

S/MIME Support Package

Release 4.1

White Paper

Contents

S/MIME Support Package	3
New in this release	3
System requirements	3
System architecture	4
PKI component support	4
Desktop-based certificate management	5
Wireless certificate management	6
Configuring default PKI component connections	6
BlackBerry security	7
BlackBerry standard encryption	7
S/MIME security	8
Certificates	8
Certificate authorities	8
S/MIME certificate types	9
S/MIME encryption	9
Enabling S/MIME messaging	11
Searching for and validating S/MIME certificates	11
S/MIME certificate search	11
S/MIME certificate revocation status	11
Storing S/MIME certificates and private keys	12
BlackBerry device storage	12
Managing S/MIME certificates and private keys	14
View S/MIME certificate details	14
Configure S/MIME certificate security options	15
Sending S/MIME protected messages	16
Message signing and encryption options	16
Verify a certificate or certificate chain status from a received S/MIME protected message	17
Fetch or import a certificate from a received S/MIME protected message	17
Add a certificate server configuration from a received S/MIME protected message	17
S/MIME message icons	17
BlackBerry Enterprise Server IT policy rules for S/MIME	18
Related resources	18

This document describes the S/MIME Support Package, which is designed to offer extended security features for BlackBerry® devices.

S/MIME Support Package

The S/MIME Support Package is designed to enable BlackBerry device users who are already sending and receiving Secure Multipurpose Internet Mail Extensions (S/MIME) messages using their desktop email program 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 Public Key Infrastructure (PKI) components including Netscape®, Entrust Authority™ Security Manager version 5 and later, and Microsoft Certificate Authorities (CAs).

The S/MIME Support Package includes tools for obtaining certificates and transferring them to the BlackBerry device. Users can sign, encrypt, and send S/MIME messages from their BlackBerry devices, and messages that are encrypted using S/MIME can also be decrypted and read on the BlackBerry device. Without the S/MIME Support Package the BlackBerry Enterprise Server sends a message to the user's 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:

- certificate and private key synchronization and management using the Certificate Synchronization Manager included in the BlackBerry Desktop Software
- encrypting and decrypting messages, including personal identification number (PIN) messages, verifying digital signatures, and digitally signing outgoing messages
- wireless fetching of certificates and certificate status using PKI protocols
- smart cards on the BlackBerry device

New in this release

Feature	Description
Encrypted message search	The user can search the text of encrypted messages on the BlackBerry device.
Address association	When a BlackBerry user receives a certificate for which there is no email address or the email address is obsolete, the user can associate an email address with the certificate.

System requirements

The S/MIME Support Package version 4.1 supports the following messaging and collaboration servers, BlackBerry Enterprise Server software, BlackBerry devices and BlackBerry Device Software.

Messaging and collaboration servers	BlackBerry Enterprise Server software	BlackBerry devices and BlackBerry device software
Microsoft® Exchange 5.5, 2000 and 2003 Servers	BlackBerry Enterprise Server version 2.1 Service Pack 3A or later for Microsoft Exchange Note: In 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 BlackBerry Enterprise Server version 4.0 or later for Microsoft Exchange, the S/MIME IT policy rules are automatically included in the BlackBerry Manager.	Java™-based BlackBerry devices that are running BlackBerry device software version 4.1 or later Note: Users must load the S/MIME Support Package on the BlackBerry device and add the Certificate Synchronization Manager to the BlackBerry Desktop Manager.

System architecture

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

- a physical connection (using a serial or USB port) from the BlackBerry device to the desktop computer to enable the Certificate Synchronization Manager to download the BlackBerry device user's private key
- 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:

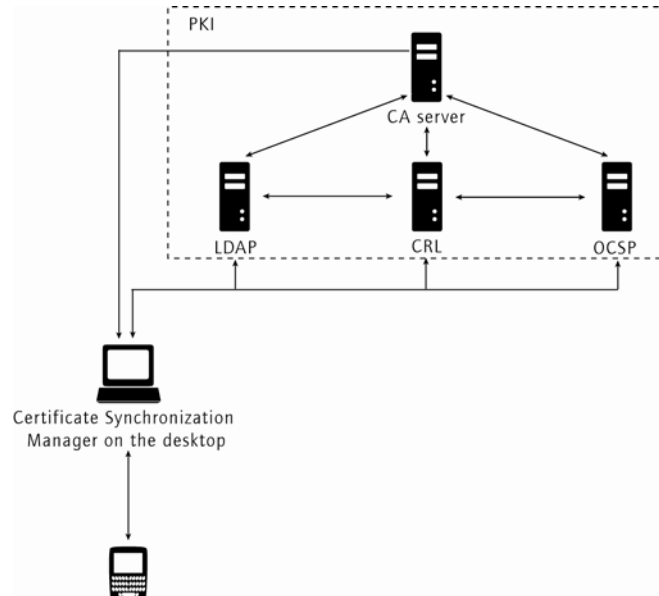
- **Lightweight Directory Access Protocol (LDAP):** the BlackBerry device and the Certificate Synchronization Manager use LDAP to search for and download certificates.
- **Online Certificate Status Protocol (OCSP):** the BlackBerry device and the Certificate Synchronization Manager use OCSP to check the certificate revocation status on demand.
- **Certificate Revocation List (CRL):** the BlackBerry device and the Certificate Synchronization Manager obtain the most recent certificate revocation status, published at a frequency set on the CA server, from CRLs.

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

Desktop-based certificate management

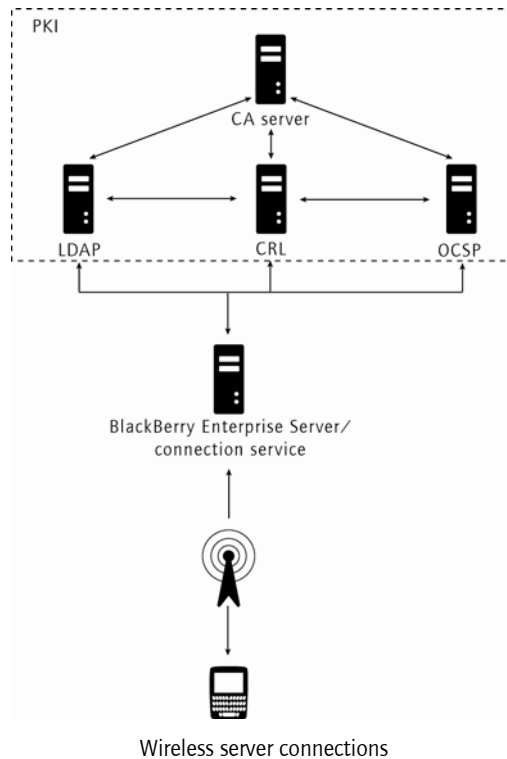
The Certificate Synchronization Manager on the BlackBerry Desktop Manager enables users to search for certificates, download the certificates to their BlackBerry device, and verify the authenticity and status of certificates. Certificate information is transported between the CA server(s), the PKI server(s),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



Desktop-based server connections

Wireless certificate management

BlackBerry Enterprise Server version 3.5 or later for Microsoft Exchange supports wireless data transfer between the BlackBerry device and the PKI. The connection service uses standard Internet protocols to enable the BlackBerry device to pull S/MIME certificates and S/MIME certificate status from the PKI protocol server(s) to their BlackBerry device over the wireless network.



Configuring default PKI component connections

You can configure 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.

Configure 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 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. Note: Each LDAP server can host multiple domains but can only search in one domain at a time. You must set a default base query.

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.

Configure 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 other than the default 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.

Configure 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**:

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

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

BlackBerry security

The current BlackBerry Infrastructure uses symmetric key cryptography to encrypt the data that is sent between the BlackBerry Enterprise Server and the BlackBerry device. BlackBerry standard encryption encrypts data using the Triple Data Encryption Standard (Triple DES) or the Advanced Encryption Standard (AES) algorithm.

BlackBerry standard 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 Security White Paper* for more information on standard BlackBerry encryption.

S/MIME security

From the time the BlackBerry device user sends a message until the BlackBerry Enterprise Server receives the message, the message is encrypted by BlackBerry standard encryption. S/MIME encryption is designed to enable sender-to-recipient authentication and confidentiality and helps 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 (private and public keys) to provide the following:

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

Certificates

Certificates are digital documents that contain information about the certificate subject. Certificates use the hierarchical structure of the X.509 standard distinguished name (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, it must trust the CA that issued the certificate. This trust relationship is indicated by a certificate chain from the user's certificate, to the CA's certificate, and continuing back through the certificates of any other authorizing entities connected to the user's certificate. 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 desktop 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 this mechanism, your organization can distribute trusted root certificates to all BlackBerry device users so that they can use the organization PKI system.

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 implementation of public key cryptography uses the following certificates:

Certificate type	Description	File extension
Certificates with private keys (personal certificates)	S/MIME uses the certificate's corresponding private key 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
Other people's certificates	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 does not identify a root CA.	<ul style="list-style-type: none"> .p7b .p7c .key
Root certificates	A root CA creates root certificates. RIM bundles authentic root certificates in 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's authenticity (for example, by verifying the certificate's 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 is installed 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 message recipient's S/MIME certificate.
2. The BlackBerry device uses standard BlackBerry encryption to encrypt the S/MIME data.
3. The BlackBerry device sends the encrypted data to the BlackBerry Enterprise Server.
4. The BlackBerry Enterprise Server removes the BlackBerry standard encryption and sends the S/MIME encrypted message to the recipient.

If the S/MIME Support Package is installed on a BlackBerry device, when the BlackBerry device receives a message, the S/MIME message is encrypted with standard BlackBerry encryption and then decrypted 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 enabled 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 data.
6. When the BlackBerry device user opens the message, the BlackBerry device decrypts the message and renders the message.

S/MIME encryption algorithms

RIM recommends using a strong algorithm for S/MIME encryption. When you enable 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 message recipient's S/MIME certificate to encrypt the message.

When a BlackBerry device user receives a signed message, the BlackBerry device uses the sender's S/MIME certificate 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 message sender's S/MIME private key to digitally sign the message.

When a user receives an encrypted message, the BlackBerry device uses the user's private key 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 Rivest Shamir Adleman (RSA), Digital Signature Algorithm (DSA), Diffie-Hellman (DH), and Elliptic Curve Cryptography (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)
RSA	1024	4096
DSA	1024	1024
DH	1024	4096
ECC	163	571

RIM recommends 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 S/MIME" on page 18 for more information.

Enabling S/MIME messaging

S/MIME messaging is turned off by default on the BlackBerry Enterprise Server. You must enable this option in the BlackBerry Manager to turn on S/MIME messaging on the BlackBerry Enterprise Server.

After you enable S/MIME messaging on the BlackBerry Enterprise Server, when a user installs the S/MIME Support Package on their BlackBerry device and includes the Certificate Synchronization option in their BlackBerry Desktop Software installation, the BlackBerry Manager automatically enables 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 enable additional types of S/MIME encryption.

BlackBerry Enterprise Server version	Encryption option	Description
4.0 and 4.1	Enable S/MIME encryption of signed and weakly encrypted messages	Enables the BlackBerry Enterprise Server to encrypt a message with S/MIME encryption a second time when a user who is enabled for S/MIME encryption receives a weakly-encrypted or signed but unencrypted S/MIME message.
4.1	Send S/MIME messages in clear-signed format	When a BlackBerry device user sends a message, 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	The BlackBerry Enterprise Server removes attachment data from any S/MIME protected messages it receives so that users on the BlackBerry Enterprise Server can receive more message text on their BlackBerry devices. The BlackBerry device cannot verify the S/MIME digital signature of the message after the attachment data is removed.
	Use Pkcs7 MIME type	The BlackBerry Enterprise Server sends messages using a newer type of MIME instead of the default legacy MIME type. If a BlackBerry device user sends an S/MIME-encrypted message to a mail system that does not support the MIME type used, the mail system does not render the S/MIME protected message properly.

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 configured LDAP certificate servers and download S/MIME certificates from the search results. BlackBerry device users can perform searches based on the S/MIME certificate subject's first name, last name, or email address.

S/MIME certificate revocation status

BlackBerry device users can perform S/MIME certificate revocation status checks when they receive a signed or signed and encrypted message, and before they send a message to an S/MIME certificate subject. BlackBerry device users can also check the revocation status of an S/MIME certificate from the BlackBerry device key store and from the S/MIME Certificate Search screen.

The BlackBerry device uses the connection service to request and retrieve either the S/MIME certificate revocation status from 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) or imports from messages
- root certificates that RIM bundles with BlackBerry software

Key store security

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

The BlackBerry device stores a Secure Hash Algorithm (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 configure 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	Configure this policy rule to prevent the back up of S/MIME private keys in the key store.
Minimal Signing Key Store Security Level	Set to one of the following levels: <ul style="list-style-type: none"> • 2 (high security): The BlackBerry device prompts the users for their key store password each time an application attempts to access their private key • 3 (medium security): The BlackBerry device prompts the users for their key store password when an application attempts to access their private key for the first time or when their private key password timeout expires
Minimal Encryption Key Store Security Level	Set to one of the following levels: <ul style="list-style-type: none"> • 2 (high security): The BlackBerry device prompts the users for their key store password each time an application attempts to

IT policy rule	Recommendation
	<p>access their private key</p> <ul style="list-style-type: none"> • 3 (medium security): The BlackBerry device prompts the users for their key store password when an application attempts to access their private key for the first time or when their private key password timeout expires

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

Setting	Description
Allow Key Store Backup/Restore	Specify whether to back up and restore S/MIME certificates, private keys, public keys, and symmetric keys in the key store.
Private Key Password Timeout	Specify the maximum amount of time that the key store remains unlocked after the BlackBerry device user types the correct key store password. Note: The 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.
Key Store Address Injector	Specify whether to add certificate contacts to the address book when the BlackBerry device user adds certificate to the BlackBerry device key store.
Certificate Service	Define the connection service that the BlackBerry device uses to fetch S/MIME certificates and certificate status from the PKI.
Certificate Status Expires After	Specify the maximum amount of time (1, 2, 4, or 12 hours, 1 day, 1 week, 1 month, or 6 months) for which the S/MIME certificate revocation status remains valid.
Change Password	Type a new key store password.

Private key security

Users can configure 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 attempts to access their private key, whether the user's private key password timeout is expired or valid.
Medium	<p>The BlackBerry device prompts the user for their key store password</p> <ul style="list-style-type: none"> • when an application attempts to access their private key for the first time • when the user's private key password timeout expires <p>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.</p>
Low	The BlackBerry device does not prompt the user when an application attempts to access the user's private key.

Memory cleaning

The memory cleaning function is designed to remove unreferenced, decrypted content from the BlackBerry device (for example, from the S/MIME application, key store, content protection and address book caches, S/MIME certificate search, and BlackBerry device clipboard).

You can configure the memory cleaning function to run automatically when the

- user synchronizes the BlackBerry device with the desktop 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 policy rule to True.
Remove decrypted content from BlackBerry device memory when the BlackBerry device is idle.	Set the Force Memory Clean When Idle policy rule to True.
Start the memory cleaner after the time specified has elapsed.	Set the Memory Cleaner Maximum Idle Time policy rule to 1 (minute).

See the *Policy Reference Guide* for more information.

Users can configure the memory cleaning function to run when their BlackBerry devices are holstered, or when their BlackBerry devices remain idle for a configured period of time (2, 5, 10, 20, 30 minutes, or 1 hour). 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
Fetch Status	click to fetch the status of the S/MIME certificate
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)

Detail	Description
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
Subject Alt Name	displays the email address, if available, for the certificate subject
Key Usage	displays approved uses for the S/MIME public key
SHA1 Thumbprint	displays the Secure Hash Algorithm (SHA-1) digital thumbprint of the certificate
MD5 Thumbprint	displays the Message-Digest algorithm (MD5) digital thumbprint of the certificate
View Issuer	click to view the certificate details for the certificate issuer

Configure S/MIME certificate security options

You can set BlackBerry Enterprise Server IT policy rules to configure 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 policy rule to True.
Prevent users from sending an S/MIME message using a certificate that has a weak corresponding public key.	Set the Disable Weak Certificate Use policy rule to True.
Prevent users from encrypting messages with a certificate that the BlackBerry device does not trust.	Set the Disable Untrusted Certificate Use policy rule to True.
Set the number of days that the BlackBerry device caches the certificate status.	Set the Certificate Status Cache Timeout policy rule to 7 (days).
Set the time after which the certificate status is no longer valid on the BlackBerry device.	Set the Certificate Status Maximum Expiry Time policy rule to 4 (hours). Note: When the certificate status expires, the BlackBerry device user must update the certificate status in the BlackBerry device key store or Certificate Synchronization Manager.
Prevent BlackBerry device users from encrypting a message using a certificate with a stale status.	Set the Disable Stale Status Use policy rule to True.
Prevent BlackBerry device users from accepting unverified CRLs when checking the status of a certificate using the connection service.	Set the Disable Unverified CRLs policy rule to True.

Users can configure 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 .

Action	Description
Remove the trust associated with the S/MIME certificate.	Click Distrust .
Invalidate the status of an S/MIME certificate.	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 configure and push to the BlackBerry device using the BlackBerry Enterprise Server IT policy. See "BlackBerry Enterprise Server IT policy rules for S/MIME" on page 18 for more information.

Message signing and encryption options

When the user selects an option 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 attempts 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 do one of the following:
 - 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, a Certificate Search application appears on the BlackBerry device. The user can refine search parameters in the Certificate Search application before the BlackBerry device attempts to fetch an appropriate S/MIME certificate from a configured 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
- 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 BlackBerry device users to send and receive plain text email and PIN messages. You can configure BlackBerry Enterprise Server IT policy rules to prevent users enabled for S/MIME from sending plain text messages.

Scenario	Recommendation
Force all S/MIME-enabled users to send signed and, or encrypted S/MIME email messages.	Set the Disable Message Normal Send policy rule to True.
Force all S/MIME-enabled users to send signed and, or encrypted S/MIME PIN messages.	Set the Disable Peer-to-Peer Normal Send 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 messages list, click a received S/MIME protected message.
2. Perform one of the following actions:

Action	Procedure
Verify the sender's certificate status. (The sender's certificate is included in the message or is stored in the recipient's BlackBerry device key store.)	> Click Check Sender's Certificate .
Verify the sender's certificate chain status. (The sender's certificate is included in the message or is stored in the recipient's BlackBerry device key store.)	> 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 messages 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 sender's certificate is not on the recipient's BlackBerry device and is not included in the message.)	> Click Fetch Sender's Certificate .
Add the sender's certificate to the BlackBerry device. (The sender's certificate is included in the message but not in the recipient's BlackBerry device key store.)	> 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 configure a new certificate server in **Security Options > Certificate Servers**.


















1. On the BlackBerry device, in the messages 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 messages 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.

Icon	Description
	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 has been verified.
	Please wait for the operation to finish.
	The certificate status is trusted.
	The certificate chain status 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.
	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.
	A digital certificate is attached to the message.

BlackBerry Enterprise Server IT policy rules for S/MIME

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	specifies the minimum DSA key size, in bits, that you consider

IT policy rule	Description
Length	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 BlackBerry devices on which the S/MIME Support Package and a smart card are installed.

IT policy rule	Description
Allow Smart Card Password Caching	specifies whether the BlackBerry device can cache the smart card password for a period of time controlled by the key store private key timeout
Force Smart Card Two Factor Authentication	specifies whether the BlackBerry device user must supply the BlackBerry device password and the smart card password
Lock on Smart Card Removal	specifies whether the BlackBerry device locks when the smart card is removed from the smart card reader, or the reader is removed from the BlackBerry device
S/MIME Force Smartcard Use	specifies whether all certificate operations must be performed using an attached smart card reader

See the *BlackBerry Smart Card Reader Security White Paper* 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 encryption managing security
<i>BlackBerry Security White Paper</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 Local Area Network (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 Transport Layer Security (TLS) and Wireless Transport Layer Security (WTLS) standards that the RIM Crypto API currently supports understanding the memory scrub process that occurs on the BlackBerry device when content protection is

Guide	Information
	enabled
<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 desktop computer• setting S/MIME options for digitally signing and encrypting messages• sending and receiving S/MIME protected messages

Part number: SWD_X_BES(EN)-172.001

© 2005 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', BlackBerry, and BlackBerry Enterprise Server are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

Entrust, Entrust Authority, and Entrust Entelligence are either registered trademarks or trademarks of Entrust, Inc. in the United States and certain countries. Java is either a registered trademark or trademark of Sun Microsystems, Inc. in the United States or other countries. Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. 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.

Certain features outlined in this document require a minimum version of BlackBerry Enterprise Server software and/or BlackBerry Device Software and may require use of specific models of BlackBerry devices, additional development or third party products and/or services for access to corporate applications.