common deployment of WebSphere Everyplace Server has highlighted segments of connections (labels 1 to 11 in the diagram). Each segment can be configured to implement confidentiality by enabling appropriate technology.

1. *Connection from Internet to WebSEAL-Lite.* For the HTTP clients from the Internet, SSL can be enabled between browsers and WebSEAL-Lite running with WebSphere Edge Server Caching Proxy.

2. Connection between WAP clients and Everyplace Wireless Gateway. The Everyplace Wireless Gateway component provides WTLS support for WAP devices. WTLS is an optimized protocol for the wireless environment and provides the same support for this environment as TLS (a newer version of SSL) provides for the wired world. This creates a security-rich environment for wireless Internet transactions. The WTLS connection is between the WAP device and the wireless gateway. Everyplace Wireless Gateway also provides the capability to enable SSL between the Everyplace Wireless Gateway and the back-end servers. Everyplace Wireless Gateway provides support for Diffie-Hellman or RSA key exchange (RSA 1024, 768 or 512 bits), encryption using RSA RC5 (40, 56 or 128 bits) algorithms and SHA 1 (Secure Hash Algorithm) Message Authentication Codes (40 to 80 bits).

3. Connection between dial-up clients and Everyplace Wireless Gateway. Everyplace Wireless Gateway can use an SSL connection and create an encrypted tunnel for clients.

4. Connection between Everyplace Wireless Client machines and Everyplace Wireless Gateway. Everyplace Wireless Gateway provides end-to-end SSL (HTTPS) for Everyplace Wireless Client machines, and for dial-up and LAN-connected clients. The feature is optional and, when enabled, the HTTPS traffic is encapsulated in the WLP protocol with Everyplace Wireless Client. Everyplace Wireless Gateway provides end-to-end SSL for these clients. The connection will not be broken in the wireless gateway in this case. After the client and server authenticate each other, an encrypted tunnel is established between the gateway and the client, using data encryption standard, RSA RC 5 or RSA triple DES. These are strong symmetric key encryption algorithms, using the keys created as part of the authentication process, double encrypting the traffic between the Everyplace Wireless Client component and the Everyplace Wireless Gateway component.

5. Connection between WebSEAL-Lite and the TPSM enrollment server. The TPSM enrollment server runs on IBM HTTP server which can be SSL-enabled. Although it's within the private network, this connection should be SSL-enabled because the subscriber enrollment involves transmitting sensitive private information.

6. Connection between WebSEAL-Lite and TPSM device manager. This connection is within the Everyplace Server domain and hence is considered trusted.

7. Connection between WebSEAL-Lite and TPSM self-care server. The self-care component involves transmitting sensitive personal information. However, this connection is considered to be trusted because it is within the WebSphere Everyplace Server domain.

8. Connection between WebSEAL-Lite and secure application servers within the Intranet. Though it is considered to be trusted, users have the option to enable SSL connection between WebSEAL-Lite and application servers.

9. Connection between WebSEAL-Lite and WebSphere Transcoding Publisher. If a client request requires proper transcoding, the connection between WebSEAL-Lite and WebSphere Transcoding Publisher cannot be encrypted.

10. Connection between WebSEAL-Lite and the Internet or intranets. Generally, this connection is considered prone to security compromise. If possible, SSL should be enabled.

11. Connection between Everyplace Wireless Gateway and the Internet and intranets. Everyplace Wireless Gateway provides the capability to enable SSL between itself and the Internet or intranet Web servers. Because the WTLS session is terminated in WebSphere Everyplace Wireless Gateway, you need to enable wireless back-end SSL for these client devices.

Authorization and access control

WebSphere Everyplace Server supports fine-grained access control to hosted services through integration with Tivoli SecureWay Policy Director. SecureWay Policy Director is included in the WebSphere Everyplace Server bundle. Fine-grained access control is defined as providing the ability to authorize individual WebSphere Everyplace Server users to gain a certain level of access (read, write, or execute) to a resource defined typically by a URL. This control is achieved through utilization of SecureWay Policy Director centralized management mechanisms, including access control lists (ACLs), user grouping capability and object name space definition tools.

Access rights are checked by WebSEAL-Lite for every HTTP request that passes through it. If a user attempts to access a URL using a level of access for which that user is not permitted (either directly or through group membership), WebSEAL-Lite denies access and returns a *forbidden* HTTP error code. This checking is achieved by calling the SecureWay Policy Director AZN APIs. However, SecureWay Policy Director is an optional component of WebSphere Everyplace Server. If it is not deployed, no authorization checks are performed for user access to URLs. Therefore, in this configuration, if a user is authenticated by WebSEAL-Lite, the user can access any resource supported by WebSEAL-Lite. Tivoli Internet Services Manager (TISM) integrates with SecureWay Policy Director by providing a bridge that creates or modifies policy information (group membership information) whenever a user is enrolled, is deleted or changes TISM Deal subscription information.

Location privacy

WebSphere Everyplace Server supports the ability to attach a user's location information (longitude and latitude, or geocentric location) to a given request. Location is often viewed as sensitive information, so WebSphere Everyplace Server provides mechanisms for users to control which applications are allowed to receive the information. This control is achieved by providing a Web graphical user interface (GUI) through which the user can enable individual applications by name to receive location information. These settings are stored in SecureWay Policy Director and checked by the WebSphere Everyplace Server location proxy component for every request that it identifies that is also destined for a location-enabled application. This enablement is provided as an opt-in for all users who actively choose to be included.

Administration security

Everyplace Wireless Gateway. Administrators for the Everyplace Wireless Gateway component can log in remotely using the Wireless Gatekeeper. The connection between the wireless gatekeeper and Everyplace Wireless Gateway can be SSL-enabled to help provide higher security. In addition, Everyplace Wireless Gateway can specify only one IP address from which a wireless gatekeeper can log in the Wireless Gateway. In this way, by locking the administrator to a trusted IP, Wireless Gateway can help minimize a security compromise.

WebSphere Edge Server. For security reasons, SSL can also be enabled for the connection between the IBM WebSphere Edge Server administration console and WebSphere Edge Server. Users should be aware that most WebSphere Everyplace Server components have access to the LDAP directory, where much sensitive information is stored for sharing by WebSphere Everyplace Server services.

MQSeries Everyplace security

IBM MQSeries Everyplace provides communication between the client and server with privacy, data integrity, data compression and authentication services for applications running on devices which have limited performance and memory. Generally, messages are passed over unsecured external networks and data is held on insecure handheld devices. MQSeries Everyplace helps provide message security and trusted message delivery in addition to the security levels adopted by all the communication channels the message goes through.

MQSeries Everyplace (MQe) can help you create a secure environment for:

- *Equipment that is limited in processing power and memory*
- *Low-bandwidth networks*

MQe offers two security levels. Standard edition includes 56-bit DES encryption while the MQe high-security version supports 128-bit encryption. The following discussion assumes the use of the MQe high-security version.

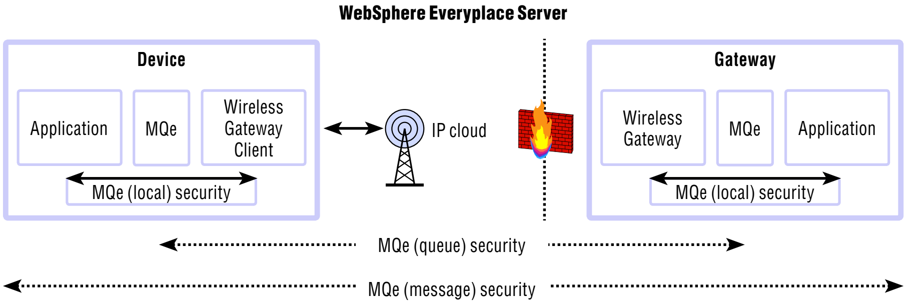

Figure 5. MQe security categories

MQe security categories

To protect a message, it must be encrypted while it is waiting in a queue or transferred over a network. In addition to security levels, with MQe, three categories of security can be invoked: local security, queue security and message security. Figure 5 shows these categories.

- *Local security can preserve the confidentiality of the information stored locally or at a back end, such as an IBM DB2® or an LDAP repository.*
- *Queue-based security is appropriate for solutions designed to use synchronous queues. Queue-based security protects the message data being transferred between an initiating queue manager and a target queue manager. Using this category of security*

automatically protects message data the moment the queue manager is initiated until it reaches the target queue.This protection is independent of whether the target queue is owned by a local or a remote queue manager.

- *As an example a target queue may have attributes to enable authentication, Triple-DES Cryptor (for encryption) and compression. When this target queue is accessed to put, get or browse a message (using putMessage, getMessage or browseMessage either locally or remotely), the queue attribute is automatically applied.*
- *In this example, the application initiating the access must satisfy access authentication before the operation is permitted. If access is permitted, the message data is automatically encrypted or decrypted using Triple-DES, and compressed ordecompressed using the compression method selected.*
- *This means, when a secured target queue is remotely accessed (putMessage or getMessage), the message data is protected as defined by the queue attribute, both during transfer between the initating and remote queue manager and in the target queue backing storage.*
- *Message-level security provides protection for message data between an initiating and a receiving MQe application.*

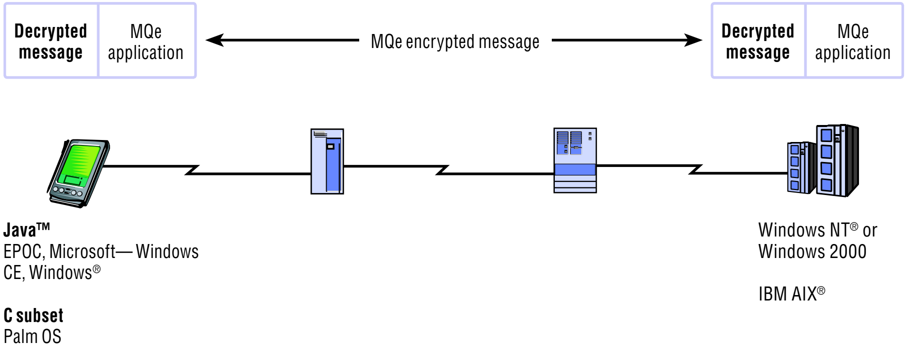

Figure 6. MQe message security offering end-to-end security features. To achieve message protection, MQe uses standard symmetric and public key cryptography.

Firewall considerations

To complete the security picture, firewalls can be used with WebSphere Everyplace Server. General objectives for firewalls are to:

- *Allow only traffic flow that is determined to be wise and in your interest.*
- *Give away a minimum of information about your private network.*
- *Track firewall activity and ask to be notified of suspicious behavior.*

Figure 7 shows a generic deployment model of WebSphere Everyplace Server which suits the needs of many content providers, network operators, service providers and enterprises. The WebSphere Everyplace Server domain can be protected by two or three firewalls. For clarity, the firewalls are labeled a, b, c and d in the diagram. Firewall a controls all access to WebSphere Everyplace Server from third-party gateways or the Internet. Firewall b is placed between the Everyplace Wireless Gateway and devices connecting from IP networks. Firewall c is optional and can be the same as Firewall a. Additionally, WebSEAL-Lite d can use the underlying WebSphere Edge Server caching proxy server component with multiple network adapters to help achieve certain firewall function as well.

Firewall configuration guidelines follow. Firewall a is configured to:

1. *Allow HTTP requests destined for WebSphere Everyplace Server services from IP addresses that are not owned by Everyplace Wireless Gateway, and route such requests to WebSEAL-Lite.*
2. *Allow HTTP requests destined for the public Web servers and/or the enrollment server from IP addresses that are not owned by Everyplace Wireless Gateway and route such requests to the Internet.*
3. *Reject all other packets.*

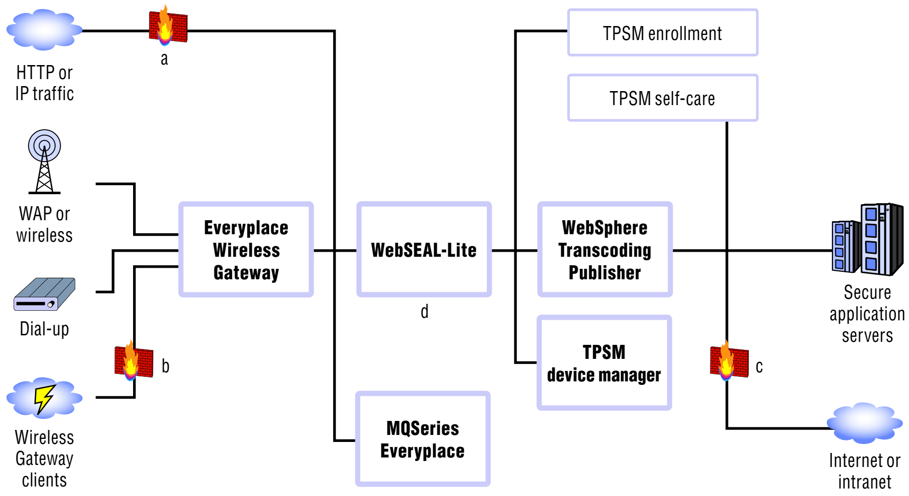

Figure 7. Firewall figure protection for the IBM WebSphere Everyplace Server domain

Firewall b is configured to:

1. *Allow IP requests destined for the predefined Wireless Gateway IP ports from any IP address.*
2. *Allow HTTP requests for Everyplace Server services.*
3. *Reject all other packets.*

Firewall c is configured to:

1. *Allow outbound HTTP requests destined for the public Web servers.*
2. *Allow inbound HTTP response for the active user session from the public Web servers.*
3. *Reject all other packets.*

Firewall d is configured to:

1. *Allow HTTP requests destined for WebSphere Edge Server services.*
2. *Use a separate network interface for the internal network.*
3. *Reject all other packets.*

Summary

Trust is important. You need built-in security-rich function. With WebSphere Everyplace Server, you get a comprehensive set of security features. WebSphere Everyplace Server allows identification and authentication of users and allows authorization of what users see or do. You can be confident that data integrity is maintained, and strong encryption used to help keep information sent secret. SSL and WTLS certificates can be implemented to add additional nonrepudiation when you need it. And you can rest assured, with use of security standards, you can maintain interoperability between multiple vendors and multiple platforms. WebSphere Everyplace Server provides an open, standards-based solution that can help you effectively reduce security risks associated with remote access to your information assets.

For more information

For more information about WebSphere Everyplace Server, Service Provider Offering, Version 2.1, contact your IBM marketing representative or visit:
ibm.com/websphere/portal

IBM Corporation
Pervasive Computing Division
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
03-02

IBM reserves the right to alter specifications and other product information without prior notice. This publication could include technical inaccuracies and typographical errors. Reference herein to IBM products and services do not imply that IBM intends to make them available in all countries. IBM provides this publication “as is” without warranty of any kind, either express or implied, including the implied warranties of merchantability or fitness for a particular purpose. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this disclaimer may not apply to you.

business software