

PGP Support Package for BlackBerry Smartphones

Version: 5.0

Security Technical Overview

Contents

| | |
|--|-----------|
| 1 BlackBerry Enterprise Solution security | 3 |
| 2 New in this release | 4 |
| 3 System requirements: PGP Support Package for BlackBerry smartphones | 5 |
| 4 Extending messaging security using PGP encryption | 6 |
| Security features of the PGP Support Package for BlackBerry smartphones | 6 |
| Processing PGP protected messages on a BlackBerry Enterprise Server | 7 |
| What happens when a BlackBerry device protects a message using PGP encryption | 7 |
| Process flow: Sending an email message using PGP encryption | 8 |
| Process flow: Receiving a PGP encrypted message | 9 |
| Encryption algorithms that the BlackBerry device supports for PGP encryption | 10 |
| Making PGP encryption mandatory | 10 |
| 5 Configuring the BlackBerry Enterprise Solution to use a PGP Universal Server | 11 |
| Enrolling and authenticating a BlackBerry device with a PGP Universal Server | 11 |
| How a BlackBerry device uses the email policy of a PGP Universal Server | 12 |
| PGP policy conditions on the PGP Universal Server that the PGP Support Package for BlackBerry smartphones supports | 12 |
| 6 PGP public keys and PGP private keys | 15 |
| Retrieving PGP keys from a PGP Universal Server or LDAP servers | 15 |
| Configuring the BlackBerry MDS Connection Service to connect to an LDAP server that stores PGP public keys | 16 |
| Protecting connections to LDAP servers | 16 |
| Where a BlackBerry device stores PGP keys | 17 |
| How a BlackBerry device protects the PGP key store | 17 |
| Protecting the PGP private key on a BlackBerry device | 17 |
| Security levels that help protect the PGP private key on a BlackBerry device | 18 |
| Accessing PGP private keys on a BlackBerry device | 18 |
| How a user can access the PGP private key on a BlackBerry device if the PGP Universal Server stores the PGP private key using server key mode | 18 |
| How a user can access the PGP private key on a BlackBerry device if the PGP Universal Server stores the PGP private key using guarded key mode | 19 |

| | |
|--|-----------|
| How a user can access the PGP private key on a BlackBerry device if the PGP Universal Server stores the PGP private key using client key mode..... | 19 |
| Changing the minimum key length that a BlackBerry device can use..... | 20 |
| Searching for PGP keys on a BlackBerry device..... | 20 |
| Checking the revocation status of a PGP key on a BlackBerry device..... | 20 |
| 7 Extending messaging security to attachments..... | 22 |
| Viewing PGP encrypted attachments on a BlackBerry device..... | 22 |
| Process flow: Viewing an attachment in a PGP encrypted message or S/MIME-encrypted message..... | 22 |
| Process flow: Viewing an attachment that is encrypted using S/MIME encryption, PGP/MIME encryption, or OpenPGP encryption..... | 23 |
| 8 Permitting a BlackBerry device to use a password for PGP encryption..... | 24 |
| 9 Using an X.509 certificate to encrypt a message or validate a digital signature..... | 25 |
| 10 Deleting decrypted PGP data from a BlackBerry device..... | 26 |
| 11 IT policy rules that apply to the PGP Support Package for BlackBerry smartphones..... | 27 |
| 12 Related resources..... | 28 |
| 13 Glossary..... | 29 |
| 14 Legal notice..... | 32 |

BlackBerry Enterprise Solution security

1

The BlackBerry® Enterprise Solution consists of various products and components that are designed to extend your organization's communication methods to BlackBerry devices. The BlackBerry Enterprise Solution is designed to help protect data that is in transit at all points between a BlackBerry device and the BlackBerry® Enterprise Server. To help protect data that is in transit over the wireless network, the BlackBerry Enterprise Server and BlackBerry device use symmetric key cryptography to encrypt the data sent between them. The BlackBerry Enterprise Solution is designed to prevent third parties, including wireless service providers, from accessing your organization's potentially sensitive information in a decrypted format.

The BlackBerry Enterprise Solution uses confidentiality, integrity, and authenticity, which are principles for information security, to help protect your organization from data loss or alteration.

| Principles | Description |
|-----------------|--|
| confidentiality | The BlackBerry Enterprise Solution uses symmetric key cryptography to help make sure that only intended recipients can view the contents of email messages. |
| integrity | <p>The BlackBerry Enterprise Solution uses symmetric key cryptography to help protect every email message that the BlackBerry device sends and to help prevent third parties from decrypting or altering the message data.</p> <p>Only the BlackBerry Enterprise Server and BlackBerry device know the value of the keys that they use to encrypt messages and recognize the format of a decrypted and decompressed message. The BlackBerry Enterprise Server or BlackBerry device reject a message automatically if it is not encrypted with keys that they recognize as valid.</p> |
| authenticity | Before the BlackBerry Enterprise Server sends data to the BlackBerry device, the BlackBerry device authenticates with the BlackBerry Enterprise Server to prove that the BlackBerry device knows the device transport key that is used to encrypt data. |

New in this release

2

This document describes the security of the PGP® Support Package for BlackBerry® smartphones and the features that the PGP Support Package 5.0 for BlackBerry smartphones and BlackBerry® Enterprise Server 5.0 SP1 or later support, unless otherwise stated.

| Feature | Description |
|---|---|
| complete text of an encrypted or signed email message included when a user replies to or forwards the email message | <p>A BlackBerry device can retrieve the complete text of the original encrypted or signed email message when a user replies to or forwards the email message. By default, a BlackBerry device does not retrieve the complete text of the original encrypted or signed message when a user replies to or forwards the email message.</p> <p>To configure this feature, you can use the PGP More All and Send Mode IT policy rule or the Message truncation mode option on the BlackBerry device.</p> |
| support for certificates with private keys (.pfx files) | <p>A user can import a certificate that includes private keys from an Advanced Security SD card or an email message into the NV store of the BlackBerry device flash memory.</p> |

System requirements: PGP Support Package for BlackBerry smartphones

3

- BlackBerry® Enterprise Server 4.1 SP3 or later for Microsoft® Exchange or BlackBerry® Enterprise Server 4.1 SP3 or later for IBM® Lotus® Domino®
- Microsoft® Exchange Server or IBM Lotus Domino server that the latest version of the BlackBerry® Enterprise Server in your organization's environment supports
- Java® based BlackBerry devices that are running BlackBerry® Device Software 4.5 or later
- PGP® Universal Server 2.0.2 or later
- PGP® Universal Satellite 2.0.2 or later or PGP® Desktop Professional 9.0.2 or later

Extending messaging security using PGP encryption

4

You can extend messaging security for the BlackBerry® Enterprise Solution and permit a BlackBerry device user to send and receive PGP® protected email messages and PGP protected PIN messages on a BlackBerry device. The BlackBerry Enterprise Solution supports the OpenPGP format and PGP/MIME format on the BlackBerry device.

To extend messaging security, you must instruct the BlackBerry device user to install the PGP® Support Package for BlackBerry® smartphones on the BlackBerry device and to transfer the PGP private key of the BlackBerry device user to the BlackBerry device. The BlackBerry device user can use the PGP private key to digitally sign, encrypt, and send PGP protected messages from the BlackBerry device. If a BlackBerry device user does not install the PGP Support Package for BlackBerry smartphones, the BlackBerry device displays an error message when the BlackBerry device user tries to open PGP protected messages.

To require the BlackBerry device user to use PGP encryption when forwarding or replying to messages, you can configure the PGP Force Digital Signature IT policy rule and the PGP Force Encrypted Messages IT policy rule.

The PGP Support Package for BlackBerry smartphones is designed to support encoding and decoding Unicode messages and permits PGP encryption using keys or passwords. The PGP Support Package for BlackBerry smartphones permits the BlackBerry device to encrypt PGP protected email messages or PGP protected PIN messages using a password that the sender and recipient both know.

For more information about the OpenPGP format, see RFC2440. For more information about the PGP/MIME format, see RFC3156.

Security features of the PGP Support Package for BlackBerry smartphones

| Feature | Description |
|---|--|
| ability to retrieve a PGP® key and check the revocation status of the PGP key over the wireless network | The PGP® Support Package for BlackBerry® smartphones can retrieve the PGP key and check the revocation status of a PGP key from a PGP® Universal Server or external LDAP server. |
| ability to encrypt outgoing messages using PGP encryption | A user can encrypt email messages and PIN messages using PGP encryption and send the messages from a BlackBerry device. |
| ability to decrypt incoming PGP encrypted messages | A user can decrypt PGP encrypted email messages and PIN messages that a BlackBerry device receives. |
| ability to sign outgoing messages using PGP private keys | A user can sign email messages and PIN messages using the user's PGP private keys, and send the messages from a BlackBerry device. |
| ability to verify PGP signatures | A user can verify the PGP signatures on email messages and PIN messages that a BlackBerry device receives. |

| Feature | Description |
|---|--|
| ability to view encrypted attachments in PGP encrypted messages | The PGP Support Package for BlackBerry smartphones can retrieve information about PGP encrypted attachments from PGP encrypted email messages. |
| support for PGP encryption using a password | A user can use a password for PGP encryption when the user sends PGP encrypted messages from a BlackBerry device. |
| support for the email policy of a PGP Universal Server | The PGP Support Package for BlackBerry smartphones is designed to use the email policy of a PGP Universal Server to determine whether a BlackBerry device must sign, encrypt, or sign and encrypt an email message. |
| support for Unicode messages | <p>A user can view, forward, and reply to PGP encrypted messages that contain Unicode characters on a BlackBerry device. The BlackBerry device decodes the Unicode characters and displays the messages. The user can also view certificates that contain Unicode characters.</p> <p>The user can encrypt and send PGP encrypted messages that contain Unicode characters on the BlackBerry device. The BlackBerry device encodes the messages to include the information that an email application requires to view the Unicode characters.</p> |

Processing PGP protected messages on a BlackBerry Enterprise Server

A user can send a PGP® protected message in PGP/MIME format or OpenPGP format to a BlackBerry® device. If the BlackBerry® Enterprise Server and the BlackBerry device support PGP technology, the BlackBerry Enterprise Server processes PGP/MIME messages, and the BlackBerry device can decrypt the PGP/MIME formatted messages that it receives. If the BlackBerry® Enterprise Server, the BlackBerry device, or both do not support PGP technology, the BlackBerry Enterprise Server does not process PGP/MIME messages, and the BlackBerry device receives PGP/MIME formatted messages as unreadable attachments.

OpenPGP formatted messages include ""BEGIN PGP MESSAGE"" headers and ""END PGP MESSAGE"" footers. When a BlackBerry device that supports PGP technology decrypts an OpenPGP formatted message, the BlackBerry device displays all message content in the headers and footers.

What happens when a BlackBerry device protects a message using PGP encryption

After you configure the BlackBerry® Enterprise Solution to support PGP® encryption, when a user composes an email message or a PIN message, the user can choose one of the following options on a BlackBerry device:

- attach PGP keys from the PGP key store on the BlackBerry device and send the keys as .asc file attachments

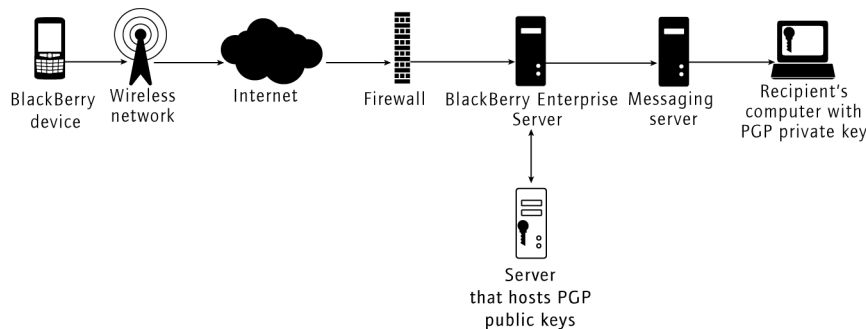
- encrypt the PGP message with a password
- send the message as plain text
- sign, encrypt, or sign and encrypt the message using PGP encryption

When a user chooses to sign, encrypt, or sign and encrypt the message, the BlackBerry device searches for a valid PGP key for the recipient in the PGP key store, the PGP® Universal Server, or any available LDAP servers. A valid PGP key is a key that is trusted, is not revoked or expired, and has a strong public key. If the BlackBerry device finds a valid PGP key, the BlackBerry device signs, encrypts, or signs and encrypts the message before it sends the message.

If the BlackBerry device does not find a valid PGP key, the BlackBerry device provides the user with options to not send the message, download a valid PGP key manually, or send the message in unencrypted form. The user can send the message in unencrypted form only if the email policy of the PGP Universal Server permits and you changed the value of the PGP Force Encrypted Messages IT policy rule to No.

If the user downloads a PGP key for the intended recipient manually, the BlackBerry device displays search criteria that the user can change. The BlackBerry device tries to retrieve the PGP key from an LDAP server. If the BlackBerry device finds the PGP key, the BlackBerry device signs, encrypts, or signs and encrypts the message before it sends the message.

Process flow: Sending an email message using PGP encryption

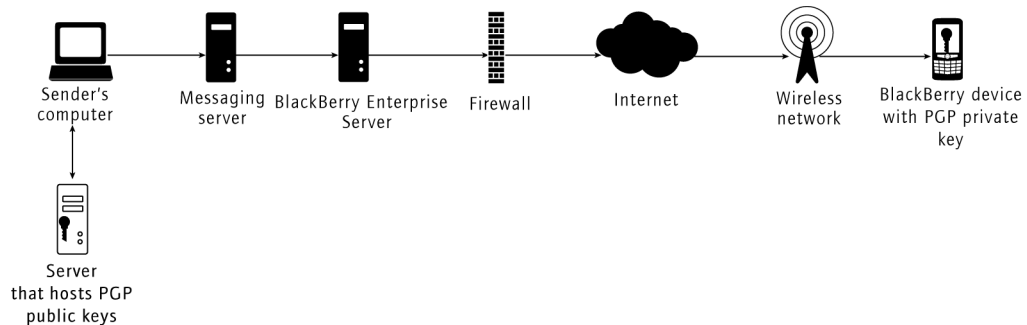


If a sender installs the PGP® Support Package for BlackBerry® smartphones on a BlackBerry device, the BlackBerry device encrypts outgoing email messages.

1. The BlackBerry device performs the following actions:
 - a. uses the BlackBerry MDS Connection Service to retrieve the PGP public key of the recipient from the PGP® Universal Server or LDAP server
 - b. encrypts the email message using the PGP public key of the recipient
 - c. uses BlackBerry transport layer encryption to encrypt the PGP encrypted message
 - d. sends the message that is encrypted using BlackBerry transport layer encryption and PGP encryption to the BlackBerry® Enterprise Server

2. The BlackBerry Enterprise Server removes the BlackBerry transport layer encryption and sends the PGP encrypted message to the recipient.

Process flow: Receiving a PGP encrypted message



If a recipient installs the PGP® Support Package for BlackBerry® smartphones on a BlackBerry device, the BlackBerry device decrypts incoming PGP encrypted messages.

1. A sender uses the PGP technology on the email application to encrypt an email message using the PGP public key of the recipient.
2. The BlackBerry® Enterprise Server performs the following actions:
 - a. retrieves the email message from the messaging server
 - b. uses BlackBerry transport layer encryption to encrypt the PGP encrypted message
 - c. sends the email message encrypted using BlackBerry transport layer encryption and PGP encryption to the BlackBerry device
3. The BlackBerry device performs the following actions:
 - a. decrypts the BlackBerry transport layer encryption and stores the PGP encrypted message in the flash memory of the BlackBerry device
 - b. decrypts the PGP encrypted message using the PGP private key of the recipient and displays the contents of the email message when the recipient opens the email message on the BlackBerry device

Encryption algorithms that the BlackBerry device supports for PGP encryption

When you turn on PGP® encryption, the default value of the PGP Allowed Content Ciphers IT policy rule specifies that a BlackBerry® device can use any of the following encryption algorithms to encrypt email messages and PIN messages: AES-256, AES-192, AES-128, CAST-128, or Triple DES-168. You can change the value to use a subset of the encryption algorithms if your organization's security policies require it.

The PGP public key of the recipient indicates which encryption algorithm the recipient's email application supports, and the BlackBerry device is designed to use that encryption algorithm. By default, if the PGP public key of the recipient does not include a list of encryption algorithms, the BlackBerry device encrypts the email message or PIN message using Triple DES.

Making PGP encryption mandatory

By default, the PGP® Support Package for BlackBerry® smartphones permits a user to send and receive plain-text email messages and PIN messages on a BlackBerry device. You can configure the Disable Message Normal Send IT policy rule and Disable Peer-to-Peer Normal Send IT policy rule to prevent the user from sending plain-text messages from the BlackBerry device.

To require the user to use PGP encryption when forwarding or replying to messages, you can configure the PGP Force Digital Signature IT policy rule and PGP Force Encrypted Messages IT policy rule.

You must make sure that any IT policy rules that you configure do not conflict with the email policy of the PGP® Universal Server.

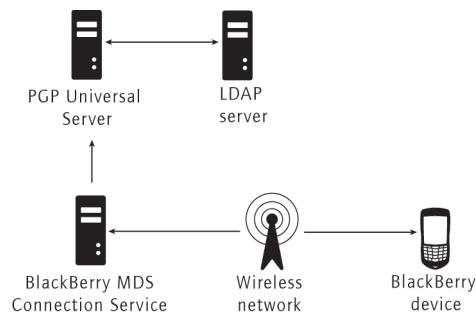
Configuring the BlackBerry Enterprise Solution to use a PGP Universal Server

5

If your organization's environment includes a PGP® Universal Server, you can connect the BlackBerry® Enterprise Server to the PGP Universal Server so that a BlackBerry device can send and receive PGP protected messages.

To configure the BlackBerry Enterprise Server to connect to the PGP Universal Server, you must configure the PGP Universal Server Address IT policy rule. When the BlackBerry device receives the PGP Universal Server address, the BlackBerry device prompts the user to enroll the BlackBerry device and authenticate with the PGP Universal Server.

The BlackBerry MDS Connection Service can connect to the PGP Universal Server and LDAP servers to search for and retrieve PGP keys.



Enrolling and authenticating a BlackBerry device with a PGP Universal Server

A user can enroll a BlackBerry® device and authenticate with a PGP® Universal Server using credentials such as the user's email address or the user's PGP user name and passphrase. You can specify how the user must authenticate with the PGP Universal Server using the PGP Universal Enrollment Method IT policy rule.

Before 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.

When the user enrolls and authenticates with the PGP Universal Server from the BlackBerry device, the BlackBerry device retrieves the following items from the PGP Universal Server over the wireless network:

- PGP keys of the user
- email policy of the PGP Universal Server
- PGP keys of recipients, when the user sends a PGP protected message

The BlackBerry device stores the PGP keys and credentials in the BlackBerry device memory. The BlackBerry device also caches the email policy of the PGP Universal Server. If the BlackBerry device resets, the credentials authenticate the BlackBerry device to the PGP Universal Server automatically.

After the user enrolls with the PGP Universal Server, the user can download PGP keys to the BlackBerry device and verify the authenticity and status of the PGP keys. The BlackBerry device and PGP Universal Server can use LDAP to search for and retrieve the PGP keys. The BlackBerry device connects to the PGP Universal Server each time the user sends or receives a PGP protected message on the BlackBerry device.

How a BlackBerry device uses the email policy of a PGP Universal Server

A BlackBerry device is designed to use the email policy of a PGP® Universal Server to determine whether to sign, encrypt, or sign and encrypt an email message that it sends. The BlackBerry device uses the minimum security requirements of the email policy and any additional security requirements that the user applies to the message when the user sends it.

If the BlackBerry device cannot retrieve PGP keys for a message recipient and the user sends the message to the PGP Universal Server, the PGP Universal Server can further process the message, using the default email policy, to determine what action to take on the message.

The BlackBerry device retrieves the data for the email policy of the PGP Universal Server at intervals that you can configure using the PGP Universal Policy Cache Timeout IT policy rule. By default, the BlackBerry device caches the email policy for a maximum of 24 hours.

For more information about sending messages to the PGP Universal Server, see the documentation for the PGP Universal Server.

PGP policy conditions on the PGP Universal Server that the PGP Support Package for BlackBerry smartphones supports

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

| Message property | Description |
|------------------|---|
| message body | <ul style="list-style-type: none"> • Is • Contains • Begins with |

| Message property | Description |
|--|---|
| | <ul style="list-style-type: none"> • 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 one of 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 |
| 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 |

| Message property | Description |
|----------------------|---|
| sender email address | <ul style="list-style-type: none"><li data-bbox="529 256 596 282">• Is<li data-bbox="529 296 665 322">• Contains<li data-bbox="529 336 691 362">• Begins with<li data-bbox="529 376 672 402">• Ends with<li data-bbox="529 416 736 442">• Matches pattern |

For more information about the policy conditions, see the documentation for the PGP® Universal Server.

PGP public keys and PGP private keys

6

The PGP® Support Package for BlackBerry® smartphones uses public key cryptography with PGP public keys and PGP private keys.

| Key | Description |
|-----------------|--|
| PGP public key | <p>The PGP Support Package for BlackBerry smartphones uses the PGP public key of the recipient to encrypt outgoing email messages and the PGP public key of the sender to verify digital signatures on incoming email messages.</p> <p>The PGP public key is designed so that recipients and senders can distribute and access the key without compromising it. The PGP public key is stored typically on the PGP® Universal Server or an LDAP server.</p> |
| PGP private key | <p>The PGP Support Package for BlackBerry smartphones uses the PGP private key of the sender to digitally sign outgoing email messages and the PGP private key of the recipient to decrypt incoming email messages.</p> <p>To make sure that security is not compromised, you must make sure that private key information remains private to the key owner. The BlackBerry device stores the PGP private key.</p> |

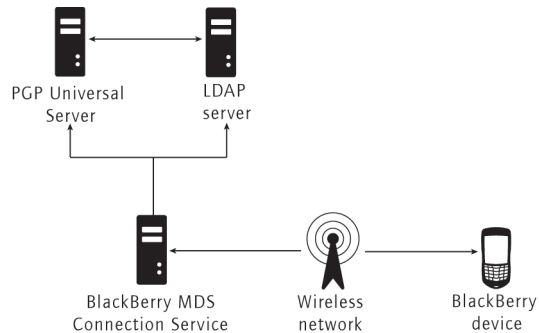
Retrieving PGP keys from a PGP Universal Server or LDAP servers

If your organization's environment includes a PGP® Universal Server, the administrator of the PGP Universal Server can configure the email policy of the PGP Universal Server. After a user installs the PGP® Support Package for BlackBerry® smartphones, a BlackBerry device can retrieve and enforce the email policy of the PGP Universal Server for all email messages that the user sends.

The BlackBerry device is designed to use the BlackBerry MDS Connection Service to connect to the PGP Universal Server or any LDAP server that a user specifies on the BlackBerry device or that you specify using the BlackBerry Administration Service. The BlackBerry MDS Connection Service uses standard protocols, such as HTTP and TCP/IP, to permit the BlackBerry device to retrieve PGP public keys, PGP key status, and X.509 certificate status from the PGP Universal Server or an LDAP server over the wireless network. The BlackBerry MDS Connection Service can connect to LDAP servers using LDAPS.

Configuring the BlackBerry MDS Connection Service to connect to an LDAP server that stores PGP public keys

To prevent a user from enrolling and authenticating with the PGP® Universal Server, you or the user can configure the BlackBerry® MDS Connection Service to retrieve PGP public keys on behalf of a BlackBerry device. The BlackBerry MDS Connection Service retrieves and verifies the authenticity and status of PGP public keys before it sends the PGP public keys to the BlackBerry device.



If you configure the BlackBerry MDS Connection Service to connect to an LDAP server, the BlackBerry MDS Connection Service performs the following actions after the user sends or receives a PGP protected message:

- connects to the LDAP server that stores the PGP public keys
- searches the LDAP server and, if necessary, obtains the PGP public keys
- returns the PGP public keys to the user

Protecting connections to LDAP servers

By default, a BlackBerry® device retrieves PGP® keys using an unprotected LDAP connection. You or a user can configure a BlackBerry device to retrieve certificates from an LDAP server using a protected (LDAPS) connection. For example, if the BlackBerry device can retrieve PGP keys from an LDAP server that is external to your organization's network, you or the user can use an LDAPS connection.

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

By default, the BlackBerry device uses port 389 for LDAP connections and port 636 for LDAPS connections.

Where a BlackBerry device stores PGP keys

After a user enrolls and authenticates with the PGP® Universal Server from a BlackBerry® device, the BlackBerry device retrieves the user's PGP keys. When the user sends a PGP protected message, the BlackBerry device retrieves the PGP public keys of the recipients.

The BlackBerry device stores PGP keys in the PGP key store and in the PGP Universal key cache that is in the BlackBerry device memory. The PGP Universal key cache is a nonpersistent, transient key store on the BlackBerry device.

The BlackBerry device stores the PGP public keys that it retrieves from the PGP Universal Server in the PGP Universal key cache. By default, the PGP Universal key cache stores the PGP public keys for 24 hours and retrieves them from the PGP Universal Server when required.

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

- PGP key pairs of the user
- PGP public keys that the BlackBerry device retrieves from LDAP servers or imports from email messages

The BlackBerry device also stores S/MIME X.509 certificates that the BlackBerry device retrieves from LDAP servers or imports from email messages in the BlackBerry device key store.

How a BlackBerry device protects the PGP key store

A BlackBerry® device protects the PGP® key store using a key store password. A user must provide the key store password to add and delete PGP public keys, PGP private keys, and S/MIME X.509 certificates that are stored on a BlackBerry device.

The BlackBerry device stores a SHA-256 hash of the key store password. The hash of the key store password is designed to prevent a potentially malicious user from determining the key store password using the contents of the BlackBerry device memory. When a user types the key store password, the BlackBerry device performs a one-way hash function on the typed characters using SHA-256, and then it compares the hashed input to the stored hashed password.

Protecting the PGP private key on a BlackBerry device

You or a user can specify a security level to help protect the PGP® private key in the PGP key store on a BlackBerry® device. The security level determines whether a BlackBerry device prompts the user for the key store password each time an application tries to access a PGP private key.

You can specify the security level using the Minimal Encryption Key Store Security Level IT policy rule and Minimal Signing Key Store Security Level IT policy rule.

A user can specify the security level on a BlackBerry device. The user can specify a security level for a PGP private key on the BlackBerry device that is higher than what you specify using the Minimal Encryption Key Store Security Level IT policy rule and Minimal Signing Key Store Security Level IT policy rule. When the user changes the security level of the PGP private key, the BlackBerry device encrypts the PGP private key again before the BlackBerry device adds the key back to the PGP key store.

Security levels that help protect the PGP private key on a BlackBerry device

| Security level | Description |
|----------------|--|
| high | A BlackBerry® device prompts a user for the key store password each time an application tries to retrieve the PGP® private key. |
| medium | A BlackBerry device prompts a user for the key store password when an application tries to retrieve the private key for the first time or when the timeout period for the key store password expires. The BlackBerry device does not prompt the user for the key store password if an application makes a subsequent attempt to retrieve the PGP private key while the timeout period is valid. |
| low | A BlackBerry device does not prompt a user when an application tries to retrieve the PGP private key. |

Accessing PGP private keys on a BlackBerry device

The PGP® Universal Server can store PGP public keys and PGP private keys using key storage modes. The key storage mode that the PGP Universal Server uses to store PGP keys impacts how a user can access the PGP private keys from a BlackBerry® device.

For more information about the key storage modes, see the documentation for the PGP Universal Server.

How a user can access the PGP private key on a BlackBerry device if the PGP Universal Server stores the PGP private key using server key mode

If the PGP® Universal Server stores the PGP private key using server key mode, the PGP Universal Server stores a user's PGP public key and PGP private key.

The user can download the PGP private key to a BlackBerry® device without a passphrase and can import the key into the PGP key store on the BlackBerry device automatically.

The BlackBerry device prompts the user for the key store password when it retrieves the PGP private key from the PGP key store so that the BlackBerry device can sign or decrypt messages.

How a user can access the PGP private key on a BlackBerry device if the PGP Universal Server stores the PGP private key using guarded key mode

If the PGP® Universal Server stores the PGP private key using guarded key mode, the PGP Universal Server stores a user's PGP public key and a passphrase-protected copy of the user's PGP private key. The user creates the passphrase when the user generates the PGP private key.

The user can download the PGP private key to a BlackBerry® device. The BlackBerry device prompts the user for the passphrase before the BlackBerry device imports 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 it retrieves the PGP private key from the PGP key store so that the BlackBerry device can sign or decrypt messages.

An administrator of the PGP Universal Server can turn on guarded key mode for a user in the administrative console of the PGP Universal Server.

How a user can access the PGP private key on a BlackBerry device if the PGP Universal Server stores the PGP private key using client key mode

If the PGP® Universal Server stores the PGP private key using client key mode, a PGP® Desktop application stores and manages a user's PGP private keys. The PGP Universal Server stores the user's PGP public key. The user can create a passphrase when the user generates the PGP private key.

The user must export the PGP private key from the PGP Desktop application and send the key to a BlackBerry® device in an email message.

After the BlackBerry device receives the email message with the attached PGP private key, the BlackBerry device prompts the user for the passphrase, if necessary, before it imports 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 it retrieves the PGP private key from the PGP key store so that the BlackBerry device can sign or decrypt messages.

An administrator of the PGP Universal Server can turn on client key mode for a user in the administrative console of the PGP Universal Server.

Changing the minimum key length that a BlackBerry device can use

The key length (also known as the key size) of a PGP® public key or PGP private key determines the key strength. The larger the PGP public key and PGP private key, the stronger the PGP key pair. The key lengths of the PGP public key and PGP private key are the same.

By default, a BlackBerry® device uses a minimum key length of 1024 bits for the DH algorithm, DSA algorithm, and RSA® algorithm. You can change the minimum key lengths to meet the security requirements of your organization using the following IT policy rules:

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

The maximum key length that the BlackBerry device supports for the RSA algorithm and DH algorithm is 4096 bits. The maximum key length that the BlackBerry device supports for the DSA algorithm is 1024 bits.

For more information about the IT policy rules, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Searching for PGP keys on a BlackBerry device

The PGP® Support Package for BlackBerry® smartphones permits a user to search for PGP® keys. A user who is not enrolled with a PGP® Universal Server can search LDAP servers that are external to your organization (for example, the PGP® Global Directory) for PGP keys using the first name, last name, or email address of the PGP key subject. The user can download PGP keys from the search results.

While the user composes an email message, the BlackBerry device searches for and retrieves PGP keys that are not on the BlackBerry device. The BlackBerry device uses the email addresses of the intended recipients to search for PGP keys.

When the user searches for a PGP key, the user can specify whether the BlackBerry device must prompt the user to download the revocation status of the PGP key before the BlackBerry device can retrieve the PGP key and add it to the PGP key store.

The user should validate PGP keys that the BlackBerry device retrieves from an LDAP server that is external to your organization using the fingerprints of the PGP keys.

For more information about the PGP Global Directory, visit keyserver.pgp.com.

Checking the revocation status of a PGP key on a BlackBerry device

In the following situations, a user can check the revocation status of a PGP® key to determine whether the PGP key is revoked:

- when receiving a signed message or signed and encrypted message on a BlackBerry® device
- before sending a message to a recipient who has an email application that supports PGP encryption
- when searching for PGP keys

The user can also check the revocation status of a PGP key from the PGP key store.

The BlackBerry device uses the BlackBerry MDS Connection Service to request and retrieve the revocation status of the PGP key from an LDAP server. If the BlackBerry device retrieves an updated PGP key, it updates the PGP key store on the BlackBerry device.

Extending messaging security to attachments

7

The BlackBerry® Enterprise Server supports attachments in PGP® encrypted messages and S/MIME-encrypted messages. It also permits a user to view encrypted attachments on a BlackBerry device. You can use the S/MIME Allowed Encrypted Attachment Mode IT policy rule and the PGP Allowed Encrypted Attachment Mode IT policy rule to specify the least restrictive mode that a BlackBerry device can use to retrieve attachment information that is PGP encrypted or S/MIME encrypted. The BlackBerry device supports OpenPGP format and PGP/MIME format for PGP encryption.

Viewing PGP encrypted attachments on a BlackBerry device

The PGP® Support Package for BlackBerry® smartphones supports OpenPGP messages that a user sends from Microsoft® Outlook® only. Microsoft Outlook preserves the file extension of the attachment. After the user installs the PGP Support Package for BlackBerry smartphones, a BlackBerry device can display encrypted attachments with the original file extension, or the original file extension with .asc added. The PGP Support Package for BlackBerry smartphones 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 smartphones cannot open, the sender might have sent the message from an email application that does not support attachments in encrypted messages. The user cannot open an attachment in a PGP protected message on the BlackBerry device if the attachment was encrypted using IBM® Lotus Notes® and PGP® Desktop Professional. A recipient also cannot open an attachment that a PGP® Universal Server encrypted in OpenPGP format and renamed Attachment1.pgp.

Process flow: Viewing an attachment in a PGP encrypted message or S/MIME-encrypted message

The S/MIME Allowed Encrypted Attachment Mode IT policy rule or PGP® Allowed Encrypted Attachment Mode IT policy rule determines how a BlackBerry® device responds when it receives a PGP/MIME encrypted message or S/MIME-encrypted message that contains an attachment. These rules determine whether the following actions occur automatically when the user opens the email message, or whether the user must request the actions manually.

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

Process flow: Viewing an attachment that is encrypted using S/MIME encryption, PGP/MIME encryption, or OpenPGP encryption

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 email message and access the attachment data that corresponds to the data in the attachment header. The BlackBerry Enterprise Server decrypts the attachment and sends the rendered attachment data to the BlackBerry device.
3. The BlackBerry device displays the attachment.

To help protect the decrypted attachment data that the BlackBerry device stores, you can turn on content protection.

Permitting a BlackBerry device to use a password for PGP encryption 8

A BlackBerry® device that is running BlackBerry® Device Software 4.6 or later and the PGP® Support Package for BlackBerry® smartphones can use a password, which both the sender and recipient know, to encrypt email messages or PIN messages using PGP encryption.

To configure a BlackBerry device to use a password for PGP encryption, you can use the PGP Allowed Encryption Types IT policy rule to permit the sender and recipient to use a password, a PGP public key, or both.

The sender and recipient share the password manually. When the sender or recipient types the password to encrypt or decrypt the PGP encrypted message, the BlackBerry device combines the password with random bytes to generate a new encryption key.

Using an X.509 certificate to encrypt a message or validate a digital signature

9

A user can install both the PGP® Support Package for BlackBerry® smartphones and the S/MIME Support Package for BlackBerry® smartphones on a BlackBerry device. If the user enrolled and authenticated with the PGP® Universal Server, each of the PGP keys of the message recipients contains an X.509 certificate. If the email policy of the PGP Universal Server permits, the BlackBerry device can encrypt the message using S/MIME encryption.

When the user receives an email message on the BlackBerry device, the BlackBerry device checks whether the PGP key of the message sender contains an X.509 certificate. If a certificate exists, the BlackBerry device stores the PGP key and provides the user with an option to choose to extract the certificate from the PGP key and import the certificate into the BlackBerry device key store.

When the BlackBerry device receives a message with an X.509 certificate attachment or when a PGP key that contains an X.509 certificate is already in the BlackBerry device key store, the BlackBerry device uses the certificate to verify the digital signature of the message.

When the user adds an S/MIME X.509 certificate to or deletes an S/MIME X.509 certificate from the BlackBerry device, a BlackBerry® Enterprise Server and the BlackBerry device synchronize certificate information over the wireless network automatically.

If the BlackBerry device stores a private key for the PGP public key and S/MIME X.509 certificate, the PGP private key is associated with the S/MIME X.509 certificate.

For more information about S/MIME encryption, see the *S/MIME Support Package for BlackBerry smartphones Security Technical Overview*.

Deleting decrypted PGP data from a BlackBerry device

10

A BlackBerry® device turns on the Java® garbage collection process when a user installs the PGP® Support Package for BlackBerry® smartphones and downloads the PGP private key to the BlackBerry device.

When the BlackBerry device turns on the garbage collection process, the BlackBerry device also runs the memory cleaner application. The memory cleaner application is designed to delete unreferenced or cached decrypted data from the BlackBerry device, including data from the PGP application, PGP key store, content protection cache, contact list cache, PGP key search, and BlackBerry device clipboard.

You or a user can configure the memory cleaner application to permanently delete decrypted data from the BlackBerry device memory when the BlackBerry device is inserted in a holster, is idle, or after a specified period of time.

For more information about the garbage collection process and the memory cleaner application, see the *BlackBerry Enterprise Solution Security Technical Overview*.

IT policy rules that apply to the PGP Support Package for BlackBerry smartphones

11

The following IT policy rules apply to only a BlackBerry® device that the PGP® Support Package for BlackBerry® smartphones is installed on:

- PGP Allowed Content Ciphers
- PGP Allowed Encrypted Attachment Mode
- PGP Allowed Encryption Types
- PGP Blind Copy Address
- PGP Force Digital Signature
- PGP Force Encrypted Messages
- PGP Minimum Strong DH Key Length
- PGP Minimum Strong DSA Key Length
- PGP Minimum Strong RSA Key Length
- PGP More All and Send Mode
- PGP Universal Enrollment Method
- PGP Universal Policy Cache Timeout
- PGP Universal Server Address

You must make sure that that any IT policy rules that you configure do not conflict with the email policy of the PGP® Universal Server.

For more information about the IT policy rules, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Related resources

12

| Resource | Description |
|--|--|
| <i>BlackBerry Enterprise Server Administration Guide</i> | <ul style="list-style-type: none"> generating and changing device transport keys configuring extended messaging encryption managing security protecting lost or stolen BlackBerry® devices configuring IT policy rules |
| <i>BlackBerry Enterprise Server Policy Reference Guide</i> | <ul style="list-style-type: none"> understanding BlackBerry® Enterprise Server IT policy rules and application control policy rules using IT policies and application control policies |
| <i>BlackBerry Enterprise Solution Security Technical Overview</i> | <ul style="list-style-type: none"> understanding how the BlackBerry Enterprise Server is designed to help protect data that is in transit between a BlackBerry device and a BlackBerry Enterprise Server or your organization's LAN managing security settings for all BlackBerry devices understanding the algorithms that the RIM® Cryptographic API provides understanding the TLS and WTLS standards that the RIM Cryptographic API supports understanding the memory scrub process that occurs on the BlackBerry device when content protection is turned on |
| user guide for the BlackBerry device | <ul style="list-style-type: none"> installing the PGP® Support Package for BlackBerry® smartphones managing PGP keys on computers and BlackBerry devices configuring PGP options for digitally signing and encrypting messages sending and receiving PGP protected messages |
| www.blackberry.com/security | <ul style="list-style-type: none"> understanding BlackBerry® Enterprise Solution security |

Glossary

13

Advanced Security SD card

An Advanced Security SD card is a media card that complies with the Advanced Security SD Extension Specification that the SD Association developed. BlackBerry devices support only microSD cards that use the MCEX security system.

AES

Advanced Encryption Standard

API

application programming interface

BlackBerry device key store

The BlackBerry device key store stores certificates, key pairs, and PGP® keys that a BlackBerry device can use to help protect messages, access web sites, and connect to an enterprise Wi-Fi® network. To access the items in the key store, the user must type a key store password.

BlackBerry device memory

The BlackBerry device memory consists of the NV store, flash memory, RAM, on-board device memory, and BlackBerry device key store.

BlackBerry MDS

BlackBerry® Mobile Data System

BlackBerry transport layer encryption

BlackBerry transport layer encryption (formerly known as standard BlackBerry encryption) uses a symmetric key encryption algorithm to help protect data that is in transit between a BlackBerry device and the BlackBerry® Enterprise Server when the data is outside an organization's firewall.

content protection

Content protection helps protect user data on a locked BlackBerry device by encrypting the user data using the content protection key and ECC private key.

content protection key

The device transport key (formerly known as the master encryption key) is unique to a BlackBerry device. The BlackBerry device and BlackBerry® Enterprise Server use the device transport key to encrypt the message keys.

device transport key

The device transport key (formerly known as the master encryption key) is unique to a BlackBerry device. The BlackBerry device and BlackBerry® Enterprise Server use the device transport key to encrypt the message keys.

DH

Diffie-Hellman

DSA

Digital Signature Algorithm

ECC private key

The ECC private key decrypts the data that a BlackBerry device received when the BlackBerry device was locked.

flash memory

The flash memory is an internal file system on a BlackBerry device that stores application data and user data.

HTTP

Hypertext Transfer Protocol

IT policy

An IT policy consists of various IT policy rules that control the security features and behavior of BlackBerry devices, BlackBerry enabled devices, the BlackBerry® Desktop Software, and the BlackBerry® Web Desktop Manager.

IT policy rule

An IT policy rule permits you to customize and control the actions that BlackBerry devices, BlackBerry enabled devices, the BlackBerry® Desktop Software, and the BlackBerry® Web Desktop Manager can perform.

LAN

local area network

LDAP

Lightweight Directory Access Protocol

LDAPS

Lightweight Directory Access Protocol over SSL

messaging server

A messaging server sends and processes messages and provides collaboration services, such as updating and communicating calendar and address book information.

message keys

The message keys encrypt the data that is sent to and from a BlackBerry device.

MIME

Multipurpose Internet Mail Extensions

NV

nonvolatile

NV store

The NV store is a nonvolatile store that persists in flash memory on a BlackBerry device. Only the operating system of the BlackBerry device can write to it. Third-party applications cannot write to the NV store.

PGP/MIME

PGP® Multipurpose Internet Mail Extensions

PIN

personal identification number

RFC

Request for Comments

S/MIME

Secure Multipurpose Internet Mail Extensions

SHA

Secure Hash Algorithm

SSL

Secure Sockets Layer

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is a set of communication protocols that is used to transmit data over networks, such as the Internet.

TLS

Transport Layer Security

Triple DES

Triple Data Encryption Standard

WTLS

Wireless Transport Layer Security

Legal notice

14

©2010 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™ and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

IBM, Domino, Lotus, and Lotus Notes are trademarks of International Business Machines Corporation. Java is a trademark of Sun Microsystems, Inc. Microsoft, Microsoft Exchange Server, and Outlook are trademarks of Microsoft Corporation. PGP is a trademark of PGP Corporation. RSA is a trademark of RSA Security. Wi-Fi is a trademark of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

The BlackBerry smartphone and other devices 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 the U.S. and in various countries around the world. Visit www.rim.com/patents for a list of RIM (as hereinafter defined) patents.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at www.blackberry.com/go/docs is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party web sites (collectively the "Third Party Products and Services"). RIM does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by RIM of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL RIM BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF RIM OR ANY AFFILIATES OF RIM HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with RIM's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with RIM's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by RIM and RIM assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with RIM.

Certain features outlined in this documentation require a minimum version of BlackBerry® Enterprise Server, BlackBerry® Desktop Software, and/or BlackBerry® Device Software.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Canada

Research In Motion UK Limited
Centrum House
36 Station Road
Egham, Surrey TW20 9LF
United Kingdom

Published in Canada