

S/MIME Support Package Security

Version 4.2

Technical Overview

Contents

S/MIME Support Package.....	3
New in this release	3
System requirements.....	4
System architecture	4
PKI component support	5
Desktop-based certificate management	5
Certificate management over the wireless network	6
Setting the default PKI component connections.....	6
BlackBerry Enterprise Solution security	8
Standard BlackBerry encryption.....	8
S/MIME Support Package security	8
Certificates	8
Certificate authorities	9
S/MIME certificate types.....	9
S/MIME encryption.....	10
Enabling S/MIME messaging.....	11
Searching for and validating S/MIME certificates	12
S/MIME certificate search.....	12
S/MIME certificate revocation status.....	13
Storing S/MIME certificates and private keys.....	13
BlackBerry device storage	13
Certificate storage on a smart card	15
Cleaning decrypted S/MIME content from the BlackBerry device	15
Managing S/MIME certificates and private keys	16
View S/MIME certificate details.....	16
Set S/MIME certificate security options	17
Sending S/MIME protected messages	18
Message signing and encryption options	18
Verify a certificate or certificate chain status from a received S/MIME protected message	19
Fetch or import a certificate from a received S/MIME protected message	19
Add a certificate server configuration from a received S/MIME protected message	20
S/MIME message icons	20
BlackBerry Enterprise Server IT policy rules for the S/MIME Support Package	21
Related resources.....	22

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

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

S/MIME Support Package

The S/MIME Support Package is designed to enable BlackBerry device users who are already sending and receiving S/MIME messages using their computer email application to send and receive S/MIME protected messages using their BlackBerry devices. The S/MIME Support Package is designed to work with S/MIME email clients including Microsoft® Outlook® and Microsoft Outlook Express, and with popular PKI components, including Netscape®, Entrust® Authority™ Security Manager version 5 and later, and Microsoft CAs.

The S/MIME Support Package includes tools for obtaining digital certificates and transferring them to the BlackBerry device. This means that BlackBerry devices with the S/MIME Support Package installed can decrypt messages that are encrypted using S/MIME encryption and users can read the decrypted messages on their BlackBerry devices, and that users can sign, encrypt, and send S/MIME messages from their BlackBerry devices. Without the S/MIME Support Package the BlackBerry Enterprise Server sends a message to the BlackBerry device in which the message body includes a statement that the S/MIME message cannot be decrypted.

The S/MIME Support Package includes support for the following features:

- certificate and private key synchronization and management using the Certificate Synchronization Manager included in the BlackBerry Desktop Software
- encrypting and decrypting messages, including PIN messages, verifying digital signatures, and digitally signing outgoing messages
- searching for and retrieving certificates and certificate status over the wireless network using PKI protocols
- smart cards on BlackBerry devices

New in this release

Feature	Description
extended BlackBerry Enterprise Server platform support for S/MIME message processing	BlackBerry Enterprise Server for IBM Lotus Domino Version 4.1.2 or later supports the same S/MIME message processing features as BlackBerry Enterprise Server for Microsoft Exchange.
message classification	You can set message classifications to require users to sign, encrypt, or sign and encrypt email messages sent from their S/MIME enabled BlackBerry devices using the BlackBerry Enterprise Server Version 4.1.2 or later.
improved certificate fetching	When a user chooses to sign or sign and encrypt an email message, the BlackBerry device automatically searches for and downloads a certificate for a recipient when the user adds that recipient to the message.

Feature	Description
additional certificate management options	<p>You can set IT policy rules in BlackBerry Enterprise Server Version 4.1.2 or later to</p> <ul style="list-style-type: none"> • specify whether or not the BlackBerry device displays a warning when the user receives a signed message on the BlackBerry device in which the email address of the sender does not appear in the certificate used to sign the message • specify whether or not the BlackBerry device should display warnings and visual indications if the user receives an email message that is signed using a certificate with stale status • specify the domain name used for the email addresses contained in certificates issued within your organization if your organization's certificates contain a long-lived email address but users typically send email messages from a shorter-lived email address with the same username component and a different domain component

System requirements

The S/MIME Support Package Version 4.2 and later supports the following software and BlackBerry devices.

Messaging and collaboration servers	BlackBerry Enterprise Server	BlackBerry devices
<ul style="list-style-type: none"> • Microsoft Exchange 5.5, 2000 and 2003 Servers • IBM® Lotus® Domino® server version 5.0.3 or later 	<ul style="list-style-type: none"> • BlackBerry Enterprise Server Version 2.1 Service Pack 3A or later for Microsoft Exchange • BlackBerry Enterprise Server Version 4.1.2 or later for IBM Lotus Domino 	<ul style="list-style-type: none"> • Java™ based BlackBerry devices that run BlackBerry Device Software Version 4.2 or later <p>Note: Users must install the S/MIME Support Package on the BlackBerry device and add the Certificate Synchronization Manager to the BlackBerry Desktop Manager.</p>

IT policy requirements

In the BlackBerry Enterprise Server Version 3.6 for Microsoft Exchange, you must import the S/MIME IT policy rules (as a separate IT policy template file) to support S/MIME messaging. In the BlackBerry Enterprise Server Version 4.0 or later for Microsoft Exchange or IBM Lotus Domino, the BlackBerry Manager automatically includes the S/MIME IT policy rules.

System architecture

The S/MIME Support Package requires the wireless network system architecture to support the following server connections:

- a physical connection (using a serial or USB port) from the BlackBerry device to the computer to enable the Certificate Synchronization Manager to download the private key of the user on the BlackBerry device
- a wireless connection established by the BlackBerry Mobile Data System™ (BlackBerry MDS™) Connection Service (connection service), which resides on the BlackBerry Enterprise Server, designed to enable the BlackBerry device to connect to the PKI

PKI component support

The S/MIME Support Package is designed to support the following PKI components:

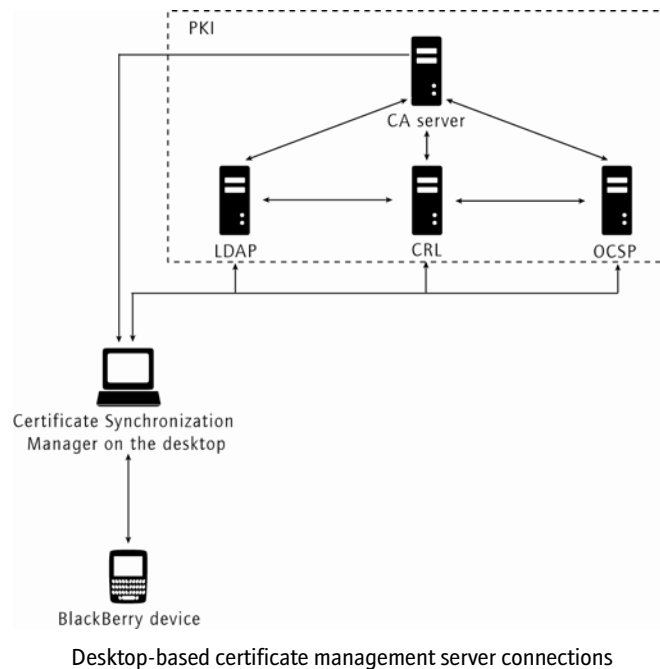
- LDAP: The BlackBerry device and the Certificate Synchronization Manager use LDAP to search for and download certificates.
- OCSP: The BlackBerry device and the Certificate Synchronization Manager use OCSP to check the revocation status of a certificate on demand.
- CRL: The BlackBerry device and the Certificate Synchronization Manager obtain the most recent revocation status of certificates, which is published at a frequency set on the CA server, from a CRL.

Certificate servers

Server type	Description
CA	<ul style="list-style-type: none"> • stores certificates and certificate status • publishes certificates to LDAP servers • publishes certificate revocation lists to CRL servers
CRL	<ul style="list-style-type: none"> • stores lists of revoked certificates that the CA publishes at a specified frequency
LDAP	<ul style="list-style-type: none"> • stores certificates and certificate status • provides certificates to the BlackBerry device
OCSP	<ul style="list-style-type: none"> • verifies certificate revocation status on demand

Desktop-based certificate management

The Certificate Synchronization Manager on the BlackBerry Desktop Manager enables users to search for certificates, download the certificates to their BlackBerry device, and verify the authenticity and status of certificates. The CA server(s), the PKI server(s), and the Certificate Synchronization Manager send certificate information between them.

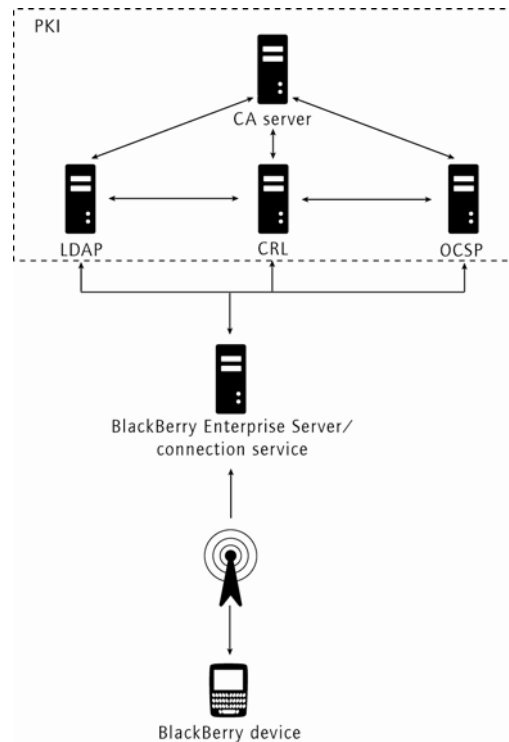


Certificate management over the wireless network

The following BlackBerry Enterprise Server versions support data transfer over the wireless network between the BlackBerry device and the PKI components:

- BlackBerry Enterprise Server Version 3.5 or later for Microsoft Exchange
- BlackBerry Enterprise Server Version 4.1.2 or later for IBM Lotus Domino

The connection service uses standard Internet protocols to enable BlackBerry devices with the S/MIME Support Package installed and turned on to retrieve S/MIME certificates and S/MIME certificate status from the PKI server(s) over the wireless network.



Certificate management server connections over the wireless network

Setting the default PKI component connections

You can set the default LDAP, OCSP and CRL connections on the BlackBerry Enterprise Server so that all BlackBerry devices on the BlackBerry Enterprise Server can connect to the PKI.

Set an LDAP server

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

5. Set the following fields:

Field	Description
Host Name	Type the name of the default LDAP server.
Port	Type the port number on which the default LDAP server listens. Note: If you typed a host name, you must type a port number.
Default Server Base Query	Type the default base query for the default LDAP server, using %20 for spaces. 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 LDAP lookup results.

Set an OCSP server

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

Field	Description
Default Responder URL	Type the default OCSP responder URL.
Use Device Responders	Enables the OCSP handler to query OCSP responders that the user can specify on the BlackBerry device (in Options > Security Options > Certificate Servers). To prevent the BlackBerry device using an OCSP responder URL other than the default value that you set, do not set this field.
Use Certificate Extension Responders	Enables the OCSP handler to use the OCSP responder extensions in a certificate when the BlackBerry device performs an OCSP lookup. To prevent the BlackBerry device using an OCSP responder URL other than the default value that you set, do not set this field.

Set a CRL server

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

Field	Description
Default CRL Server URL	Type the CRL server URL.

Users can add and set LDAP, OCSP, and CRL servers from the BlackBerry device. See the *S/MIME Support Package User Guide Supplement* for more information.

BlackBerry Enterprise Solution security

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

Standard BlackBerry encryption

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

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

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

S/MIME Support Package security

From the time the BlackBerry device user sends a message until the BlackBerry Enterprise Server receives the message, the standard BlackBerry encryption encrypts the message. S/MIME technology is designed to enable sender-to-recipient authentication and confidentiality and help maintain data integrity and privacy from the time that the BlackBerry device user sends a message until the message recipient decodes and reads the message.

S/MIME technology relies on public key cryptography (using private and public keys) to provide the following components of a security solution:

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

Certificates

Certificates are digital documents that contain information about the certificate subject. Certificates use the hierarchical structure of the X.509 standard DN syntax to define the certificate subject attributes.

Common certificate subject attributes

Attribute	Description	Example
C	Country name	C=United States
CN	Common name	CN=Amy Krul
E	Email address	E=akrul@rim.com
L	Locality	L=San Francisco
O	Organization name	O=Research In Motion
OU	Organizational unit name	OU=Pixelvibe Division
ST	State or province	ST=California

A certificate binds the association between the certificate subject identity and the public key of the certificate subject, providing a level of trust in the authenticity of the association.

Certificate authorities

A CA issues certificates. For the BlackBerry device to trust the certificate, the BlackBerry device must trust the CA that issued the certificate. This trust relationship is indicated by a certificate chain from the certificate of the user to the certificate of the CA and continuing back through the certificates of any other authorizing entities connected to the certificate of the user. The original certificate in a chain is called a root certificate.

When the user installs the S/MIME Support Package on the BlackBerry device and adds the Certificate Synchronization Manager to their BlackBerry Desktop Manager, the Certificate Synchronization Manager prompts the BlackBerry device user to download their existing S/MIME private key from their computer to their BlackBerry device. When the BlackBerry device user downloads the private key, it automatically downloads the corresponding certificate and all certificates in the chain as well. By using this mechanism, your organization can distribute trusted root certificates to all BlackBerry device users so that they can use the PKI system of your organization. The user can choose to trust a selected certificate only, or trust the root certificate to trust an entire certificate chain.

The S/MIME Support Package supports cross-certification between CAs. A CA can issue a certificate that contains the name and public key of another CA, which enables users from one organization to chain to a root certificate in another organization.

S/MIME certificate types

The S/MIME Support Package uses public key cryptography with the following certificates:

Certificate type	Description	File extension
Certificates with private keys (personal certificates)	S/MIME uses the corresponding private key of the certificate to <ul style="list-style-type: none"> decrypt a message encrypted with the public key in the certificate produce a digital signature 	<ul style="list-style-type: none"> .pfx .p12
Certificates of other people	S/MIME uses the public key in the certificate to <ul style="list-style-type: none"> encrypt messages that the certificate subject receives verify digital signatures that the certificate subject produces 	<ul style="list-style-type: none"> .cer .der .cert .crt
Intermediate certificates	A root CA can issue intermediate certificates that in turn issue end entity certificates to facilitate certificate distribution within an organization. An intermediate certificate is one of the certificates in a certificate chain, but it does not identify a root CA.	<ul style="list-style-type: none"> .p7b .p7c .key
Root certificates	A root CA creates root certificates. RIM provides authentic root certificates with the BlackBerry Device Software so that users do not have to verify the root certificate authenticity. Note: If a BlackBerry device user receives a root certificate from a source that the BlackBerry device does not trust, the BlackBerry device user should manually verify the root certificate authenticity (for example, by verifying the certificate thumbprint) before trusting it.	

BlackBerry device users can view and manage certificates stored in the Certificate Synchronization Manager. See the *S/MIME Support Package User Guide Supplement* for more information.

S/MIME encryption

If the S/MIME Support Package exists on a BlackBerry device, when the BlackBerry device user sends a message, the BlackBerry device encrypts the message once with S/MIME encryption and once with standard BlackBerry encryption using the following process:

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

If the S/MIME Support Package exists on a BlackBerry device, when the user receives a message on the BlackBerry device, the BlackBerry device encrypts the S/MIME message with standard BlackBerry encryption and then decrypts the message using the following process:

1. The BlackBerry Enterprise Server receives the S/MIME protected message.
2. If the message is signed-only or weakly encrypted, the BlackBerry Enterprise Server encrypts the message a second time with S/MIME encryption if you have turned on this option using the BlackBerry Manager. See "Enabling additional S/MIME messaging options" on page 11 for more information.
3. The BlackBerry Enterprise Server uses standard BlackBerry encryption to encrypt the S/MIME data.
4. The BlackBerry Enterprise Server sends the encrypted message to the BlackBerry device.
5. The BlackBerry device removes the BlackBerry standard encryption and stores the S/MIME encrypted message.
6. When the user opens the message on the BlackBerry device, the BlackBerry device decrypts the S/MIME encrypted message and renders the message content.

S/MIME encryption algorithms

The BlackBerry device is designed to support the use of a strong algorithm for S/MIME encryption. When you turn on S/MIME encryption on the BlackBerry Enterprise Server, the S/MIME Allowed Content Ciphers IT policy rule default setting specifies that the BlackBerry device can use any of the supported algorithms (other than the two weakest RC2 algorithms, RC2 (64-bit) and RC2 (40-bit)) to encrypt S/MIME messages.

You can set the S/MIME Allowed Content Ciphers IT policy rule to encrypt S/MIME messages using any of AES (256-bit), AES (192-bit), AES (128-bit), CAST (128-bit), RC2 (128-bit), Triple DES, RC2 (64-bit), and RC2 (40-bit).

If the BlackBerry device has previously received a message from the intended recipient, the BlackBerry device is designed to recall which content ciphers the recipient can support, and use one of those ciphers. The BlackBerry device encrypts the message using Triple DES by default if it does not know the decryption capabilities of the recipient.

S/MIME certificates

When a user sends an encrypted message from the BlackBerry device, the BlackBerry device uses the S/MIME certificate of the message recipient to encrypt the message.

When a BlackBerry device user receives a signed message, the BlackBerry device uses the S/MIME certificate of the message sender to verify the message signature.

S/MIME private keys

When a user sends a signed message from the BlackBerry device, the BlackBerry device uses the S/MIME private key of the user to digitally sign the message.

When a user receives an encrypted message, the BlackBerry device uses the private key of the user to decrypt the message.

S/MIME key strength

The length (size) of an S/MIME public or private key determines its strength. You can enforce a minimum strength level by setting the minimum RSA, DSA, DH, and ECC algorithm key lengths using BlackBerry Enterprise Server IT policy rules. The following table lists the default minimum and maximum key lengths for the supported public key algorithms.

Algorithm	Default minimum strong key length (bits)	Maximum key length (bits)
DH	1024	4096
ECC	163	571
DSA	1024	1024
RSA	1024	4096

The BlackBerry device is designed to support using a strong S/MIME public key to protect messages by

- setting the S/MIME Minimum Strong ECC Key Length IT policy rule to 163
- setting the following IT policy rules to 1024:
 - S/MIME Minimum Strong DH Key Length
 - S/MIME Minimum Strong DSA Key Length
 - S/MIME Minimum Strong RSA Key Length

See "BlackBerry Enterprise Server IT policy rules for the S/MIME Support Package" on page 21 for more information.

Enabling S/MIME messaging

S/MIME messaging is turned off by default on the BlackBerry Enterprise Server. You must set the Enable S/MIME Message Processing option in the BlackBerry Manager to turn on S/MIME messaging on the BlackBerry Enterprise Server.

After you turn on S/MIME messaging on the BlackBerry Enterprise Server, when a user installs the S/MIME Support Package on their BlackBerry device and selects the Certificate Synchronization option during their BlackBerry desktop software installation process, the BlackBerry Manager automatically turns on S/MIME messaging for the user.

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

Enabling additional S/MIME messaging options

In BlackBerry Enterprise Server Version 4.0 and later, you can set additional S/MIME encryption types in the BlackBerry Manager.

BlackBerry Enterprise Server version	Encryption option	Description
<ul style="list-style-type: none"> • BlackBerry Enterprise Server for Microsoft Exchange Version 4.0 and later • BlackBerry Enterprise Server for IBM Lotus Domino Version 4.1.2 and later 	Enable S/MIME encryption of signed and weakly encrypted messages	Requires the BlackBerry Enterprise Server to encrypt messages with S/MIME encryption a second time when users receive weakly encrypted or signed but unencrypted S/MIME messages on their S/MIME enabled BlackBerry devices

BlackBerry Enterprise Server version	Encryption option	Description
<ul style="list-style-type: none"> BlackBerry Enterprise Server for Microsoft Exchange Version 4.1 and later BlackBerry Enterprise Server for IBM Lotus Domino Version 4.1.2 and later 	Send S/MIME messages in clear-signed format	When a user sends a signed S/MIME message from the BlackBerry device, the text of the message appears in the message body, followed by the digital signature. A message recipient whose mail client does not support S/MIME can still read the text of the message, but cannot verify the digital signature.
	Remove attachment data from signed S/MIME messages	<p>The BlackBerry Enterprise Server removes attachment data from any signed-only S/MIME messages it receives so that users on the BlackBerry Enterprise Server can receive more message text on their BlackBerry devices.</p> <p>The BlackBerry device cannot verify the S/MIME digital signature of the message after the BlackBerry Enterprise Server removes the attachment data from the message.</p>
	Use the Pkcs7 MIME type	<p>The BlackBerry Enterprise Server sends encrypted S/MIME messages using a newer MIME content-type, in accordance with PKCS#7, instead of the default legacy MIME content-type.</p> <p>If a BlackBerry device user sends an S/MIME encrypted message to a mail system that does not support the MIME content-type used the mail system does not render the S/MIME protected message properly.</p>
<ul style="list-style-type: none"> BlackBerry Enterprise Server for Microsoft Exchange Version 4.1.2 and later BlackBerry Enterprise Server for IBM Lotus Domino Version 4.1.2 and later 	Enable message classification	<p>The BlackBerry Enterprise Server requires the BlackBerry device to use specific S/MIME protected messaging levels according to the classification level that the user selects when composing a message on the BlackBerry device.</p> <p>You can use the Message Classification IT policy rule to add a set of message classifications available to users to apply to email messages sent using the BlackBerry Enterprise Server. Message classifications can require users to sign, encrypt, or sign and encrypt messages.</p>

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

Searching for and validating S/MIME certificates

S/MIME certificate search

The S/MIME Support Package includes an S/MIME Certificate Search application on the BlackBerry device. BlackBerry device users can query set LDAP certificate servers, download S/MIME certificates from the search results, and add certificates to the BlackBerry device key store. The BlackBerry device automatically searches for and downloads certificates that are not on the BlackBerry device based on the email addresses of the specified

recipients while the user is composing an email message. BlackBerry device users can perform manual searches based on the first name, last name, and email address of the S/MIME certificate subject.

S/MIME certificate revocation status

Users can perform S/MIME certificate revocation status checks when they receive a signed or signed and encrypted message on their BlackBerry devices, and before they send messages to S/MIME certificate subjects. Users can also check the revocation status of an S/MIME certificate from their BlackBerry device key stores and in the S/MIME Certificate Search screen.

The BlackBerry device uses the connection service to request and retrieve the S/MIME certificate revocation status from either an OCSP or CRL server. The user can request the status of a single certificate or an entire certificate chain.

On the BlackBerry device, in the S/MIME Certificate Search Options screen, users can set whether they are prompted to fetch the S/MIME certificate revocation status when they download an S/MIME certificate and add it to the BlackBerry device key store.

Storing S/MIME certificates and private keys

BlackBerry device storage

The S/MIME key store, which is part of the BlackBerry device flash memory, stores

- S/MIME certificate and private key pairs that the BlackBerry device receives from the Certificate Synchronization Manager
- S/MIME certificates that the BlackBerry device receives from the Certificate Synchronization Manager, fetches from the LDAP certificate server(s), imports from a smart card, or imports from email messages
- root certificates that RIM provides with BlackBerry software

Key store security

BlackBerry device users must supply the key store password to add and remove S/MIME certificates stored on the BlackBerry device.

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

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

IT policy rule	Recommendation
Minimum Password Length	Set a key store password that is between 4 and 12 alphanumeric characters in length.
Forbidden Passwords	Specify weak passwords to prevent.
Key Store Password Maximum Timeout	Specify the maximum length of time (0, 1, 2, 5, 10, 20, 30 minutes, or 1 hour) that the key store remains unlocked after the user types the correct key store password
Disable Key Store Backup	Set this IT policy rule to prevent the back up of S/MIME private keys in the key store.

IT policy rule	Recommendation
Minimal Signing Key Store Security Level	<p>Set to one of the following levels:</p> <ul style="list-style-type: none"> • 2 (high security): The BlackBerry device prompts the users for their key store password each time an application tries to access their private key • 3 (medium security): The BlackBerry device prompts the users for their key store password when an application tries to access their private key for the first time or when their private key password timeout expires
Minimal Encryption Key Store Security Level	<p>Set to one of the following levels:</p> <ul style="list-style-type: none"> • 2 (high security): The BlackBerry device prompts the users for their key store password each time an application tries to access their private key • 3 (medium security): The BlackBerry device prompts the users for their key store password when an application tries to access their private key for the first time or when their private key password timeout expires

Users can set the following additional key store security options on the BlackBerry device (in **Security Options > Key Stores**).

Setting	Description
Allow Key Store Backup/Restore	<p>Specify whether to back up and restore S/MIME certificates, private keys, public keys, and symmetric keys in the key store.</p> <p>Note: The BlackBerry device does not permit you to back up and restore S/MIME private keys if you have set the Disable Key Store Backup IT policy rule to True.</p>
Private Key Password Timeout	<p>Specify the maximum amount of time that the key store remains unlocked after the BlackBerry device user types the correct key store password.</p> <p>Note: The BlackBerry device does not enforce the value that the user specifies for this rule if it is greater than the value that you specify using the Key Store Password Maximum Timeout IT policy rule.</p>
Key Store Address Injector	<p>Specify whether to add certificate contacts to the address book when the BlackBerry device user adds certificate to the BlackBerry device key store.</p>
Certificate Service	<p>Define the connection service that the BlackBerry device uses to fetch S/MIME certificates and certificate status from the PKI.</p>
Certificate Status Expires After	<p>Specify the maximum amount of time (1, 2, 4, or 12 hours, 1 day, 1 week, 1 month, or 6 months) for which the S/MIME certificate revocation status remains valid.</p>
Change Password	<p>Type a new key store password.</p>

Private key security

Users can set additional private key security for digitally signing keys and decryption keys using the Certificate Synchronization Manager on the BlackBerry Desktop Manager. The BlackBerry device does not enforce the security level that the user specifies for this rule if it is lower than the value that you specify using the Minimal Signing Key Store Security Level and the Minimal Encryption Key Store Security Level IT policy rules.

Security level	Description
High	The BlackBerry device prompts the user for their key store password each time an application tries to access their private key, whether the private key password timeout period for the user is expired or valid.
Medium	The BlackBerry device prompts the user for their key store password <ul style="list-style-type: none"> when an application tries to access their private key for the first time when the private key password timeout period for the user expires The BlackBerry device does not prompt the user for their key store password if an application makes a subsequent attempt to access the private key while the private key password timeout is still valid.
Low	The BlackBerry device does not prompt the user when an application tries to access the private key of the user.

Certificate storage on a smart card

The BlackBerry Smart Card Reader™ for BlackBerry devices is an accessory that, when used in proximity to certain Bluetooth® enabled BlackBerry devices, integrates smart card use with the BlackBerry Enterprise Solution™. The BlackBerry Smart Card Reader creates a reliable two-factor authentication environment for granting a user access to BlackBerry and PKI applications and enables the wireless digital signing and encryption of wireless email messages using the S/MIME Support Package.

See the *BlackBerry Smart Card Reader Security Technical Overview* for more information on BlackBerry Smart Card Reader features.

Importing an S/MIME certificate from a smart card

If a user has a smart card authenticator, smart card driver, and smart card reader driver installed on their Bluetooth enabled BlackBerry device, the user can perform a Bluetooth pairing process followed by a secure pairing process with the BlackBerry Smart Card Reader. After the BlackBerry device and the BlackBerry Smart Card Reader establish a secure pairing, you can set the S/MIME Force Smartcard Use IT policy rule to require the use of the smart card to import certificates, sign, encrypt, or sign and encrypt S/MIME protected messages on the BlackBerry device.

Cleaning decrypted S/MIME content from the BlackBerry device

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

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

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

You can set the memory cleaning function to run automatically when the following events occur:

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

Scenario	Recommendation
Remove decrypted content from BlackBerry device memory when the BlackBerry device is holstered.	Set the Force Memory Clean When Holstered IT policy rule to True.
Remove decrypted content from BlackBerry device memory when the BlackBerry device is idle.	Set the Force Memory Clean When Idle IT policy rule to True.
Start the memory cleaner after the time specified has elapsed.	Set the Memory Cleaner Maximum Idle Time IT policy rule to the desired time (for example, 10 minutes).

See the *Policy Reference Guide* for more information.

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

See the *S/MIME Support Package User Guide Supplement* for more information.

Managing S/MIME certificates and private keys

View S/MIME certificate details

Users can view S/MIME certificate details on their BlackBerry device (in **Security Options** > **Certificates**) by clicking a specific certificate and selecting **Details**. Some or all of the following details might appear.

Detail	Description
Revocation Status	displays the status of the S/MIME certificate at a specified date and time
Trust Status	displays the status of the S/MIME certificate trust level <ul style="list-style-type: none"> • Explicitly trusted: the S/MIME certificate is trusted • Implicitly trusted: the S/MIME certificate chains to an explicitly trusted certificate on the BlackBerry device • Not trusted: the S/MIME certificate is not explicitly trusted, and does not chain to an explicitly trusted certificate on the BlackBerry device
Expiration Date	displays the expiration date that the issuing CA sets
Certificate Type	displays the certificate format (the BlackBerry device supports X.509 and WTLS certificates)
Public Key Type	displays the types of public keys contained in the certificate (the BlackBerry device supports RSA, DSA, DH, and ECC keys)
Subject	displays information about the certificate subject in X.509 DN syntax Note: See "Common certificate subject attributes" on page 8 for more information.
Issuer	displays identifying information about the certificate issuer in X.509 DN syntax
Serial Number	displays the serial number of the certificate, set by the issuing CA
Key Usage	displays approved uses for the S/MIME public key
Subject Alt Name	displays the email address, if available, for the certificate subject
SHA1 Thumbprint	displays the SHA 1 digital thumbprint of the certificate
MD5 Thumbprint	displays the MD5 algorithm digital thumbprint of the certificate

The certificate details view also includes the following options:

- Click **Fetch Status** to fetch the status of the certificate.
- Click **View Issuer** to view the certificate details for the certificate issuer.

Set S/MIME certificate security options

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

Scenario	Recommendation
Prevent users from sending an S/MIME encrypted message using a certificate that the BlackBerry device cannot verify.	Set the Disable Unverified Certificate Use IT policy rule to True.
Prevent users from sending an S/MIME encrypted message using a certificate that has a weak corresponding public key.	Set the Disable Weak Certificate Use IT policy rule to True.
Prevent users from sending an S/MIME encrypted message using a certificate that the BlackBerry device does not trust.	Set the Disable Untrusted Certificate Use IT policy rule to True.
Prevent users from sending an S/MIME encrypted message from the BlackBerry device using a certificate that is expired on the BlackBerry device.	Set the Disable Invalid Certificate Use IT policy rule to True.
Prevent users from sending an S/MIME encrypted message from the BlackBerry device using a certificate that is revoked on the BlackBerry device.	Set the Disable Revoked Certificate Use IT policy rule to True.
Require that the BlackBerry device display a warning when the user receives a signed message on the BlackBerry device in which the email address of the sender does not appear in the certificate used to sign the message.	Set the Disable Certificate Email Address Checks IT policy rule to False. This is the default behavior.
Require that the BlackBerry device display warnings and visual indications if the user chooses to send or receive an email message that is signed using a stale certificate.	Set the Disable Stale Certificate Status Checks IT policy rule to False. This is the default behavior.
Prevent users from sending an S/MIME encrypted message using a certificate with a stale status.	Set Disable Stale Status Use IT policy rule to True.
Set the time after which the certificate status is no longer valid on the BlackBerry device.	Set the Certificate Status Maximum Expiry Time IT policy rule to 4 (hours). Note: When the certificate status expires, the certificate status on the BlackBerry device appears stale. The BlackBerry device user should update the certificate status in the BlackBerry device key store or Certificate Synchronization Manager.
Prevent BlackBerry device users from sending an S/MIME encrypted message using a certificate with a stale status.	Set the Disable Stale Status Use IT policy rule to True.

Scenario	Recommendation
Prevent BlackBerry device users from accepting unverified CRLs when checking the status of a certificate using the connection service.	Set the Disable Unverified CRLs IT policy rule to True.
Set a string of trusted certificate thumbprints to prevent users from adding certificates with thumbprints that are not included in the string to the trusted key store.	Set the Trusted Certificate Thumbprints IT policy rule to a semi-colon separated list of Hex-ASCII certificate thumbprints that are generated using either SHA 1 or MD5.

Users can set S/MIME certificate security options on their BlackBerry device (in **Security Options > Certificates**) by clicking a specific certificate and selecting an action.

Action	Description
Trust the S/MIME certificate.	Click Trust .
Remove the trust associated with the S/MIME certificate.	Click Distrust .
Invalidate the status of an S/MIME certificate in the BlackBerry device key store.	Click Revoke .
Remove an S/MIME certificate from the BlackBerry device key store.	Click Delete .
Send an S/MIME certificate in an email message.	Click Send via Email .
Send an S/MIME certificate in a PIN message.	Click Send via PIN .
Download the status of the S/MIME certificate.	Click Fetch Status .
Download the status of the entire S/MIME certificate chain.	Click Fetch Chain Status .

Sending S/MIME protected messages

The S/MIME Support Package includes digital signing and encryption options that the user can define on the BlackBerry device, or that you can set and push to the BlackBerry device using the BlackBerry Enterprise Server IT policy. See "BlackBerry Enterprise Server IT policy rules for the S/MIME Support Package" on page 21 for more information.

Message signing and encryption options

When the user selects an encoding option on the BlackBerry device or is required by the message classification that they select on the BlackBerry device to send an encrypted or signed and encrypted S/MIME message, one of the following conditions occurs:

- If the BlackBerry device user has an appropriate (in other words, trusted, not revoked, not expired, and with a strong public key) S/MIME certificate for the recipient, the BlackBerry device sends the message.
- If the BlackBerry device user does not have an appropriate S/MIME certificate for the recipient, the BlackBerry device tries to fetch a certificate automatically. If it finds an appropriate certificate, the BlackBerry device sends the message. If it does not find an appropriate certificate, the BlackBerry device prompts the user to choose one of the following options:
 - not send the message
 - manually fetch an appropriate S/MIME certificate
 - send the message in unencrypted form

Manually fetching an S/MIME certificate

If the user responds to the BlackBerry device prompt by choosing to manually fetch an appropriate S/MIME certificate for the intended recipient, the BlackBerry device displays a Certificate Search application. The user can refine search parameters in the Certificate Search application before the BlackBerry device tries to fetch an appropriate S/MIME certificate from a set LDAP certificate server. If it finds an appropriate S/MIME certificate, the BlackBerry device sends the message.

Sending a message in unencrypted form

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

- Attach S/MIME certificates from the BlackBerry device key store and send the keys as .cer file attachments.
- Attach certificate server configuration information.
- Send the message as plain text.

See the *S/MIME Support Package User Guide Supplement* for more information.

By default, the S/MIME Support Package permits users to send and receive plain text email and PIN messages on their BlackBerry devices. You can set BlackBerry Enterprise Server IT policy rules to prevent users from sending plain text messages from their S/MIME enabled BlackBerry devices.

Scenario	Recommendation
Force users to send signed and, or encrypted S/MIME email messages from their S/MIME enabled BlackBerry devices.	Set the Disable Message Normal Send IT policy rule to True.
Force users to send signed and, or encrypted S/MIME PIN messages from their S/MIME enabled BlackBerry devices.	Set the Disable Peer-to-Peer Normal Send IT policy rule to True.

Verify a certificate or certificate chain status from a received S/MIME protected message

1. On the BlackBerry device, in the message list, click a received S/MIME protected message.
2. Perform one of the following actions:

Action	Procedure
Verify the certificate status of the sender. (The certificate of the sender is included in the message or is stored in the BlackBerry device key store of the message recipient.) Note: If the certificate status of the sender is stale, the BlackBerry device fetches an updated certificate status automatically.	> Click Check Sender's Certificate .
Verify the certificate chain status of the sender. (The certificate of the sender is included in the message or is stored in the BlackBerry device key store of the message recipient.)	> Click Check Sender's Cert Chain .

Fetch or import a certificate from a received S/MIME protected message

1. On the BlackBerry device, in the message list, click a received S/MIME protected message.
2. Perform one of the following actions:

Action	Procedure
Retrieve a certificate from the LDAP certificate server. (The certificate of the message sender is not in the BlackBerry device key store of the message recipient and is not included in the message.)	> Click Fetch Sender's Certificate .
Add the certificate of the message sender to the BlackBerry device. (The certificate of the message sender is included in the message but not in the BlackBerry device key store of the message recipient.)	> Click Import Sender's Certificate .

Add a certificate server configuration from a received S/MIME protected message














Import the certificate server attachment included in the message to set a new certificate server in **Security Options > Certificate Servers**.




1. On the BlackBerry device, in the message list, click a received S/MIME protected message containing a certificate server attachment.
2. Click **Import Server**.

See the *S/MIME Support Package User Guide Supplement* for more information.

S/MIME message icons

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

Icon	Description
	The message is strongly encrypted.
	The message is weakly encrypted.
	The BlackBerry device has verified the message signature.
	The BlackBerry device could not verify the message signature.
	The BlackBerry device requires more data to verify the message signature.
	The BlackBerry Enterprise Server has verified the message signature and indicated that verification to the BlackBerry device.
	Please wait for the operation to finish.
	The certificate status is trusted, or the certificate chain is trusted.
	The trust status of the certificate chain is unknown.
	There was an error determining the trust status of the certificate chain.
	The certificate chain has expired.
	The certificate chain has been revoked or is not trusted.
	A signed receipt was requested with the message.

Icon	Description
	A digital certificate is included in the message.
	Several digital certificates are included in the message.
	The message contains an LDAP, OCSP, or CRL server attachment.

BlackBerry Enterprise Server IT policy rules for the S/MIME Support Package

The following BlackBerry Enterprise Server IT policy rules apply only to BlackBerry devices on which the S/MIME Support Package is installed. See the *Policy Reference Guide* for more information.

IT policy rule	Description
S/MIME Allowed Content Ciphers	specifies the content ciphers that the BlackBerry device can use to encrypt S/MIME messages
S/MIME Blind Copy Address	specifies an email address that is added as a BCC recipient to all outgoing S/MIME encrypted messages
S/MIME Force Digital Signature	specifies whether all outgoing S/MIME messages must be digitally signed
S/MIME Force Encrypted Messages	specifies whether all outgoing S/MIME messages must be encrypted
S/MIME Minimum Strong DH Key Length	specifies the minimum DH key size, in bits, that you consider strong, for use with S/MIME
S/MIME Minimum Strong DSA Key Length	specifies the minimum DSA key size, in bits, that you consider strong, for use with S/MIME
S/MIME Minimum Strong ECC Key Length	specifies the minimum ECC key size, in bits, that you consider strong, for use with S/MIME
S/MIME Minimum Strong RSA Key Length	specifies the minimum RSA key size, in bits, that you consider strong, for use with S/MIME
Entrust Messaging Server (EMS) Email Address	specifies the email address for an Entrust Entelligence™ Messaging Server

The following IT policy rules apply only to users using a smart card certificate on BlackBerry devices running BlackBerry Device Software Version 3.6 or earlier with the S/MIME Support Package Version 4.0 or later installed or BlackBerry Device Software Version 4.0 or later (S/MIME Support Package optional) on which the BlackBerry Smart Card Reader driver is installed.

IT policy rule	Description
Force Smart Card Two Factor Challenge Response	specifies whether or not the BlackBerry device requires the user to choose a smart card certificate for use with smart card two factor authentication
S/MIME Force Smartcard Use	specifies whether all certificate operations must be performed using a paired BlackBerry Smart Card Reader and smart card

See the *BlackBerry Smart Card Reader Security Technical Overview* for information on BlackBerry Enterprise Server IT policy rules that apply only to BlackBerry devices on which the S/MIME Support Package and the BlackBerry Smart Card Reader are installed.

Related resources

Guide	Information
<i>BlackBerry Enterprise Server System Administration Guide</i>	<ul style="list-style-type: none"> • generating and changing master encryption keys • enabling S/MIME • enabling encryption options • setting IT policy rules • setting message classifications
<i>BlackBerry Enterprise Solution Security Technical Overview</i>	<ul style="list-style-type: none"> • preventing the decryption of information at an intermediate point between the BlackBerry device and the BlackBerry Enterprise Server or company LAN • managing security settings for all BlackBerry devices • protecting data in transit between the BlackBerry device and BlackBerry Enterprise Server • understanding the algorithms provided by the RIM cryptographic application programming interface (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>S/MIME Support Package User Guide Supplement</i>	<ul style="list-style-type: none"> • installing the S/MIME Support Package • managing certificates on the BlackBerry device and computer • setting S/MIME options for digitally signing and encrypting messages • sending and receiving S/MIME protected messages
Visit www.blackberry.com/security .	<ul style="list-style-type: none"> • information about BlackBerry Solution security

Part number: 8670357 Version 3

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

The Bluetooth word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by Research In Motion Limited is under license. Entrust, Entrust Authority, and Entrust Entelligence are either registered trademarks or trademarks of Entrust, Inc. in the United States and certain countries. IBM, Lotus, Domino, and Lotus Notes are registered trademarks of IBM in the United States and/or other countries. Java is either a registered trademark or trademark of Sun Microsystems, Inc. in the United States or other countries. Microsoft and Outlook are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Netscape is either a registered trademark or trademark of Netscape Communication Corporation. Novell and GroupWise are either registered trademarks or trademarks of Novell, Inc., in the United States and other countries. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

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

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

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