



IBM Software Group

IBM WebSphere® Partner Gateway V6.1.1

Multiple certificates support



@business on demand.

© 2008 IBM Corporation
Updated August 14, 2008

This presentation provides details on the new feature Multiple Certificate Support that is available in IBM WebSphere Partner Gateway V6.1.1 release.

Goals

- Overview of security features in WebSphere partner gateway
- Comprehend how certificates were used in WebSphere Partner Gateway V6.0 and earlier versions
- What is new or changed in WebSphere Partner Gateway V6.1.1



In this presentation, you will go through various security features provided by WebSphere Partner Gateway, and understand how certificates are used for various operations like Digital Signature, Encryption, and SSL. Also, you will take a quick look at what is new in this release.

Agenda

- Security overview
- Setting up certificates in WebSphere Partner Gateway 6.1 or its prior versions
- New features in this release
- Summary and references



The session will start with an overview of different security functions supported in prior releases of WebSphere Partner Gateway. Then you will learn about configuring certificates in WebSphere Partner Gateway V6.1 or its prior versions. You will also take a quick look at the new features related to certificates that are added in this release, and then summarize.

Security features

- Message level security
 - ▶ Encryption and decryption
 - Encryption is a mechanism by which a message is transformed so that only the sender and recipient can see
 - ▶ Digital signature and verification
 - Digital signature is a mechanism by which a message is authenticated
 - ▶ Non-repudiation
 - Receipt
 - Content and origin
- Transport level security
 - ▶ SSL (server and client authentication)



WebSphere Partner Gateway provides security at message level and at transport level.

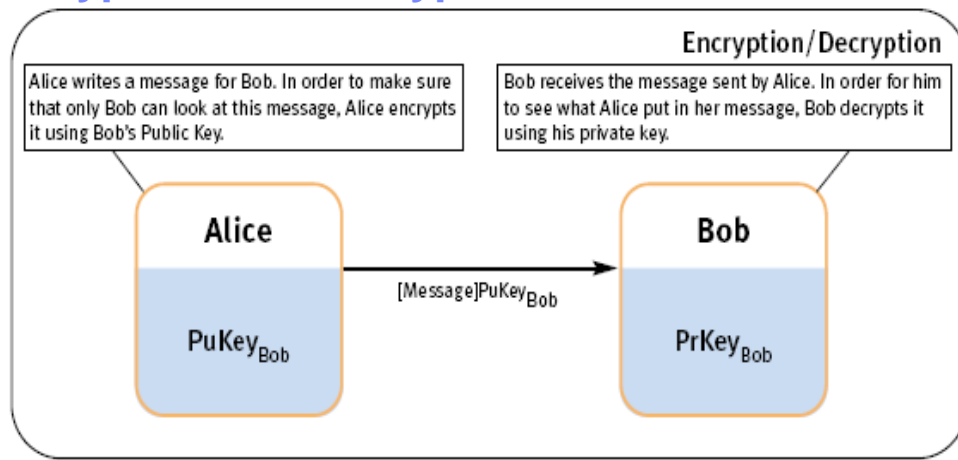
There are different message level securities that are supported; the first one being Encryption. This is a mechanism by which the sender encrypts the message and only the recipient can read it.

The next one is the Digital Signature, which is used to authenticate the sender. It also assures message integrity.

The last one is Non-Repudiation, which is supported by certain business protocols like AS, Rosettanet, and so on. At the receiver end, it provides a means for making sure the sender does not deny the origin of the message. At the sender end, it allows them to make sure the receiver does not deny the receipt of the message.

At transport Level, SSL is supported to make sure that there is a secure transfer of message from sender to receiver.

Encryption and decryption



- Encryption (at Alice)
 - ▶ External Partner >> Certificates >> Public Certificate (PuKey_{Bob})
- Decryption (at Bob)
 - ▶ Hub Operator >> Certificates >> Private Key (PrKey_{Bob})



Shown here is an example which helps you understand what Encryption and Decryption is all about.

Encryption is a mechanism by which the sender encrypts the message that is to be sent to the receiver and only the receiver can decrypt and read the message after its encrypted.

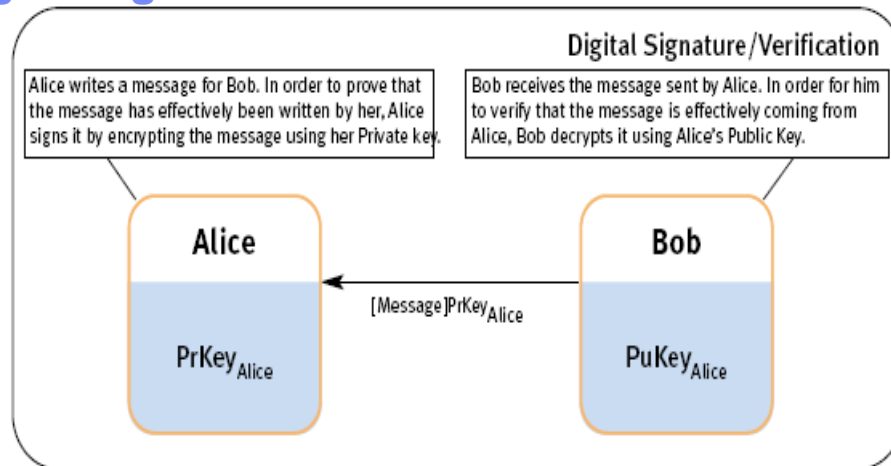
In the example shown above, Alice is the sender and Bob is the receiver.

Alice encrypts the message using the public certificate of Bob and transfers the encrypted message to Bob. Alternatively, Bob uses his private key to decrypt the message and extracts the content.

To setup encryption certificates, Alice has to load Bob's public certificate PuKey_{Bob} as Encryption certificate for partner Bob.

On the other side, Bob has to load his private key PrKey_{Bob} as encryption for the hub-operator.

Digital signature and verification



- Digital Signature (At Alice)
 - ▶ Hub-Operator >> Certificates >> Private Key (PRKey_{Alice}) as Digital Signature certificate.
- Sign Verification (At Bob)
 - ▶ External Partner (Alice) >> Certificates >> Public (PuKey_{Alice}) as Digital Signature certificate



Here is an example which explains about Digital Signature and Verification process.

Digital Signature is a mechanism by which the sender signs the message that is to be sent to the receiver. On receipt of the message, receiving partner tries to verify the signature of the sender to make sure the sender is legitimate.

In the above example, Alice is the sender and Bob is the receiver. Alice signs the message using the private key and transfers the signed message to Bob. Bob in turn uses Alice's public certificate to verify the signature and extracts the content.

To setup Digital Signature certificates at Alice's end, use Alice's private key PRKey_{Alice} as Digital Sign certificate for hub-operator. At Bob's end, load Alice's public certificate PuKey_{Alice} as external partner (Alice) digital signature certificate.

Section

New functions in V6.1.1



The next section covers the new function in WebSphere Partner Gateway V6.1.1

What is new

- All new wizard to simplify loading and configuring certificates
- New features
 - Certificates can be associated to internal partners
 - Multiple certificates can be loaded for same usage, for example digital signature
 - Certificate sets to group primary and secondary certificates
 - Ability to vary certificates based on
 - Partner pair
 - Operation mode
 - Package
 - Global settings for internal partner
 - Where-used capability for certificates and certificate sets
 - Validate function in console to validate certificates



A completely new wizard is provided to load and configure certificates for partners.

Private Keys can now be directly associated to internal partners as opposed to hub-operator in the prior versions of WebSphere Partner Gateway. You can load more than one certificate for the same function like Digital Signature or Encryptions. In addition, Certificate sets are newly introduced to group primary and secondary certificates.

You can now vary certificate on Partner Pair that is, from a specific sender to a specific receiver. Certificates can also vary on Operation modes like test, production, and so on. Similarly, there can be different certificates for packaging like AS, RNIF, and so on. You can also load default certificates that are used for all internal partners. The where-used capability is extended for certificate related artifacts in this release. Also, new Validate function is provided in console to validate the certificate path and expiry.

Multiple certificates

- In prior versions, internal partners can have one set of active certificates
- In V6.1.1, you can load multiple certificates for different internal partners
 - ▶ Certificate usage (sign / encrypt / SSL client)
 - ▶ Operation mode (production / test)
- It allows users to vary certificates based on:
 - ▶ Partner pair
 - ▶ Operation mode
 - ▶ Package



The prior versions of WebSphere Partner Gateway allowed internal partner to have just one set of certificate for usage, like digital signature.

In V6.1.1, you can load more than one certificate to a partner for the same usage. You can also have multiple certificates based on the operation mode.

You can now choose to use one certificate for one participant connection in one operation mode. But, it does not allow a certificate being associated to protocol or document at the packaging level.

Certificate sets

- Introduced in this release to group a primary & secondary certificate
- Users associate sets for sign / encrypt / decrypt as opposed certificates in V6.0 or prior
- Set can be marked default so that it is used for ALL possible combinations of:
 - ▶ Receiving partner
 - ▶ Operation mode
 - ▶ Package
- Sets are applicable for:
 - ▶ Internal partners – digital sign & SSL client
 - ▶ External partners - encryption



Certificate sets is a new feature included in this release. It is used for grouping primary and secondary certificates. Users can now associate certificate sets to participant connections as opposed to associating certificates in the prior releases.

A set can be marked default so that users can default this set for all connections in which the current partner is the initiating partner for all receiver partners. It can also be default set for ALL / Selected operation mode, and for all packaging options.

Alternatively, this can be a default for connections in which the current partner is the receiving partner.

Certificate sets are used by internal partners who hold private key that is used for digital signature or SSL. It is also used by external partner's public certificate, which is used for encryption.

Validate and where-used functions

- **Validate**
 - ▶ Allows users to make sure the certificate is valid by checking:
 - Certificate expiry
 - Certificate path validation
- **Where-used**
 - ▶ Allow users to lookup participant connections where a certificate set is used



WebSphere Partner Gateway V6.1.1 has new Validate and “Where-used” functions.

The new Validate function in console allows users to validate a certificate before it is actually used at runtime. You can now verify if the certificate and dependent certificates are all loaded (cert path validation); check if the certificate and its dependents are active and not expired.

The “where-used” function is for certificate related artifacts. You can now select a certificate and click where-used to figure out which certificate set this belongs to. If you choose where-used on a certificate-set, you can view the list of connections to which this certificate can be applied.

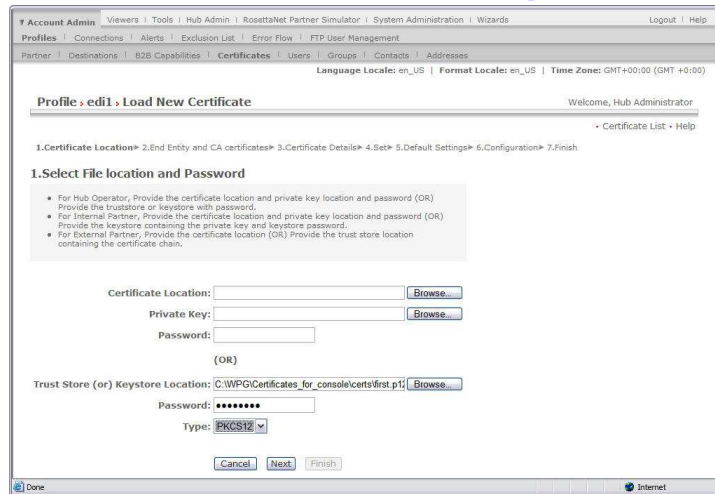
Section

Load certificate wizard



The next section covers the load new certificate wizard.

Load new certificate wizard: Step 1



Certificate location

- You can choose to upload a public certificate (individual / multiple from trust-store) / private key (individual / from key-store)

15

Multiple certificates support

© 2008 IBM Corporation

This is a completely new wizard provided to simplify the process of loading and configuring certificates for partners. It is a six step process where you choose the certificate location in the first step and proceed to upload and configure the certificate in the last step.

This is how you load the certificate using the wizard.

In step 1 of the wizard, if you are logged in as hub-operator, you can load certificates either for hub-operator / internal / external partner. In case you are logged in as internal partner, then you are allowed to load certificates just for internal and external partners. You can choose to upload a public certificate / private key (p8) format / one or more certificates or keys from a Trust Store or Key Store.

Load new certificate wizard: Step 2

End entity and CA certificates

- If you are loading from a key / trust store, you can choose the certificate / certificates to be uploaded



If you are loading certificates / key from either trust store or key store, then you are taken to step 2 of the wizard. Here, you are asked to select one or more certificates / key that you want to upload. You are also allowed to load only one key / certificate at a time, but can load multiple Trusted / Intermediate certificates.

Load new certificate wizard: Step 3

Profile: edi1 - Load New Certificate

1. Certificate Location > 2. End Entity and CA certificates > 3. Certificate Details > 4. Set > 5. Default Settings > 6. Configuration > 7. Finish

3. Provide certificate details

The following certificates will be loaded

- Leaf Certificate - Subject DN: Common Name (CN)=Santosh; Serial Number=4771 6E2A

Leaf certificate Name:

Description:

Certificate Type: Digital Signature Encryption

Certificate Usage: Select One

Operation Mode: Production, Test, RN Simulator External Partner, RN Simulator Internal Partner

Status: Enabled Disabled

Set Management: Add New Set Update Existing Set

Cancel Next Finish

Certificate details

- Provide details on certificate usage and operation mode - primary / secondary



In step 3 of the wizard, you have to provide details about the certificate / key information. You have to provide information such as the purpose of the certificate (SSL / Sign / Encryption), operation modes (test/production), if it is a primary or secondary certificate, and so on. If this is a private key or encryption certificate of the external partner, then you have to choose to add this certificate to an existing set or create a new one.

Load new certificate wizard: Step 4

The screenshot shows a web-based wizard interface for loading a new certificate. The browser address bar indicates the user is logged in as 'Hub Administrator'. The navigation menu includes 'Account Admin', 'Profiles', 'Connections', 'Alerts', 'Exclusion List', 'Error Flow', 'FTP User Management', 'Partner', 'Destinations', 'B2B Capabilities', 'Certificates', 'Users', 'Groups', 'Contacts', and 'Addresses'. The current step is '4. Set', which is highlighted in the progress bar. The wizard title is 'Profile: edi1 : Load New Certificate'. The progress bar shows the following steps: 1. Certificate Location, 2. End Entity and CA certificates, 3. Certificate Details, 4. Set (current), 5. Default Settings, 6. Configuration, and 7. Finish. The main content area is titled '4. Create a new Set' and contains the following fields and options:

- Set Name:** A text input field with a red asterisk indicating it is required.
- Description:** A text input field.
- Status:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Make Default Settings:** A checked checkbox.

At the bottom of the form are three buttons: 'Cancel', 'Next', and 'Finish'.

- Associate the certificate to an existing certificate set / a new certificate set



In step 4 of the wizard, you can associate the certificate to an existing set. There is a drop down shown with the list of existing sets that this certificate can fit into, else you can create a new set. You can also choose to make this set as the default set. If the set is chosen to be default, it means all documents are initiated by the partner to whom this certificate belongs to, that is, internal partner. This certificate also applies for all documents that this partner shall be receiving (in case of external partner.)

Load new certificate wizard: Step 5

Profile: edi1 - Load New Certificate Welcome, Hub Administrator

1. Certificate Location ▶ 2. End Entity and CA certificates ▶ 3. Certificate Details ▶ 4. Set ▶ 5. Default Settings ▶ 6. Configuration ▶ 7. Finish

5. Assign the Set to default operation modes

Operation Mode	Current Default Settings	
	SSL Client	Digital Signature
Production	No Set Selected ▼	No Set Selected ▼
Test	No Set Selected ▼	No Set Selected ▼
RN Simulator External Partner	No Set Selected ▼	No Set Selected ▼
RN Simulator Internal Partner	No Set Selected ▼	No Set Selected ▼
test	No Set Selected ▼	No Set Selected ▼

Default settings

- If the set in step 4 was defined as default, then it applies to all receiving partners for all protocols. In this step, you will associate the set to different operation modes



Step 5 of the wizard loads only if the set was chosen to be the default, and the set belongs to internal partner. In this page, you can associate the set to external partners. Also, you can associate this set to different operation modes.

Load new certificate wizard: Step 6

Profile: edi1 - Load New Certificate

1.Certificate Location> 2.End Entity and CA certificates> 3.Certificate Details> 4.Set> 5.Default Settings> 6.Configuration> 7.Finish

6.Configure certificate sets for participant connections

From Partner: edi1 To Partner: All

From Package: All To Package: All

Click on the button to load the previous selected values for the selected criteria

Operation Mode	From Partner Certificate Sets	
	SSL Client	Digital Sig
Production	No Set Selected	TrustSet
Test	No Set Selected	TrustSet
RI Simulator External Partner	No Set Selected	TrustSet
RI Simulator Internal Partner	No Set Selected	TrustSet
test	No Set Selected	TrustSet

Default settings

- Associate the set to a combination of partner, package, operation mode, and certificate use



The step 6 of the wizard loads only if the set was chosen to be the default, and the set belongs to the external partner. In this page, you can associate the set to internal partners. Also, you can associate this set to different operation modes.

Section

Summary and references



The next section covers the summary and references.

Summary

- Certificates can be directly associated to internal partners
- Wizard to load and configure certificates
- Multiple certificates for internal & external partners
- Certificate sets
- Ability to vary certificates based on:
 - ▶ Partner pair
 - ▶ Operation mode
 - ▶ Package
- Enhanced utility functions:
 - ▶ Validate and where-used



There are several new certificate related enhancements in V6.1.1.

You can load certificates of internal partners directly to internal partners as opposed to loading them for hub-operator. The new load certificate wizard simplifies loading and configuring certificates for internal and external partners. You can also have more than one certificate active for internal or external partner. The Certificate sets are introduced to group primary and secondary certificates of certain types. You can now choose to vary certificate based on participant connection / operation mode. Last but not the least, “where-used” function is enhanced and a new validate function is introduced to validate certificate path and expiry.

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send e-mail feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_wpg611_MultipleCertificatesSupport.ppt

This module is also available in PDF format at: [../wpg611_MultipleCertificatesSupport.pdf](http://wpg611_MultipleCertificatesSupport.pdf)



You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM WebSphere

A current list of other IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

© Copyright International Business Machines Corporation 2008. All rights reserved.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.