

# **S/MIME Support Package**

**Version 4.1**

**User Guide Supplement**

S/MIME Support Package Version 4.1 User Guide Supplement

Last modified: 14 October 2005

Part number: SWD\_X\_HH(EN)-074.001

At the time of publication, this documentation is based on the S/MIME Support Package version 4.1.

Send us your comments on **product documentation**: <https://www.blackberry.com/DocsFeedback>.

©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", the "envelope in motion" symbol, BlackBerry, BlackBerry Enterprise Server and the BlackBerry logo are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

Entrust, Entelligence, and Entrust Authority are either trademarks or registered trademarks of Entrust, Inc. in the United States and certain countries. Microsoft and Windows are either trademarks or registered trademarks 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, the BlackBerry Smart Card Reader 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](http://www.rim.com/patents.shtml) for a listing of applicable RIM 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's 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's 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.

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

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

Published in Canada



# Contents

1	S/MIME Support Package installation.....	7
2	BlackBerry Certificate Synchronization Manager .....	9
3	Certificates.....	15
4	Certificate servers .....	21
5	S/MIME messages.....	23
6	Search.....	27
7	Memory cleaning.....	29
8	Smart cards.....	31
9	Legal notice .....	33



# S/MIME Support Package installation

## About the S/MIME Support Package

Install the S/MIME Support Package on your desktop computer computer

Install the S/MIME Support Package on your BlackBerry device

## About the S/MIME Support Package

Install Secure Multipurpose Internet Mail Extension (S/MIME) support on your BlackBerry® device to include BlackBerry device applications that are designed to support S/MIME signing and encryption. Use the custom setup in the BlackBerry Desktop Software to add the Certificate Synchronization Manager.

## Install the S/MIME Support Package on your desktop computer

Insert the BlackBerry® Desktop Software installation CD into your CD drive. Complete the on-screen instructions.

- In the Setup Type window, select **Custom**.
- In the Custom Setup window, click **Certificate Synchronization**. Select **This feature, and all subfeatures, will be installed on local hard drive**.

### Related topics

[Legal notice \(See page 33.\)](#)

## Install the S/MIME Support Package on your BlackBerry device

1. Verify that your BlackBerry® device is connected to your computer.
2. On the taskbar, click **Start**.
3. Click **Programs > BlackBerry > Desktop > Desktop Manager**.
4. Double-click the **Application Loader** icon.
5. Click **Next**.
6. Select the **BlackBerry S/MIME Support Package** check box.
7. To download Department of Defence (DoD) root certificates, select the **DoD Root Certificates** check box.
8. Click **Next**.
9. Click **Finish**.

### Related topics

[Legal notice \(See page 33.\)](#)

## User Guide Supplement

# BlackBerry Certificate Synchronization Manager

About the BlackBerry Certificate Synchronization Manager

Open the BlackBerry Certificate Synchronization Manager

About certificate information icons

View certificates

View certificate information

View certificate status

Synchronize certificates

Import certificates from your company's network

Search for a certificate on an LDAP server

Change certificate labels

Set the security level of private keys

View OCSP or CRL certificate server information

View LDAP certificate server information

Add OCSP or CRL certificate servers

Add LDAP certificate servers

Manage certificate servers

About Entrust digital IDs

Use Entrust digital IDs with the BlackBerry Certificate Synchronization Manager

## About the BlackBerry Certificate Synchronization Manager

The BlackBerry® Certificate Synchronization Manager is designed to enable users of supported BlackBerry devices to obtain certificates from numerous sources, download certificates to their BlackBerry device, and verify the authenticity and status of certificates.






Certificate status information and certificate server information is designed to be sent between Certificate Authority (CA), Lightweight Directory Access Protocol (LDAP), Online Certificate Status Protocol (OCSP), and Certificate Revocation List (CRL) servers and the BlackBerry Certificate Synchronization Manager on the desktop computer, and from the desktop computer to the BlackBerry device through the standard synchronization process (across a serial or USB connection).

## Open the BlackBerry Certificate Synchronization Manager

Verify that your BlackBerry® device is connected to your computer. On the taskbar, click **Start**. Click **Programs > BlackBerry > Desktop > Desktop Manager**. Double-click the **Certificate Sync** icon.

## About certificate information icons

In the BlackBerry® Certificate Synchronization Manager, on the Personal Certificates, Other People's Certificates, and Root Certificates tab, the following icons appear:

-  A selected check box indicates that the certificate is stored on the BlackBerry device.
-  The icons in this column provide information about the properties of a certificate.
-  The certificate chain is trusted. The certificate chain revocation status is good, and the certificate chain is valid.
-  The revocation status of the certificate chain is unknown, or a public key in the certificate chain is weak.
-  The certificate chain is untrusted, revoked, expired, not yet valid or could not be verified.

## View certificates

In the BlackBerry® Certificate Synchronization Manager, perform one of the following actions:

- To view certificates that are assigned to you, click the **Personal Certificates** tab.
- To view certificates for another person that have been validated by a root Certificate Authority and to authenticate the identity of the person to whom they are assigned, click the **Other People's Certificates** tab.
- To view certificates that originate from a root Certificate Authority and are considered trustworthy, click the **Root Certificates** tab.

On the server tabs, the following fields appear:

- **Certificate Label:** This field specifies the name of the certificate. By default, the name of the certificate holder is used.
- **Security:** This field specifies the security level of the certificate that contains a private key. This field only appears on the Personal Certificates tab.

- **Email Address:** This field specifies the email address of the certificate holder.
- **Subject:** This field specifies detailed information about the certificate holder.
- **Issuer:** This field specifies detailed information about the certificate issuer.
- **Serial Number:** This field specifies the certificate serial number in hexadecimal format.
- **Certificate Source:** This field specifies the display name of the certificate server on which the certificate resides or the Microsoft® Windows® store in which the certificate was found.

## View certificate information

In the BlackBerry® Certificate Synchronization Manager, click a server tab. Right-click a certificate. Click **View Certificate**.

- **Serial Number:** This field specifies the certificate serial number in hexadecimal format.
- **Issuer:** Detailed information about the certificate issuer.
- **Valid From:** This field specifies the date from which the certificate is valid as set by the issuing Certificate Authority.
- **Valid To:** This field specifies the expiration date that is set by the issuing Certificate Authority.
- **Subject:** Detailed information about the certificate holder.
- **Public key:** This field specifies the standard to which the public key complies. The BlackBerry device supports Rivest Shamir Adleman (RSA), Digital Signature Algorithm (DSA), and Elliptic Curve Cryptography (ECC) keys.
- **Subject Alternative Name:** This field specifies the email address for the certificate.
- **Key Usage:** This field specifies approved uses for the key.

- **SHA1 thumbprint:** This field specifies the Secure Hash Algorithm, version 1 (SHA1) digital thumbprint of the certificate.
- **MD5 thumbprint:** This field specifies the Message-Digest Algorithm, version 5 (MD5) digital thumbprint of the certificate.

## View certificate status

In the BlackBerry® Certificate Synchronization Manager, click a server tab. Right-click a certificate. Click **Edit Certificate Properties**. Click **View Certificate**. Click **Certification Path**.

## Synchronize certificates

To synchronize certificates manually, in the BlackBerry® Certificate Synchronization Manager, click a server tab. Select the check box beside a certificate. Click **Synchronize**.

### Note:

Selected certificates are added to the BlackBerry device. Certificates that are not selected are removed from the device.

To set the BlackBerry Desktop Software to synchronize certificate information automatically, in the BlackBerry Certificate Synchronization Manager, click **Options**. Click the **Desktop Preferences** tab. Perform one of the following actions:

- To specify an interval after which certificates should be synchronized, set the **Synchronize every** field.
- To synchronize certificates each time your device is connected to your computer, select the **Synchronize every time the BlackBerry device is connected** option.

### Warning:

Verify that you have a Public Key Infrastructure (PKI) system license for the certificate that you want to download.

## Import certificates from your company's network

In the BlackBerry® Certificate Synchronization Manager, click **Import Certificate**. Select a file. Click **Open**.

### Note:

You can import certificates that are packaged with private keys and have a .pfx or .p12 file extension (for example, personal certificates). You can import other certificates with a .cer, .der, .crt, .p7b, .p7c, or .key file extension.

## Search for a certificate on an LDAP server

1. In the BlackBerry® Certificate Synchronization Manager, click the **Other People's Certificates** tab.
2. Click **Find in LDAP**.
3. Select one or more LDAP server(s).
4. Type certificate holder information in one or more of the following fields: **First Name**, **Last Name**, **Email**.
5. Click **Search Now**.

### Note:

To store a certificate in the BlackBerry Certificate Synchronization Manager, select a query result. Click **Mark for addition**.

## Change certificate labels

In the BlackBerry® Certificate Synchronization Manager, click a server tab. Right-click a certificate. Click **Edit Certificate Properties**. Perform one of the following actions:

- To specify a name for the certificate, in the **Certificate Label** section, type a name.

- To use the common name that is associated with the certificate, click **Use Common Name**.

## Set the security level of private keys

In the BlackBerry® Certificate Synchronization Manager, click a server tab. Right-click a certificate. Click **Edit Certificate Properties**. In the **Private Key Security Level** section, perform one of the following actions:

- To prompt users for their key store password each time a program attempts to access their private key, select **High**.
- To prompt users for their key store password when a program attempts to access their private key for the first time or when their private key password timeout is expired, select **Medium**.
- To display no notification when an application attempts to access a user's private key, select **Low**.

### Note:

Private key security levels apply to private keys synchronized to the BlackBerry device.

## View OCSP or CRL certificate server information

In the BlackBerry® Certificate Synchronization Manager, click **Options**. Click the **OCSP Servers** or **CRL Servers** tab.

- **Friendly Name:** This parameter specifies the common name that is associated with the server.
- **Use OCSP or Use CRL:** A selected check box indicates that OCSP or CRL server use is enabled. You must enable OCSP or CRL server use before you can configure and connect to OCSP or CRL servers.
- **Server URL:** This parameter specifies the web address URL of the server.
- **Certificate Extensions:** A selected check box indicates that certificate extension use is enabled.

Certificate extensions can include the URL of the Certificate Authority, OCSP responder and/or a CRL location which the BlackBerry Certificate Synchronization Manager uses to check certificate status.

- **Use specified servers:** A selected check box indicates that servers that are specified in the server pane are used to check certificate status. You must enable Use Specified Servers before you can add and configure OCSP or CRL servers.
- **Update Now:** Click to download the certificate revocation lists from the CRL servers and update the certificate status accordingly. When you synchronize your certificates, the certificate revocation lists are queried for the certificates' revocation status.
- **Update the cached CRL:** This parameter indicates (in hours) how frequently the certificate revocation lists are downloaded to the cache. When you synchronize your certificates, the certificate revocation lists are queried for the certificates' revocation status. 0 indicates that the automatic CRL cache updates feature is disabled.

## View LDAP certificate server information

In the BlackBerry® Certificate Synchronization Manager, click **Options**. Click the **LDAP Servers** tab.

- **Friendly Name:** This parameter specifies the common name that is associated with the server.
- **Server Name:** This parameter specifies the name of the server.
- **Base Query:** This parameter specifies query information as it is configured in your LDAP server. Content appears in X.509 DN syntax.
- **Port:** This parameter specifies the port as it is configured on your company network.
- **Crawl Server:** This parameter indicates whether the BlackBerry Certificate Synchronization

Manager polls the LDAP server at startup and automatically downloads all certificates found on the LDAP server to the BlackBerry Certificate Synchronization Manager. Yes indicates that the crawl feature is enabled.

**Warning:** Crawling LDAP servers are network intensive and can result in reduced performance. Contact your system administrator before you enable this feature.

- **Use BlackBerry device address book contents when searching LDAP servers:** A selected check box indicates that the BlackBerry Certificate Synchronization Manager queries the LDAP server to look for certificates that are assigned to people who are listed in your BlackBerry device address book.

**Warning:**

This feature is network intensive and can result in reduced performance. Contact your system administrator before you enable this feature.

## Add OCSP or CRL certificate servers

In the BlackBerry® Certificate Synchronization Manager, click **Options**. Click the **OCSP Servers** or **CRL Servers** tab. Click **Add**. Perform the following actions:

- **Friendly Name:** Type a name for the server.
- **Server URL:** Type the URL for the server.

**Note:**

Contact your system administrator for the name of server.

## Add LDAP certificate servers

In the BlackBerry® Certificate Synchronization Manager, click **Options**. Click the **LDAP Servers** tab. Click **Add**. Perform the following actions:

- **Friendly Name:** Type a name for the server.

- **Server Name:** Type the server name.
- **Port:** Type the port number of the server. The default is 389.
- **Base Query:** Type the base query information.
- **Auth. Type:** Select **Simple** if you are required to provide credentials when you attempt to connect to an LDAP server. Select **Anonymous** if you can connect to an LDAP server without providing credentials.
- **Crawl this LDAP Server:** Select this check box to poll the LDAP server to automatically download all certificates found on the LDAP server to the BlackBerry Certificate Synchronization Manager.

**Note:**

Contact your system administrator for the name, port, base query, and authentication type of your server.

## Manage certificate servers

In the BlackBerry® Certificate Synchronization Manager, click **Options**. Click a server tab. Select a server. Click one of the following menu items:

- **Edit**
- **Delete**

## About Entrust digital IDs

You can use Entrust® digital IDs with the BlackBerry® Certificate Synchronization Manager. The Entrust desktop security store contains managed certificates and their corresponding private keys. The BlackBerry Desktop Software can access these keys and certificates through Entrust Entelligence™ version 6.0 or 6.1 for synchronization to the BlackBerry device.

Before you can use Entrust digital IDs, the certification authority administrator must configure Entrust policies to enable PKCS#12 export of private key and certificate information. This action is performed using the Entrust Authority™ Security Manager Administration tool.

See appropriate Entrust documentation for configuration information.

## Use Entrust digital IDs with the BlackBerry Certificate Synchronization Manager

In the BlackBerry® Certificate Synchronization Manager, click **Options**. On the **Entrust Preferences** tab. If you are using an Entrust PKI, select the **Use Entrust** check box. Locate the entrust.ini file. The default location is C:\WINNT\system.

### Note:

The first time that you use Entrust® Entelligence™, you are notified that the BlackBerry Certificate Synchronization Manager extension is attempting to access Entrust. Click **Yes**.

# Certificates

About the key store  
Fetch the status of a certificate or certificate chain  
Fetch certificates  
Set certificates to trusted  
Set certificates to untrusted  
Send certificates  
Add email addresses to certificates  
View certificate information  
View certificate chain information  
Filter certificates  
Search for certificates  
Add certificates  
Set options for adding certificates  
Edit certificate labels  
Revoke certificates  
Delete certificates  
Change the key store password  
Set key store options  
Certificate shortcuts

## About the key store

The key store contains your certificates, or public keys, and private keys. In the key store, the status of certificates is indicated by an icon.

A key icon indicates that a certificate has a corresponding private key either on the BlackBerry® device or on a smart card.

A check mark icon indicates that a certificate chain is trusted, the certificate chain revocation status is good, and the certificate chain is valid.

A question mark icon indicates that the revocation status of a certificate is unknown, or a public key in the certificate chain is weak.

An "X" icon indicates that a certificate chain is untrusted, revoked, expired, not yet valid or could not be verified.

## Fetch the status of a certificate or certificate chain

In the device options, click **Security Options**. Click **Certificates**. Click a certificate. Click one of the following menu items:

- **Fetch Status**
- **Fetch Chain Status**

### Note:

Fetching the chain status of a certificate verifies the status of the certificate and also all other certificates in the chain, back to the issuing root certificate.

### Related topics

About the key store (See page 15.)

Fetch certificates (See page 15.)

## Fetch certificates

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Click the trackwheel.

4. Click **Fetch Certificates**.
5. Select a server.
6. Type certificate holder information in one or more of the **First Name**, **Last Name**, or **Email** fields.
7. Click the trackwheel.
8. Click **Search**.

**Note:**

A selected check box beside a certificate indicates that the certificate is fetched and stored in the key store.

**Related topics**

[About the key store \(See page 15.\)](#)

[Add certificates \(See page 17.\)](#)

## Set certificates to trusted

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Click an untrusted certificate.
4. Click **Trust**.
5. If the certificate is not a root certificate, a prompt appears. To trust only the selected certificate, click **Selected Certificate**. To trust the entire certificate chain by trusting the root certificate, click **Entire Chain**.

**Related topics**

[About the key store \(See page 15.\)](#)

[Revoke certificates \(See page 18.\)](#)

[Send certificates \(See page 16.\)](#)

## Set certificates to untrusted

In the device options, click **Security Options**. Click **Certificates**. Click a trusted certificate. Click **Distrust**.

**Related topics**

[About the key store \(See page 15.\)](#)

[Revoke certificates \(See page 18.\)](#)

[Send certificates \(See page 16.\)](#)

## Send certificates

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Click a certificate.
4. Click **Send via Email** or **Send via PIN**.
5. Click a contact.
6. Click **Email <Contact Name>** or **PIN <Contact Name>**.
7. Type a message.
8. Click **Send**.

**Note:**

When you send certificates, private keys are not sent.

**Related topics**

[Add certificate attachments to messages \(See page 25.\)](#)

[Import certificates \(See page 24.\)](#)

## Add email addresses to certificates

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Click a certificate.
4. Click **Associate Addresses**.
5. Click the trackwheel.
6. Click **Add Address**.
7. Select [**Use Once**].
8. Click **Email**.
9. Type an email address.
10. Click the trackwheel.
11. Click **Continue**.

**Related topic**

About the key store (See page 15.)

**View certificate information**

In the device options, click **Security Options**. Click **Certificates**. Click a certificate. Click **Details**.

- **Revocation Status:** This field specifies the status of the certificate at a specified date and time.
- **Trust Status**
  - **Explicitly trusted:** The certificate is trusted.
  - **Implicitly trusted:** The certificate chains to a certificate that is trusted on the BlackBerry® device.
  - **Not trusted:** The certificate is not explicitly trusted and does not chain to a trusted certificate on the device.
- **Expiration Date:** This field specifies the expiration date that is set by the issuing Certificate Authority.
- **Serial Number:** This field specifies the certificate serial number in hexadecimal format.

**Related topics**

Edit certificate labels (See page 18.)

Change the key store password (See page 19.)

**View certificate chain information**

In the device options, click **Security Options**. Click a certificate. Click **Show Chain**.

**Note:**

To expand or collapse certificate chain information, press the **Space** key.

**Related topic**

View certificate information (See page 17.)

**Filter certificates**

In the device options, click **Security Options**. Click **Certificates**. Click the trackwheel. Click one of the following menu items:

- **Show My Certs**
- **Show Others Certs**
- **Show CA Certs**
- **Show Root Certs**
- **Show All Certs**

**Note:**

The current filter is indicated in the upper right corner of the screen.

**Related topic**

Certificate shortcuts (See page 19.)

**Search for certificates**

1. In the certificate search program, set the **Server** field.
2. Type the certificate holder information in one or more of the following fields: **First Name**, **Last Name**, and **Email**.
3. Click the trackwheel.
4. Click **Search**.

**Related topics**

Add certificates (See page 17.)

Set options for adding certificates (See page 18.)

**Add certificates**

1. In the certificate search program, in a search results list, select a certificate with an unchecked check box.
2. Click the trackwheel.

3. Click **Add to Certificate Key Store**.
4. Type your key store password.
5. Click **OK**.

#### Related topics

Set options for adding certificates (See page 18.)

### Set options for adding certificates

1. In the certificate search program, click the trackwheel.
2. Click **Options**.
3. Perform the following actions:
  - To fetch the certificate status automatically when you add a certificate to the key store, set the **Fetch Status** field to **Yes**.
  - To set a label for added certificates using the certificate common name or a custom label, set the **Prompt for Label** field to **Yes**.
4. Click the trackwheel.
5. Click **Save**.

#### Related topics

Add certificates (See page 17.)

Fetch the status of a certificate or certificate chain (See page 15.)

### Edit certificate labels

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Click a certificate.
4. Click **Change Label**.
5. Type a new certificate label.
6. Click **OK**.

#### Related topic

Change the key store password (See page 19.)

### Revoke certificates

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Click a certificate.
4. Click **Revoke**.
5. Click **Yes**.
6. Select one of the following options:
  - **Unknown:** The reason is unspecified.
  - **Key Compromise:** The private key value might have been revealed.
  - **CA Compromise:** The issuing private key of the Certificate Authority might have been revealed.
  - **Change in Affiliation:** The person no longer works in the company.
  - **Superseded:** A new certificate is replacing an existing certificate.
  - **Cessation of Operation:** The certificate is no longer required.
  - **Certificate Hold:** The certificate is temporarily revoked, but you can reinstate by pressing **Cancel Hold** on the BlackBerry® device key store menu.
  - **Removed from CRL:** The revoked certificate is removed from the Certificate Revocation List (CRL).

#### Note:

If you revoke a certificate, the certificate is only revoked in the key store on your device. The revocation is not communicated back to the Certificate Authority or CRL servers.

#### Related topics

About the key store (See page 15.)

Set certificates to trusted (See page 16.)

Send certificates (See page 16.)

## Delete certificates

In the device options, click **Security Options**. Click **Certificates**. Click a certificate. Click **Delete**.

### Related topic

Revoke certificates (See page 18.)

## Change the key store password

1. In the device options, click **Security Options**.
2. Click **Security Settings**.
3. Click **Key Stores**.
4. Click the trackwheel.
5. Click **Change Password**.
6. Type your existing key store password.
7. Type a new key store password.
8. Type your new key store password again.

## Set key store options

In the device options, click **Security Options**. Click **Key Stores**. Set the following options:

- **Allow Key Store Backup/Restore:** Specify whether you want to back up or restore certificates, private keys, public keys and, symmetric keys.
- **Private Key Password Timeout:** Set the key store password timeout. After a password timeout occurs, you must type your password to access private keys.
- **Key Store Address Injector:** Specify whether you want to add contacts from certificates to the address book when certificates are added to the BlackBerry® device key store.
- **Certificate Service:** Specify the service record for the corporate BlackBerry Mobile Data Service that is used to fetch certificates. If you are unsure about your service record, contact your system administrator.

- **Certificate Status Expires After:** Specify the length of time that a certificate revocation status can be stored before it is stale. If you send an S/MIME message with a required certificate that is stale, the device is designed to automatically attempt to fetch an updated status for the certificate.
- **Accept unverified CRLs:** Specify whether to accept certificate status results from CRLs that cannot be verified by the BlackBerry Mobile Data Service.

### Related topic

Change the key store password (See page 19.)

## Certificate shortcuts

To display the certificate label, press the **Space** key.

To display certificate information, press the **Enter** key.

To display all certificates, press the **Alt** key + **A**.

To display the Certificate Authority certificates, press the **Alt** key + **C**.

To display the end entity certificates (for example, personal certificates and other people's certificates), press the **Alt** key + **E**.

To display the certificate label for a certificate, press the **Alt** key + **L**.

To display personal certificates that contain private keys, press the **Alt** key + **P**.

To display other people's certificates, press the **Alt** key + **O**.

To display root certificates, press the **Alt** key + **R**.

To display the serial number for a certificate, press the **Alt** key + **S**.

## User Guide Supplement

# Certificate servers

Add certificate servers

Manage certificate servers

Send certificate server information

## Add certificate servers

1. In the device options, click **Security Options**.
2. Click **Certificate Servers**.
3. Click a server.
4. Click **New Server**.
5. Type server information.
6. Click the trackwheel.
7. Click **Save**.

## Manage certificate servers

In the device options, click **Security Options**. Click **Certificate Servers**. Click a server. Click one of the following menu items:

- **View**
- **Edit**
- **Delete**

## Send certificate server information

1. In the device options, click **Security Options**.
2. Click **Certificate Servers**.
3. Click a server.
4. Click **PIN Server** or **Email Server**.
5. Click a contact.

6. Click **Email <Contact Name>** or **PIN <Contact Name>**.

7. Click **Send**.

### Related topics

Send certificates (See page 16.)

Add certificate attachments to messages (See page 25.)

## User Guide Supplement

# S/MIME messages

About S/MIME message status icons  
Open S/MIME messages  
View encryption information  
Verify certificate or certificate chain status  
Fetch certificates  
Import certificates  
Import certificate servers  
Forward S/MIME messages  
Send S/MIME messages  
Add certificate attachments to messages  
Set message icon size  
Set signing options  
Set encryption options  
Set key verification options

## About S/MIME message status icons

When you open a message, message status icons appear.

A lock icon indicates that the message is strongly encrypted.

A lock icon with a question mark indicates that the message is weakly encrypted.

A check mark icon indicates that the message digital signature is verified.

An "X" icon indicates that the message digital signature is not verified.

A question mark icon indicates that more data is required to verify the digital signature.

## Open S/MIME messages

In the messages list, open the S/MIME message.

### Related topics

Import certificates (See page 24.)

Import certificate servers (See page 24.)

Fetch certificates (See page 24.)

## View encryption information

In an open S/MIME message, click the encryption icon. Perform one of the following actions:

- To view the certificate information, click **Display Encryption Certificate**.
- To view the weak public key algorithm that is used to encrypt a message, click **Encryption Details**.

### Note:

The BlackBerry Enterprise Server® might re-encrypt messages that are sent with a weak encryption algorithm or a digital signature.

## Verify certificate or certificate chain status

In an open S/MIME message, click the digital signature or trust status icon. Click **Check Sender's Certificate** or **Check Sender's Cert Chain**.

### Note:

The Check Sender's Certificate and Check Sender's Cert Chain menu items only appear if the sender's certificate is included in the message or is stored in your BlackBerry® device key store.

## Fetch certificates

In an open S/MIME message, click the digital signature or trust status icon. Click **Fetch Sender's Certificate**.

### Note:

The Fetch Sender's Certificate menu item only appears if the sender's certificate is not included in your BlackBerry® device key store or the sender's message.

## Import certificates

1. In an open S/MIME message, click the digital signature or trust status icon.
2. Click **Import Sender's certificate**.
3. Type your key store password.
4. Click **OK**.
5. Type a certificate label.
6. Click **OK**.

### Note:

To import a certificate from an attachment, in an open message, click the paper clip icon. Click **Retrieve Certificate Attachment**. Click the attachment icon. Click **Import Certificate**.

### Related topics

[Open S/MIME messages \(See page 23.\)](#)

## Import certificate servers

In an open S/MIME message, click an S/MIME server icon. Click **Import Server**.

### Related topic

[Manage certificate servers \(See page 21.\)](#)

## Forward S/MIME messages

In an open S/MIME message, click the trackwheel. Click **Forward**.

### Note:

By default, the forwarded message uses the same signing and encryption options as the original message. To change these options, in the message you are forwarding, set the **Using** field.

### Related topic

[Send S/MIME messages \(See page 24.\)](#)

## Send S/MIME messages

1. In the messages list, click the trackwheel.
2. Click **Compose Email**.
3. Type an email address.
4. Click **Email <Contact Name>**.
5. Perform one of the following actions:
  - To attach a digital signature, set the **Using** field to **Sign**.
  - To encrypt the message, set the **Using** field to **Encrypt**.
  - To attach a digital signature and encrypt the message, set the **Using** field to **Sign and Encrypt**.
6. Type a message.
7. Click the trackwheel.
8. Click **Send**.

### Note:

To send an encrypted S/MIME PIN message, the contacts must have a personal identification number (PIN) and an email address that matches the certificate that you are using to encrypt the message.

### Related topics

[Set signing options \(See page 25.\)](#)

[Set key verification options \(See page 25.\)](#)

[Add email addresses to certificates \(See page 16.\)](#)

## Add certificate attachments to messages

1. When composing a message, click the trackwheel.
2. Click **Attach Certificates**.
3. Click a certificate.

### Related topic

Send certificates (See page 16.)

## Set message icon size

1. In the device options, click **Security Options**.
2. Click **S/MIME**.
3. Perform one of the following actions:
  - To display small S/MIME icons and include brief information in messages, set the **Message Viewer Icons** field to **Small**.
  - To display large S/MIME icons and include descriptive information in messages, set the **Message Viewer Icons** field to **Large**.
4. Click the trackwheel.
5. Click **Save**.

### Related topic

Open S/MIME messages (See page 23.)

## Set signing options

1. In the device options, click **Security Options**.
2. Click **S/MIME**.
3. Set the **Signing Options Certificate** field.
4. Perform one of the following actions:
  - To request a signed receipt when the message is read, set the **Request S/MIME Receipts** field to **Yes**.
  - To make sure that a signed receipt is not requested when the message is read, set the **Request S/MIME Receipts** field to **No**.

5. Click the trackwheel.
6. Click **Save**.

### Related topics

Set key verification options (See page 25.)

Send S/MIME messages (See page 24.)

## Set encryption options

1. In the device options, click **Security Options**.
2. Click **S/MIME**.
3. Set the **Encryption Options Certificate** field.
4. Set the **Allowed Content Ciphers** field.
5. Click the trackwheel.
6. Click **Save**.

### Note:

To protect messages in the Sent Items folder and prevent users from decrypting these messages, in the **Encryption Options** section, set the **Certificate** field to **None**.

### Related topics

Set key verification options (See page 25.)

Send S/MIME messages (See page 24.)

## Set key verification options

1. In the device options, click **Security Options**.
2. Click **S/MIME**.
3. Perform one of the following actions:
  - To verify the cryptographic validity of private and public keys before sending S/MIME messages, set the **Verify Keys Before Use** field to **Yes**.
  - To not verify the cryptographic validity of private and public keys before sending S/

MIME messages, set the **Verify Keys Before Use** field to **No**.

4. Click the trackwheel.
5. Click **Save**.

**Related topics**

Set encryption options (See page 25.)

Send S/MIME messages (See page 24.)

# Search

Search for signed messages

Search for encrypted messages

## Search for signed messages

1. In the search program, in the **Text** field, type text to search for.
2. In the **Name** field, type a contact name to search for.
3. Select the **Messages** check box.
4. Click the trackwheel.
5. Click **Search**.

## Search for encrypted messages

1. In the search program, in the **Text** field, type text to search for.
2. In the **Name** field, type a contact name to search for.
3. Select the **Messages** check box.
4. Select the **Encrypted Messages** check box.
5. Click the trackwheel.
6. Click **Search**.

### Note:

If the security level for the private key is set to medium or high, you may be prompted to type your key store password before search results appear.

## User Guide Supplement

# Memory cleaning

About memory cleaning

Set memory cleaning options

Clean memory

## About memory cleaning

The memory cleaning program on the BlackBerry® device is designed to delete sensitive content from memory.

The device memory is designed to be cleaned automatically when the device

- is inserted in the holster
- remains idle for a configured period of time
- synchronized with your computer
- time or time zone is changed
- is locked

## Set memory cleaning options

1. In the device options, click **Security Options**.
2. Click **Memory Cleaning**.
3. Perform one or more of the following actions:
  - To clean the BlackBerry® device memory every time the device is inserted in the holster, set the **Clean When Holstered** to **Yes**.
  - To clean the device memory after the device remains idle for a specified time period, set the **Clean When Idle** to **Yes**. To set the time period, set the **Idle Timeout** field.
  - To display the **Memory Cleaner** icon on the Home screen, set the **Show Icon on Home Screen field** to **Yes**.

4. Click the trackwheel.

5. Click **Save**.

### Related topics

About memory cleaning (See page 29.)

Clean memory (See page 29.)

## Clean memory

In the device options, click **Security Options**. Click **Memory Cleaning**. Click the trackwheel. Click **Clean Now**.

### Related topics

About memory cleaning (See page 29.)

Set memory cleaning options (See page 29.)

## User Guide Supplement

# Smart cards

About smart cards

Set a user authenticator password

Unlock the device using a smart card

Download smart card certificates

## About smart cards

Certificates and private keys are stored on smart cards. Certificates can be imported to your BlackBerry® device key store, but private keys can only be stored on smart cards. As a result, private key operations such as signing and decryption are enabled on the smart card, and public key operations such as verification and encryption are enabled on the device using public certificates.

You can download certificates from the smart card to the your device using a smart card reader, set your user authenticator passwords, and send S/MIME messages with your smart card certificates.

## Set a user authenticator password

1. Verify that your smart card is inserted in the smart card reader.
2. In the device options, click **Security Options**.
3. Click **General Settings**.
4. Set the **User Authenticator Password** field to **Enabled**.
5. Click **Save**.
6. Type a user authenticator password for the smart card.
7. Click **OK**.

## Unlock the device using a smart card

After you connect the smart card reader to your BlackBerry® device, the device sends an authentication request to the card each time that you unlock your device.

To unlock the device, on the Lock screen, roll the trackwheel. Click **Unlock**. In the **Enter Device Password** field, type your device password. In the **Enter Authenticator Password** field, type your user authenticator password.

## Download smart card certificates

1. In the device options, click **Security Options**.
2. Click **S/MIME**.
3. Click the trackwheel.
4. Click **Import Smart Card Certs**.
5. Select a certificate.
6. Click **OK**.
7. Type your key store password.
8. Click **OK**.

### Note:

To download a certificate, you must have a PKI system license for the certificate.

## User Guide Supplement

## Legal notice

©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", the "envelope in motion" symbol, BlackBerry, BlackBerry Enterprise Server and the BlackBerry logo are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

Entrust, Entelligence, and Entrust Authority are either trademarks or registered trademarks of Entrust, Inc. in the United States and certain countries. Microsoft and Windows are either trademarks or registered trademarks 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, the BlackBerry Smart Card Reader 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](http://www.rim.com/patents.shtml) for a listing of applicable RIM 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's 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's 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.