

PGP Support Package for BlackBerry Devices

Version 4.5

Security Technical Overview

Contents

| | |
|--|----|
| PGP Support Package for BlackBerry devices..... | 3 |
| Processing PGP protected messages on the BlackBerry Enterprise Server..... | 3 |
| New in this release of the PGP Support Package for BlackBerry devices..... | 4 |
| System requirements..... | 4 |
| System architecture | 4 |
| PGP Universal..... | 5 |
| External LDAP servers for PGP keys | 6 |
| BlackBerry Enterprise Solution security | 7 |
| Standard BlackBerry encryption..... | 7 |
| PGP security..... | 7 |
| PGP key types..... | 7 |
| PGP encryption..... | 7 |
| Storing PGP keys..... | 9 |
| PGP Universal storage | 9 |
| BlackBerry device storage | 10 |
| Clearing decrypted PGP content from the BlackBerry device | 12 |
| Searching for and validating PGP keys | 12 |
| LDAP PGP key servers..... | 12 |
| Types of LDAP server connections | 13 |
| Searching external LDAP servers for PGP keys | 13 |
| Managing PGP keys..... | 14 |
| View PGP key details..... | 14 |
| Set security options for PGP keys | 14 |
| Sending and receiving PGP protected messages..... | 15 |
| Digital signing and encryption options on PGP protected messages | 15 |
| Viewing attachments in PGP encrypted messages..... | 17 |
| Download or import a PGP key from a received PGP protected message..... | 17 |
| Download or import S/MIME X.509 certificates from a received PGP protected message | 18 |
| Add a configuration for an external LDAP server from a received PGP protected message | 18 |
| PGP message icons..... | 18 |
| BlackBerry Enterprise Server IT policy rules for the PGP Support Package for BlackBerry devices..... | 19 |
| Granular PGP policy conditions that the PGP Support Package for BlackBerry devices supports | 20 |
| Related resources..... | 22 |

This document describes features that PGP® Support Package Version 4.5 for BlackBerry® devices and the BlackBerry® Enterprise Server Version 4.1 SP5 or later support, unless otherwise stated. See the documentation for earlier software versions of the PGP Support Package for BlackBerry devices 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 for BlackBerry devices

The PGP Support Package for BlackBerry devices is designed to offer extended security features for BlackBerry devices by providing support for using OpenPGP (RFC 2440) and PGP/MIME (RFC 3156) message formatting on the BlackBerry device. It lets users who already send and receive PGP protected messages in OpenPGP and PGP/MIME formats using their computer email applications send and receive PGP protected messages in these formats using their BlackBerry devices. The PGP Support Package for BlackBerry devices 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 for BlackBerry devices includes tools for obtaining PGP keys and transferring them to BlackBerry devices so that those devices 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. To devices without the PGP Support Package for BlackBerry devices, the BlackBerry Enterprise Server sends PGP encrypted messages as unreadable cipher text, and PGP signed messages as plain text messages without digital signature information.

Within the PGP Universal environment, the PGP Universal Server works 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 for BlackBerry devices installed enforces compliance with the PGP Universal secure email policies for all email messages.

The PGP Support Package for BlackBerry devices includes support for the following features:

- using the PGP Universal Server to retrieve and enforce a secure email policy
- retrieving PGP keys and PGP key status over the wireless network 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

Processing PGP protected messages on the BlackBerry Enterprise Server

PGP protected messages that BlackBerry device users receive in PGP/MIME format consist of several parts. Supported BlackBerry Enterprise Server versions process PGP/MIME messages to display correctly when forwarding PGP/MIME messages to BlackBerry devices. If either or both the BlackBerry Enterprise Server and the recipient BlackBerry device does not support using PGP technology, the BlackBerry Enterprise Server does not process PGP/MIME messages that it receives and the BlackBerry device receives PGP/MIME format messages as unreadable attachments.

BlackBerry devices always send and can receive PGP protected messages in OpenPGP format. OpenPGP format messages include "-----BEGIN PGP MESSAGE" headers and corresponding footers, also known as PGP armor. All message content, when decrypted successfully on a supported BlackBerry device, appears within the PGP armor.

The BlackBerry Enterprise Server does not process the OpenPGP format message before forwarding it to the recipient BlackBerry device unless the OpenPGP encrypted message includes an attachment. The BlackBerry Enterprise Server reads the encrypted attachment header data and sends the message and the encrypted message key to the BlackBerry device automatically. If the BlackBerry Enterprise Server supports PGP technology but the recipient BlackBerry device does not, the BlackBerry Enterprise Server does not forward the OpenPGP format message to the recipient BlackBerry device. The BlackBerry device notifies the user that it

cannot decrypt the message and that the user can read the message using the computer email application. If the message is a signed OpenPGP format message, the BlackBerry Enterprise Server forwards the message to the recipient BlackBerry device and the BlackBerry device can open the message.

New in this release of the PGP Support Package for BlackBerry devices

| Feature | Description |
|---|---|
| The ability to view encrypted attachments in PGP protected messages | With the BlackBerry Enterprise Server Version 4.1 SP5, the BlackBerry Enterprise Server administrator can use the PGP Allowed Encrypted Attachment Mode IT policy rule to specify the least restrictive mode that the BlackBerry device can use to retrieve PGP encrypted attachment information. |

System requirements

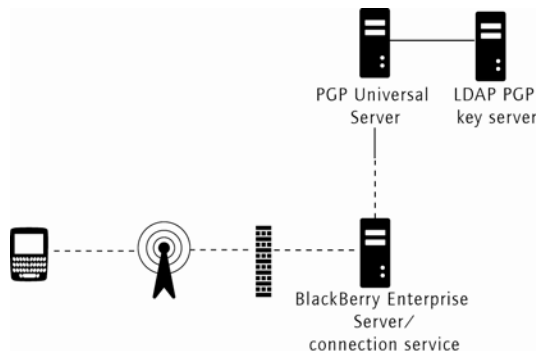
| Messaging and collaboration servers | BlackBerry Enterprise Server | BlackBerry devices |
|---|--|--|
| <ul style="list-style-type: none"> Microsoft® Exchange 5.5, 2000, and 2003 <p>Note: The PGP Universal Server does not support Microsoft Exchange Server 5.5.</p> <ul style="list-style-type: none"> IBM® Lotus® Domino® Version 5.0.3 or later | <ul style="list-style-type: none"> BlackBerry® Enterprise Server Version 4.0 SP2 or later for Microsoft® Exchange BlackBerry® Enterprise Server Version 4.1 or later for IBM® Lotus® Domino® | <p>Java® based BlackBerry devices that run BlackBerry® Device Software Version 4.5 or later</p> <p>Note: Users must add the PGP Support Package for BlackBerry devices to their BlackBerry devices.</p> |

System architecture

The BlackBerry device is designed to use the BlackBerry MDS Connection Service, which resides on the BlackBerry Enterprise Server, to connect to the PGP Universal Server and to external LDAP PGP key servers that the user sets on the BlackBerry device. The BlackBerry MDS Connection Service uses a standard protocol, such as HTTP or TCP/IP, to allow 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

With the PGP Universal Server, users can 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 retrieve PGP keys.



Connection from the BlackBerry device to the PGP Universal Server

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

- The BlackBerry device lets the user download PGP keys to the BlackBerry device over the wireless network. The BlackBerry device stores keys in the PGP Key Store and the PGP Universal Key Cache.
- The BlackBerry device automatically retrieves 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 process, 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.

Note: The BlackBerry Enterprise Server turns on user-level support for sending PGP/MIME formatted messages from the PGP Support Package for BlackBerry devices only after the user activates the BlackBerry device.

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 retrieves the data for the secure email policy 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 data for the secure email policy for a maximum of 24 hours.

Note: The `net_rim_bb_pgp.cod` file enforces the secure email policy on the BlackBerry device. Assign an application control policy for `net_rim_bb_pgp.cod` with the Disposition rule set to Required to prevent the device user from deleting `net_rim_bb_pgp.cod` from the BlackBerry device.

PGP key storage and retrieval

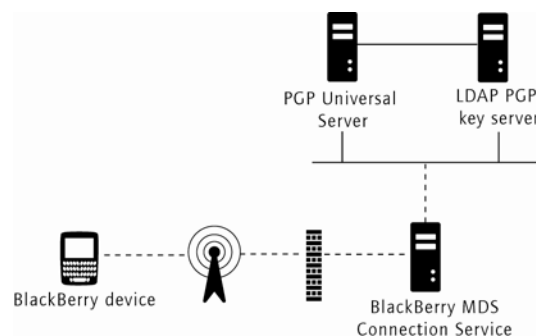
When a user sends a PGP protected message from the BlackBerry device, the PGP Universal Server retrieves PGP public keys on behalf of the BlackBerry device user for the intended message recipients, as needed, and validates the keys before returning them to the user. See “PGP Universal storage” on page 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 BlackBerry device user responds to the prompt by automatically enrolling 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 flash memory on the BlackBerry device
 - refreshes the data for secure email policy, 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 servers for PGP keys

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 BlackBerry MDS Connection Service to contact external LDAP servers that are set to search for the required PGP keys only.



Connection from the BlackBerry device to the external LDAP server

Data transfer process with external LDAP servers for PGP keys

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

- contacts set external LDAP PGP key servers
- searches LDAP server, and obtains the PGP public keys, as needed
- returns the PGP public keys to the BlackBerry device 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 algorithm or the AES algorithm. See the *BlackBerry Enterprise Solution Security Technical Overview* for more information about 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 master encryption key for the BlackBerry device and then decompresses the message.

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

PGP security

From the time the BlackBerry device user sends a message until when the BlackBerry Enterprise Server receives the message, the standard BlackBerry encryption encrypts the message. PGP technology is designed to allow sender-to-recipient authentication and confidentiality. It is also designed to maintain the integrity and privacy of the data from the time that the BlackBerry device user sends a message over the wireless network until when 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 help 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 for BlackBerry devices 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 for BlackBerry devices exists 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 PGP public key of the message recipient.

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 for BlackBerry devices exists on a BlackBerry device, when the BlackBerry device receives a message, the BlackBerry device decrypts the message 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 default setting for the PGP Allowed Content Ciphers IT policy rule 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 allow the BlackBerry device 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 a 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 key lengths for the RSA, DSA, and DH algorithm using BlackBerry Enterprise Server IT policy rules.

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

The BlackBerry device is designed to set the following IT policy rules to 1024 by default to support using a strong PGP public key to protect messages:

- 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 for BlackBerry devices” on page 19 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

How the PGP Universal Server stores the PGP keys 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 can automatically import the key into the PGP key store on the BlackBerry device. The BlackBerry device prompts the user for the key store password when accessing PGP private keys in the PGP 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 PGP key store on the BlackBerry device. 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. |

| Key storage mode | Description | Impact on BlackBerry device user |
|------------------|---|---|
| client key mode | <p>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.</p> <p>Note: The user can create a passphrase when creating the PGP private key.</p> | <p>The user must export the PGP private key from the PGP Desktop and then send the key to the BlackBerry device.</p> <p>When the BlackBerry device receives the email message with the attached PGP private key, the BlackBerry device prompts the user for the passphrase, if one exists, to import the key into the key store on the BlackBerry device. 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.</p> |

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

BlackBerry device storage

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

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

- PGP public and private key pairs
- PGP public keys that the BlackBerry device retrieves from external PGP key servers or imports from messages

The key store on the BlackBerry device stores X.509 certificates that the BlackBerry device downloads 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 delete 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 a user with malicious intent determining the password from the contents of the BlackBerry device memory. 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 security requirements for the key store password. See the *Policy Reference Guide* for more information.

| IT policy rule | Possible use |
|------------------------------------|---|
| 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. |

| IT policy rule | Possible use |
|---|--|
| Disable Key Store Backup | Set this policy rule to prevent the BlackBerry device from backing up 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"> High security: The BlackBerry device prompts users for their key store passwords each time an application tries to access private keys that indicate that they can be used for signing. Medium security: The BlackBerry device prompts users for their key store passwords when an application tries to access private keys that indicate that they can be used for signing for the first time, or when their private key password timeout expires. |
| Minimal Encryption Key Store Security Level | Set to one of the following levels: <ul style="list-style-type: none"> High security: The BlackBerry device prompts users for their key store passwords each time an application tries to access private keys that indicate that they can be used for encryption. Medium security: The BlackBerry device prompts users for their key store passwords when an application tries to access private keys that indicate that they can be used for encryption the first time, or when their private key password timeout expires. |

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

| Setting | Description |
|----------------------------------|---|
| Allow Key Store Backup/Restore | Specify whether to back up and restore PGP keys (private keys and public keys) and symmetric keys in the key store. Note: The BlackBerry device does not permit the user to back up and restore PGP private keys if you have set the Disable Key Store Backup IT policy rule to True. |
| 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 BlackBerry device user cannot select a value that exceeds the value that you specify using the Key Store Password Maximum Timeout IT policy rule. |
| Certificate Service | Define the BlackBerry MDS Connection Service that the PGP key search uses to retrieve 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 revocation status of the PGP key remains valid. |
| Change Password | Type a new key store password. |

Allowing users to change the security level of private keys in the PGP key store on their BlackBerry devices

Users can set the security level at which the PGP key store on their BlackBerry devices stores a private key. The security level controls whether the BlackBerry device prompts users for their key store passwords each time an application tries to access a PGP private key.

Users can choose a security level for a PGP private key on their BlackBerry devices that is higher than what the BlackBerry Enterprise Server administrator sets using the Minimal Encryption Key Store Security Level IT policy rule and the Minimal Signing Key Store Security Level IT policy rule. When users change the security level of the

PGP private key, the BlackBerry device re-encrypts the PGP private key before adding it back to the PGP key store.

Clearing decrypted PGP content from the BlackBerry device

The BlackBerry device automatically turns on the feature for secure garbage collection when the PGP Support Package for BlackBerry devices is installed and the private key of the user is on the BlackBerry device. When feature for 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 clear any caches and make available the memory associated with unused, sensitive application data
- automatically overwrites the memory that the memory cleaner application makes available when it runs

The memory cleaner application is designed to delete unreferenced or cached decrypted content from the BlackBerry device, including content from the PGP application, PGP key store, content protection cache, address book cache, 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 | Possible solution |
|--|--|
| Delete decrypted content from BlackBerry device memory when the BlackBerry device is in its holster. | Set the Force Memory Clean When Holstered IT policy rule to True. |
| Delete 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 application 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 cleaner application to run while their BlackBerry devices are in their holsters, 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 BlackBerry MDS Connection Service to enable wireless synchronization of PGP keys and their status from external LDAP servers for PGP keys.

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 server that you set in the BlackBerry Manager, or on external LDAP servers for PGP keys that the user sets on the BlackBerry device only. The BlackBerry MDS Connection Service can contact these LDAP servers to download and verify the authenticity and status of a PGP key.

Types of LDAP server connections

When a BlackBerry device user searches for PGP keys, the BlackBerry device uses the connection type specified in the LDAP server properties on the BlackBerry device. The BlackBerry device retrieves the PGP key using an unprotected LDAP connection, by default.

The BlackBerry device is designed to use an LDAP or LDAPS connection when the user searches for PGP keys using the BlackBerry device. The BlackBerry device user can specify the connection type for external LDAP servers for PGP keys on the BlackBerry device. Refer to <KB article TBD> for information about how to change the connection type for the external LDAP server for your organization.

Set an external LDAP server for your organization

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 number on which the default LDAP server listens. Note: If you typed a host name, you must type a port number. |
| LDAP User ID | Type a user ID if the LDAP server requires simple authentication. |
| LDAP Password | Type a password if the LDAP server requires simple authentication. |
| LDAP Password (confirm) | Type the authentication password again. |
| 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 servers for PGP keys

The PGP Support Package for BlackBerry devices includes a feature for PGP key searches. BlackBerry device users that are not enrolled with the PGP Universal Server can query set external LDAP servers for PGP keys, such as the PGP Global Directory, on their BlackBerry devices 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 let PGP users find the public keys of other PGP users with whom they want to exchange encrypted email messages.

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

Securing connections to external LDAP servers

The user can set an SSL/TLS option on the BlackBerry device to require the BlackBerry device to use an LDAPS connection in proxy mode. The BlackBerry device does not support end-to-end LDAPS connections.

The BlackBerry device automatically uses port 636 for LDAPS connections and port 389 for LDAP connections to external LDAP servers for PGP keys.

Revocation status for PGP keys

BlackBerry device users can check the revocation status of PGP keys from their BlackBerry devices when they receive a digitally signed message or a 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 PGP key store on their BlackBerry devices and from the PGP Key Search screen.

The BlackBerry device uses the BlackBerry MDS Connection Service to request and retrieve either the revocation status of the PGP key or an updated PGP key (if the revocation status has expired) from a set external LDAP server for PGP keys. If the BlackBerry device retrieves an updated PGP key, it updates the PGP key store on the BlackBerry device.

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

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 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 security options for PGP keys

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

| Action | Procedure |
|---|-------------------------|
| Explicitly trust the PGP key. | Click Trust . |
| Delete the trust associated with an explicitly trusted PGP key. | Click Distrust . |
| Invalidate the status of a PGP key. | Click Revoke . |
| Delete a PGP key from the PGP key store on the | Click Delete . |

| Action | Procedure |
|---|--------------------------------------|
| Explicitly trust the PGP key. | Click Trust . |
| Delete the trust associated with an explicitly trusted PGP key. | Click Distrust . |
| BlackBerry device. | |
| 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 for BlackBerry devices installed, a BlackBerry device on which a user has completed enrollment with the PGP Universal Server automatically applies the secure email policies that the PGP Universal Server administrator designs to all email messages 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 its IT policy. See “BlackBerry Enterprise Server IT policy rules for the PGP Support Package for BlackBerry devices” on page 19 for more information.

Digital signing and encryption options on PGP protected messages

The PGP Support Package for BlackBerry devices includes digital signing and encryption options that the user can specify on their BlackBerry devices when they send messages. When a 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 download 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 downloading a PGP key

If the user responds to the BlackBerry device prompt by choosing to manually download 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 retrieve 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 X.509 certificate to encrypt a message

When a user sends a message from a BlackBerry device with the PGP Support Package for BlackBerry devices and the S/MIME Support Package for BlackBerry devices installed, and that user has enrolled and authenticated with the PGP Universal Server, if each of the message recipients' PGP keys contains an X.509 certificate, and the PGP Universal Server policy allows, 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.
4. The BlackBerry Enterprise Server deletes the standard BlackBerry encryption and sends the S/MIME encrypted message to the recipient.

Using an X.509 certificate to validate a digital signature

If the PGP Support Package for BlackBerry devices and the S/MIME Support Package for BlackBerry devices 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 email message on that BlackBerry device, the BlackBerry device checks whether the message sender's PGP key contains an X.509 certificate. If a certificate exists, the BlackBerry device prompts the user to choose whether to extract the certificate from the PGP key and import the certificate into the key store on the BlackBerry device.

When the BlackBerry device receives a message with an X.509 certificate attachment or a PGP key that contains an X.509 certificate that is already in the key store on the BlackBerry device, the BlackBerry device 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 PGP key store on the BlackBerry device 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 for BlackBerry devices permits BlackBerry device users to send and receive email and PIN messages in plain text format. You can set BlackBerry Enterprise Server IT policy rules to prevent PGP enabled BlackBerry device users from sending messages in plain text format.

| 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.

Viewing attachments in PGP encrypted messages

The BlackBerry Enterprise Server administrator can use the PGP Allowed Encrypted Attachment Mode IT policy rule to specify the least restrictive mode that the BlackBerry device can use to retrieve PGP (OpenPGP (RFC 2440) and PGP/MIME (RFC 3156) message formatting) encrypted attachment information.

When a user receives an OpenPGP encrypted message that includes an attachment, the BlackBerry Enterprise Server reads the attachment header data and sends the message and the encrypted message key to the BlackBerry device automatically.

The PGP Support Package for BlackBerry devices supports receiving OpenPGP messages from a desktop email client only where the client is Microsoft® Outlook®. Microsoft Outlook preserves the file extension of the attachment. BlackBerry devices with the PGP Support Package for BlackBerry devices can view encrypted attachments with the original file extension, or the original file extension with .asc added. In other words, the PGP Support Package for BlackBerry devices supports the formats *filename.xxx* or *filename.xxx.asc*, but not the format *filename.asc*.

If a user receives an encrypted attachment that the BlackBerry device with the PGP Support Package for BlackBerry devices cannot open, the message might have been sent from an email account that does not support attachments in encrypted messages. Users cannot open an attachment in a PGP protected message on the BlackBerry device that an IBM® Lotus Notes® client working with PGP Desktop Professional, or that a PGP Universal® Server has encrypted in PGP (OpenPGP) format and renamed Attachment1.pgp.

When a user receives a PGP/MIME encrypted message that includes an attachment on their BlackBerry device, depending on the setting of the PGP Allowed Encrypted Attachment Mode IT policy rule, the following actions can occur automatically when the user opens the message, or when the user requests them manually.

1. The BlackBerry device sends the message key and a request for the attachment header data to the BlackBerry Enterprise Server.
2. The BlackBerry Enterprise Server uses the message key to decrypt the message and access the attachment header data.
3. The BlackBerry Enterprise Server sends the attachment header data to the BlackBerry device.
4. The BlackBerry device processes the attachment header data with the message and displays the associated attachment information so that the user can select the attachment for viewing.

When the user tries to view an attachment that is encrypted using PGP/MIME or OpenPGP on the BlackBerry device, the following actions occur:

1. The BlackBerry device sends the message key and a request for the attachment data to the BlackBerry Enterprise Server.
2. The BlackBerry Enterprise Server uses the message key to decrypt the message and access the attachment data that corresponds to the attachment header data.
3. The BlackBerry Enterprise Server decrypts the attachment and sends the rendered attachment data to the BlackBerry device.
4. The BlackBerry device displays the attachment.

Note: Turn on content protection to protect the decrypted attachment data that the BlackBerry device stores.

Download 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.

1. On the BlackBerry device, in the message list, click a received PGP protected message.

2. Perform one of the following actions:

| Action | Procedure |
|--|---|
| Download 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 PGP key store on the message recipient's BlackBerry device.) | > Click Import PGP Key . |

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

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

A PGP key can contain an S/MIME X.509 certificate that the PGP Universal Server has digitally signed. When a user with the PGP Support Package for BlackBerry devices and the S/MIME Support Package for BlackBerry devices installed on a BlackBerry device adds the PGP key to the BlackBerry device, the BlackBerry device performs the following actions:

- stores the PGP key
- prompts the user to choose whether to store the S/MIME X.509 certificate in the key store

The BlackBerry Enterprise Server and the BlackBerry device automatically synchronize specific certificate information between them over the wireless network when the BlackBerry device user adds an S/MIME X.509 certificate to or deletes an S/MIME X.509 certificate from the BlackBerry device.

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 a configuration for an external LDAP server 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 verified the message digital signature. |
|  | The BlackBerry device could not verify the message digital signature. |

| Icon | Description |
|---|---|
|  | 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 for BlackBerry devices

The following BlackBerry Enterprise Server IT policy rules apply only to BlackBerry devices on which the PGP Support Package for BlackBerry devices 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 |

| IT policy rule | Description |
|------------------------------------|--|
| PGP Universal Policy Cache Timeout | specifies the maximum amount of time, in hours, that the BlackBerry device caches the PGP Universal Server policy before retrieving it from the PGP Universal Server again |
| PGP Universal Server Address | specifies the host name of the PGP Universal Server that your organization uses to enforce a secure email policy and access PGP keys and key status |

See the *Policy Reference Guide* for more information.

Granular PGP policy conditions that the PGP Support Package for BlackBerry devices supports

| Message property | Operators |
|---|---|
| Message body | <ul style="list-style-type: none"> • Is • Contains • Begins with • Ends with • Matches pattern |
| Message has attachment with file name that | <ul style="list-style-type: none"> • Is • Contains • Begins with • Ends with • Matches pattern |
| Message header <header> (where <header> is "subject", "importance", or "sensitivity") | <ul style="list-style-type: none"> • Is • Contains • Begins with • Ends with • Matches pattern |
| Message size | <ul style="list-style-type: none"> • Is • Is greater than • Is less than |
| Recipient Email Address | <ul style="list-style-type: none"> • Is • Contains • Begins with • Ends with • Matches pattern |

| Message property | Operators |
|----------------------|--|
| Recipient domain | <ul style="list-style-type: none">• Is• Contains• Begins with• Ends with• Matches pattern• Is in subdomain of |
| Sender Domain | <ul style="list-style-type: none">• Is• Contains• Begins with• Ends with• Matches pattern |
| Sender Email Address | <ul style="list-style-type: none">• Is• Contains• Begins with• Ends with• Matches pattern |

Note: The PGP Support Package for BlackBerry devices does not currently support message properties and operators that are designed to control dictionaries, mailing lists, and user groups.

Related resources

| Resource | Information |
|--|---|
| <i>BlackBerry Enterprise Server System Administration Guide</i> | <ul style="list-style-type: none"> • generating and changing master encryption keys • turning on encryption options • 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 organization's 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 turned on |
| <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 for BlackBerry devices • 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 Enterprise Solution security |

Part number: 10975680 Version 1

©2008 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, Domino, and Lotus Notes are trademarks of International Business Machine Corporation. Java is a trademark of Sun Microsystems, Inc. Microsoft and Outlook are trademarks of Microsoft Corporation. PGP is a trademark of PGP Corporation. 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.