

PGP Support Package Security

Version 4.2

Technical Overview

Contents

PGP Support Package.....	3
New in this release	3
System requirements.....	4
System architecture	4
PGP Universal.....	4
External LDAP PGP key servers.....	6
BlackBerry Enterprise Solution security	6
Standard BlackBerry encryption.....	6
PGP security.....	6
PGP key types	7
PGP encryption.....	7
Storing PGP keys.....	9
PGP Universal storage	9
BlackBerry device storage	9
Cleaning decrypted PGP content from the BlackBerry device	11
Searching for and validating PGP keys	12
LDAP PGP key servers.....	12
Searching external LDAP PGP key servers.....	12
Managing PGP keys.....	13
View PGP key details.....	13
Set PGP key security options	13
Sending and receiving PGP protected messages.....	14
Digital signing and encryption options on PGP protected messages	14
Fetch or import a PGP key from a received PGP protected message	15
Fetch or import S/MIME X.509 certificates from a received PGP protected message	16
Add an external LDAP PGP key server configuration from a received PGP protected message	16
PGP message icons.....	16
BlackBerry Enterprise Server IT policy rules for the PGP Support Package	17
Related resources.....	18

This document describes features that the PGP Support Package Version 4.2, which is designed to offer extended security features for BlackBerry® devices, and the BlackBerry Enterprise Server Version 4.1.2 or later (with the correct IT policy template) support, unless otherwise stated. See the documentation for earlier software versions of the PGP Support Package and the BlackBerry Enterprise Server to determine if an earlier version supports a specific feature.

See the *BlackBerry Enterprise Solution Security Acronym Glossary* for the full terms substituted by the acronyms in this document.

PGP Support Package

The PGP Support Package is designed to provide support for using OpenPGP (RFC 2440) and PGP/MIME (RFC 3156) message formatting on the BlackBerry device to enable users who already send and receive PGP® protected messages in OpenPGP and PGP/MIME formats using their computer email applications to send and receive PGP protected messages in these formats using their BlackBerry devices. The PGP Support Package is designed to work with PGP Universal™ 2.0.2 or later, with either PGP Universal Satellite 2.0.2 or later or PGP Desktop Professional 9.0.2 or later.

The PGP Support Package includes tools for obtaining PGP keys and transferring them to the BlackBerry device so that BlackBerry devices with the PGP Support Package installed can decrypt PGP protected messages and users can read the decrypted messages on their BlackBerry devices. Users can digitally sign, encrypt, and send PGP protected messages from their BlackBerry devices. Without the PGP Support Package, the BlackBerry device receives PGP protected messages as unreadable cipher text.

Within the PGP Universal environment, the PGP Universal Server operates as a network appliance. The PGP Universal Server specifies secure email policies that the PGP Universal Server administrator designs. The BlackBerry device with the PGP Support Package installed enforces compliance with the PGP Universal secure email policies for all email messages.

The PGP Support Package includes support for the following:

- using the PGP Universal Server to retrieve and enforce a secure email policy
- wireless fetching of PGP keys and PGP key status using either a PGP Universal Server or an external LDAP PGP key server
- encrypting and decrypting PGP protected email and PIN messages
- verifying digital signatures on received email and PIN messages, and digitally signing outgoing email and PIN messages

New in this release

Feature	Description
Support for S/MIME X.509 certificates	Users who have installed and enabled both the PGP Support Package and the S/MIME Support Package on their BlackBerry devices can download PGP keys that include S/MIME X.509 digital certificates from the PGP Universal Server and use the certificates in compliance with the PGP Universal secure email policy.
Support for PGP/MIME protected messages	PGP enabled users can receive PGP/MIME format messages on their BlackBerry devices. The PGP Support Package continues to support OpenPGP format messages.
Message classification	Set message classifications that require PGP enabled users to digitally sign, encrypt, or digitally sign and encrypt email messages sent from their BlackBerry devices using the BlackBerry Enterprise Server Version 4.1.2 or later.
Improved PGP key fetching	When a PGP enabled user chooses to encrypt or digitally sign and encrypt an email message on the BlackBerry device, the BlackBerry device automatically searches for a PGP key when the user adds a recipient to the message.

Feature	Description
Separate PGP Universal Server and external LDAP key server fetching	After the user enrolls with the PGP Universal Server on the BlackBerry device, the BlackBerry device searches the PGP Universal Server for all PGP keys. The user cannot search for PGP keys on an external LDAP server on the BlackBerry device and the BlackBerry device does not automatically fetch PGP keys from an external LDAP server.
Additional PGP key management option	Set the Disable Certificate Email Address Checks IT policy rule in the BlackBerry Enterprise Server Version 4.1.2 or later to specify whether or not the BlackBerry device displays a warning when the user receives a digitally signed message on the BlackBerry device in which the sender's email address does not appear in the PGP key used to digitally sign the message or the email address of the sender does not match the email address inside the PGP key.

System requirements

The PGP Support Package Version 4.2 and later supports the following software and BlackBerry devices.

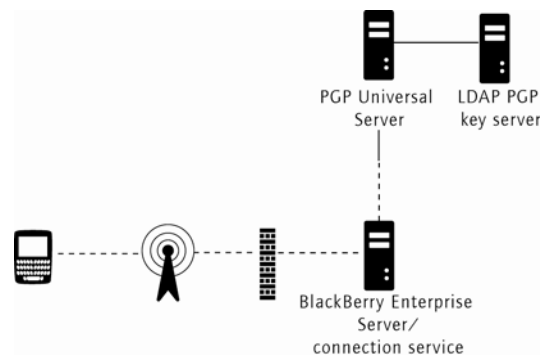
Messaging and collaboration servers	BlackBerry Enterprise Server	BlackBerry devices
<ul style="list-style-type: none"> Microsoft® Exchange 5.5, 2000 and 2003 Servers IBM® Lotus® Domino® server version 5.0.3 or later <p>Note: The PGP Universal Server does not support Microsoft Exchange 5.5 Server.</p>	<ul style="list-style-type: none"> BlackBerry Enterprise Server Version 4.0 Service Pack 2 or later for Microsoft Exchange BlackBerry Enterprise Server Version 4.1 or later for IBM Lotus Domino 	<ul style="list-style-type: none"> Java™ based BlackBerry devices that run BlackBerry Device Software Version 4.1 or later <p>Note: Users must load the PGP Support Package on their BlackBerry devices.</p>

System architecture

The BlackBerry device is designed to use the BlackBerry Mobile Data System™ (BlackBerry MDS™) Connection Service, which resides on the BlackBerry Enterprise Server, to connect to the PGP Universal Server and to the external LDAP PGP key server(s) that the user sets on the BlackBerry device. The connection service uses a standard protocol, such as HTTP or TCP/IP, to enable the BlackBerry device to retrieve PGP keys and PGP key status from the PGP Universal Server or an external LDAP PGP key server over the wireless network.

PGP Universal

The PGP Universal Server enables users to download PGP keys to their BlackBerry devices and verify the authenticity and status of the PGP keys. The BlackBerry device and the PGP Universal Server can use LDAP to search for and download PGP keys.



BlackBerry device to PGP Universal Server connection

When a user enrolls and authenticates with the PGP Universal Server from the BlackBerry device, the following events occur:

- The BlackBerry device enables users to download their PGP keys to their BlackBerry devices over the wireless network. The BlackBerry device stores keys in the PGP Key Store and the PGP Universal Key Cache.
- The BlackBerry device automatically fetches the secure email policy and required PGP keys from the PGP Universal Server on demand without additional action from the BlackBerry device user.

Enrollment and authentication

When you set the PGP Universal Server Address IT policy rule, the BlackBerry Enterprise Server pushes the PGP Universal Server address to the BlackBerry device, which prompts the user to enroll with that PGP Universal Server.

Using the default enrollment method, users must type their email addresses on their BlackBerry devices to complete the enrollment process. You can specify the preferred enrollment method (by domain user name and password authentication or by email address authentication) using the PGP Universal Enrollment Method IT policy rule.

Until the user completes the enrollment process the following events occur:

- An Enroll with PGP Universal Server menu item appears on the PGP options screen.
- The BlackBerry device prompts the user to enroll with the PGP Universal Server when the user tries to send a message from the BlackBerry device and when the BlackBerry device resets.

After the user completes the enrollment, the BlackBerry device stores the long term authentication information included in the enrollment response. If the BlackBerry device resets, the stored authentication information automatically authenticates the BlackBerry device to the PGP Universal Server.

Secure email policy

The BlackBerry device is designed to use the secure email policy from the PGP Universal Server to determine whether to digitally sign, encrypt, or digitally sign and encrypt the email messages that it sends, based on the minimum security requirements of the secure email policy and any additional security that the user applies to the message when sending it from the BlackBerry device.

The BlackBerry device fetches the secure email policy data from the PGP Universal Server at a frequency set by the PGP Universal Policy Cache Timeout IT policy rule. By default, the BlackBerry device caches the secure email policy data for a maximum of 24 hours.

PGP key storage and retrieval

When a user sends a PGP protected message from the BlackBerry device, the PGP Universal Server fetches PGP public keys on behalf of the BlackBerry device user for the intended message recipients, as needed, and validates the fetched keys before returning them to the user. See "PGP Universal storage" on page 9 for more information.

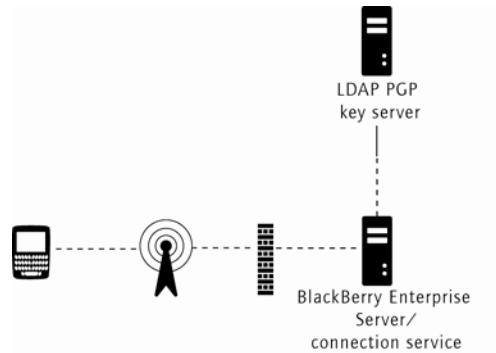
Data transfer process with PGP Universal Server integration

1. The BlackBerry Enterprise Server pushes the PGP Universal Server Address IT policy rule to the BlackBerry device.
2. The BlackBerry device prompts the user to enroll with the PGP Universal Server.
3. The user responds to the prompt on the BlackBerry device and automatically enrolls with the PGP Universal Server.
4. The PGP Universal Server sends an enrollment response to the BlackBerry device.
5. The BlackBerry device performs the following actions:
 - stores the long term authentication information that the PGP Universal Server includes in the enrollment response in the BlackBerry device flash memory
 - refreshes the secure email policy data, if necessary, and then stores that data temporarily

6. The BlackBerry device contacts the PGP Universal Server each time the user sends or receives a message on the BlackBerry device and uses the secure email policy from the PGP Universal Server to determine how to encode each message.
7. The PGP Universal Server obtains the PGP public keys as needed and validates them before returning them to the BlackBerry device user.

External LDAP PGP key servers

If you do not require the user to enroll and authenticate with the PGP Universal Server, you can set the BlackBerry device to use the connection service to contact the external LDAP PGP key server(s) that are set to search for the required PGP keys.



BlackBerry device to external LDAP server connection

Data transfer process with external LDAP PGP key servers

When the user sends or receives a message on the BlackBerry device that requires PGP keys, the BlackBerry device performs the following actions:

- contacts the set external LDAP PGP key server(s)
- searches the LDAP server(s), obtains the PGP public keys as needed
- returns the PGP public keys to the user

BlackBerry Enterprise Solution security

The current BlackBerry Infrastructure uses symmetric key cryptography to encrypt the data that the BlackBerry Enterprise Server and the BlackBerry device send between them. Standard BlackBerry encryption encrypts data using the Triple DES or the AES algorithm. See the *BlackBerry Enterprise Solution Security Technical Overview* for more information on BlackBerry Enterprise Solution security features.

Standard BlackBerry encryption

Before sending a message, the BlackBerry device compresses the message and then encrypts the message using the master encryption key, which is unique to that BlackBerry device.

When the BlackBerry Enterprise Server receives the message from the BlackBerry device, the BlackBerry Enterprise Server decrypts the message using the BlackBerry device master encryption key and then decompresses the message.

See the *BlackBerry Enterprise Solution Security Technical Overview* for more information on standard BlackBerry encryption.

PGP security

From the time the BlackBerry device user sends a message until the BlackBerry Enterprise Server receives the message, the standard BlackBerry encryption encrypts the message. PGP technology is designed to enable

sender-to-recipient authentication and confidentiality and help maintain data integrity and privacy from the time that the BlackBerry device user sends a message over the wireless network until the message recipient decodes and reads the message.

PGP technology relies on public key cryptography (using private and public key pairs) to provide the following components of a security solution:

- **Confidentiality:** PGP technology uses encryption to make sure that only the intended message recipient can view the contents of the message.
- **Integrity:** PGP technology uses digital signatures to verify that a third party has not altered the message data.
- **Authenticity:** PGP technology uses digital signatures to permit the message recipient to identify and trust the message sender.

PGP key types

The PGP Support Package uses public key cryptography with the following keys:

Key type	Description
PGP public key	The BlackBerry device uses the recipient's PGP public key to encrypt outgoing email messages, and uses the sender's PGP public key to verify digital signatures on received email messages. The PGP public key is designed to be distributed and accessed by message recipients and senders without compromising security conditions.
PGP private key	The BlackBerry device uses the PGP private key to digitally sign outgoing email messages and decrypt received email messages. Private key information should remain private to the key owner.

PGP encryption

If the PGP Support Package is installed on a BlackBerry device, when a user sends a message from that BlackBerry device, the BlackBerry device encrypts the message using the following process:

1. The BlackBerry device encrypts the message using the message recipient's PGP public key.
2. The BlackBerry device uses standard BlackBerry encryption to encrypt the PGP encrypted message.
3. The BlackBerry device sends the encrypted message to the BlackBerry Enterprise Server.
4. The BlackBerry Enterprise Server removes the standard BlackBerry encryption and sends the PGP encrypted message to the recipient.

If the PGP Support Package is installed on a BlackBerry device, when the BlackBerry device receives a message, the PGP message is encrypted with standard BlackBerry encryption and then decrypted, using the following process:

1. The BlackBerry Enterprise Server receives the PGP protected message.
2. The BlackBerry Enterprise Server uses standard BlackBerry encryption to encrypt the PGP encrypted message.
3. The BlackBerry Enterprise Server sends the encrypted message to the BlackBerry device.
4. The BlackBerry device removes the standard BlackBerry encryption and stores the PGP encrypted message.
5. When the user opens the message on the BlackBerry device, the BlackBerry device decrypts the PGP encrypted message and renders the message contents.

PGP encryption algorithms

The BlackBerry device is designed to support the use of a strong algorithm for PGP encryption. The PGP Allowed Content Ciphers IT policy rule default setting specifies that the BlackBerry device can use any of the supported algorithms to encrypt PGP messages. You can set the PGP Allowed Content Ciphers IT policy rule to encrypt PGP messages using any of AES (256-bit), AES (192-bit), AES (128-bit), CAST (128-bit), and Triple DES (168-bit).

The message recipient's PGP key indicates which content ciphers the recipient can support, and the BlackBerry device is designed to use one of those ciphers. The BlackBerry device encrypts the message using Triple DES by default if the recipient's PGP key does not include a list of ciphers.

PGP public keys

When a user sends a message from the BlackBerry device, the BlackBerry device uses the message recipient's PGP public key to encrypt the message.

Recipients can verify the digital signature on the message if they have the sender's PGP public key. PGP public keys might contain multiple cryptographic keys, including a parent key that is typically used for digital signature verification, and zero or more subkeys that are typically used for encryption. The PGP parent key digitally signs all of the other information (for example, the user identity information, the subkeys, and expiry information) in a PGP key.

PGP public key strength

The length (size) of a PGP public key determines its encryption strength. The parent key and the subkeys of a PGP public key can have different strengths.

You can set the encryption key length by setting the minimum RSA, DSA, and DH algorithm key lengths using BlackBerry Enterprise Server IT policy rules. The following table lists the default minimum and maximum key lengths for the supported key generation algorithms.

Algorithm	Default minimum strong key length (bits)	Maximum key length (bits)
RSA	1024	4096
DSA	1024	1024
DH	1024	4096

RIM recommends using a strong PGP public key to protect messages by setting the following IT policy rules to 1024:

- PGP Minimum Strong DH Key Length
- PGP Minimum Strong DSA Key Length
- PGP Minimum Strong RSA Key Length

See "BlackBerry Enterprise Server IT policy rules for the PGP Support Package" on page 17 for more information.

PGP private keys

When a user sends a message from the BlackBerry device, the BlackBerry device uses the message sender's PGP private key to digitally sign the message.

When a user receives a PGP protected message, the BlackBerry device uses the user's PGP private key to decrypt the message.

PGP private key strength

The public key length and the private key length are the same. The larger the PGP public key and the PGP private key, the stronger the PGP key pair.

Storing PGP keys

PGP Universal storage

PGP keys are stored on the PGP Universal Server in one of three ways: client key mode, guarded key mode, or server key mode. The key storage mode impacts the user's access to PGP private keys.

Key storage mode	Description	Impact on BlackBerry device user
server key mode	The PGP Universal Server stores the user's PGP public key and private key.	The user can download the PGP private key on the BlackBerry device without a passphrase prompt and automatically import the key into the BlackBerry device key store. The BlackBerry device prompts the user for the key store password when accessing PGP private keys in the key store to digitally sign or decrypt messages.
guarded key mode	The PGP Universal Server stores the user's PGP public key and a passphrase-protected copy of the user's PGP private key. Note: The user creates the passphrase when creating the PGP private key.	The user can download the PGP private key on the BlackBerry device. The BlackBerry device prompts the user for the passphrase to import the PGP private key into the BlackBerry device key store. The BlackBerry device prompts the user for the key store password when accessing private keys in the key store to digitally sign or decrypt messages.
client key mode	The BlackBerry device user's PGP Desktop software stores and manages the user's PGP private keys. The PGP Universal Server stores the user's PGP public key. Note: The user can create a passphrase when creating the PGP private key.	The user can download the PGP private key to the BlackBerry device using the BlackBerry Desktop Manager. The BlackBerry device prompts the user for the passphrase, if one exists, to import the PGP private key into the BlackBerry device key store. When the BlackBerry device accesses private keys in the key store to digitally sign or decrypt messages, the BlackBerry device prompts the user for the key store password.

The PGP Universal Server administrator can turn on either client key mode or guarded key mode for a user in the PGP Universal Server's administrative console. See the documentation that PGP Corporation provides for more information.

BlackBerry device storage

The PGP Universal Key Cache (a non-persisted, transient key store on the BlackBerry device) stores PGP public keys that the BlackBerry device fetches from the PGP Universal Server. The PGP Universal Key Cache stores the keys for 24 hours and then fetches them again as needed.

The PGP key store, which is part of the BlackBerry device flash memory, stores the following keys:

- PGP public and private key pairs
- PGP public keys that the BlackBerry device fetches from external PGP key server(s) or imports from messages
- S/MIME X.509 certificates that the BlackBerry device fetches from external PGP key server(s) or imports from messages

Key store security features

BlackBerry device users must supply the key store password to add and remove PGP public keys, PGP private keys, and S/MIME X.509 certificates stored on the BlackBerry device.

The BlackBerry device stores a SHA 256 hash of the key store password. The hash of the password is designed to protect the actual key store password by preventing the possibility of an attacker determining the password from the BlackBerry device memory contents. When the user types the key store password, the BlackBerry device performs a one-way hash function on the entered characters using SHA 256, and then compares the hashed input to the stored hashed password.

You can set BlackBerry Enterprise Server IT policy rules to set the key store password security requirements. See the *Policy Reference Guide* for more information.

IT policy rule	Recommendation
Minimum Password Length	Set a key store password that is between 4 and 12 alphanumeric characters in length.
Forbidden Passwords	Specify weak passwords to prevent.
Key Store Password Maximum Timeout	Specify the maximum length of time (0, 1, 2, 5, 10, 20, 30 minutes, or 1 hour) that the key store remains unlocked after the BlackBerry device user types the correct key store password.
Disable Key Store Backup	Set this policy rule to prevent the BlackBerry device from performing backups of PGP private keys in the key store.
Minimal Signing Key Store Security Level	Set to one of the following levels: <ul style="list-style-type: none"> • 2 (high security): The BlackBerry device prompts the user for the BlackBerry device key store password each time an application tries to access the private key of the user • 3 (medium security): The BlackBerry device prompts the user for the BlackBerry device key store password when an application tries to access the private key of the user for the first time or when the private key password timeout expires on the BlackBerry device
Minimal Encryption Key Store Security Level	Set to one of the following levels: <ul style="list-style-type: none"> • 2 (high security): The BlackBerry device prompts the user for the BlackBerry device key store password each time an application tries to access the private key of the user • 3 (medium security): The BlackBerry device prompts the user for the BlackBerry device key store password when an application tries to access the private key of the user for the first time or when the private key password timeout expires on the BlackBerry device

Users can set additional key store security requirements on their BlackBerry devices (**Security Options > Key Stores**).

Setting	Description
Allow Key Store Backup/Restore	Specify whether or not to back up and restore PGP keys (private keys and public keys) and symmetric keys in the key store.
Private Key Password Timeout	Specify the maximum amount of time that the key store remains unlocked after the BlackBerry device user types the correct key store password. Note: The value that you specify for this rule cannot be greater than the value that the Key Store Password Maximum Timeout IT policy rule specifies.
Certificate Service	Define the connection service that the PGP key search uses to fetch a PGP key status.
Certificate Status Expires After	Specify the maximum amount of time (1, 2, 4, or 12 hours, 1 day, 1 week, 1 month, or 6 months) for which the PGP key revocation status remains valid.
Change Password	Type a new key store password.

Cleaning decrypted PGP content from the BlackBerry device

The BlackBerry device automatically turns on the secure garbage collection function when the PGP Support Package is installed and the private key of the user is on the BlackBerry device. When secure garbage collection is turned on, the BlackBerry device performs the following actions:

- overwrites the memory reclaimed by the standard garbage collection process with zeroes
- periodically runs the memory cleaner application, which tells BlackBerry device applications to empty any caches and free memory associated with unused, sensitive application data
- automatically overwrites the memory freed by the memory cleaner application when it runs

The memory cleaner application is designed to remove unreferenced, decrypted content from the BlackBerry device, including content from the PGP application, key store, content protection and address book caches, PGP key search, and BlackBerry device clipboard.

You can set the memory cleaning application to run automatically when the

- user synchronizes the BlackBerry device with the computer
- user locks the BlackBerry device
- BlackBerry device locks after a specified amount of idle time
- user changes the time or time zone on the BlackBerry device

Scenario	Recommendation
Remove decrypted content from BlackBerry device memory when the BlackBerry device is holstered.	Set the Force Memory Clean When Holstered IT policy rule to True.
Remove decrypted content from BlackBerry device memory when the BlackBerry device is idle.	Set the Force Memory Clean When Idle IT policy rule to True.
Start the memory cleaner after the time specified has elapsed.	Set the Memory Cleaner Maximum Idle Time IT policy rule to 1 (minute).

See the *Policy Reference Guide* for more information.

Users can set the memory cleaning application to run while their BlackBerry devices are holstered, or when their BlackBerry devices remain idle for a set period of time (2, 5, 10, 20, 30 minutes, or 1 hour). Users can also manually run the memory cleaner application on their BlackBerry devices or run specific registered memory cleaners in the BlackBerry device Security options.

See the *PGP Support Package User Guide Supplement* for more information.

Searching for and validating PGP keys

You must turn on the connection service to enable wireless synchronization of PGP keys and their status from external LDAP PGP key servers.

LDAP PGP key servers

LDAP servers can store information about PGP keys. If the BlackBerry device user is not enrolled with the PGP Universal Server, the user's BlackBerry device can search for PGP keys on the external LDAP servers that you set in the BlackBerry Manager or the user sets from the BlackBerry device. The connection service can contact these set external LDAP PGP key servers to fetch and verify the authenticity and status of a PGP key.

The BlackBerry device user should manually validate the fingerprint of PGP keys that the BlackBerry device obtains from external LDAP PGP key servers.

Set an external LDAP server

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Enterprise Server.
2. Click the **Connection Service** tab.
3. Click **Edit Properties**.
4. Click **LDAP**.
5. Set the following fields:

Field	Description
Host Name	Type the name of the default LDAP server.
Port	Type the port on which the default LDAP server listens. Note: If you typed a host name, you must type a port number.
Default Server Base Query	Type the default base query for the default LDAP server, using %20 for spaces (for example, o=PGP%20Keys). Note: Each LDAP server can host multiple domains but can only search in one domain at a time. You might need to set a default base query for some LDAP servers.
Query Limit	Type the maximum number of entries to return for each query.
Enable Data Compression	In the drop-down list, click True to compress results from an LDAP lookup.

See the *BlackBerry Enterprise Server System Administration Guide* for more information.

Users can add external LDAP server settings from the BlackBerry device. See the *PGP Support Package User Guide Supplement* for more information.

Searching external LDAP PGP key servers

The PGP Support Package includes a PGP key search feature. BlackBerry device users that are not enrolled with the PGP Universal Server can query set external LDAP PGP key servers, such as the PGP Global Directory, on the

BlackBerry device based on the first name, last name, or email address of the PGP key subject, and download PGP keys from the search results.

The PGP Global Directory is a free, publicly available, key server hosted by PGP Corporation at keyserver.pgp.com. The PGP Global Directory is designed to enable PGP users to find the public keys of other PGP users with whom they want to exchange encrypted email messages.

PGP key revocation status

BlackBerry device users can perform PGP key revocation status checks from the BlackBerry device when they receive a digitally signed or digitally signed and encrypted message, and before they send a message to the subject of a PGP key. Users can also check the revocation status of a PGP key from the BlackBerry device key store and from the PGP Key Search screen.

The BlackBerry device uses the connection service to request and retrieve either the PGP key revocation status or an updated PGP key (if the PGP key revocation status has expired) from a set external LDAP PGP key server. If the BlackBerry device retrieves an updated PGP key, it updates the BlackBerry device key store.

On the BlackBerry device, in the PGP Key Search Options screen, users can set whether they are prompted to fetch the PGP key revocation status when they try to add a PGP key to the BlackBerry device key store.

Managing PGP keys

View PGP key details

To view PGP key details on a BlackBerry device, click **Security Options > PGP keys > Details**.

Detail	Description
Revocation Status	displays the status of the PGP key at a specified date and time
Trust Status	displays the status of the PGP key trust level <ul style="list-style-type: none"> • Explicitly trusted: the PGP key is trusted • Implicitly trusted: the PGP key corresponds to a PGP private key on the BlackBerry device or a chain of digital signatures to a trusted key exists • Not trusted: the PGP key is not explicitly trusted or does not correspond to a trusted PGP private key on the BlackBerry device, or a chain of digital signatures to a trusted key does not exist
Fingerprint	displays the PGP fingerprint in hexadecimal format, which the BlackBerry device user can use to validate the authenticity of the PGP public key

Set PGP key security options

Users can set PGP key security options on a BlackBerry device (in **Security Options > PGP keys**).

Action	Procedure
Trust the PGP key.	Click Trust .
Remove the trust associated with the PGP key.	Click Distrust .
Invalidate the status of a PGP key.	Click Revoke .
Remove a PGP key from the BlackBerry device key store.	Click Delete .
Send a PGP key in an email message.	Click Send via Email .
Send a PGP key in a PIN message.	Click Send via PIN .
Download the status of the PGP key.	Click Fetch Status .
Download updated PGP keys from an LDAP server.	Click Fetch Updated PGP Key .

See the *PGP Support Package User Guide Supplement* for more information.

Sending and receiving PGP protected messages

By default, with the PGP Support Package installed, a BlackBerry device on which a user has completed enrollment with the PGP Universal Server automatically applies the secure email policies designed by the PGP Universal Server administrator to all email that the user sends. The BlackBerry device automatically digitally signs, encrypts, or digitally signs and encrypts messages based on the secure email policy.

When a user receives an email message on the BlackBerry device, the BlackBerry device uses its IT policy settings to determine the message encoding format. When a user sends an email message from the BlackBerry device, the BlackBerry device uses its IT policy settings, the secure email policy settings on the PGP Universal Server, and additional encoding requirements that the user applies to the message when sending it from the BlackBerry device to determine the message encoding format.

If the BlackBerry device cannot retrieve PGP keys for one or more message recipients and the BlackBerry device user sends the message to the PGP Universal Server, the PGP Universal Server can further process the message, using the default secure email policy to determine what action to take on the message. See the documentation that PGP Corporation provides for more information.

You can set digital signing and encryption options on the BlackBerry device using IT policy. See "BlackBerry Enterprise Server IT policy rules for the PGP Support Package" on page 17 for more information.

Digital signing and encryption options on PGP protected messages

The PGP Support Package includes digital signing and encryption options that the user can specify on the BlackBerry device when they send a message. When the user selects an option on the BlackBerry device to send an encrypted or digitally signed and encrypted PGP message, one of the following conditions occurs:

1. If the BlackBerry device has an appropriate PGP key (in other words, a key that has a strong public key and is trusted, not revoked, and not expired) for the recipient, the BlackBerry device sends the message.
2. If the BlackBerry device does not have an appropriate PGP key for the recipient, the BlackBerry device automatically consults the PGP Universal Server (and possibly external LDAP servers set on the BlackBerry device) to search for an appropriate key. If the BlackBerry device does not find an appropriate PGP key for the intended recipient, the BlackBerry device prompts the user to perform one of the following actions:
 - not send the message
 - manually fetch an appropriate PGP key if the BlackBerry device user is not enrolled with the PGP Universal Server
 - send the message in unencrypted form if the secure email policy on the PGP Universal Server permits and you have set the PGP Force Encrypted Messages IT policy rule to False

Manually fetching a PGP key

If the user responds to the BlackBerry device prompt by choosing to manually fetch an appropriate PGP key for the intended recipient, a PGP Key Search application appears on the BlackBerry device. The user can refine search parameters in the PGP Key Search application on the BlackBerry device before the BlackBerry device tries to fetch an appropriate PGP key from a set external LDAP PGP key server. If it finds an appropriate PGP key, the BlackBerry device sends the message.

Using an S/MIME X.509 certificate to encrypt a message

When a user sends a message from a BlackBerry device with the PGP Support Package and S/MIME Support Package installed, and that user has enrolled and authenticated with the PGP Universal Server, if each of the message recipients' PGP keys contains an S/MIME X.509 certificate, the BlackBerry device encrypts the message using the following process:

1. The BlackBerry device encrypts the message with the message recipient's S/MIME certificate.
2. The BlackBerry device uses standard BlackBerry encryption to encrypt the S/MIME data.
3. The BlackBerry device sends the encrypted data to the BlackBerry Enterprise Server.

- The BlackBerry Enterprise Server removes the standard BlackBerry encryption and sends the S/MIME encrypted message to the recipient.

Using an S/MIME X.509 certificate to validate a digital signature

If the PGP Support Package and the S/MIME Support Package are installed on a BlackBerry device and the BlackBerry device user has enrolled and authenticated with the PGP Universal Server, when the user receives an S/MIME message on that BlackBerry device, if the message sender’s PGP key contains an S/MIME X.509 certificate, the BlackBerry device extracts the certificate from the PGP key and uses the certificate to verify the digital signature on the message.

Sending a message in unencrypted form

When composing a message, users can select the following options on the BlackBerry device:

- attach PGP keys from the BlackBerry device key store and send the keys as .asc file attachments
- use conventional encryption to encrypt the PGP message with a passphrase
- send the message as plain text

By default, the PGP Support Package permits BlackBerry device users to send and receive plain text email and PIN messages. You can set BlackBerry Enterprise Server IT policy rules to prevent PGP enabled BlackBerry device users from sending plain text messages.

Scenario	Recommendation
Force all PGP enabled users to send digitally signed, encrypted, or digitally signed and encrypted PGP email messages.	Set the Disable Message Normal Send IT policy rule to True. Warning: If you apply this IT policy rule, you might overrule secure email policy settings on the PGP Universal Server.
Force all PGP enabled users to send digitally signed, encrypted, or digitally signed and encrypted PGP PIN messages.	Set the Disable Peer-to-Peer Normal Send IT policy rule to True. Warning: If you apply this IT policy rule, you might overrule secure email policy settings on the PGP Universal Server.

See the *PGP Support Package User Guide Supplement* for more information.

Fetch or import a PGP key from a received PGP protected message

If the BlackBerry device user has enrolled and authenticated with the PGP Universal Server, the following options are not available on the BlackBerry device.

- On the BlackBerry device, in the message list, click a received PGP protected message.
- Perform one of the following actions:

Action	Procedure
Retrieve a PGP key from the external LDAP PGP key server. (The sender’s PGP key is not on the recipient’s BlackBerry device and is not included in the message.)	> Click Fetch Sender’s PGP Key .
Add the sender’s PGP key to the BlackBerry device. (The sender’s PGP key is included in the message but not in the recipient’s BlackBerry device key store.)	> Click Import PGP Key .

See the *PGP Support Package User Guide Supplement* for more information.

Fetch or import S/MIME X.509 certificates from a received PGP protected message

When a user with the PGP Support Package and the S/MIME Support Package installed on a BlackBerry device adds a new PGP key that contains an S/MIME X.509 certificate digitally signed by the PGP Universal Server to the BlackBerry device, the BlackBerry device stores the PGP key and prompts the user to choose whether or not to store the S/MIME X.509 certificate in the key store.

If there is a private key for the original PGP key or the S/MIME X.509 certificate, depending on which of the two (the PGP key or the X.509 certificate) already exists on the BlackBerry device, that private key also corresponds to the generated PGP key or certificate.

Add an external LDAP PGP key server configuration from a received PGP protected message















If the BlackBerry device user has enrolled and authenticated with the PGP Universal Server, the following option is not available on the BlackBerry device.

Import the LDAP PGP key server attachment included in the message to set a new, external LDAP PGP key server (in **Security Options > Certificate Servers**).

1. On the BlackBerry device, in the message list, click a received PGP protected message.
2. Click **Import Server**.

PGP message icons

PGP protected messages appear in the message list. The messages appear with security icons that represent additional information about the validity of the source and the confidentiality of the content.

Icon	Description
	The message is strongly encrypted.
	The message is weakly encrypted.
	The BlackBerry device has verified the message digital signature.
	The BlackBerry device could not verify the message digital signature.
	The BlackBerry device requires more data to verify the message digital signature.
	Please wait for the operation to finish.
	The PGP key is trusted.
	The trust status of the PGP key is unknown.
	There was an error determining the trust status of the PGP key.
	The PGP key has expired.
	The PGP key has been revoked or is not trusted.
	A PGP key is included in the message.
	Several PGP keys are included in the message.
	The message contains an LDAP server attachment.

BlackBerry Enterprise Server IT policy rules for the PGP Support Package

The following BlackBerry Enterprise Server IT policy rules apply only to BlackBerry devices on which the PGP Support Package is installed. Verify that any IT policy rules you set using the BlackBerry Manager are not in conflict with your secure email policy settings on the PGP Universal Server.

IT policy rule	Description
PGP Allowed Content Ciphers	specifies the content ciphers that the BlackBerry device can use to encrypt PGP messages
PGP Blind Copy Address	specifies an email address that is added as a BCC recipient to all outgoing PGP encrypted messages
PGP Force Digital Signature	specifies whether all outgoing PGP messages are digitally signed Warning: If you apply this IT policy rule, you might overrule secure email policy settings on the PGP Universal Server.
PGP Force Encrypted Messages	specifies whether all outgoing PGP messages are encrypted Warning: If you apply this IT policy rule, you might overrule secure email policy settings on the PGP Universal Server.
PGP Minimum Strong DH Key Length	specifies the minimum DH key size, in bits, that you consider strong, for use with PGP encryption
PGP Minimum Strong DSA Key Length	specifies the minimum DSA key size, in bits, that you consider strong, for use with PGP encryption
PGP Minimum Strong RSA Key Length	specifies the minimum RSA key size, in bits, that you consider strong, for use with PGP encryption
PGP Universal Enrollment Method	specifies the method by which BlackBerry device users must enroll with the PGP Universal Server
PGP Universal Policy Cache Timeout	specifies the maximum amount of time, in hours, that the BlackBerry device caches the PGP Universal Server policy before fetching it from the PGP Universal Server again
PGP Universal Server Address	specifies the URL of a PGP Universal Server

See the *Policy Reference Guide* for more information.

Related resources

Guide	Information
<i>BlackBerry Enterprise Server System Administration Guide</i>	<ul style="list-style-type: none"> • generating and changing master encryption keys • enabling encryption • managing security features
<i>BlackBerry Enterprise Solution Security Technical Overview</i>	<ul style="list-style-type: none"> • preventing the decryption of information at an intermediate point between the BlackBerry device and the BlackBerry Enterprise Server or company LAN • managing security settings for all BlackBerry devices • protecting data in transit between the BlackBerry device and BlackBerry Enterprise Server. • understanding the algorithms provided by the RIM cryptographic API (Crypto API) • understanding the TLS and WTLS standards that the RIM Crypto API currently supports • understanding the memory scrub process that occurs on the BlackBerry device when content protection is enabled
<i>Policy Reference Guide</i>	<ul style="list-style-type: none"> • using BlackBerry Enterprise Server IT policies
<i>PGP Support Package User Guide Supplement</i>	<ul style="list-style-type: none"> • installing the PGP Support Package • managing PGP keys on the BlackBerry device • setting PGP options for digitally signing and encrypting messages • sending and receiving PGP protected messages
Visit www.blackberry.com/security .	<ul style="list-style-type: none"> • information about BlackBerry Solution security

Part number: 9476326 Version 3

©2006 Research In Motion Limited. All Rights Reserved. The BlackBerry and RIM families of related marks, images, and symbols are the exclusive properties of Research In Motion Limited. RIM, Research In Motion, "Always On, Always Connected", the "envelope in motion" symbol, and BlackBerry are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

IBM, Lotus, and Domino are either registered trademarks or trademarks of International Business Machines Corporation in the United States, other countries, or both. Java is either a registered trademark or trademark of Sun Microsystems, Inc. in the United States or other countries. Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. PGP is either a registered trademark or trademark of PGP Corporation in the United States and other countries. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

The BlackBerry device and/or associated software are protected by copyright, international treaties and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Other patents are registered or pending in various countries around the world. Visit www.rim.com/patents.shtml for a current list of RIM [as hereinafter defined] patents.

This document is provided "as is" and Research In Motion Limited and its affiliated companies ("RIM") assume no responsibility for any typographical, technical, or other inaccuracies in this document. RIM reserves the right to periodically change information that is contained in this document; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this document to you in a timely manner or at all. RIM MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR COVENANTS, EITHER EXPRESS OR IMPLIED (INCLUDING WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, MERCHANTABILITY, DURABILITY, TITLE, OR RELATED TO THE PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE REFERENCED HEREIN OR PERFORMANCE OF ANY SERVICES REFERENCED HEREIN). IN CONNECTION WITH YOUR USE OF THIS DOCUMENTATION, NEITHER RIM NOR ITS RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, OR CONSULTANTS SHALL BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER BE THEY DIRECT, ECONOMIC, COMMERCIAL, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR INDIRECT DAMAGES, EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF BUSINESS REVENUE OR EARNINGS, LOST DATA, DAMAGES CAUSED BY DELAYS, LOST PROFITS, OR A FAILURE TO REALIZE EXPECTED SAVINGS.

This document might contain references to third-party sources of information, hardware or software, products or services and, or third-party web sites (collectively the "Third-Party Information"). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third-Party Information. The inclusion of Third-Party Information in this document does not imply endorsement by RIM of the Third-Party Information or the third-party in any way. Installation and use of Third-Party Information with RIM products and services may require one or more patent, trademark, or copyright licenses in order to avoid infringement of the intellectual property rights of others. Any dealings with Third-Party Information, including, without limitation, compliance with applicable licenses and terms and conditions, are solely between you and the third-party. You are solely responsible for determining whether such third-party licenses are required and are responsible for acquiring any such licenses relating to Third-Party Information. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use Third-Party Information until all such applicable licenses have been acquired by you or on your behalf. Your use of Third-Party Information shall be governed by and subject to you agreeing to the terms of the Third-Party Information licenses. Any Third-Party Information that is provided with RIM products and services is provided "as is." RIM makes no representation, warranty, or guarantee whatsoever in relation to the Third-Party Information and RIM assumes no liability whatsoever in relation to the Third-Party Information even if RIM has been advised of the possibility of such damages or can anticipate such damages.