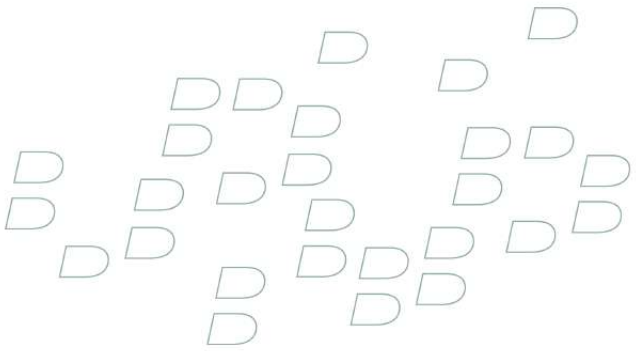

User Guide Supplement

S/MIME Support Package for BlackBerry Smartphones
BlackBerry 8700 Series

Manual abstract:

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....3 Certificate basics...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....9 Certificate servers....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....

.....

.....
.....
.....
.....

.....
....23 2 Certificates Certificate basics Download a certificate from an LDAP certificate server 1.
In the device options, click Security Options. 2. 3. 4. 5.
6. 7. 8. 9. Click Certificates. Click the trackwheel. Click Fetch Certificates. Specify the search criteria. Click the trackwheel. Click Search.

Click a certificate. Click Add Certificate to Key Store. View properties for a certificate 1. 2. 3. 4. In the device options, click Security Options. Click Certificates. Click a certificate. Click Details.
Certificate properties Revocation Status: This field displays the revocation status of the certificate at a specified date and time. Trust Status: This field displays the trust status of the certificate chain. @@@@Certificate Type: This field displays the certificate format. @@Your device supports RSA®, DSA, Diffie-Hellman, and ECC keys. @@Issuer: This field displays information about the certificate issuer.
Serial Number: This field displays the certificate serial number in hexadecimal format. Key Usage: This field displays approved uses of the public key. Subject Alt Name: This field displays an alternate email address for the certificate subject, if an alternate email address is available. SHA1 Thumbprint: This field displays the SHA-1 digital thumbprint of the certificate. MD5 Thumbprint: This field displays the MD5 digital thumbprint of the certificate.
View one type of certificate in the certificate list 1. In the device options, click Security Options. 2. Click Certificates. 3. Click the trackwheel. 4. Click one of the following menu items: · Show My Certs · Show Others Certs · Show CA Certs · Show Root Certs To view all the certificates on your BlackBerry® device, click the trackwheel. Click Show All Certs. Send a certificate When you send a certificate, your BlackBerry® device sends the public key, but does not send the corresponding private key.

1. 2. 3. 4. In the device options, click Security Options. Click Certificates. Highlight a certificate. Click the trackwheel. 4 5. Click Send via Email or Send via PIN.
Delete a certificate 1. 2. 3. 4. 5.
In the device options, click Security Options. Click Certificates. Highlight a certificate. Click the trackwheel. Click Delete.
View the certificate chain for a certificate 1. 2. 3. 4. 5. In the device options, click Security Options. Click Certificates. Highlight a certificate. Click the trackwheel. Click Show Chain.

Certificate status Certificate status indicators : The certificate has a corresponding private key that is stored on your BlackBerry® device or a smart card. : The certificate chain is trusted and valid, and the revocation status of the certificate chain is good. : The revocation status of the certificate chain is unknown, or a public key for a certificate in the certificate chain is weak. : The certificate is untrusted or revoked, or a certificate in the certificate chain is untrusted, revoked, expired, not valid, or cannot be verified. Check the revocation status of a certificate or certificate chain 1. In the device options, click Security Options. 2. Click Certificates. 3. Highlight a certificate.
5 4. Click the trackwheel. 5. Click Fetch Status or Fetch Chain Status. Change the trust status of a certificate 1.
2. 3. 4. 5. 6.
In the device options, click Security Options. Click Certificates. Highlight a certificate. Click the trackwheel. Click Trust or Distrust. If necessary, perform one of the following actions: · To trust the highlighted certificate, click Selected Certificate. · To trust the highlighted certificate and all the other certificates in the chain, click Entire Chain. Revoke a certificate If you revoke a certificate, the certificate is revoked only in the key store on your BlackBerry® device. Your device does not update the revocation status on the certificate authority or CRL servers. 1.

2. 3. 4. 5. 6. 7. 8. In the device options, click Security Options. Click Certificates. Highlight a certificate.
Click the trackwheel. Click Revoke. Click Yes. Change the Reason field. Click OK.
To cancel a certificate hold, highlight the certificate. Click the trackwheel. Click Cancel Hold. Certificate revocation reasons Unknown: The revocation reason does not match any of the predefined reasons. Key Compromise: A person who is not the key subject might have discovered the private key value. CA Compromise: Someone might have revealed the private key of the certificate issuer. Change in Affiliation: The certificate subject no longer works for the organization. 6 Superseded: A new certificate is replacing an existing certificate. Cessation of Operation: The certificate subject no longer requires the certificate. Certificate Hold: You want to revoke the certificate temporarily. Certificate options Change the display name for a certificate 1. In the device options, clicame: Type a display name for the certificate server. Server URL: Type the web address of the certificate server. Send connection information for a certificate server 1. 2.

3. 4. 5. In the device options, click Security Options. Click Certificate Servers. Highlight a certificate server. Click the trackwheel. Click Email Server or PIN Server. Delete a certificate server 1. 2.
3. 4. 5. In the device options, click Security Options. Click Certificate Servers.
Highlight a certificate server. Click the trackwheel. Click Delete. 12 Key stores About the key store The key store on your BlackBerry® device might store the following items. To access these items in the key store, you must type a key store password.
@@2. 3. 4. In the device options, click Security Options. Click Key Stores. Click the trackwheel. @@2. 3. 4. 5.

In the device options, click Security Options. Click Key Stores. Change the Private Key Password Timeout field. Click the trackwheel. @@In the device options, click Security Options. 2. Click Key Stores. 13 3. Change the Key Store Address Injector field to Enabled.

4.

Click the trackwheel. 5. @@For more information, contact your administrator. 1. 2.

3. 4. 5. In the device options, click Security Options. Click Key Stores.

Change the Certificate Service field. Click the trackwheel. @@@@1. 2. 3. 4. 5. In the device options, click Security Options. Click Key Stores. Change the Allow Key Store Backup/Restore field to No.

Click the trackwheel. @@2. 3. 4. 5. In the device options, click Security Options. Click Key Stores. Change the Certificate Status Expires After field. Click the trackwheel. @@In the device options, click Security Options.

14 2. 3. 4. 5. Click Key Stores.

Change the Accept Unverified CRLs field to No. Click the trackwheel. @@@@@@Encryption is designed to keep messages confidential. @@Recipients use their private key to decrypt the message. @@@@1.

When composing a message, change the Encoding field. 2. @@1. 2. 3. 4. 5. When composing a message, click the trackwheel. Click Attach Certificates. Highlight a certificate.

Click the trackwheel. @@1. @@2. Click the trackwheel. 3. @@In a message, highlight a digital signature indicator. 2. Click the trackwheel. 3. @@2. 3. 4. In a message, click the certificate attachment. Click Retrieve Certificate Attachment. Click the certificate.

@@In a message, highlight the certificate server indicator. 2. Click the trackwheel. 3. @@@@2.

Click the trackwheel. 3. Click Display Sender's Certificate or Display Encryption Certificate. View encryption information for a weakly encrypted message 1. In a weakly encrypted message, highlight the encryption status indicator. 2. Click the trackwheel. 3. Click Encryption Details. S/MIME-protected message status Digital signature indicators : Your BlackBerry® device verified the digital signature.

: 18 Your device cannot verify the digital signature. : Your device requires more data to verify the digital signature. : Your device trusts the certificate chain. : The sender's email address does not match the email address of the certificate subject, or the sender's certificate is revoked, is not trusted, cannot be verified , or is not on your device. : The certificate is weak, the certificate status is not current, or your device requires more data to verify the trust status of the certificate. : The sender's certificate is expired. Encryption status indicators Your administrator sets whether messages that you receive are considered to be strong or weak. : The message is strongly encrypted. : The message is weakly encrypted. Check the status of a certificate or certificate chain If a certificate is included in a received message, or is already stored in the key store on your BlackBerry® device, you can check the status of the sender's certificate, or you can check the status of the sender's certificate and all other certificates in the certificate chain.

1. In a message, highlight a digital signature indicator. 2. Click the trackwheel. 3.

Click Check Sender's Certificate or Check Sender's Cert Chain. S/MIME-protected message options Change your signing or encryption certificate Your BlackBerry® device uses your encryption certificate to encrypt messages in the sent items folder and includes your encryption certificate in messages that you send so that recipients can encrypt their reply messages. 19 1. 2. 3.

4. 5. In the device options, click Security Options. Click S/MIME. In the Signing Options section or the Encryption Options section, change the Certificate field. Click the trackwheel. Click Save. Change the default signing and encryption option Your BlackBerry® device is designed to use the default signing and encryption option when you send a message to a contact that you have not sent a message to or received a message from previously. If you have sent a message to or received message from the contact previously, your device tries to use the signing and encryption option that was used for the last message. 1.

2. 3. 4. 5. In the device options, click Advanced Options. Click Default Services. Change the Default Encoding field. Click the trackwheel. Click Save. About message classifications If your BlackBerry® device is associated with an email account that uses a BlackBerry® Enterprise Server that supports this feature and your administrator turns on message classifications, the BlackBerry Enterprise Server applies a minimum set of security actions to each message that you compose, forward, or reply to, based on the classification that you assign to the message.

Your administrator specifies the message classifications that you can use. If you receive a message that uses message classifications, you can view the abbreviation for the classification in the subject line of the message and the full description for the classification in the body of the message. You can also view the abbreviation and full description for the classification for a sent message in the sent items folder. Change the default message classification Verify that your administrator has turned on message classifications. Your BlackBerry® device is designed to use the default message classification when you send a message to a contact that you have not sent a message to or received a message from previously.

If you have sent a message to or received message from the contact previously, your device tries to use the message classification that was used for the last message. 1. 2. 3. 4.

5. In the device options, click Advanced Options. Click Default Services. Change the Default Classification field. Click the trackwheel. Click Save. 20 Change the size of S/MIME indicators in messages 1. 2. 3. 4.

5. In the device options, click Security Options. Click S/MIME. Change the Message Viewer Icons field. Click the trackwheel. Click Save. Change the encryption algorithms for S/MIME-protected messages If a message has multiple recipients, your BlackBerry® device uses the first selected encryption algorithm in the list that all recipients are known to support. 1. 2. 3.

4. 5. In the device options, click Security Options. Click S/MIME. Select the check box beside one or more encryption algorithms.

Click the trackwheel. Click Save. Request delivery notification for signed S/MIME-protected messages 1. 2. 3.

4. 5. In the device options, click Security Options. Click S/MIME. Change the Request S/MIME Receipts field to Yes. Click the trackwheel. Click Save. Turn off the prompt that appears before an S/MIME-protected message is truncated 1. 2. 3.

4. 5. In the device options, click Security Options. Click S/MIME. Change the Warn about truncated messages field to No. Click the trackwheel. @@In the device options, click Security Options. 2. Click S/MIME. 21 3.

Change the Warn about problems with my certificates field to No. 4. Click the trackwheel. 5. Click Save.

@@@@@@You cannot open an attachment in a PGP® protected message that was encrypted using the OpenPGP format by an IBM® Lotus Notes® client working with PGP® Desktop Professional or that was encrypted by the PGP® Universal Server. 22 Smart cards About using a smart card with your device Smart cards store certificates and private keys.

You can use a smart card reader to import certificates from a smart card to the key store on your BlackBerry® device, but you cannot import private keys. As a result, private key operations such as signing and decryption use the smart card, and public key operations such as verification and encryption use the public certificates on your device. If you use a smart card certificate to authenticate to your device, after you connect your smart card reader to your device, your device requests authentication from the smart card each time that you unlock your device.
If the S/MIME Support Package for BlackBerry® devices is installed on your device, you can use smart card certificates to send S/MIMEprotected messages. Import a certificate from a smart card 1. 2. 3. 4. 5. 6. 7. 8. 9.

In the device options, click Security Options. Click Certificates. Click the trackwheel. Click Import Smart Card Certs. Type your smart card password. Select the check box beside a certificate. Click OK. Type your key store password. Click OK. 23 .