

IBM WebSphere Everyplace Suite v1.1

Security White Paper

2 January 2001



Tom Covalla

WebSphere Everyplace Suite Security

Increasingly, we rely on the electronic creation, transmission, and storage of personal, financial, and other confidential information. In order to give people convenient access to such information and allow them to easily take action virtually anywhere anytime, IBM WebSphere Everyplace Suite (Everyplace Suite) is designed to enable increasing numbers of mobile personal and professional transactions using a new class of intelligent and portable devices. Pervasive e-business, the accessing and transferring sensitive information, usually involves transmission over the Internet and other public networks. Therefore, creating a safe computing environment that provides high security for confidential transactions is imperative.

This paper will address the security implementation within Everyplace Suite. First, the general security objectives for data communication will be explained. Second, the security design of Everyplace Suite will be presented. Third, the three types of security implementations within Everyplace Suite, namely TCP/IP security, wireless security, and MQSeries Everyplace security will be described. Finally, firewall use with Everyplace Suite will be explained.

The major functions of IBM WebSphere Everyplace Suite are listed following. Note that Websphere Everyplace Suite supports a selectable install and many of the components may be used independent of others that may or may not be installed.

Connectivity:

- ✓ *Everyplace Gateway*: Provides security-rich wired and wireless connectivity between the IT network and the Communications Network (e.g. GSM, CDMA/TDMA, ISDN, GPRS), protocol translation (e.g. TCP/IP - WAP), and support for short messaging (SMS).

Content Adaptation:

- ✓ *WebSphere Transcoding Publisher*: Allows transformation of arbitrary content into a form that can be presented on a device that is different from the originally intended target, such as changing HTML content intended for desktop PCs to WML content suitable for the new class of smart phones.
- ✓ *MQSeries Everyplace*: Enables pervasive devices to queue messages and transactions, and helps assure their completion (once and only once), efficiently and with security in both connected and disconnected end user scenarios.
- ✓ *Everyplace Synchronization Manager*: Enables pervasive devices to operate applications "off-line", and synchronize the results of their activities with a server database when connectivity is re-established.

Management Services:

- ✓ *Tivoli Personalized Services Manager*: TPSM provides 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:

- ✓ *Everyplace Authentication Server*: Provides the user and device authentication capabilities which enable a single, device-independent user log-on, and pass-through of authentication information to web application servers.

WebSphere Everyplace Suite Security

- ✓ *Everyplace Client Encryption*: Provides use of Two-Party Key Distribution Protocol (2PKDP). This is a security protocol that combines bi-directional authentication with key distribution using a minimal number of messages. 2PKDP provides encryption/decryption support for all signals coming into and going out of WebSphere Everyplace Suite, with a choice of either DES or RC5 encryption algorithms
- ✓ *WAP Client*: Utilizes WTLS for communication between a WAP-enabled device and the Everyplace Wireless Gateway.
- ✓ *Firewall support*: Support for integrating IBM SecureWay Firewall by Tivoli and popular 3rd party firewalls to protect against unauthorized access and viruses.

Performance Optimization:

- ✓ *WebSphere Edge Server*: Provides highly scalable caching functions on a server to 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 Suite processors which are deployed in a configuration.

Base (Common) Services:

- ✓ *SecureWay Directory*: A central DAP directory which contains runtime information about active sessions, users, devices, and networks. This database makes it easy for the various components of WebSphere Everyplace Suite (and any server that is added to the configuration) to access the runtime information centrally, without having to replicate the data in other repositories.
- ✓ *Everyplace Suite Console*: Provides a single console for system administrators to perform installation and diagnostic procedures, administrative procedures, and system maintenance procedures.

Background

Security for data communication has been well documented ever since the Internet became popular. Everyplace Suite provides a foundation for expansion into pervasive e-business that is both solid and secure. Following is an explanation of five common security requirements for pervasive e-business.

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's server, you want to make sure that it is who it claims to be. This is called "server authentication". "Client authentication" is the means to establish your identity. The combined authentication of server to client and client to server is called bi-directional authentication.

Confidentiality: As a synonym of secrecy, confidentiality means to protect the data communication from eavesdropping.

WebSphere Everyplace Suite Security

Integrity: Integrity means to verify the data has not been altered in transit by a third party. This is to prevent forgery, tampering, and unauthorized alteration.

Authorization: Authorization limits the improper user of the data and services. Authorization limits what information the user is allowed to see or what actions one may take to minimize the chance of exposure of sensitive information to malicious attack or unauthorized alteration.

Non-repudiation: Methods to aid in the prevention of parties in the data transaction from denying their actions after the transactions are done. This is to enforce the accountability for the electronic transactions.

These are the five characteristics normally required by on-line content and application services which involve data communication. Another important requirement for computing security is creation of a boundary for the service domain. This reduces the chance of being attacked by hackers from public networks. Firewalls are most commonly used to prevent such attacks such as denial of service, packet spoofing, and impersonation.

Everyplace Suite Security

IBM WebSphere Everyplace Suite is designed to help create a safe environment to support pervasive e-business. It provides for centralized user authentication from limited points of entry. Everyplace Suite exploits the single sign-on for user friendly implementation of credential sharing across the services hosted by the suite. Everyplace Suite relies on a set of industry standards for security such as TLS/SSL and WTLS to achieve the security objectives for the service domain. Everyplace Suite uses the proxy technology in conjunction with firewalls to define the boundary for the service domain.

Authentication

The user authentication function within Everyplace Suite is performed by the Everyplace Gateway and the Everyplace Authentication Server. On the other hand, the administrator authentication within Everyplace Suite is component dependent.

Everyplace Suite employs several industry standard technologies to perform authentication. The Everyplace Authentication Server uses the HTTP basic authentication process to authenticate the users coming from the Internet and third-party gateways. For this reason, the clients and/or the gateway proxy for the clients must support HTTP.

The Everyplace Gateway authenticates users from three different types of connections. Each type of user connection uses different a authentication process. These will be examined later in this paper.

Confidentiality

Everyplace Suite utilizes a set of industry standard security technologies to implement the goal of confidentiality. Such technologies include the Secure Socket Layer (SSL) and Wireless Transport Layer Security (WTLS). In addition, the Everyplace Gateway uses a modified version of Point-to-Point Protocol (PPP) called Wireless Optimized Link Protocol to create encrypted tunnels to aid in confidentiality for the clients with Wireless Client software applications installed.

Authorization

WebSphere Everyplace Suite Security

The access control in Everyplace Suite is implemented using HTTP proxy technology. To implement finer levels of access control, it may be done at individual Everyplace Suite components and application servers. This can be done by integrating the Tivoli SecureWay Policy Director with the Everyplace Suite services.

Data integrity

Everyplace Suite provides for data integrity using features such as message digest and certificates included in the security technologies SSL and WTLS.

Non-repudiation

Since Everyplace Suite utilizes SSL and WTLS with certificates the objectives of non-repudiation can be also implemented at the transaction level. Everyplace Suite has implemented a set of industry standard security technologies such as TLS/SSL and WTLS to achieve various security objectives.

Security Implementation

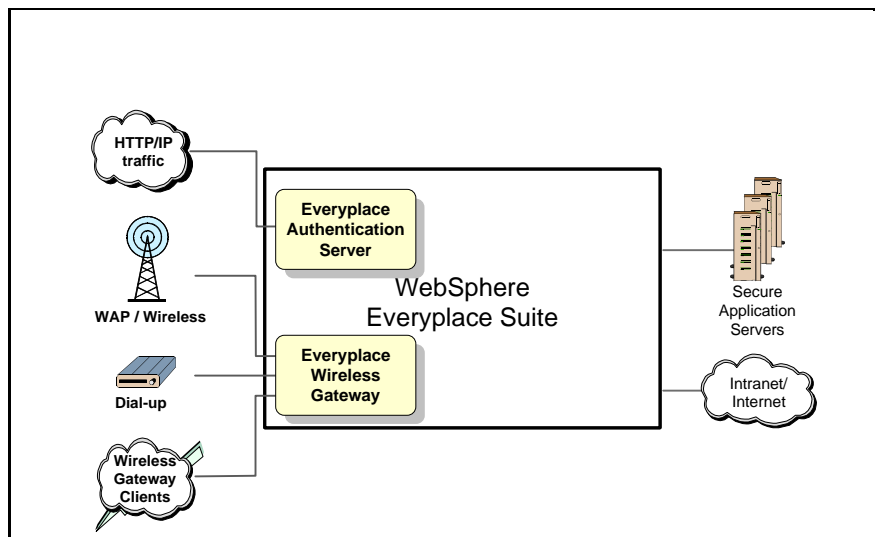
Single Sign-on

Everyplace Suite allows users to connect to it through either the Everyplace Gateway or the Everyplace Authentication Server (as shown in Figure 1).

Users from Internet or third-party gateways are only allowed to connect to the Everyplace Gateway through Everyplace Authentication Server. Users may also access Everyplace Suite using three types of links through Everyplace Wireless Gateway:

- Dial-up connection based on Point to Point Protocol (PPP)
- Wireless Client created connection over Wireless or IP networks
- Wireless connection based on Wireless Application Protocol (WAP)

The user authentication will be conducted at both points of entries by Everyplace Gateway and Everyplace Authentication Server.



WebSphere Everyplace Suite Security

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

Everyplace Suite is designed to achieve single sign-on, namely to authenticate the users only once for their access to the services hosted by the Edge Server. This authentication design is achieved by sharing user credentials through a centralized repository. This centralized repository consists of a TPSM user or subscriber database, an Active Session Table (AST) database, and a SecureWay Directory database (DAP). As shown in Figure 2, both the Everyplace Gateway and the Everyplace Authentication Server use centralized RADIUS to authenticate users. They both deposit user active session entries into the AST database to share the user credential and profiles with the Edge Server services. Information sharing among the Edge Server services is achieved by their access to the AST and DAP.

In addition to credential sharing across Everyplace Suite components, the single sign-on relies on coordination between the two authentication agents, namely the Everyplace Gateway and the Everyplace Authentication Server.

To enable single sign-on access to Everyplace Suite services, the Everyplace Authentication Server is used as the central point for authentication. The Everyplace Authentication Server is designed to be as the first entry point for all HTTP traffic from the Internet and third-party gateways. The Everyplace Gateway also routes all HTTP requests to the Everyplace Authentication Server which is the next non-firewall hop after the Everyplace Gateway. Users already authenticated by the Everyplace Gateway will not be re-authenticated by the Everyplace Authentication Server.

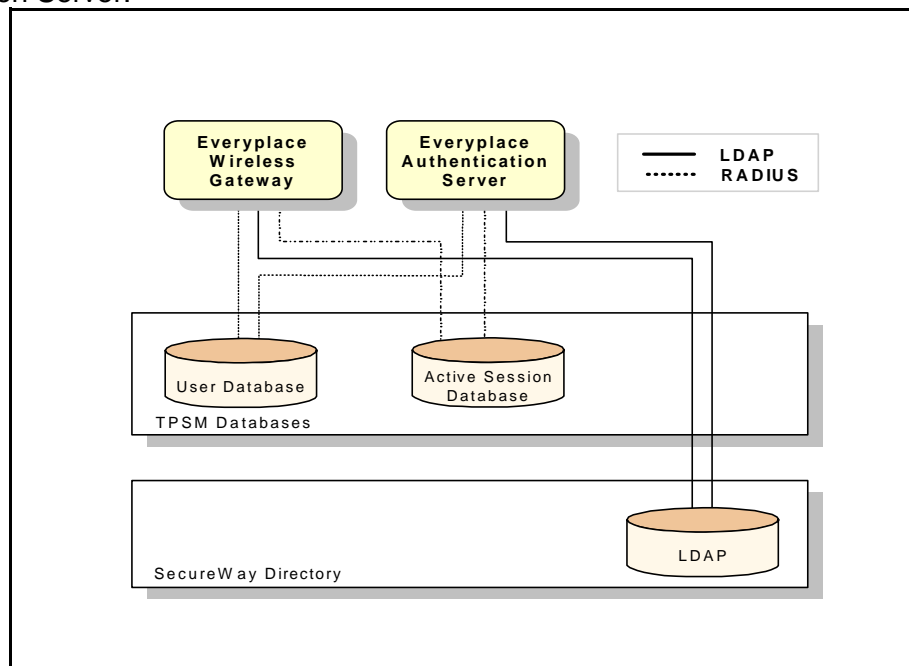


Figure 2. Single sign-on implementation in the WebSphere Everyplace Suite.

Authentication

As mentioned earlier, three types of links can be used to access the Everyplace Gateway. Users of either link are authenticated using appropriate protocols. After authentication, each connection is encrypted using proper encryption provided by those protocols.

WebSphere Everyplace Suite Security

Devices with wireless client application software installed can access Everyplace Suite via the Everyplace Gateway. The client and server authentications are simultaneously completed using two party key exchange protocol included in the Wireless Optimized Link Protocol (WLP).

WLP was developed by IBM research and is particularly useful in a wireless environment where transmissions can potentially be readily intercepted and "spoofing" (e.g. a fake pretends it is the server or the client) 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 via the exchange of four radio network packets. The authentication is an option, and can be enforced on a per user basis. The client authentication is performed using the handshake protocol of Wireless Transport Layer Security (WTLS). During the handshake process, in addition to negotiating security algorithm and exchanging cipher secrets, the user also enters a user ID and password. The server authentication can be done using X.509 certificates supported by WTLS. The client authentication can also be done using the Diffie-Hellman key exchange protocol.

WAP clients can access the wireless gateway using the Wireless Application Protocol (WAP). Client authentication is done using the handshake protocol of Wireless Transport Layer Security (WTLS). During the handshake process, in addition to negotiating security algorithms and exchanging cipher secrets, the user also enters a user ID and password. Authentication can be done using mini-certificates supported by WTLS. In addition, client authentication can also be done using HTTP basic authentication. Currently WAP client authentication is not implemented using WTLS certificates.

Everyplace Gateway supports cookies on behalf its WAP clients. It can open SSL connection to destined Web and application servers on behalf of WAP clients if WAP clients request a HTTP-S connection.

WAP client connections authenticated by the Everyplace Gateway are assigned with the trusted Everyplace Gateway IP address. Once the user is authenticated, the Everyplace Gateway inserts the trusted IP address into the user's HTTP request header and passes it on to the Everyplace Authentication Server.

When the Everyplace Authentication Server receives the HTTP request from the Everyplace Gateway, it inspects the request header and acknowledges the trusted IP address. The Everyplace Authentication Server skips the authentication process since the user request is considered to be trusted. It looks up the session information in an active session table entered by the wireless gateway and creates a session ID and inserts device and network information in the header and passes the HTTP request on to the target Web and application server.

Secured Connections

Confidentiality is achieved by providing encrypted connections between clients and the Everyplace Authentication Server, as well as between Everyplace Suite components. As displayed in Figure 3, the most common deployment of Everyplace Suite has highlighted segments of connections (label 1 to 11 in the figure). Each segment can be configured to implement confidentiality by enabling appropriate technology.

WebSphere Everyplace Suite Security

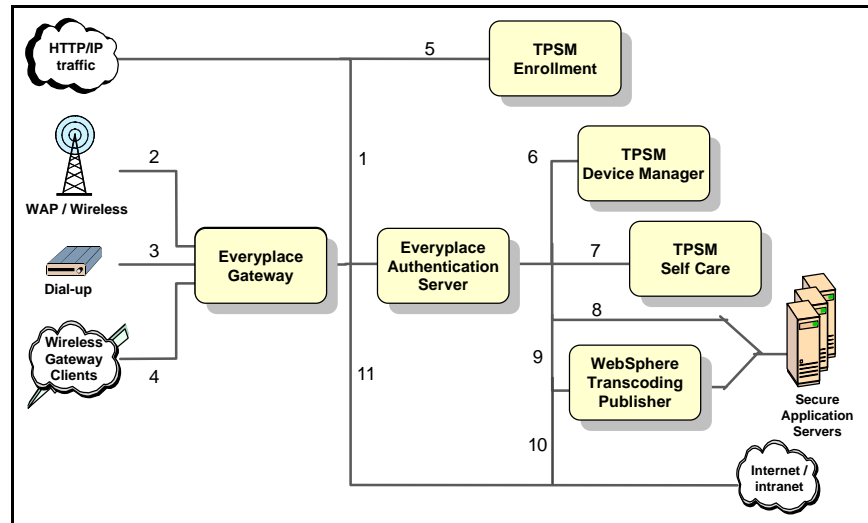


Figure 3. Confidentiality in the Everyplace Suite environment.

1. Connection from Internet to Everyplace Authentication Server: for the HTTP clients from the Internet, SSL can be enabled between browsers and the Everyplace Authentication Server running with Web Traffic Express server.

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

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

4. Connection between wireless clients and Everyplace Gateway: the Everyplace Gateway provides end-to-end SSL (HTTP-S) for the wireless clients as well as for dial up and LAN connected clients. The feature is optional and when enabled, the HTTP-S traffic is encapsulated in the WLP protocol with the wireless client. The Everyplace 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, DES, RSA's RC 5 or triple DES which are strong "symmetric key" encryption algorithms using the keys created as part of the authentication process, double encrypting the traffic between the wireless client and the Everyplace Wireless Gateway.

5. Connection between HTTP clients and the TPSM enrollment server. The TPSM enrollment server runs above IBM HTTP server which can be SSL-enabled. Since the subscriber

WebSphere Everyplace Suite Security

enrollment involves transmitting sensitive private information across the public network, it is recommended that this connection be SSL-enabled.

6. Connection between Everyplace Authentication Server and TPSM device manager: this connection is within the Everyplace Suite domain and hence is considered trusted.

7. Connection between Everyplace Authentication Server and TPSM Self Care Server: the self care again would involve transmitting sensitive personal information. However, this connection is considered to be trusted since it is within the Everyplace Suite domain.

8. Connection between Everyplace Authentication Server and secure application servers within the Intranet: even though it is considered to be trusted, users have the option to enable SSL connection between Everyplace Authentication Server and application servers.

9. Connection between Everyplace Authentication Server and WebSphere Transcoding Publisher: if the client requests requires proper transcoding, the connection between the Everyplace Authentication Server and WebSphere Transcoding Publisher can not be encrypted. Otherwise, WebSphere Transcoding Publisher would not be able to transcode.

10. Connection between Everyplace Authentication Server and Internet/Intranet: this connection generally is considered prone to security compromise. It is recommended that SSL is enabled if possible.

11. Connection between Everyplace Gateway and Internet/Intranet: the Everyplace Gateway provides the capability to enable SSL between the itself and the Internet/Intranet web servers. Since the connection is always broken in the wireless gateway, it is highly recommended to enable wireless backend SSL for these client devices.

Administration Security

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

WebSphere Edge Server administration console. For security reason, SSL can also be enabled for the connection between the WebSphere Edge Server administration console and WebSphere Edge Server.

Please note that most components of Everyplace Suite have access to the DAP directory, where much sensitive information is stored for sharing by Everyplace Suite services.

MQSeries Everyplace Security

The primary goal for IBM MQSeries Everyplace (MQe) security is to provide privacy, data integrity, data compression and authentication services for applications running on devices which are low in performance and memory. Generally, messages are passed over unsecured external networks and data is held on insecure handheld devices. These expectations led to the need to provide a comprehensive asynchronous and synchronous application to application security with trusted message delivery. Message security can be provided regardless of the

WebSphere Everyplace Suite Security

security levels adopted by all the media the message goes through including fixed networks, mobile service providers and gateways.

MQe provides security for:

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

MQe security is an optimized security that provides security for connections between device applications and back-end applications.

There are two different security levels provided by MQe. Standard edition includes 56-bit DES encryption while the MQe high-security version supports 128-bit encryption. The following assumes the use of the MQe high-security version.

MQe security categories

To protect a message, it must be encrypted while it is waiting in queue or transferred over a network. With MQe, three different categories of security can be invoked: local, Q-based, and message levels. These categories are illustrated in Figure 4.

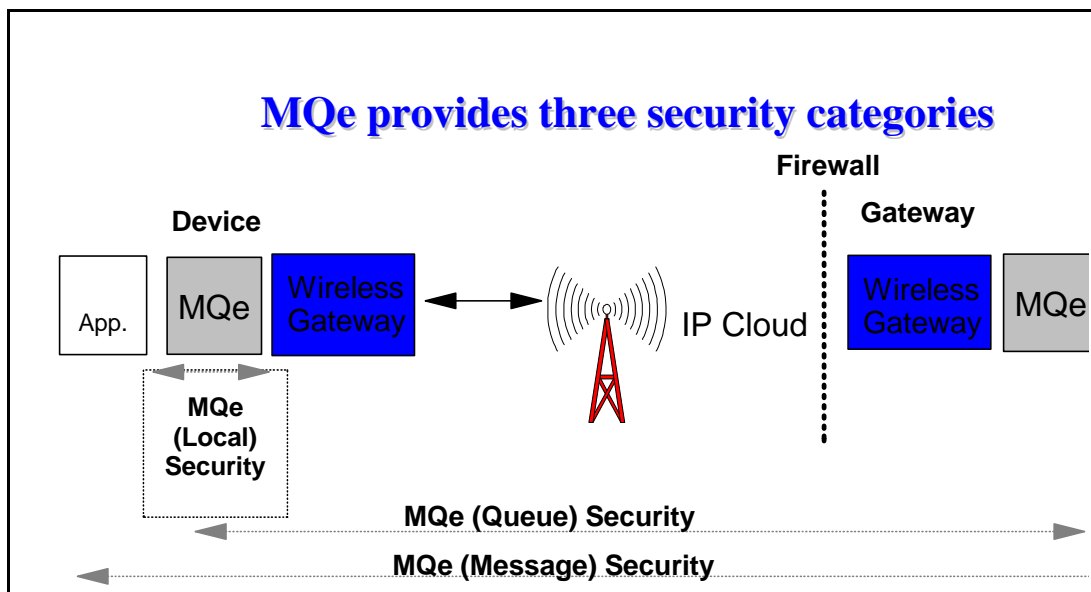


Figure 4 MQe security categories

WebSphere Everyplace Suite Security

1. Local security



<p>Protect message data (or any MQeFields data) e.g. a message on a queue Protect data on a hand held device</p> 	<p>Protect data and save it to a file Using MQeLocalSecure class</p> 
<p>Protection steps: create MQeAttribute (with chosen Authenticator, Cryptor and Compressor) create MQeKey provide key 'seed' to set MQeKey's local Enc/Decryption key attach MQeKey to MQeAttribute activate MQeAttribute attach MQeAttribute to MQeMsgObject use MsgObject.dump() to encode (protect) use MsgObject.restore() to decode (unprotect)</p>	<p>Protection steps : create MQeAttribute (with chosen Authenticator, Cryptor and Compressor) create MQeLocalSecure use MQeLocalSecureobject.open to define target file use MQeLocalSecureobject.write to encode and save to the target file use MQeLocalSecureobject.read to read from the target file and encode</p>

Figure 5. Local security options

To protect local data using a cryptor (secret key). In this category we can:

1. Authenticate, encrypt/decrypt, compress/decompress data and write/read it to/from a file.
2. Authenticate, encrypt/decrypt, compress/decompress data and write/read it to/from any message data (or any MQe Fields data). This can be needed to protect data then save it to a back end such as DB2 or DAP server.

2. Queue-based security

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

WebSphere Everyplace Suite Security

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 method. When this target queue is accessed to put, get or browse a message (using putMessage, getMessage or browseMessages either locally or remotely), the queue attribute is automatically applied.

In this example, the application initiating the access has to satisfy access authentication before the operation is permitted. If access is permitted, the message data is automatically encrypted/decrypted using Triple DES and compressed/decompressed using the compression method selected.

This means, when a secured target queue is remotely accessed (put or get Message) security automatically helps ensure that the message data is protected as defined by the queue attribute, both during transfer between the initiating and remote queue manager and in the target queue backing storage.

3. Message-level security

Message-level security provides protection for message data between an initiating and receiving MQe application.

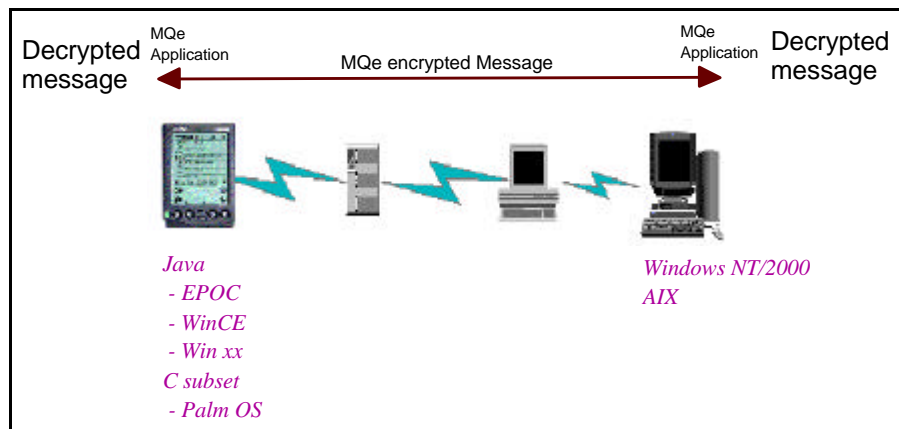


Figure 6. MQe message security offers end-to-end security features

To use these security mechanisms MQ uses secret-keys, public/private keys to be communicated and a certificate to identify the other party entity.

Firewall Considerations

To complete the security picture, firewalls are utilized with Everyplace Suite.

The general objectives for firewalls are to:

- only allow traffic flow that is determined safe and in our interests
- give away a minimum of information about our private network

WebSphere Everyplace Suite Security

- keep track of firewall activity and be notified of suspicious behavior

The most generic deployment model of Everyplace Suite which suits the needs of many content providers, network operators, service providers, and enterprises is depicted in Figure 7. The Everyplace Suite domain can be protected by two or three firewalls. For clarity, the firewalls are labelled a, b, c, and d in the figure. Firewall a controls all access to Everyplace Suite from third party gateways or the Internet. Firewall b is placed between the Everyplace Gateway and devices connecting from IP networks. Firewall c is optional and can be the same as firewall a. Additionally, the Everyplace Authentication Server (d) can use the underlying Edge Server - Caching Proxy server with multiple network adaptors to achieve certain firewall function as well.

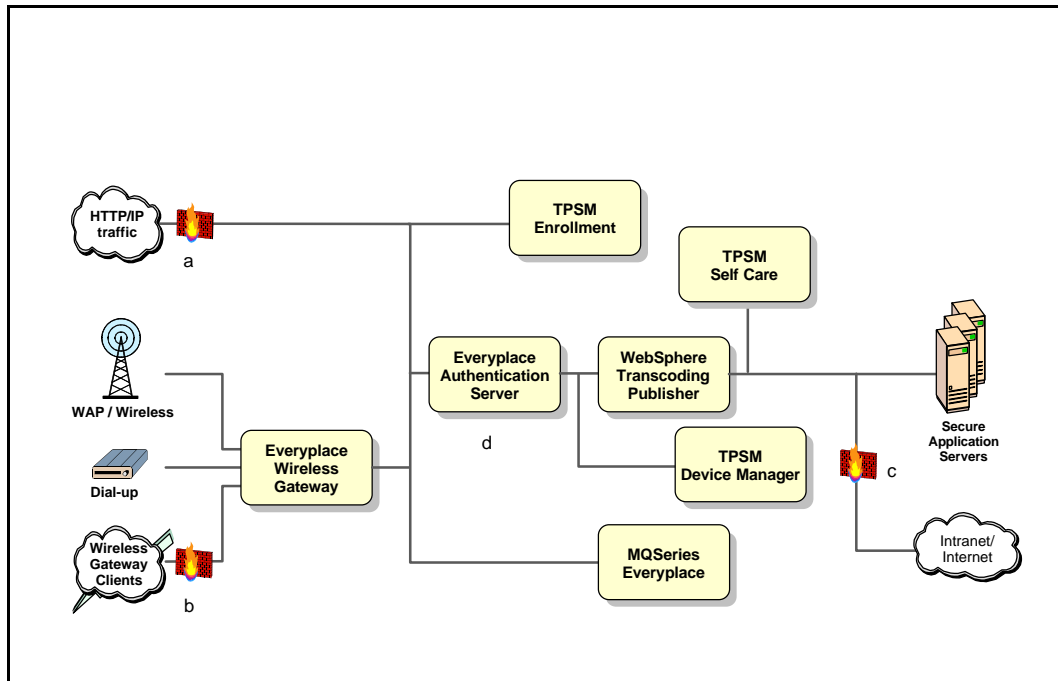


Figure 7. Firewall Figure protection for the IBM WebSphere Everyplace Suite domain.

The firewall configuration guidelines are given as the following:

Firewall **a** is configured to:

1. Allow HTTP requests destined for the Everyplace Suite services from IP addresses that are not owned by everyplace wireless gateway and route such requests to the authentication proxy.
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 Internet and/or enrollment server.
3. Reject all other packets.

Firewall **b** is configured to:

WebSphere Everyplace Suite Security

1. Allow IP requests destined for the pre-defined wireless gateway IP ports but from any IP address.
2. Allow HTTP requests for Everyplace Suite 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 the Edge Server services.
2. Use separate network interface for the internal network.
3. Reject all other packets.

Summary

Security matters because it is about *trust*. When the public Internet is used to convey confidential information, security becomes even more important. And when that information is transmitted from a highly portable device, security becomes critical.

As has been shown above security is built into the WebSphere Everyplace Suite. It provides a comprehensive set of security features. The Suite will allow identification and authentication of users and will allow authorization of what they may do or see. Data integrity is maintained and strong encryption can be used to keep information sent secret. SSL and WTLS certificates may also be implemented to add additional protection for non-repudiation when needed. And to maintain interoperability between multiple vendors and multiple platforms security standards are followed.

Your WebSphere Everyplace Suite provides an open, standards based solution that effectively reduces security risks associated with remote access.

WebSphere Everyplace Suite Security

Trademarks and Disclaimer

Trademarks

Java is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

Windows and Windows NT are trademarks of Microsoft Corporation.

Other company, product or service names may be trademarks or service marks of others.

Disclaimer

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.