

OpenPGP certificates are supported in WebSphere® Partner Gateway V6.2.1.



The coverage of this presentation is as follows:

What is PGP and OpenPGP?

What are the OpenPGP functionalities implemented in this release?

How to configure WebSphere Partner Gateway console to support OpenPGP?



This section briefs about what PGP and OpenPGP means.

PGP stands for Pretty Good Privacy. It is a security software that provides cryptographic privacy and authentication for data communication.

OpenPGP is the open Standard that was specified for PGP.

The OpenPGP supported in this release follows RFC 4880.



This section covers the OpenPGP functionalities supported in this release of WebSphere Partner Gateway.

The implemented OpenPGP provides functionalities such as encryption, compression, and radix-64 conversion. Note that it does not support digital signing.

In entirety, five encryption algorithms and three compression algorithms are supported.

Encryption with modification detection is also supported. By using modification detection along with encryption, you can enforce message integrity check, which verifies whether the message has been tampered during transition.

Armor is also supported. By using it, data can be encoded into ASCII Armor.

	IBM
Configuring WebSphere Partner Gateway console to supp OpenPGP	port
1. Configure console properties under system Administration	
2. Apply bouncy castle jars	
3. Apply security jars	
4. Restart the server	
5. Setup partner connections	
6. Upload certificates	
7. Set the routing object attributes for target connection on sender hub	
5 OpenPGP	© 2011 IBM Corporation

This slide shows the various steps to be followed to configure WebSphere Partner Gateway Console to support OpenPGP.



Step one shows the properties that need to be set in the common properties page of System administration for OpenPGP.



Obtain or procure these library files externally, as IBM does not ship them. In case of distributed mode, place the jar files in all the computers where Document Manager and Console are installed.

		IBM
Step	3: Applying security jars	
 Down websi 	nload the unlimited jurisdiction strength policy jars from the IBM site: http://www.ibm.com/developerworks/java/jdk/security/50/.	SDK Policy files
 Place Install – loc – US 	e those unrestricted policy jars in the <websphere application="" s<br="">llation>/java/jre/lib/security folder. Name of the jars are given bel ocal_policy.jar JS_export_policy.jar</websphere>	Server low:
8	OpenPGP	© 2011 IBM Corporation

Encryption algorithms like Twofish, TripleDES, and AES require unrestricted cryptography jurisdiction policy files.

Ensure that there are no legal issues in installing the cryptographic files.



After applying the bouncy castle jars and security jars, restart the server.

In the next step, you need to set up partner connections.

	IBM
Step 6: Uploading certificates	
 In Sender hub, upload OpenPGP certificate for encryption at external partner level In Receiver hub, upload OpenPGP certificate for decryption at internal partner level 	
• In Receiver hub, upload OpenPGP certificate for decryption at internal partner level	
Truststore, keystore or keyring location: C. Documents and Settings lavanya wiy Doc Brows	ə
Type: OpenFGF V	
10 OpenPGP © 201	1 IBM Corporation

After setting up the required partner connection, the next step is to upload certificates for external partner on the sender hub and for the internal partner on the receiver hub. Few certificates have sub-key option, which is optional while uploading certificates.



OpenPGP specific connection attributes need to be set on the hub, which encrypts the document.



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

