

BlackBerry Enterprise Solution

Version: 5.0

Security Technical Overview

Contents

Overview	6
Benefits of security for wireless devices	7
Threats to wireless devices.....	7
BlackBerry Enterprise Solution security	8
New security features.....	8
BlackBerry Enterprise Solution security features	9
Encryption keys on BlackBerry devices	10
Master encryption key of the BlackBerry device	10
Message keys.....	14
Content protection keys	16
Grand master keys	18
Standard BlackBerry encryption	19
Algorithms for standard BlackBerry encryption	19
Permitting third-party applications to encode data on the BlackBerry device.....	20
BlackBerry device memory.....	21
Wireless messaging security for the BlackBerry Enterprise Solution	22
Process flow: Receiving an email message on a BlackBerry device.....	22
Process flow: Sending an email message from a BlackBerry device.....	22
How the BlackBerry Enterprise Solution secures attachments.....	23
PIN messaging	24
Sending SMS text messages and MMS messages	24
Best practice: Controlling unsecured wireless messaging in your organization	24
Best practice: Turning off unsecured messaging	25
Extending messaging security for a BlackBerry device.....	26
Using the PGP Support Package for BlackBerry smartphones.....	26
Process flow: Sending a message using PGP encryption.....	27
Process flow: Receiving a PGP encrypted message.....	27
Using the S/MIME Support Package for BlackBerry smartphones.....	27
Process flow: Sending a message using S/MIME encryption	28
Process flow: Receiving an S/MIME-encrypted message	28
Using IBM Lotus Notes encryption on BlackBerry devices	29
Enrolling certificates on BlackBerry devices over the wireless network	32
Process flow: Enrolling a certificate when the certificate authority approves certificate requests automatically	32

Process flow: Enrolling a certificate when a certificate authority administrator approves certificate requests	33
Process flow: Enrolling a certificate using an RSA certificate authority.....	33
Protecting stored data	35
Protecting stored messages that are located on the messaging server	35
IT policy signing and storage on the BlackBerry device	35
Using the password keeper to manage application passwords on BlackBerry devices.....	36
Protecting data stored on external memory devices	36
Protecting user data on a locked BlackBerry device	37
Protected storage of master encryption keys on a locked BlackBerry device.....	38
Protected storage of master encryption keys on a BlackBerry device during a reset.....	39
Cleaning the BlackBerry device memory.....	39
BlackBerry Enterprise Solution architecture	41
Messaging server security.....	42
Storing data and encryption keys in the BlackBerry Configuration Database.....	42
Protecting the BlackBerry Infrastructure connections.....	45
Authenticating the BlackBerry Enterprise Server with the BlackBerry Infrastructure	45
How the BlackBerry Enterprise Server and BlackBerry Infrastructure exchange information.....	45
How the BlackBerry Enterprise Server and BlackBerry Infrastructure manage undeliverable messages	46
BlackBerry Router protocol authentication	46
Authentication during wireless activation.....	47
TCP/IP connection	48
Protecting the connection between the messaging server and the email application.....	49
Protecting connections between the BlackBerry Desktop Manager and its components	49
BlackBerry MDS connections.....	50
Using two-factor authentication to protect connections to enterprise Wi-Fi networks	51
WAP gateway connections.....	52
Instant messaging server connections	52
Using a segmented network architecture	53
Protecting BlackBerry Device Software updates over the wireless network	54
How the BlackBerry Enterprise Solution authenticates requests for BlackBerry Device Software updates over the wireless network.....	54
How a BlackBerry device protects user data during a BlackBerry Device Software update over the wireless network.....	55
Battery power requirements for BlackBerry Device Software updates over the wireless network.....	55
Protecting Wi-Fi connections to the BlackBerry Enterprise Solution	56
Security features of the enterprise Wi-Fi network architecture.....	56

Accessing the BlackBerry Infrastructure	56
Supported security features of Wi-Fi enabled BlackBerry devices	57
Enterprise Wi-Fi security methods that the BlackBerry device supports.....	57
IEEE 802.1X environment components.....	60
How the IEEE 802.1X environment controls access to the enterprise Wi-Fi network.....	60
Managing enterprise Wi-Fi network solution security using IT policy rules and configuration settings...61	
Requiring protected connections to enterprise Wi-Fi networks	61
VPN solution on a Wi-Fi enabled BlackBerry device.....	63
Using VPNs to protect connections to enterprise Wi-Fi networks.....	63
Using captive portals to protect connections to enterprise Wi-Fi networks or Wi-Fi hotspots.....	64
Authenticating a user.....	65
Authenticating a user using a password	65
Using the BlackBerry Smart Card Reader	65
Controlling BlackBerry devices	67
Controlling BlackBerry devices using IT policy rules.....	67
Enforcing BlackBerry device and BlackBerry Desktop Software security	68
Controlling BlackBerry device access to the BlackBerry Enterprise Server.....	68
Protecting Bluetooth connections on BlackBerry devices.....	68
Controlling location-based services on the BlackBerry device.....	69
How the BlackBerry device protects its operating system and the BlackBerry Device Software	70
Protecting the BlackBerry device against malware.....	70
Protecting lost, stolen, or replaced BlackBerry devices.....	74
Remotely resetting the password of a BlackBerry device that is content protected.....	74
Deleting all device data.....	75
Process flow: Deleting all device data from the BlackBerry device.....	76
Remotely erasing data from BlackBerry device memory and making the BlackBerry device unavailable.....	76
Remotely resetting a BlackBerry device to factory default settings.....	77
Deleting data from BlackBerry device memory and making the BlackBerry device unavailable using the standard security wipe process	77
Process flow: Scrubbing the memory on BlackBerry devices.....	78
Memory scrub processes for flash memory on BlackBerry devices	79
Unbinding the smart card from the BlackBerry device.....	79
RIM Cryptographic API	80
Cryptographic features that the RIM Cryptographic API provides	80
TLS and WTLS standards that the RIM Cryptographic API supports.....	81
Limitations of RIM Cryptographic API support for key establishment algorithm cipher suites.....	82

Power and electromagnetic side-channel attacks and countermeasures	84
Process flow: Running the masking operation during the initial AES algorithm calculation when content protection is turned on	84
Process flow: Running the masking operation during subsequent AES algorithm calculations when content protection is turned on	84
Process flow: Running the masking operation uses when content protection is turned off	84
BlackBerry Router protocol.....	86
How the BlackBerry Router protocol uses the Schnorr identification scheme	86
Examples of attacks that the BlackBerry Router protocol is designed to prevent.....	86
Process flow: Using the BlackBerry Router protocol to open an authenticated connection.....	87
Process flow: Using the BlackBerry Router protocol to close an authenticated connection	88
Algorithm suites that the BlackBerry device supports for negotiating SSL connections.....	89
Protocol that you use to reset the password on a content-protected BlackBerry device from the BlackBerry Enterprise Server	90
Cryptosystem parameters	90
Process flow: Sending the Set a Password and Lock Handheld IT administration commands.....	91
Related resources	92
Glossary	94
Provide feedback	100
Legal notice	101

Overview

This document describes the security features that the BlackBerry® Enterprise Server version 5.0, BlackBerry® Desktop Software version 5.0, and BlackBerry® Device Software version 5.0 support, unless otherwise stated. To determine if an earlier software version supports a security feature, see the documentation for earlier versions of the BlackBerry Enterprise Server, BlackBerry Desktop Software, and BlackBerry Device Software.

Benefits of security for wireless devices

Organizations that use wireless devices experience an increased demand for mobile content and face the potential for security threats. You must address the security needs and requirements of your organization when you evaluate wireless solutions. Wireless devices such as mobile phones and personal digital assistants can access and store the sensitive data of your organization. Without an effective security model, users with malicious intent might access sensitive data remotely using wireless devices. Users with malicious intent might expose or otherwise use sensitive data, resulting in financial and legal implications for your organization.

Threats to wireless devices

Threats to wireless devices include the following events:

- a user with malicious intent who intercepts data when a user sends and receives messages and accesses your organization's data on a wireless device
- an attack using malicious application code (for example, a virus) that steals data
- the wireless device is stolen

BlackBerry Enterprise Solution security

The BlackBerry® Enterprise Solution is designed to encrypt data that is in transit at all points between BlackBerry devices and the BlackBerry® Enterprise Server to help protect your organization from data loss or alteration. Only the BlackBerry Enterprise Server and BlackBerry devices can decrypt the data that they send between each other. If events that threaten the wireless security of your organization occur, the BlackBerry Enterprise Solution is designed to prevent third parties, including wireless service providers, from accessing potentially sensitive information in a decrypted format.

The BlackBerry Enterprise Solution uses symmetric key cryptography to encrypt messages and data that it sends over the transport layer. Symmetric key cryptography provides security for wired and wireless solutions using the following criteria.

Criteria	Description
Confidentiality	The BlackBerry Enterprise Solution uses encryption to help make sure that only the intended message recipients can view the contents of email messages.
Integrity	<p>The BlackBerry Enterprise Solution uses one or more message keys to help protect every message that a BlackBerry device sends. To help prevent a third party from decrypting or altering the message data, the BlackBerry Enterprise Solution is designed so that the message keys consist of random data.</p> <p>Only the BlackBerry Enterprise Server and a BlackBerry device know the value of a master encryption key, recognize the format of a decrypted and decompressed message, and automatically reject a message that is not encrypted with the correct master encryption key.</p>
Authenticity	A BlackBerry device authenticates with the BlackBerry Enterprise Server to prove that the BlackBerry device knows the master encryption key before the BlackBerry Enterprise Server can send data to the BlackBerry device.

If the BlackBerry device or BlackBerry Enterprise Server do not recognize the format of a data packet or receive a data packet that is encrypted with the wrong encryption key, they reject the data packet. The BlackBerry device prompts the user to generate a new master encryption key.

New security features

Feature	Supported software versions	Description
Enroll certificates over the wireless network	<ul style="list-style-type: none"> BlackBerry® Enterprise Server version 5.0 BlackBerry® Device Software version 5.0 	You can configure the BlackBerry Enterprise Server to permit BlackBerry devices to enroll certificates over the wireless network. Permitting BlackBerry devices to enroll the certificates is an alternative to instructing users to send the certificates to themselves in an email message or using the certificate synchronization tool in the BlackBerry® Desktop Software.
Encrypt messages using IBM® Lotus® Notes® encryption on the BlackBerry device	<ul style="list-style-type: none"> BlackBerry Enterprise Server version 5.0 BlackBerry Device Software version 5.0 	You can configure the BlackBerry Enterprise Server to permit users to encrypt messages using IBM Lotus Notes encryption. When users create, forward, or reply to messages, they can indicate whether they want the BlackBerry Enterprise Server to encrypt the messages.

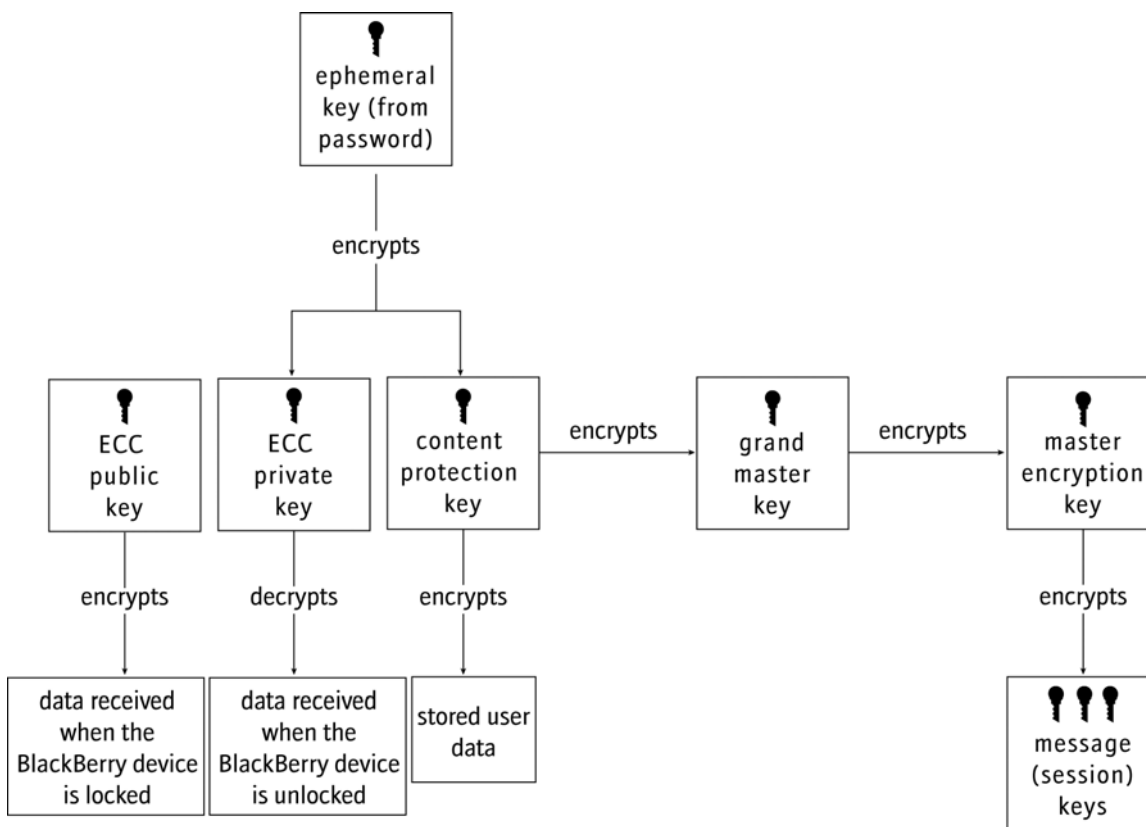
BlackBerry Enterprise Solution security features

Feature	Description
data protection	<ul style="list-style-type: none"> • Encrypt data that is in transit between the BlackBerry® Enterprise Server and BlackBerry device. • Encrypt data that is in transit between your organization's messaging server and the email application on the user's computer. • Use protocols that are designed to be highly secure to connect the BlackBerry Enterprise Server to the BlackBerry® Infrastructure. • Encrypt data on the BlackBerry device. • Encrypt data in the BlackBerry Configuration Database. • Authenticate a user to the BlackBerry device using a smart card with a password or pass phrase. • Verify the authenticity and integrity of the operating system of the BlackBerry device and BlackBerry® Device Software automatically.
encryption keys protection	<ul style="list-style-type: none"> • Encrypt encryption keys on the BlackBerry device.
control of BlackBerry device connections	<ul style="list-style-type: none"> • Control which BlackBerry devices can connect to the BlackBerry Enterprise Server. • Control Bluetooth® connections to and from the BlackBerry device. • Control BlackBerry® Smart Card Reader connections. • Control Wi-Fi® enabled BlackBerry device connections to enterprise Wi-Fi networks.
control of BlackBerry devices and BlackBerry Desktop® Software	<ul style="list-style-type: none"> • Send IT administration commands to label a BlackBerry device with owner information, delete application data from BlackBerry devices, and lock BlackBerry devices. • Send IT policies to BlackBerry devices to change security settings for user accounts or groups that you assigned to a BlackBerry Enterprise Server. • Send application control policies to BlackBerry devices to control whether third-party application are available and able to connect to BlackBerry devices. • Enforce BlackBerry device and BlackBerry Smart Card Reader passwords.

Encryption keys on BlackBerry devices

By default, the BlackBerry® Enterprise Solution generates the master encryption key and message key that the BlackBerry® Enterprise Server and BlackBerry devices use to encrypt and decrypt all data that they send between each other. The BlackBerry device uses a PIN encryption key to encrypt PIN messages.

You can permit the BlackBerry device to generate and use the content protection key to encrypt user data on the BlackBerry device when the BlackBerry device is locked. You can permit the BlackBerry device to generate and use the grand master key to encrypt the master encryption key when the BlackBerry device is locked.



Master encryption key of the BlackBerry device

The master encryption key encrypts the message keys. The BlackBerry® Enterprise Server and a BlackBerry device each store a copy of the master encryption key of the BlackBerry device. The BlackBerry® Enterprise Solution is designed so that only the BlackBerry Enterprise Server and the BlackBerry device know the value of the master encryption key. When you activate the BlackBerry device over the wireless network, the BlackBerry Enterprise Server and BlackBerry device use an authenticated connection to communicate the value of the master encryption key to each other.

The BlackBerry Enterprise Server and BlackBerry device must store matching copies of the master encryption key. If the master encryption keys do not match, the following actions occur:

- the BlackBerry Enterprise Server and BlackBerry device delete messages that they receive from each other because they cannot decrypt them
- the BlackBerry device prompts the user to generate a new master encryption key

States of master encryption keys

State	Description
Current	The current master encryption key is the master encryption key that the BlackBerry® device currently uses to encrypt and decrypt message keys.
previous	<p>The previous master encryption keys are the master encryption keys that the BlackBerry device used before the user generated the current master encryption key.</p> <p>The BlackBerry device stores previous master encryption keys in flash memory for 7 days, which is the maximum amount of time that the BlackBerry® Enterprise Server queues a pending message for delivery. The BlackBerry device stores previous master encryption keys so that a user can decrypt messages even when the user generates a new master encryption key multiple times while messages are queued on the BlackBerry Enterprise Server.</p> <p>The messaging server and BlackBerry Configuration Database store only the previous master encryption key that is most recent.</p>
pending	<p>The pending master encryption key is the master encryption key that you generate in the BlackBerry Administration Service to replace the current master encryption key.</p> <p>The BlackBerry® Desktop Software sends the pending master encryption key to the BlackBerry device when the user connects the BlackBerry device to the computer. The current master encryption key becomes the previous master encryption key, and the pending master encryption key becomes the current master encryption key.</p> <p>Only the messaging server and BlackBerry Configuration Database store the pending master encryption key.</p>

Storage locations of the master encryption keys

The BlackBerry® Enterprise Server, messaging server, and BlackBerry device store different types of encryption keys, including the current master encryption key.

A BlackBerry device stores the master encryption key in a key store database in flash memory. This storage location is designed to prevent an attacker from extracting the key data from flash memory by backing up the data from the BlackBerry device on to a computer.

Messaging server	Storage location in the messaging server	Storage location in the BlackBerry device	Storage location in the BlackBerry Enterprise Server
IBM® Lotus® Domino®	BlackBerry profiles database	key store database in flash memory	BlackBerry Configuration Database
Microsoft® Exchange	mail box of the email application on the user's computer	key store database in flash memory	BlackBerry Configuration Database
Novell® GroupWise®	not stored in the messaging server	key store database in flash memory	BlackBerry Configuration Database

The BlackBerry Enterprise Server, messaging server, and BlackBerry device can also store previous and pending master encryption keys. The BlackBerry Configuration Database stores all master encryption keys with the user data of the BlackBerry devices. To avoid compromising the master encryption keys, you should protect the BlackBerry Configuration Database and the storage location of the master encryption key on the messaging server.

Related topics

Protecting the connection between the messaging server and the email application
Algorithm suites that the BlackBerry device supports for negotiating SSL connections
Protecting the BlackBerry Configuration Database

Where Microsoft Exchange stores the master encryption keys

A Microsoft® Exchange server stores the master encryption keys in a hidden folder that is named BlackBerryHandheldInfo. The BlackBerryHandheldInfo folder is located in a root folder of the mail box for the user. The BlackBerryHandheldInfo folder stores the following data:

- a message of class RIM.BlackBerry.Handheld.Config that contains the user's configuration information, including the data for the master encryption key
- the master encryption keys in binary form with tags that indicate whether the keys are pending, current, or previous

The 0x6002 tag indicates a pending master encryption key, the 0x6003 tag indicates a current master encryption key, and the 0x6004 tag indicates a previous master encryption key.

Where IBM Lotus Domino stores the master encryption keys

An IBM® Lotus® Domino® server stores the master encryption keys in a database that is named BlackBerryProfiles.nsf. The BlackBerry profiles database contains configuration information for every user account that exists in the Data directory. The BlackBerry profiles database stores an account record that contains the RIMCurrentEncryptionKeyText field, which stores the master encryption keys for every user account in alphanumeric representation of a hexadecimal string.

Generating a master encryption key using the BlackBerry Desktop Software

When a user connects a BlackBerry® device to the computer for the first time, the BlackBerry® Desktop Software generates the master encryption key and sends it to the BlackBerry device and messaging server. The next time that a user connects a BlackBerry device to the computer, the user can prompt the BlackBerry Desktop Software to regenerate the master encryption key.

By default, the BlackBerry® Enterprise Server sends a request to the BlackBerry Desktop Software every 31 days to prompt users to regenerate the master encryption key on the BlackBerry devices, even if the user chooses to generate keys manually in the BlackBerry® Desktop Manager.

Process flow: Generating a master encryption key using BlackBerry Desktop Software version 4.0 or later

In BlackBerry® Desktop Software version 4.0 or later, the function for generating master encryption keys uses the current time as the seed for the srand function from the C programming language. The srand function gathers randomness using the following process:

1. The BlackBerry Desktop Software prompts the user to move the mouse. The srand function examines the lowest 12 bits of the x and y coordinates of the new mouse location. If the bits are different from the previous sample, the BlackBerry Desktop Software stores the bits, which generates 3 bytes of randomness. If the bits are the same as the bits in the previous sample, the BlackBerry Desktop Software does not store any bits.
2. The function waits for a random interval between 50 and 150 milliseconds, and then continues to store bits until it gathers 384 bytes of randomness.
3. The BlackBerry Desktop Software retrieves 384 bytes of randomness from the Microsoft® Cryptographic API, for a total of 768 bytes.
4. The BlackBerry Desktop Software hashes the 384 bytes of randomness from the mouse coordinates of the user and the 384 bytes of randomness from the MSCAPI with SHA-512 to produce 512 bits of data.
5. The BlackBerry Desktop Software frees the memory that is associated with the unused bits.
6. If the BlackBerry Desktop Software uses AES encryption, it uses the first 256-bits of data to generate the master encryption key. If the BlackBerry Desktop Software uses Triple DES encryption, it uses the first 128 bits of data to generate the master encryption key.
7. The BlackBerry Desktop Software discards any bits of data that it does not use to generate the master encryption key.

Process flow: Generating a master encryption key using a BlackBerry Desktop Software version earlier than version 4.0

When a BlackBerry® Enterprise Server or BlackBerry® Desktop Software version earlier than version 4.0 calls the function that they use to generate master encryption keys, the srand function from the C programming language srand function is seeded with the current time to generate a seed for the rand function. When a user responds to the BlackBerry Desktop Software prompt by moving the mouse, the rand function is designed to generate random data based on the randomness that the mouse movement gathers.

1. The BlackBerry Desktop Software prompts the user to move the mouse. When the user moves the mouse, the BlackBerry Enterprise Server or BlackBerry Desktop Software generates 2 or 4 bits, depending on whether the mouse movement changed one or both of the x and y axes. The BlackBerry Enterprise Server or BlackBerry Desktop Software generate bit samples in this way until they accumulate at least 8 bits.
2. The srand function generates a random integer.
3. The BlackBerry Enterprise Server or BlackBerry Desktop Software examines the least significant bit of the integer. If the bit is a 1, the BlackBerry Enterprise Server or BlackBerry Desktop Software stores 1s complement of the 8 accumulated bits; otherwise, the BlackBerry Enterprise Server or BlackBerry Desktop Software stores the unmodified 8 accumulated bits. This process is designed to make sure that, even if a user can replicate a previous user's mouse movements, the resulting value is still unique.
4. The algorithm continues until the BlackBerry Enterprise Server or BlackBerry Desktop Software generates a sample of 256 random bits from the mouse movements of the user.
5. The BlackBerry Enterprise Server or BlackBerry Desktop Software uses the SHA-1 function to hash the 256-bits.
6. The BlackBerry Enterprise Server or BlackBerry Desktop Software generates the master encryption key of the BlackBerry device using the first 128 bits of the hash.

Generating master encryption keys over the wireless network

During the wireless activation process, the BlackBerry® Enterprise Server and BlackBerry device negotiate to select the strongest algorithm that they both support and use the algorithm to generate a master encryption key.

If a user wants to request a new master encryption key on an activated BlackBerry device, the user can click in the Options menu, on the Security options screen, Regenerate Encryption Key. The BlackBerry device sends the key regeneration request to the BlackBerry Enterprise Server over the wireless network.

In the BlackBerry Administration Service, you can start regeneration of a master encryption key for a BlackBerry device. By default, the BlackBerry device generates a new master encryption key every 30 days.

Related topics

Authentication during wireless activation

Protocol that the BlackBerry Enterprise Server uses to establish an initial master encryption key

The BlackBerry® Enterprise Server uses the initial key establishment protocol during wireless activation to generate the first master encryption key for a BlackBerry device. The initial key establishment protocol uses the SPEKE authentication method with the activation password to generate long-term public keys on the BlackBerry device and create a strong, cryptographically protected connection between the BlackBerry device and the BlackBerry Enterprise Server. The initial key establishment protocol is designed to perform the purposes described in the following table.

Purpose	Description
provide strong authentication and integrity	The protocol verifies that only an authorized user can activate a BlackBerry device that you associated with a BlackBerry Enterprise Server.
prevent offline dictionary attacks	The protocol verifies that it is computationally infeasible for a user with malicious intent to determine a user's password by viewing the protocol packets that the BlackBerry device and BlackBerry Enterprise Server send between each other.
prevent online dictionary attacks	The protocol verifies that the BlackBerry Enterprise Server prevents a user with malicious intent from activating a

Purpose	Description
	BlackBerry device if the user with malicious intent types an incorrect activation password more than five times.
exchange long-term public keys	The protocol verifies that the BlackBerry device and BlackBerry Enterprise Server exchange keys in a highly secure manner for use with the key rollover protocol.

For more information about the SPEKE authentication method, visit <http://grouper.ieee.org/groups/> to read IEEE P1363.2 Password Based Public Key Cryptography.

Protocol that the BlackBerry device, BlackBerry Enterprise Server, and BlackBerry Desktop Software use to regenerate master encryption keys

The BlackBerry® device and the BlackBerry® Enterprise Server use the key rollover protocol to regenerate the master encryption key. If a pending master encryption key exists, when a user connects a BlackBerry device to a computer, the current master encryption key on the BlackBerry device becomes the previous master encryption key and the pending master encryption key becomes the current master encryption key. If no pending master encryption key exists, the BlackBerry® Desktop Software generates a new master encryption key.

The key rollover protocol generates the master encryption key using existing long-term public keys and the ECMQV algorithm to negotiate a common key. This method ensures that an unauthorized user cannot calculate the same master encryption key.

For more information on the MQV protocol, see *NIST: Special Publication 800-56: Recommendation on Key Establishment schemes, Draft 2.0* and the *Guide to Elliptic Curve Cryptography*.

A user with malicious intent cannot use the previous master encryption key to learn the new master encryption key. The BlackBerry device and BlackBerry Enterprise Server discard the key pair when the key rollover protocol completes. If an attack compromises both the static and ephemeral private keys for a specific key rollover protocol, the master encryption keys that the BlackBerry device and BlackBerry Enterprise Server generates from other key rollover protocols are designed to remain secure.

The key rollover protocol is designed for the following purposes.

Purpose	Description
provide strong authentication	Only a BlackBerry device that a user authenticates with or a BlackBerry Enterprise Server can initiate the key rollover protocol. A user with malicious intent cannot use a device to impersonate an activated BlackBerry device and regenerate a master encryption key.
password independent	The user does not require an activation password and you do not have to perform any actions during the key rollover protocol.
flexible initiation	You or a user can initiate the key rollover protocol at any time.
perfect forward secrecy	New master keys are independent of previous master keys. A master encryption key does not help the attacker decrypt that another master encryption key protects.
automatic updates	The BlackBerry Enterprise Server initiates the key rollover protocol after 30 days automatically.

Related topics

Authentication during wireless activation

Message keys

The BlackBerry® Enterprise Server and the BlackBerry device generate one or more message keys which are designed to protect the integrity of the data (for example, short keys or large messages), that they send. If a message consists of several data packets and exceeds 2 KB, the BlackBerry Enterprise Server and BlackBerry device generate a unique message key for each data packet.

Each message key consists of random data so that it is difficult for a third party to decrypt, re-create, or duplicate the message key.

The message key is a session key. The BlackBerry device does not store the message key persistently but frees the memory that is associated with the message key after the BlackBerry device uses the message key to decrypt the message.

Process flow: Generating message keys on the BlackBerry Enterprise Server

The BlackBerry® Enterprise Server is designed to seed a DSA PRNG function to generate a message key. For more information about the DSA PRNG function, see *Federal Information Processing Standard – FIPS PUB 186-2*.

1. The BlackBerry Enterprise Server retrieves random data from multiple sources for the seed, using a technique that the BlackBerry Enterprise Server derives from the initialization function of the ARC4 encryption algorithm.
2. The BlackBerry Enterprise Server uses the random data to reorder the contents of a 256-byte (also known as 2048-bit) state array.

If the MSCAPI exists on the computer that hosts the BlackBerry Enterprise Server, the BlackBerry Enterprise Server requests 512 bits of randomness from the MSCAPI to increase the amount of randomness.

3. The BlackBerry Enterprise Server inputs the state array into the ARC4 algorithm to further randomize the array.
4. The BlackBerry Enterprise Server draws 521 bytes from the ARC4 state array.

The BlackBerry Enterprise Server draws the additional 9 bytes ($512 + 9 = 521$) to make sure that the pointers before and after the call are not in the same place, and to allow for the fact that the first few bytes of the ARC4 state array might not be truly random.

5. The BlackBerry Enterprise Server uses SHA-512 to hash the 521-byte value to 64 bytes.
6. The BlackBerry Enterprise Server uses the 64-byte value to seed the DSA PRNG function.

The BlackBerry Enterprise Server stores a copy of the seed in a file. When the BlackBerry Enterprise Server restarts, it reads the seed from the file and uses the XOR function to compare the stored seed with the new seed.

7. The DSA PRNG function generates 128 pseudo-random bits for use with Triple DES and 256 pseudo-random bits for use with AES.
8. The BlackBerry Enterprise Server uses the pseudo-random bits with either Triple DES or AES to generate the message key.

Process flow: Generating message keys on the BlackBerry device

The BlackBerry® device is designed to seed a DSA PRNG function to generate a message key. For more information about the DSA PRNG function, see *Federal Information Processing Standard – FIPS PUB 186-2*.

1. The BlackBerry device retrieves random data from multiple sources for the seed using a technique that the BlackBerry device derives from the initialization function of the ARC4 encryption algorithm.
2. The BlackBerry device uses the random data to reorder the contents of a 256-byte (also known as 2048-bit) state array.
3. The BlackBerry device inputs the state array into the ARC4 algorithm to further randomize the state array.
4. The BlackBerry device draws 521 bytes from the ARC4 state array.

The BlackBerry device draws the additional 9 bytes ($512 + 9 = 521$) to make sure that the pointers before and after the call are not in the same place, and to allow for the fact that the first few bytes of the ARC4 state array might not be truly random.

5. The BlackBerry device uses SHA-512 to hash the 521-byte value to 64 bytes.
6. The BlackBerry device uses the 64-byte value to seed the DSA PRNG function. The BlackBerry device stores a copy of the seed in a file. When the BlackBerry device restarts, it reads the seed from the file and uses the XOR function to compare the stored seed with the new seed.

7. The DSA PRNG function generates 128 pseudo-random bits for use with Triple DES and 256 pseudo-random bits for use with AES.
8. The BlackBerry device uses the pseudo-random bits with either Triple DES or AES to generate the message key.

Content protection keys

When you or a user turns on content protection for a BlackBerry® device, the BlackBerry device generates encryption keys, including the content protection key, that are designed to encrypt user data on the BlackBerry device when the user locks it.

During the encryption process that begins when the BlackBerry device is locked, the BlackBerry device frees the memory that it associates with the content protection key and ECC private key that it stores in RAM. The BlackBerry device then uses the ECC public key, an asymmetric key, to encrypt new user data that it receives.

When a user unlocks a BlackBerry device, the BlackBerry device decrypts the content protection key and ECC private key in flash memory. When the user wants to view data, the BlackBerry device uses the content protection key or the ECC private key to decrypt the data before the BlackBerry device displays it. An unlocked BlackBerry device uses the content protection key to encrypt new data that the user types on or adds to the BlackBerry device, or that the BlackBerry device receives.

Related topics

Protecting user data on a locked BlackBerry device

Process flow: Turning on content protection using the BlackBerry Enterprise Server

When you configure the Content Protection Strength IT policy rule to turn on content protection for a BlackBerry® device, the following process occurs:

1. The BlackBerry® Enterprise Server performs the following actions:
 - selects b randomly
 - calculates $B = bP$
 - stores b in the BlackBerry Configuration Database
2. The BlackBerry Enterprise Server sends B in the IT policy to the BlackBerry device.
3. The BlackBerry device receives B and verifies that B is a valid public key.
4. The BlackBerry device performs the following actions:
 - selects d randomly
 - calculates $D = dP$
 - store D in flash memory
 - calculates $K = dB$
5. The BlackBerry device uses K to encrypt the current BlackBerry device password, and uses the encrypted password to encrypt the content protection key.
6. The BlackBerry device deletes d and K permanently.

When the BlackBerry device deletes d permanently, the data that remains on the BlackBerry device is not sufficient to recover K . Only the BlackBerry Enterprise Server knows b and can recalculate $K = dB = dbP = bD$ if it is provided with d .

Related topics

Cryptosystem parameters

Process flow: Generating content protection keys

When you or the BlackBerry® device user turns on content protection for the first time, the following process occurs:

1. The BlackBerry device uses a DSA PRNG function to generate a content protection key randomly. The content protection key is a semi-permanent key that uses 256-bit AES encryption.
2. The BlackBerry device generates an ECC key pair with a bit length that you or the user determines.
3. The BlackBerry device prompts the user to type the BlackBerry device password.

4. The BlackBerry device derives an ephemeral key that uses 256-bit AES encryption from the BlackBerry device password, using PKCS #5.
5. The BlackBerry device uses the ephemeral key to encrypt the content protection key and the ECC private key.
6. The BlackBerry device stores the encrypted content protection key, encrypted ECC private key, and ECC public key in flash memory.

If the user changes the BlackBerry device password, the BlackBerry device uses the new password to derive a new ephemeral key and uses the new ephemeral key to re-encrypt the versions of the content protection key and the ECC private key in flash memory.

For more information about the DSA PRNG function, see *Federal Information Processing Standard – FIPS PUB 186-2*. For more information about PKCS #5, visit www.rsa.com to read *PKCS #5: Password-Based Cryptography Standard*.

Related topics

Process flow: Deriving the ephemeral key that protects the content protection key and ECC private key

Process flow: Deriving the ephemeral key that protects the content protection key and ECC private key

The BlackBerry® device uses an ephemeral 256-bit AES encryption key to encrypt the content protection key and ECC private key. The BlackBerry device derives the ephemeral 256-bit AES encryption key from the BlackBerry device password using the following process:

1. The BlackBerry device selects a 64-bit salt (random data that it mixes with the BlackBerry device password). This prevents two identical passwords from turning into the same key.
2. The BlackBerry device concatenates the salt, password, and salt again into a byte array (for example, Salt|Password|Salt).
3. The BlackBerry device hashes the byte array with SHA-256.
4. The BlackBerry device stores the resulting hash in a byte array called a key.
(key) = SHA256(Salt|Password|Salt)
5. The BlackBerry device hashes the key 18 more times. It stores the result into a key each time. For example, for i=0 to 18, the BlackBerry device performs the following actions:

(key) = SHA256(key)

i++

done

6. The final hash creates the ephemeral key.

For more information, visit www.rsa.com to read *PKCS #5: Password-Based Cryptography Standard*.

Process flow: Encrypting user data on a locked BlackBerry device

1. When a BlackBerry® device locks for the first time after you or a user turns on content protection, the BlackBerry device uses the content protection key to encrypt the bulk of its stored user and application data automatically.
2. The BlackBerry device frees the memory that is associated with the decrypted content protection key and the decrypted ECC private key that is stored in RAM.
3. The locked BlackBerry device uses the ECC public key to encrypt data that it receives.

Process flow: Decrypting user data on an unlocked BlackBerry device

1. A user types the correct BlackBerry® device password to unlock it.
2. The BlackBerry device uses the password to derive the ephemeral key that uses 256-bit AES encryption.
3. The BlackBerry device uses the ephemeral key to decrypt the encrypted content protection key and ECC private key in flash memory.
4. The BlackBerry device stores the decrypted content protection key and ECC private key in RAM.

5. If a user tries to access user data that the BlackBerry device encrypted while it was unlocked, the BlackBerry device uses the decrypted content protection key to decrypt the user data.
6. If a user tries to access user data (for example, open a message) that the BlackBerry device encrypted while it was locked, the BlackBerry device uses the decrypted ECC private key to decrypt the user data and access the ECC-encrypted items (for example, the message body, subject, or recipient).
7. When the BlackBerry device opens 128 ECC-encrypted items (which is usually less than 40 messages), the BlackBerry device uses the ECC private key to decrypt the ECC-encrypted items, and the BlackBerry device re-encrypts them with the content protection key the next time that the BlackBerry device locks. If the BlackBerry device does not complete the re-encryption process before the user unlocks the BlackBerry device, the BlackBerry device resumes re-encryption when it locks again.

Grand master keys

When you turn on content protection for master encryption keys, the BlackBerry® device uses a grand master key to encrypt the master encryption keys that are stored on the BlackBerry device in flash memory. When the BlackBerry device receives data that the master encryption key encrypts while the BlackBerry device is locked, it uses the grand master key to decrypt the required master encryption key in flash memory and receive the data.

Related topics

Protected storage of master encryption keys on a locked BlackBerry device

Process flow: Generating grand master keys

When you turn on content protection for master encryption keys on the BlackBerry® device for the first time, the following process occurs:

1. The BlackBerry device generates the grand master key, a 256-bit AES encryption key.
2. The BlackBerry device stores the decrypted grand master key in RAM.
3. The BlackBerry device uses the existing content protection key to encrypt the grand master key.
4. The BlackBerry device stores the encrypted grand master key in flash memory.
5. The BlackBerry device uses the decrypted grand master key to encrypt the master encryption keys that are stored in the flash memory of the BlackBerry device.

Standard BlackBerry encryption

Standard BlackBerry® encryption is designed to provide strong security. Standard BlackBerry encryption uses a symmetric key encryption algorithm to protect data in transit between a BlackBerry device and the BlackBerry® Enterprise Server when the data is outside your organization's firewall.

Standard BlackBerry encryption is designed to encrypt data in the following scenarios:

- from the time that a user sends a message from the BlackBerry device until the time when the BlackBerry Enterprise Server receives the message
- from the time that the BlackBerry Enterprise Server receives a message until the time that the recipient reads the message on the BlackBerry device

Before the BlackBerry device sends a message, it compresses the message and encrypts the message using the master encryption key of the BlackBerry device. When the BlackBerry Enterprise Server receives a message from the BlackBerry device, the BlackBerry Dispatcher decrypts the message using the master encryption key, and then decompresses the message.

Related topics

Extending messaging security for a BlackBerry device

Algorithms for standard BlackBerry encryption

The BlackBerry® Enterprise Solution uses Triple DES or AES as the symmetric key encryption algorithms for standard BlackBerry encryption. A symmetric key encryption algorithm is designed so that only the parties that know the secret key can decrypt the encrypted data or cipher text of the scrambled message. By default, the BlackBerry® Enterprise Server uses the strongest algorithm that both the BlackBerry Enterprise Server and the BlackBerry device support for symmetric key encryption.

If you configure the BlackBerry Enterprise Server to use Triple DES and AES for symmetric key encryption, and a user uses the BlackBerry® Device Software or BlackBerry® Desktop Software version 3.7 or earlier, the BlackBerry Enterprise Solution generates the master encryption keys of the BlackBerry device using Triple DES. Otherwise, the BlackBerry Enterprise Solution generates master encryption keys using AES.

How the BlackBerry Enterprise Solution uses AES

The BlackBerry® Enterprise Solution uses AES in CBC mode to generate message keys and master encryption keys. The keys are 256-bits of data. AES offers a larger key size than Triple DES to provide greater security against brute-force attacks.

BlackBerry devices are designed to use AES to protect user data and encryption keys on BlackBerry devices from traditional attacks and side-channel attacks. Side-channel attacks can occur in the form of power analysis readings or electromagnetic radiation emissions.

BlackBerry devices are designed to use AES for countermeasures (for example, masking operations, table splitting, and random mask applications) to hide the true operations that take place on the BlackBerry devices. These countermeasures are designed to help protect the cryptographic keys and plain-text data against potential side-channel attacks at all points during the AES encryption and decryption operations so that the attacks do not reveal data that can expose the master encryption key.

By default, when the BlackBerry device supports AES, the BlackBerry Enterprise Solution uses AES for BlackBerry transport layer encryption. For more information about how the BlackBerry® Enterprise Server uses AES for BlackBerry transport layer encryption to communicate with BlackBerry devices, visit www.blackberry.com/support to read article KB05429.

Related topics

Limitations of RIM Cryptographic API support for key establishment algorithm cipher suites

How the BlackBerry Enterprise Server uses Triple DES

The BlackBerry® Enterprise Solution uses a two-key Triple DES encryption algorithm to generate message keys and master encryption keys. In the three iterations of the DES algorithm, the first 56-bit key in outer CBC mode encrypts

the data, the second 56-bit key decrypts the data, and the first key encrypts the data again. For more information about Triple DES, see *Federal Information Processing Standard - FIPS PUB 81 [3]*.

The BlackBerry Enterprise Solution stores the message keys and master encryption keys as 128-bit long binary strings, with each parity bit in the least significant bit of each of the 8 bytes of key data. The message keys and master encryption keys have overall key lengths of 112 bits and include 16 bits of parity data.

Software requirements for BlackBerry symmetric key encryption algorithms

Encryption algorithm	BlackBerry® Enterprise Server	BlackBerry® Device Software	BlackBerry® Desktop Software
Triple DES	any version	any version	any version
AES	4.0 or later	4.0 or later	4.0 or later

Process flow: Sending a message using standard BlackBerry encryption

When a BlackBerry® device sends a message, the BlackBerry device and BlackBerry® Enterprise Server use symmetric key cryptography to encrypt and decrypt the message.

1. The BlackBerry device compresses the message.
2. The BlackBerry device encrypts the message using the message key.
3. The BlackBerry device encrypts the message key using the master encryption key of the BlackBerry device.
4. The BlackBerry device sends the encrypted message key and encrypted message.
5. The BlackBerry Enterprise Server receives the encrypted message key and encrypted message from the BlackBerry device.
6. The BlackBerry Enterprise Server decrypts the message key using the master encryption key.
7. The BlackBerry Enterprise Server decrypts the message using the message key.
8. The BlackBerry Enterprise Server decompresses the message, and forwards the message to the recipient.

Process flow: Receiving a message using standard BlackBerry encryption

1. The BlackBerry® Enterprise Server receives the message.
2. The BlackBerry Enterprise Server compresses the message.
3. The BlackBerry Enterprise Server encrypts the message using the message key.
4. The BlackBerry Enterprise Server encrypts the message key using the master encryption key of the BlackBerry device.
5. The BlackBerry Enterprise Server sends the encrypted message and encrypted message key to the BlackBerry device.
6. The BlackBerry device receives the encrypted message and encrypted message key.
7. The BlackBerry device decrypts the message key using the master encryption key.
8. The BlackBerry device decrypts the message using the message key.
9. The BlackBerry device decompresses the message.

Permitting third-party applications to encode data on the BlackBerry device

The BlackBerry® Enterprise Server and BlackBerry® Device Software support the Transcoder API that permits third-party application developers to create encoding schemes that encrypt, convert, or change the format of data, and apply an encoding scheme to data on the BlackBerry device using transcoder application code. The Transcoder API is part of the BlackBerry® Java® Development Kit. The third-party encoding scheme prepends a transcoder ID to the data that it encodes and the BlackBerry® Enterprise Solution encrypts the transcoder-encoded data using standard BlackBerry encryption.

The BlackBerry Enterprise Solution permits only third-party encoding schemes that the Research In Motion signing authority system has signed digitally using the RIM Cryptographic API public key to access the Transcoder API to create the transcoder application code. To apply the third-party encoding scheme, the BlackBerry device must run corresponding transcoder application code.

Third-party application developers can use the Transcoder API to add cryptographic components that, by default, the RIM Cryptographic API does not support to their third-party encoding schemes. The BlackBerry Enterprise Solution applies the third-party encoding schemes to any outgoing data that the standard BlackBerry encryption applies to. The Transcoder API supports the use of all of the cryptography that the RIM Cryptographic API supports.

If you permit third-party applications to use the Transcoder API on BlackBerry devices and the applications do not run correctly, there might be an impact to the security, usability, and performance of the BlackBerry Enterprise Solution, and this might result in a loss of data on the BlackBerry device. To use the third-party encoding scheme, you must use the Security Transcoder Cod File Hashes IT policy rule to specify the .cod file for the third-party encoding scheme that the BlackBerry device permits to register as a transcoder. For more information about using the Security Transcoder Cod File Hashes IT policy rule, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Related topics

RIM Cryptographic API

BlackBerry device memory

Type of memory	Description
NV store	NV store is a non-volatile store that persists in flash memory and only the operating system of the BlackBerry® device can overwrite it. Third-party application code cannot write to the NV store. The BlackBerry device erases flash memory when you or a user deletes all BlackBerry device data.
flash memory (internal to the BlackBerry device)	Flash memory is a file system that stores application and user data on a BlackBerry device. You cannot physically remove it from the BlackBerry device. Sections of flash memory can store files that a user downloads or saves manually to the flash memory of the BlackBerry device.
memory card file system (external or internal to the BlackBerry device)	<p>The memory card file system stores files that a user saves on a BlackBerry device manually. The user might save files to an external memory file system (for example, a removable media card) or to the internal memory file system that the BlackBerry device uses and exposes similar to an external memory file system. The BlackBerry device erases the internal memory when you delete all BlackBerry device data.</p> <p>You can install, access, and encrypt external memory file systems on a BlackBerry device. A BlackBerry device does not erase external memory file systems when you delete all BlackBerry device data.</p>

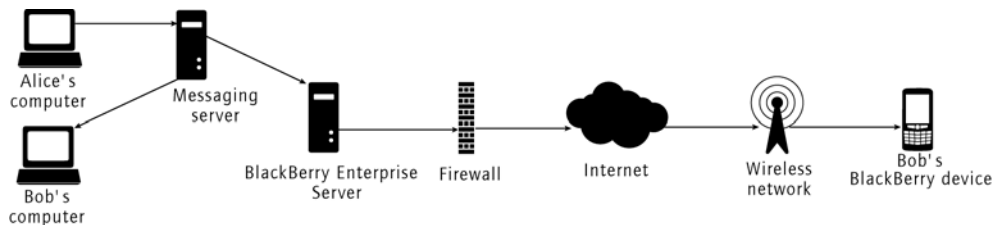
Related topics:

Deleting all device data

Wireless messaging security for the BlackBerry Enterprise Solution

The BlackBerry® Enterprise Solution is designed to work seamlessly with existing networks while enabling users to send and receive email messages securely. Email messages remain encrypted in transit between BlackBerry devices and the BlackBerry® Enterprise Server.

Process flow: Receiving an email message on a BlackBerry device

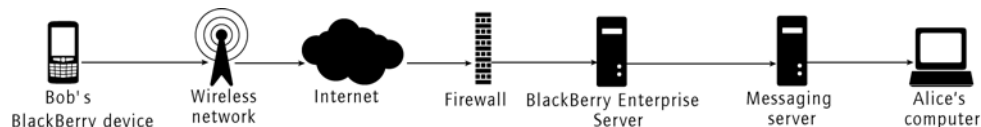


1. Alice sends a message to Bob from her computer. Alice and Bob work at the same organization.
2. The messaging server receives the email message and notifies the BlackBerry® Enterprise Server that the message has arrived.
3. The messaging server sends the message to Bob's computer.
4. The BlackBerry Enterprise Server retrieves the message from the messaging server.
5. The BlackBerry Enterprise Server queries the messaging server for user preferences to determine whether to forward the message to Bob's BlackBerry device.
6. The BlackBerry Enterprise Server compresses and encrypts the message.
7. The BlackBerry Enterprise Server places the message in the outgoing queue.

The BlackBerry Enterprise Server is designed to maintain a constant, direct outbound TCP/IP connection to the wireless network over the Internet through the firewall on port 3101 (or port 4101 if using a Wi-Fi® enterprise network). This constant connection permits the efficient, continuous delivery of data to and from the BlackBerry device.

8. The wireless network sends the encrypted message to Bob's BlackBerry device.
9. Bob's BlackBerry device receives the encrypted message. The BlackBerry device decrypts and displays the message for Bob to read.

Process flow: Sending an email message from a BlackBerry device



1. Bob responds to Alice's message by composing an email message on his BlackBerry® device. When Bob sends the message, the BlackBerry device compresses, encrypts, and sends the message over the wireless network to the BlackBerry® Infrastructure.

All messages that users create on their BlackBerry devices contain the BlackBerry® Enterprise Server routing information for the wireless network to ensure that the wireless network delivers the message to the appropriate BlackBerry Enterprise Server.

2. The BlackBerry Infrastructure sends the encrypted message to the BlackBerry Enterprise Server that the user account is assigned to.

The connection from the BlackBerry Enterprise Server to the BlackBerry Infrastructure is a two-way TCP connection on port 3101. The BlackBerry Infrastructure directs messages from the BlackBerry device over this connection using the routing information in the message.

3. The BlackBerry Enterprise Server receives the message.
4. The BlackBerry Enterprise Server decrypts, decompresses, and sends the message to the messaging server.

The BlackBerry Enterprise Server does not store a copy of the message.

5. The messaging server delivers the message to Alice's computer.

How the BlackBerry Enterprise Solution secures attachments

BlackBerry® devices support attachment viewing using the BlackBerry Attachment Service. The BlackBerry Attachment Service permits users to open supported attachments on their BlackBerry devices. For information about which attachment file format are supported, see the *BlackBerry Enterprise Server Feature and Technical Overview*.

The BlackBerry Attachment Service is designed to prevent malicious applications from accessing data on BlackBerry devices. The BlackBerry Attachment Service uses binary format parsing to open the attachments and prepare them to be sent to a BlackBerry device for rendering. BlackBerry devices do not run applications that they receive as attachments in email messages or meeting invitations.

You can install the BlackBerry Attachment Service on a computer that is separate from the computer that hosts the BlackBerry Enterprise Server and place the BlackBerry Attachment Service on its own network segment to prevent the spread of potential attacks from the BlackBerry Attachment Service to other computers within your organization's network.

Related topics

Using a segmented network architecture

Process flow: Viewing attachments in PGP encrypted or S/MIME-encrypted messages

You can use the S/MIME Allowed Encrypted Attachment Mode IT policy rule and the PGP® Allowed Encrypted Attachment Mode IT policy rule to specify the least restrictive mode that a BlackBerry® device can use to retrieve PGP (OpenPGP or PGP/MIME message formatting) encrypted and S/MIME-encrypted attachment information.

When a user receives an OpenPGP encrypted message that includes an attachment, the BlackBerry® Enterprise Server reads the attachment header data and is designed to send the message and the encrypted message key to the BlackBerry device automatically.

How a BlackBerry device responds when it receives a PGP/MIME encrypted or S/MIME encrypted message that contains an attachment depends on the value of the S/MIME Allowed Encrypted Attachment Mode IT policy rule or the PGP Allowed Encrypted Attachment Mode IT policy rule. These rules determine if the following actions occur automatically when the user opens the message, or if the user must request the actions manually:

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

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

When a user tries to view an attachment that is encrypted using S/MIME, PGP/MIME, or OpenPGP on a BlackBerry® device, the following actions occur:

1. The BlackBerry device sends the message key and the request for the attachment data to the BlackBerry® Enterprise Server.
2. The BlackBerry Enterprise Server uses the message key to decrypt the message and access the attachment data that corresponds to the attachment header data.

3. The BlackBerry Enterprise Server decrypts the attachment and sends the rendered attachment data to the BlackBerry device.
4. The BlackBerry device displays the attachment.

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

PIN messaging

A PIN identifies each BlackBerry® device and BlackBerry enabled device on the wireless network. If a user knows the PIN of another BlackBerry device, the user can send a PIN message to the BlackBerry device. Unlike a message that a user sends to an email address, a PIN message bypasses the BlackBerry® Enterprise Server and your organization's network.

BlackBerry devices scramble PIN messages using the PIN encryption key. By default, all BlackBerry devices share a global PIN encryption key which allows all BlackBerry devices to decrypt every PIN message that they receive. PIN messages are designed to be scrambled, but not encrypted, messages.

Generating a PIN encryption key that is specific to your organization

During the manufacturing process, Research In Motion loads a global PIN encryption key on BlackBerry® devices. To limit the number of BlackBerry devices that can receive and decrypt PIN messages in your organization, you can generate a PIN encryption key that is specific to your organization. A BlackBerry device that has a PIN encryption key that is specific to your organization can send and receive PIN messages with other BlackBerry devices on your organization's network that have the same PIN encryption key. These PIN messages use scrambling that is specific to your organization instead of the default global scrambling.

You can also configure the Firewall Block Incoming Messages IT policy rule to limit the number of BlackBerry devices in your organization that can receive PIN messages that use scrambling that is specific to your organization, PIN messages that use the default global scrambling, or both.

You should generate a new PIN encryption key if you know that the current key is compromised. You can update and resend the PIN encryption key for users in the BlackBerry Administration Service.

Sending SMS text messages and MMS messages

Supported BlackBerry® devices can send SMS text messages and MMS messages over the wireless TCP/IP connection. BlackBerry devices do not encrypt or scramble text messages.

Best practice: Controlling unsecured wireless messaging in your organization

You can control unsecured messaging methods such as PIN, SMS text messages, and MMS message in your organization using the following IT policy rules:

Scenario	IT policy rule	Value
prevent applications from initiating external connections (for example, to WAP, SMS, MMS or other public gateways) on a BlackBerry® device	Allow External Connections	No
require a user to confirm that they want to send the message before they send an email message, PIN message, SMS text message, or MMS message	Confirm on Send	Yes
<ul style="list-style-type: none"> • prevent a user from forwarding or replying to a message using a BlackBerry® Enterprise Server that did not deliver the original message • prevent a user from using an email account to forward or reply to a PIN message or reply to an email message with a PIN message 	Disable Forwarding Between Services	Yes
prevent a user from sending plain-text PIN messages when using a secure messaging package, such as the S/MIME Support Package for BlackBerry®	Disable Peer-to-Peer Normal Send	Yes

Scenario	IT policy rule	Value
smartphones or the PGP® Support Package for BlackBerry® smartphones		
limit the number of BlackBerry devices in your organization's environment that can receive SMS text messages, MMS messages, BlackBerry® Internet Service messages, PIN messages that use scrambling that is specific to your organization, and PIN messages that use the default global scrambling	Firewall Block Incoming Messages	Yes

Best practice: Turning off unsecured messaging

You can turn off unsecured messaging to make sure that all communication for BlackBerry® devices that starts in your organization travels through your organization's messaging environment.

Scenario	Description
turn off PIN messaging	Change the Allow Peer-to-Peer Messages IT policy rule to No. When you turn off PIN messaging, users cannot send PIN messages from their BlackBerry devices; however, they can still receive PIN messages on their BlackBerry devices.
turn off SMS text messaging	Change the Allow SMS IT policy rule to No.
turn off MMS messaging	Change the Disable MMS IT policy rule to Yes.

Extending messaging security for a BlackBerry device

When a user sends a message from a BlackBerry® device using standard BlackBerry encryption, the BlackBerry® Enterprise Server does not encrypt the message when the BlackBerry Enterprise Server forwards the message to the recipient. To extend the messaging security that standard BlackBerry encryption provides, a user must install secure messaging technology on the BlackBerry device, and you must configure the BlackBerry device to use the secure messaging technology.

When you turn on PGP® encryption or S/MIME encryption on a BlackBerry device, you permit sender-to-recipient authentication and confidentiality for email messages or PIN messages. These encryption technologies help to maintain the integrity and privacy of the data from the time that a user sends a message from a BlackBerry device to the time that the message is decrypted and the recipient opens the message.

Using the PGP Support Package for BlackBerry smartphones

The PGP® Support Package for BlackBerry® smartphones is designed to support OpenPGP and PGP/MIME message formatting on BlackBerry devices. Users who send and receive PGP protected messages in OpenPGP and PGP/MIME formats using the email applications on their computers can send and receive PGP protected messages using their BlackBerry devices.

The PGP Support Package for BlackBerry smartphones includes tools that you can use to retrieve PGP keys and transfer them to BlackBerry devices. This permits users to digitally sign, encrypt, and send PGP protected messages from BlackBerry devices. If a user does not install the PGP Support Package for BlackBerry smartphones, the BlackBerry devices receive PGP protected messages as unreadable cipher text.

If your organization's environment includes a PGP® Universal Server, the administrator of the PGP Universal Server can design secure email policies. BlackBerry devices with the PGP Support Package for BlackBerry smartphones installed enforce compliance with the secure email policies for all email messages.

The PGP Support Package for BlackBerry smartphones is designed to support the following actions:

- use the PGP Universal Server to retrieve and enforce secure email policies
- search for and retrieve PGP keys, PGP key status, and X.509 certificate status over the wireless network using a PGP Universal Server or an external LDAP key server
- configure BlackBerry devices to connect to external LDAP key servers using SSL or TLS (also known as LDAPS) connections
- encrypt and decrypt PGP protected email and PIN messages
- use PGP key-only encryption when BlackBerry devices send PGP protected messages
- verify digital signatures on incoming email and PIN messages, and digitally sign outgoing email and PIN messages
- encode and decode Unicode messages

BlackBerry devices are designed to use the BlackBerry MDS Connection Service, to connect to the PGP Universal Server and to any external LDAP key server that users specify on their BlackBerry devices. The BlackBerry MDS Connection Service uses standard protocols, such as HTTP and TCP/IP, to permit BlackBerry devices to retrieve PGP keys and PGP key status from the PGP Universal Server or an external LDAP key server over the wireless network.

For more information about OpenPGP, see RFC 2440. For more information about PGP/MIME, see RFC 3156.

PGP key types

PGP® technology relies on public key cryptography which uses private and public key pairs to provide confidentiality, integrity, and authenticity.

The PGP® Support Package for BlackBerry® smartphones uses public key cryptography with the following keys:

Key type	Description
PGP public key	BlackBerry devices use the recipient's PGP public key to encrypt outgoing email messages and the sender's PGP public key to verify digital signatures on incoming email messages. The PGP public key is designed so that message recipients and senders can distribute and access without compromising security conditions.
PGP private key	BlackBerry devices use the PGP private key to digitally sign outgoing email messages and decrypt incoming email messages. To make sure that security is not compromised, private key information must remain private to the key owner.

Process flow: Sending a message using PGP encryption

If the user installs the PGP® Support Package for BlackBerry® smartphones on a BlackBerry device, the BlackBerry device encrypts the outgoing messages using the following process:

1. The BlackBerry device encrypts the message using the message recipient's PGP public key.
2. The BlackBerry device uses standard BlackBerry encryption to encrypt the PGP encrypted message.
3. The BlackBerry device sends the encrypted message to the BlackBerry® Enterprise Server.
4. The BlackBerry Enterprise Server removes the standard BlackBerry encryption and sends the PGP encrypted message to the recipient.

Process flow: Receiving a PGP encrypted message

If the user installs the PGP® Support Package for BlackBerry® smartphones on a BlackBerry device, the BlackBerry device decrypts the incoming message using the following process:

1. The BlackBerry® Enterprise Server receives the PGP protected message.
2. The BlackBerry Enterprise Server uses standard BlackBerry encryption to encrypt the PGP encrypted message.
3. The BlackBerry Enterprise Server sends the encrypted message to the BlackBerry device.
4. The BlackBerry device decrypts the standard BlackBerry encryption and stores the PGP encrypted message.
5. When the user opens the message on the BlackBerry device, the BlackBerry device decrypts the PGP encrypted message and displays the contents of the message.

PGP encryption algorithms

The default value of the PGP Allowed Content Ciphers IT policy rule specifies that a BlackBerry® device can use any supported algorithm to encrypt PGP® protected messages. You can configure the PGP Allowed Content Ciphers IT policy rule to encrypt PGP messages using AES-256, AES-192, AES-128, CAST-128, and Triple DES-168 ciphers.

The recipient's PGP key indicates which content ciphers that the recipient's email application can support, and the BlackBerry device is designed to use one of those ciphers. By default, if the recipient's PGP key does not include a list of ciphers, the BlackBerry device encrypts the message using Triple DES.

For more information, see the *PGP Support Package for BlackBerry Devices Security Technical Overview*.

Using the S/MIME Support Package for BlackBerry smartphones

The S/MIME Support Package for BlackBerry® smartphones is designed to permit users who send and receive S/MIME messages using the email applications on their computers to send and receive S/MIME-protected messages using their BlackBerry devices. The S/MIME Support Package for BlackBerry smartphones is designed to work with S/MIME email applications including Microsoft® Outlook®, Microsoft Outlook Express, and IBM® Lotus Notes®, and with popular PKI components, including Netscape®, Entrust® Authority™ Security Manager version 5 and later, and Microsoft certificate authorities.

The S/MIME Support Package for BlackBerry smartphones includes tools that you can use to retrieve certificates and transfer them to BlackBerry devices. This permit users to decrypt messages that are encrypted using S/MIME

encryption and sign, encrypt, and send S/MIME messages from BlackBerry devices. Without the S/MIME Support Package for BlackBerry smartphones, the BlackBerry® Enterprise Server sends messages that contain message bodies with statements that the S/MIME message cannot be decrypted to BlackBerry devices.

The S/MIME Support Package for BlackBerry smartphones supports the following actions:

- synchronize and manage certificates and private keys using the certificate synchronization tool that is included in the BlackBerry® Desktop Software
- encrypt and decrypt messages (including PIN messages), verify digital signatures, and digitally sign outgoing messages
- permit BlackBerry devices to use a password that the sender and recipient share manually between them to encrypt S/MIME-protected email or PIN messages
- search for and retrieve certificates and certificate status using PKI protocols over the wireless network
- use smart cards on BlackBerry devices
- encode and decode Unicode messages

PKI component support

The S/MIME Support Package for BlackBerry® smartphones is designed to support the following PKI components:

PKI component	Description
LDAP	BlackBerry devices and the certificate synchronization tool of the BlackBerry® Desktop Software use LDAP or LDAPS to search for and download certificates.
OCSP	BlackBerry devices and the certificate synchronization tool use OCSP to check the revocation status of a certificate on demand.
Certificate revocation list	BlackBerry devices and the certificate synchronization tool retrieve the most recent revocation status of certificates from a certificate revocation list. The certificate authority publishes the certificate revocation list at a frequency that the certificate authority administrator configures.

Process flow: Sending a message using S/MIME encryption

If the user installs the S/MIME Support Package for BlackBerry® smartphones on a BlackBerry device, the BlackBerry device encrypts the outgoing messages using the following process:

1. The BlackBerry device encrypts the message with the S/MIME certificate of the recipient or a shared password. If the user types the shared password, the BlackBerry device combines the password with random bytes to generate a new encryption key.
2. The BlackBerry device uses standard BlackBerry encryption to encrypt the S/MIME-encrypted message.
3. The BlackBerry device sends the encrypted data to the BlackBerry® Enterprise Server.
4. The BlackBerry Enterprise Server decrypts the standard BlackBerry encryption and sends the S/MIME-encrypted message to the recipient.

Process flow: Receiving an S/MIME-encrypted message

If the user installed the S/MIME Support Package for BlackBerry® smartphones, the BlackBerry device decrypts the incoming message using the following process:

1. The BlackBerry® Enterprise Server receives the S/MIME-protected message.
2. If the message is signed-only or weakly encrypted and you turned on the Turn on S/MIME encryption on signed and weakly encrypted messages option in the BlackBerry Administration Service, the BlackBerry Enterprise Server encrypts the message a second time with S/MIME encryption.

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 decrypts the standard BlackBerry encryption and stores the S/MIME-encrypted message.
6. When the user opens the message on the BlackBerry device, the BlackBerry device decrypts the S/MIME-encrypted message and displays the message contents. If the message is encrypted with a shared password, the user types the shared password to decrypt the S/MIME-protected message.

S/MIME encryption algorithms

When you turn on S/MIME encryption on the BlackBerry® Enterprise Server, the default value of the S/MIME Allowed Content Ciphers IT policy rule specifies that BlackBerry devices can use any of the supported algorithms except the two weakest RC2 algorithms, RC2 (64-bit) and RC2 (40-bit) to encrypt S/MIME messages.

You can use the Weak Digest Algorithms IT policy rule to specify algorithms that your organization considers weak. BlackBerry devices use the list of weak algorithms in the Weak Digest Algorithms IT policy rule when they verify the following information:

- that an S/MIME-enabled application did not use a weak hash digest to generate the digital signatures on messages that the BlackBerry devices receive
- that the certificate chains for the certificates that an S/MIME-enabled application used to sign messages that the BlackBerry devices receive do not contain hashes generated using a weak digest

You can configure the S/MIME Allowed Content Ciphers IT policy rule to permit BlackBerry devices to encrypt S/MIME messages using 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 a BlackBerry device received a message from an intended recipient previously, the BlackBerry device is designed to recall which content ciphers the recipient can support, and use one of those ciphers. By default, if the BlackBerry device does not know the decryption capabilities of the recipient, the BlackBerry device encrypts the message using Triple DES.

S/MIME certificates

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

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

S/MIME private keys

When a user sends a signed message from a BlackBerry® device, the BlackBerry device hashes the message using SHA-1, SHA-256, SHA-384, SHA-512, or MD5, and then uses the S/MIME private key of the BlackBerry device user to digitally sign the message hash.

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

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

Using IBM Lotus Notes encryption on BlackBerry devices

By default, when using BlackBerry® Enterprise Server version 4.1 or later for IBM® Lotus® Domino® in an environment that includes IBM® Lotus Notes® API version 7.0 or later, BlackBerry devices can decrypt messages that are encrypted using IBM Lotus Notes encryption or S/MIME encryption. The BlackBerry Enterprise Server uses the AES algorithm with the master encryption key of the BlackBerry device to encrypt the Notes .id file and password and store the file and password in the BlackBerry Messaging Agent memory.

In BlackBerry Enterprise Server version 5.0 or later and BlackBerry® Device Software version 5.0 or later, users can encrypt messages using IBM Lotus Notes encryption. When users create, forward, or reply to messages, users can indicate whether they want the BlackBerry Enterprise Server to encrypt the messages.

You can configure the default behavior of BlackBerry devices using the following methods:

- Use the Disable Notes Native Encryption Forward And Reply IT policy rule to prevent users from forwarding and replying to IBM Lotus Notes encrypted messages on BlackBerry devices.
- Use the Notes Native Encryption Password Timeout IT policy rule to specify the maximum duration (in minutes) that the BlackBerry device stores the Notes .id password that the user types.
- Use the Require Notes Native Encryption For Outgoing Messages IT policy rule to require users to forward and reply to messages using IBM Lotus Notes encryption.

Process flow: Decrypting a message using IBM Lotus Notes encryption

1. A user receives an IBM® Lotus Notes® encrypted message on the BlackBerry® device.
2. The BlackBerry Messaging Agent decrypts the user's cached Lotus Notes .id password and uses the password to decrypt the message.

If the BlackBerry Messaging Agent does not have the Lotus Notes .id password, the user must select More, More All, or Open Attachment to send the decrypted message to the BlackBerry device.
3. The BlackBerry® Enterprise Server deletes the decrypted Lotus Notes .id password from memory. The encrypted Lotus Notes .id password remains cached.
4. The BlackBerry Enterprise Server sends the decrypted message to the BlackBerry device.

Process flow: Encrypting a message using IBM Lotus Notes encryption

1. The user indicates that the BlackBerry® Enterprise Solution must encrypt the message.
2. The BlackBerry device prompts the user for the IBM® Lotus Notes® .id password.
3. The BlackBerry device configures the message for Lotus Notes encryption.
4. The BlackBerry device sends the message and the Lotus Notes .id password to the BlackBerry® Enterprise Server.
5. The BlackBerry Messaging Agent decrypts the cached Lotus Notes .id password of the user and validates the password that the BlackBerry device sent.
6. If the BlackBerry Messaging Agent can verify the password, the BlackBerry Messaging Agent uses the password to encrypt the message.
7. The BlackBerry Enterprise Server sends the encrypted message to the messaging server so that the messaging server can deliver it to the recipient.

How the BlackBerry Messaging Agent protects the Lotus Notes .id password

After a user imports the IBM® Lotus Notes® .id file and password (which is stored in the Lotus Notes .id file), the BlackBerry® device and the BlackBerry Messaging Agent perform the following actions:

- The BlackBerry device encrypts the password that is located in the BlackBerry device memory using AES with the master encryption key of the BlackBerry device.
- The BlackBerry Messaging Agent encrypts the password in the BlackBerry Messaging Agent memory using AES with the master encryption key of the BlackBerry device.
- The BlackBerry device decrypts the password before it calls the required IBM® Lotus Notes® API security functions.

The BlackBerry Messaging Agent deletes the Lotus Notes .id files and plain-text passwords that it stores when the following events occur:

- the BlackBerry® Enterprise Server cannot decrypt a message
- the BlackBerry Enterprise Server restarts
- the password times out (the default expiration is 24 hours)

The encrypted Lotus Notes .id password remains stored in the memory cache of the BlackBerry Messaging Agent. You can change the duration that the BlackBerry Messaging Agent caches the password. For more information about

how to change the duration that the BlackBerry Messaging Agent caches the password for, visit www.blackberry.com/support to read article KB12420.

If a user types an incorrect password more than 10 times consecutively within one hour, the BlackBerry Messaging Agent makes secure messaging unavailable for one hour. The temporary disabling period increases by 10 minute increments for a maximum of 24 hours. It increments each time a user exceeds the maximum number of failed password tries, and defaults back to one hour when the user types the correct password.

How the BlackBerry device protects the Lotus Notes .id password

After a user imports the IBM® Lotus Notes® .id file and password (which is stored in the Lotus Notes .id file), the BlackBerry® device encrypts the password in BlackBerry device memory using AES with the master encryption key of the BlackBerry device. The BlackBerry device decrypts the password before it calls the required IBM Lotus Notes API security functions.

The BlackBerry device deletes the Notes .id files and plain-text passwords from the BlackBerry device memory when the following events occur:

- the BlackBerry® Enterprise Server notifies the BlackBerry device that the BlackBerry Enterprise Server could not decrypt a message
- the BlackBerry device resets
- the password times out (the default expiration period is 24 hours)

You can change the timeout value to 0 to require the user to type the Lotus Notes .id password to decrypt and read every Lotus Notes protected message that the user receives on the BlackBerry device.

When secure messaging is not available, a user can turn on secure messaging manually by importing the Lotus Notes .id file, or changing the Lotus Notes .id password using the BlackBerry® Desktop Software or Domino Web Access client.

Enrolling certificates on BlackBerry devices over the wireless network

You can configure the BlackBerry® Enterprise Server to permit BlackBerry devices to enroll certificates over the wireless network. You can permit BlackBerry devices to enroll the certificates over the wireless network so that you do not have to instruct users to send the certificates to themselves in an email message or to use the certificate synchronization tool in the BlackBerry® Desktop Software.

You can enroll certificates from one of the following certificate authorities:

- RSA® certificate authority
- Microsoft® standalone certificate authority
- Microsoft enterprise certificate authority

For more information about configuring the BlackBerry Enterprise Server to permit BlackBerry devices to enroll certificates over the wireless network, see the *BlackBerry Enterprise Server Administration Guide*.

Process flow: Enrolling a certificate when the certificate authority approves certificate requests automatically

After a BlackBerry® device receives an IT policy that includes a certificate authority profile, the enrollment process can start automatically, or you can instruct a user to start it. The process flow assumes that the certificate authority in your organization's environment is a Microsoft® enterprise certificate authority.

1. The CA Profile Manager on the BlackBerry device generates the public-private key pair for the certificate.
2. The BlackBerry MDS Connection Service authenticates the user account.
3. The BlackBerry device requests the user's distinguished name from the BlackBerry® Enterprise Server.
4. The BlackBerry Enterprise Server retrieves the user's distinguished name from the messaging server and sends it to the BlackBerry device.
5. The BlackBerry device encrypts the public-private key pair and stores the key pair, distinguished name, and profile ID for the certificate authority in the persistent store in flash memory.
6. The CA Profile Manager creates the PKCS#10 certificate request, and signs it with the private key.
7. The BlackBerry device sends the certificate request, profile ID for the certificate authority, and the Windows login information to the BlackBerry MDS Connection Service.
8. One of the following events occur:
 - If the certificate chain is in the BlackBerry MDS Connection Service cache, the BlackBerry MDS Connection Service sends the certificate chain to the BlackBerry Enterprise Server.
 - If the certificate chain is not in the BlackBerry MDS Connection Service cache, the BlackBerry MDS Connection Service retrieves the certificate chain from the certificate authority and sends it to the BlackBerry Enterprise Server.
9. The BlackBerry Enterprise Server sends the certificate chain to the BlackBerry device.
10. The BlackBerry MDS Connection Service sends a status update to the BlackBerry device and sends the certificate request to the certificate authority that is associated with the profile ID.
11. The certificate authority issues the certificate, publishes it to an LDAP server, and notifies the BlackBerry MDS Connection Service that the certificate is available.
12. The BlackBerry MDS Connection Service retrieves the certificate from the LDAP server that the certificate authority publishes the certificate to.
13. The BlackBerry MDS Connection Service sends the certificate to the BlackBerry Enterprise Server.
14. The BlackBerry Enterprise Server verifies the certificate by checking if the public key matches the public key that is stored in the BlackBerry Configuration Database.

15. The BlackBerry Enterprise Server sends the certificate to the BlackBerry device over the mobile network.
16. The BlackBerry device adds the certificate and private key to the key store.

Process flow: Enrolling a certificate when a certificate authority administrator approves certificate requests

After a BlackBerry® device receives an IT policy that includes a certificate authority profile, the enrollment process can begin automatically or you can instruct a user to start it from the BlackBerry device. The process flow assumes that the certificate authority in your organization's environment is a Microsoft® enterprise certificate authority.

1. The CA Profile Manager on the BlackBerry device generates the public-private key pair for the certificate.
2. The BlackBerry MDS Connection Service authenticates the user account.
3. The BlackBerry device requests the user's distinguished name from the BlackBerry® Enterprise Server.
4. The BlackBerry Enterprise Server retrieves the user's distinguished name from the messaging server and sends it to the BlackBerry device.
5. The BlackBerry device encrypts the public-private key pair and stores the key pair, distinguished name, and profile ID for the certificate authority in the persistent store in flash memory.
6. The CA Profile Manager creates the PKCS #10 certificate request, and signs it with the private key.
7. The BlackBerry device sends the certificate request, profile ID for the certificate authority, and the Windows login information to the BlackBerry MDS Connection Service.
8. One of the following events occur:
 - If the certificate chain is in the BlackBerry MDS Connection Service cache, the BlackBerry MDS Connection Service sends the certificate chain to the BlackBerry Enterprise Server.
 - If the certificate chain is not in the BlackBerry MDS Connection Service cache, the BlackBerry MDS Connection Service retrieves the certificate chain from the certificate authority and sends it to the BlackBerry Enterprise Server.
9. The BlackBerry Enterprise Server sends the certificate chain to the BlackBerry device.
10. The BlackBerry MDS Connection Service sends a status update to the BlackBerry device and sends the certificate request to the certificate authority that is associated with the profile ID.
11. The certificate authority waits for the certificate authority administrator to approve the certificate request.
12. When the certificate authority administrator approves the certificate request, the certificate authority issues the certificate and sends the certificate to the user in an email message.
13. The BlackBerry MDS Connection Service polls, at specified intervals, for the certificate.
14. Once the BlackBerry MDS Connection Service retrieves the certificate, the BlackBerry MDS Connection Service sends the certificate to the BlackBerry Enterprise Server.
15. The BlackBerry Enterprise Server verifies the certificate by checking if the public key matches the public key that is stored in the BlackBerry Configuration Database.
16. The BlackBerry Enterprise Server sends the certificate to the BlackBerry device.
17. The BlackBerry device adds the certificate and private key to the key store.

Process flow: Enrolling a certificate using an RSA certificate authority

After a BlackBerry® device receives an IT policy that includes a certificate authority profile, the enrollment process can start automatically, or you can instruct a user to start it.

1. The CA Profile Manager on the BlackBerry device generates the public-private key pair for the certificate.
2. The BlackBerry device requests the user's distinguished name from the BlackBerry® Enterprise Server.
3. The BlackBerry Enterprise Server retrieves the user's distinguished name from the messaging server and sends it to the BlackBerry device.

4. The BlackBerry device encrypts the public-private key pair and stores the key pair, distinguished name, and profile ID for the certificate authority in the persistent store in flash memory.
5. The CA Profile Manager creates the PKCS#10 certificate request, and signs it with the private key.
6. The BlackBerry device sends the certificate request and the name of the certificate authority profile to the BlackBerry MDS Connection Service.
7. One of the following events occur:
 - If the certificate chain is in the BlackBerry MDS Connection Service cache, the BlackBerry MDS Connection Service sends the certificate chain to the BlackBerry Enterprise Server.
 - If the certificate chain is not in the BlackBerry MDS Connection Service cache, the BlackBerry MDS Connection Service retrieves the certificate chain from the certificate authority and sends it to the BlackBerry Enterprise Server.
8. The BlackBerry Enterprise Server sends the certificate chain to the BlackBerry device.
9. The BlackBerry MDS Connection Service sends a status update to the BlackBerry device and sends the certificate request to the certificate authority that is associated with the name of the certificate authority profile.
10. The certificate authority waits for the certificate authority administrator to approve the certificate request.
11. When the certificate authority administrator approves the certificate request, the certificate authority issues the certificate and sends, in an email message to the user, the URL for the certificate.
12. The BlackBerry Messaging Agent receives the email message and extracts the issue ID of the message from the URL and stores it in the BlackBerry Configuration Database.
13. The BlackBerry MDS Connection Service polls the BlackBerry Configuration Database every 5 minutes for the issue ID of the message, reconstructs the URL, and sends the URL to the CA to retrieve the certificate.
14. When the BlackBerry MDS Connection Service retrieves the certificate, the BlackBerry MDS Connection Service sends the certificate to the BlackBerry Enterprise Server.
15. The BlackBerry Enterprise Server verifies the certificate by checking if the public key matches the public key that is stored in the BlackBerry Configuration Database.
16. The BlackBerry Enterprise Server sends the certificate to the BlackBerry device.
17. The BlackBerry device adds the certificate and private key to the key store.

Protecting stored data

Protecting stored messages that are located on the messaging server

The IBM® Lotus® Domino® server and the Microsoft® Exchange server perform all message storage and specific user data storage. In a Novell® GroupWise® server environment, the Post-Office Agent where a user's messaging account is located stores messages and user data.

Messaging server	Storage location
IBM Lotus Domino server	IBM Lotus Domino databases within the IBM Lotus Domino environment
Microsoft Exchange server	hidden folders in Microsoft Exchange mailboxes that are associated with a user account
Novell GroupWise	Post-Office Agent

Storing message and user data in IBM Lotus Domino databases

The BlackBerry® Enterprise Server creates and uses the following IBM® Lotus® Domino® databases to manage BlackBerry device messages:

Database	Message storage method
BlackBerry state database	This database stores an entry that establishes a connection between each original message in a user's IBM® Lotus Notes® Inbox and the same message on the user's BlackBerry device. Each user has a uniquely named BlackBerry state database.
BlackBerry profiles database	<ul style="list-style-type: none">This database stores important configuration information for each user, including the identification information for the BlackBerry device and master encryption key.This database stores a link to a user's BlackBerry state database and stores other information that the BlackBerry Enterprise Server uses to manage the flow of messages to and from the BlackBerry device.

IT policy signing and storage on the BlackBerry device

An IT policy is a collection of one or more IT policy rules. An IT administration command is a function that you can send over the wireless network to immediately control access to a BlackBerry® device or change ownership information on a BlackBerry device.

After the BlackBerry® Enterprise Server installation process creates the BlackBerry Configuration Database, the BlackBerry Enterprise Server generates a unique private and public key pair to authenticate the IT policy and IT administration commands, and digitally signs the Default IT policy before sending it and the IT policy public key to each BlackBerry device automatically.

A BlackBerry device stores the digitally signed IT policy and the IT policy public key in the NV store in flash memory, binding the IT policy to the BlackBerry device.

The BlackBerry Enterprise Server stores the IT policy private key in the BlackBerry Configuration Database. The BlackBerry Enterprise Server uses the IT policy private key to sign all IT policy packets that it sends to the BlackBerry device. The BlackBerry device uses the IT policy public key in the NV store to authenticate the digital signature on the IT policy.

Process flow: How the BlackBerry Enterprise Solution digitally signs and stores IT policies and IT administration commands

1. The BlackBerry® Enterprise Server installation process creates the BlackBerry Configuration Database.
2. The BlackBerry Enterprise Server generates a unique private and public key pair to authenticate the IT policy and the IT administration commands.

3. The BlackBerry Enterprise Server uses the private key to digitally sign the Default IT policy.
4. The BlackBerry Enterprise Server sends the IT policy and the public key to the BlackBerry device.
5. The BlackBerry device stores the digitally signed IT policy and the public key in the NV store in flash memory, binding the IT policy to that particular BlackBerry device.
6. The BlackBerry Enterprise Server stores the private key in the BlackBerry Configuration Database.
7. The BlackBerry Enterprise Server uses the private key to sign all IT policy packets that it sends to the BlackBerry device.
8. The BlackBerry device uses the public key in the NV store to authenticate the digital signature on the IT policy.

Using the password keeper to manage application passwords on BlackBerry devices

A user can use the password keeper to create and store passwords that they use to gain access to applications and web sites on a BlackBerry® device. A user must remember only the master password of the password keeper to retrieve the stored passwords.

The first time that a user opens the password keeper on the BlackBerry device, the user must create the master password for the password keeper. The password keeper encrypts the information that it stores using 256-bit AES, and uses the master password to decrypt the information when the user types the master password to gain access to the password keeper. The BlackBerry device deletes all its data if a user types the master password incorrectly ten times.

In the password keeper, a user can perform the following actions:

- type a password and its identifying information (for example, which application the user can access using the password), and save the information
- generate random passwords that are designed to improve password strength
- copy passwords and paste them into an application or password prompt for a web site

Protecting data stored on external memory devices

The External File System Encryption Level IT policy rule or the corresponding BlackBerry device setting determine how BlackBerry® devices encrypt multimedia data that they store on external memory devices.

BlackBerry devices are designed to perform the following actions:

- use AES to encrypt specific files on external memory devices using AES
- use code signing with 1024-bit RSA to control access to objects on external memory devices

External file system encryption does not apply to files that users transfer manually to external memory devices (for example, from a USB mass storage device).

The BlackBerry devices, any computer operating system, and other devices that use external memory devices can modify encrypted files (for example, truncate files) on external memory devices. The BlackBerry device is not designed to perform integrity checks on the encrypted file data.

How BlackBerry devices protect the encryption keys of external memory devices

External memory devices store the media card master keys that BlackBerry® devices are designed to use to decrypt and encrypt the files on the external memory devices. BlackBerry devices are designed to use a device key stored in the NV store in BlackBerry device RAM or a password that the user provides to encrypt the media card master keys.

BlackBerry devices are designed to permit code signing keys in the header information of the encrypted file on external memory devices. BlackBerry devices are designed to check the code signing keys when they open the input or output streams of the encrypted file.

Process flow: Generating encryption keys for external memory files

When you or a user turns on encryption of external memory files for the first time, the following process occurs:

1. The BlackBerry® device generates a 256-bit AES encryption key.
2. The BlackBerry device stores the encryption key in the NV store in RAM on the BlackBerry device.
3. The BlackBerry device XORs the AES key with another 256-bit AES encryption key that is encrypted using a password to generate the encryption key for external memory files (a session key).
4. The BlackBerry device encrypts the encryption key for external memory files using the AES encryption key.
5. The BlackBerry device stores the encrypted encryption key for external memory files on the external memory device.

Encrypting files stored in external memory on the BlackBerry device

When a user stores a file in external memory for the first time after you or a user turns on encryption of external memory files, the BlackBerry® device decrypts the encryption key for external memory files and uses it to automatically encrypt the stored file.

For more information, see *Enforcing Encryption of Internal and External File Systems on BlackBerry Devices Technical Overview*.

Protecting user data on a locked BlackBerry device

If you or a user turns on content protection, a locked BlackBerry® device is designed to protect user data in the following ways:

- uses 256-bit AES encryption to encrypt stored data when the BlackBerry device is locked
- uses a ECC public key encryption to encrypt data that the BlackBerry device receives when it is locked

When you or a user turns on content protection on the BlackBerry device, the BlackBerry device uses content protection to encrypt user data items, including the following:

Item	Description
AutoText	all text that automatically replaces the text a user types on the BlackBerry device
BlackBerry® Browser	<ul style="list-style-type: none"> • content that web sites or third-party applications push to the BlackBerry device • web sites that the user saves on the BlackBerry device • browser cache
Calendar	<ul style="list-style-type: none"> • subject • location • organizer • attendees • notes included in the appointment or meeting request
contacts (in the address book)	<p>all information except the contact title and category</p> <p>You can change the Force Include Address Book In Content Protection IT policy rule to Yes to prevent the user from turning off the Include Address Book option on the BlackBerry device. The BlackBerry device permits the Caller ID and Bluetooth Address Book transfer features to work when you or a user turns on content protection and the BlackBerry device is locked.</p>
Email	<ul style="list-style-type: none"> • subject • email addresses • message body • attachments

Item	Description
memo list	<ul style="list-style-type: none"> • title • information included in the body of the note
RSA SecurID® Library	the contents of the .sdtid file seed stored in flash memory
Tasks	<ul style="list-style-type: none"> • subject • information included in the body of the task
third-party application data	all data that is associated with third-party applications that a user installs on the BlackBerry device

Turning on protected storage of BlackBerry device data

You can turn on protected storage of data on the BlackBerry® device using the Content Protection Strength IT policy rule. You can choose a strength level that corresponds to the ECC key strength that your organization requires.

If a user turns on content protection on the BlackBerry device, in the BlackBerry device options, in the Security Options screen, the user can configure the content protection strength to the same levels that you can configure using the IT policy rule.

When a content-protected BlackBerry device decrypts a message that it received while locked, the BlackBerry device uses the ECC private key. The longer the ECC private key, the more time the ECC decryption operation adds to the BlackBerry device decryption process. Choose a content protection strength level that optimizes the ECC encryption strength or the decryption process.

If you change the content protection strength to Stronger (to use a 283-bit ECC private key) or to Strongest (to use a 571-bit ECC private key), consider changing the Minimum Password Length IT policy rule to enforce a minimum password length of 12 characters or 21 characters, respectively, for the BlackBerry device. These password lengths maximize the encryption strength that the longer ECC private keys are designed to provide. The BlackBerry device uses the password to generate the ephemeral 256-bit AES encryption key that the BlackBerry device uses to encrypt the content protection key and the ECC private key. A weak password produces a weak ephemeral key.

Related topics

Process flow: Generating content protection keys

Protected storage of master encryption keys on a locked BlackBerry device

If you turn on content protection of master encryption keys, a BlackBerry® device uses the grand master key to encrypt the master encryption keys stored in flash memory. The BlackBerry device encrypts the grand master key using the content protection key. When the BlackBerry device receives data that is encrypted with a master encryption key while the BlackBerry device is locked, it uses the decrypted grand master key to decrypt the master encryption key in flash memory, and then uses the decrypted master encryption key to decrypt and receive the data.

The BlackBerry device stores the decrypted master encryption keys and the decrypted grand master key in RAM only. When you, a user, or a password timeout locks the BlackBerry device, the wireless transceiver remains on and the BlackBerry device does not delete the RAM associated with these keys. The BlackBerry device is designed to prevent the decrypted grand master keys and the decrypted master encryption keys from appearing in flash memory.

Related topics

Process flow: Generating grand master keys

Turning on protected storage of master encryption keys on a locked BlackBerry device

You turn on protected storage of master encryption keys on a BlackBerry® device when you configure the Force Content Protection of Master Keys IT policy rule. When you turn on content protection of master encryption keys, a BlackBerry device uses the same ECC key strength that it uses to encrypt BlackBerry device user and application data when encrypting the master encryption keys.

Related topics

Turning on protected storage of BlackBerry device data

Protected storage of master encryption keys on a BlackBerry device during a reset

If you turn on content protection of master encryption keys, a BlackBerry® device performs the following actions during a reset:

- turns off the wireless transceiver
- turns off serial bypass
- frees the memory associated with all data and encryption keys stored in RAM, including the decrypted grand master key
- locks itself

The wireless transceiver and serial bypass are designed to be turned off while the content protection key is unavailable to decrypt the grand master key in flash memory. Until a user unlocks the BlackBerry device using the correct password, the BlackBerry device cannot receive and decrypt data.

When a user unlocks the BlackBerry device after a reset, the BlackBerry device performs the following actions:

- uses the content protection key to decrypt the grand master key in flash memory
- stores the decrypted grand master key in RAM again
- re-establishes the wireless connection to the BlackBerry® Infrastructure
- resumes serial bypass
- receives data from the BlackBerry® Enterprise Server

Cleaning the BlackBerry device memory

By default, a BlackBerry® device continually runs a standard Java® garbage collection process to reclaim BlackBerry device memory that the BlackBerry device no longer references.

If garbage collection is turned on, a BlackBerry device performs the following additional actions:

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

Conditions for running the garbage collection process

Any of the following conditions permit the BlackBerry® device to run the garbage collection process:

- you or a user turn on content protection for BlackBerry devices
- an application uses the RIM Cryptographic API to create a private or symmetric key
- a third-party application turns on garbage collection by registering with the memory cleaner
- a user installs the S/MIME Support Package for BlackBerry® smartphones
- a user installs the PGP® Support Package for BlackBerry® smartphones

Configuring memory cleaning

Users can configure the memory cleaner application to run when their BlackBerry® devices are holstered or when their BlackBerry devices remain idle for a specified period of time. Users can also manually run the memory cleaner application on their BlackBerry devices, run specific registered memory cleaners in the BlackBerry device options, in the Security Options screen, and turn the memory cleaner application on and off. If garbage collection is turned on, when the memory cleaner application runs, it starts the garbage collection process.

You can configure the memory cleaner application to run when the following actions occur:

- a user synchronizes the BlackBerry device with the computer
- a user locks the BlackBerry device

- a BlackBerry device locks after remaining idle for a specified period of time
- a user changes the time or time zone on the BlackBerry device

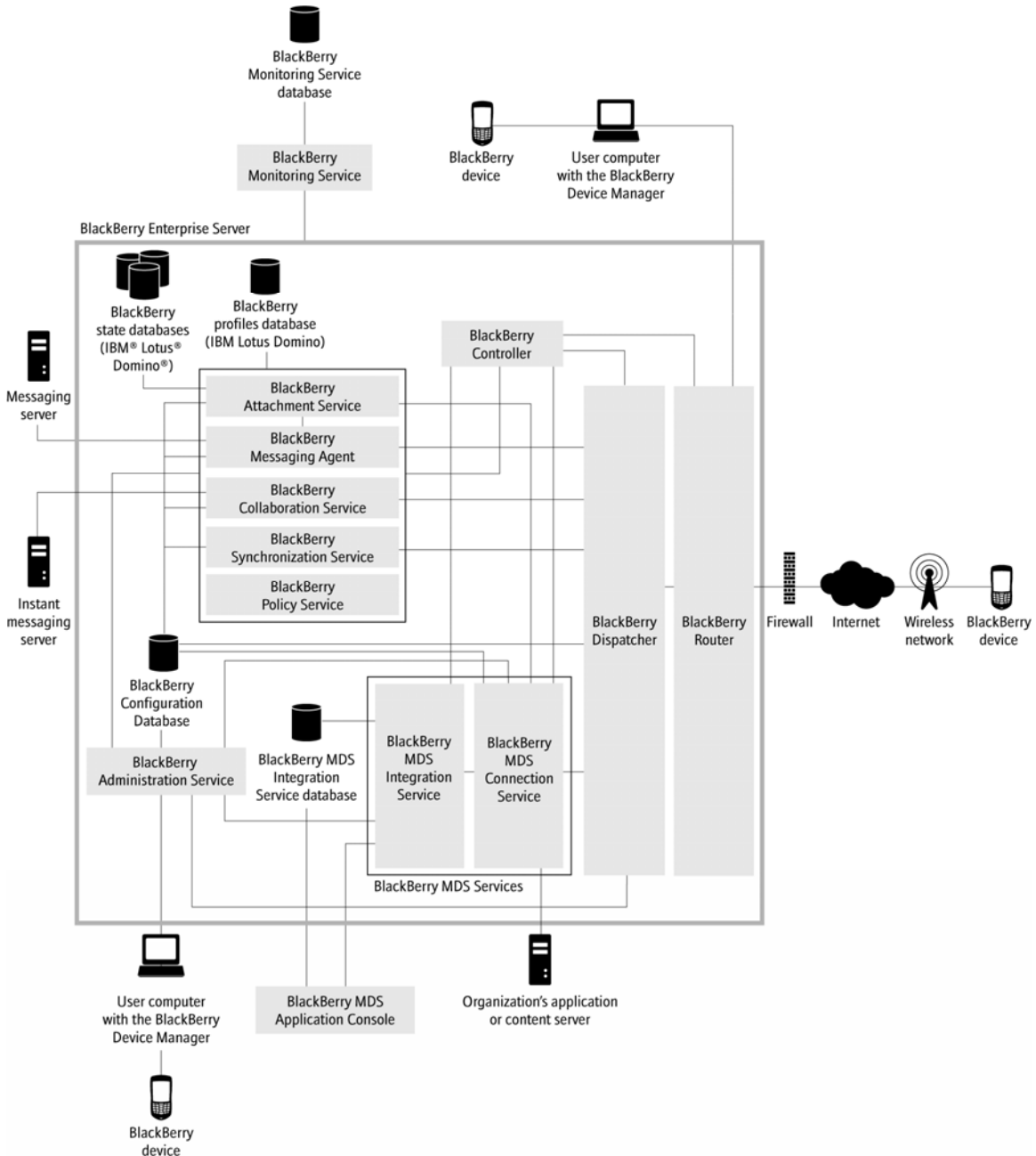
You cannot turn off memory cleaning on the BlackBerry device if any of the following conditions are true:

- content protection is turned on
- a user installed the S/MIME Support Package for BlackBerry® smartphones and a private key exists on the BlackBerry device
- an application uses the RIM Cryptographic API to create a private or symmetric key
- an application requires that memory cleaning be turned on
- a user installed the PGP® Support Package for BlackBerry® smartphones and a private key exists on the BlackBerry device

For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

BlackBerry Enterprise Solution architecture

The BlackBerry® Enterprise Server consists of services that provide features and components that monitor other services and processes, send, compress, and encrypt data, and communicate with the BlackBerry® Infrastructure over the wireless network.



For more information about the BlackBerry Enterprise Server architecture, see the *BlackBerry Enterprise Server Feature and Technical Overview*.

To improve the security and performance of the BlackBerry Enterprise Server components, you can separate your organization's network into multiple segments with firewalls to create a segmented network architecture. Each network segment can manage network traffic destined for a specific component.

Messaging server security

The BlackBerry® Enterprise Solution is designed to work with messaging servers such as Microsoft® Exchange, IBM® Lotus® Domino®, and Novell® GroupWise®. The BlackBerry Enterprise Solution is designed to use existing messaging server security. The messaging server continues to receive, send, and store all email messages, and the BlackBerry® Enterprise Server sends these email messages to BlackBerry devices and receives email messages from BlackBerry devices.

Storing data and encryption keys in the BlackBerry Configuration Database

The BlackBerry® Enterprise Server components that do not connect to a messaging server can access the information that the BlackBerry Configuration Database stores.

For example, the BlackBerry Configuration Database stores the following information:

- BlackBerry Enterprise Server names
- unique SRP authentication keys and unique SRP IDs, or UIDs, that each BlackBerry Enterprise Server uses in the SRP authentication process to open a connection to the wireless network
- IT policy private keys of the IT policy public and private key pair that the BlackBerry Enterprise Server generates for each BlackBerry device
- PIN of each BlackBerry device
- read-only copies of each master encryption key
- user account lists for each BlackBerry device
- copy of your organization's address book
- a semi-permanent reference to user data using the GroupWise MessageID in the MBMailSync, MBCalendarSync, MBPIMSync, and MBFolderSync database synchronization tables (BlackBerry® Enterprise Server for Novell® GroupWise® only)

Protecting the BlackBerry Configuration Database

Your organization's environment might benefit from configuring the Microsoft® SQL Server® to provide optimal security of the BlackBerry® Configuration Database and the encryption keys for each BlackBerry device that the BlackBerry Configuration Database stores. The following table describes some of the options for securing the Microsoft SQL Server:

Option	Recommendations
shield the Microsoft SQL Server installation from Internet-based attacks	<ul style="list-style-type: none">• Require Windows® Authentication Mode for connections to Microsoft SQL Server to restrict connections to Windows user accounts and domain user accounts, and turn on credentials delegation. Windows Authentication Mode does not require you to store passwords on the computer.• Use stronger authentication protocols and mandatory password complexity and expiration.
Password-protect the sa account	Assign a password to the sa account on the Microsoft SQL Server, even on servers that require Windows Authentication. A string password is designed to prevent an empty or weak sa password from being exposed if a database administrator resets the Microsoft SQL Server for Mixed Mode Authentication.

Option	Recommendations
Limit the privilege level of the Microsoft SQL Server	<p>Associate each Microsoft SQL Server service with a Windows account from which the service derives its security context.</p> <p>Microsoft SQL Server permits the sa account and in some cases other user accounts to access operating system calls based on the security context of the account that runs the service. If you do not limit the privilege level of the Microsoft SQL Server, a malicious user might use these operating system calls to attack any other resource to which the account has access.</p>
Use the Microsoft SQL Server Management Studio	<ul style="list-style-type: none"> • Use the Microsoft SQL Server Management Studio to change the account associated with a Microsoft SQL Server service, if required. The Microsoft SQL Server Management Studio configures the appropriate permissions on the files and registry keys that the Microsoft SQL Server uses. • Do not use the Microsoft Management Console Services applet to change the account associated with a Microsoft SQL Server service. To use this applet, you must manually adjust registry and NTFS file system permissions and Windows user rights. <p>For more information, visit support.microsoft.com to read article KB283811.</p>
Make the Microsoft SQL Server ports that are monitored by default on your organization's firewall unavailable	<p>Configure your organization's firewall to filter packets that are addressed to TCP port 1433, addressed to UDP port 1434, or packets that are associated with named instances.</p>
Use a secure file system	<ul style="list-style-type: none"> • Use NTFS for the Microsoft SQL Server because it is more stable and recoverable than FAT file systems, and permits security options such as file and directory ACLs and EFS. • Do not change the permissions that the Microsoft SQL Server specifies during installation. The Microsoft SQL Server creates appropriate ACLs on registry keys and files if it detects NTFS. • If you must change the account that runs the Microsoft SQL Server, decrypt the files that you could access using the old account and re-encrypt them for access using the new account.
Delete unsecured, old setup files	<p>Delete Microsoft SQL Server setup files that might contain plaintext, credentials encrypted with weak public keys, or sensitive information that the Microsoft SQL Server logged to a Microsoft SQL Server version-dependent location during the installation process.</p> <p>Microsoft distributes a free tool, Killpwd, which is designed to locate and delete passwords from unsecured, old setup files on your organization's system. For more information, visit support.microsoft.com to read article KB263968.</p>
Audit connections to the Microsoft SQL Server	<ul style="list-style-type: none"> • At a minimum, log failed connection attempts to the Microsoft SQL Server and review the log regularly. • When possible, save log files to a different hard disk drive than the one on which the data files are stored.

Changing the BlackBerry Configuration Database

If you move the BlackBerry® device to a BlackBerry® Enterprise Server that uses a different BlackBerry Configuration Database, you or a user must permanently delete all user and application data, the master encryption key, and the IT policy public key from the BlackBerry device.

You or the user must start regeneration of a new master encryption key. The BlackBerry Enterprise Server that you move the BlackBerry device to must generate a unique IT policy private and public key pair and digitally sign and

send the Default IT policy and the IT policy public key to the BlackBerry device before the BlackBerry device can communicate with the BlackBerry Enterprise Server.

The new BlackBerry Configuration Database stores the new BlackBerry Enterprise Server name and the master encryption key of the BlackBerry device and IT policy private key.

Related topics

Deleting all device data

Protecting the BlackBerry Infrastructure connections

The BlackBerry® Enterprise Server is designed to communicate with the BlackBerry® Infrastructure using SRP authentication to establish a connection to the wireless network. SRP is a point-to-point protocol that runs over TCP/IP. The BlackBerry Enterprise Server contacts the BlackBerry Infrastructure to establish an initial connection that uses SRP to perform the following actions:

- authenticate the BlackBerry Infrastructure with the BlackBerry Enterprise Server, and the BlackBerry Enterprise Server with the BlackBerry Infrastructure
- exchange configuration information between the BlackBerry Enterprise Server and the BlackBerry Infrastructure
- send and receive transactions between the BlackBerry Enterprise Server and the BlackBerry Infrastructure

Authenticating the BlackBerry Enterprise Server with the BlackBerry Infrastructure

The BlackBerry® Enterprise Server is designed to establish a secure, two-way connection between a user's email account and the user's BlackBerry device. The BlackBerry Enterprise Server uses the connection to send email messages inside your organization's firewall.

The BlackBerry® Infrastructure and BlackBerry Enterprise Server must authenticate with each other before they can transfer data. The authentication is performed using a 20-byte shared secret encryption key (the SRP authentication key) on both the BlackBerry Enterprise Server and the BlackBerry Infrastructure.

If the authentication fails, the BlackBerry Infrastructure and BlackBerry Enterprise Server closes the SRP connection. If a BlackBerry Enterprise Server uses the same SRP authentication key and SRP ID to connect to (and then disconnect from) the BlackBerry Infrastructure 5 times in 1 minute, the BlackBerry Infrastructure deactivates the SRP ID to prevent a malicious user from using the same SRP ID (for example, to try to create a Denial of Service condition).

How the BlackBerry Enterprise Server and BlackBerry Infrastructure exchange information

After the BlackBerry® Enterprise Server and BlackBerry® Infrastructure establish an initial connection over the Internet, the BlackBerry Enterprise Server is designed to send a basic information packet to the BlackBerry Infrastructure immediately. The BlackBerry Enterprise Server and BlackBerry Infrastructure can both recognize the packet format. The BlackBerry Enterprise Server and BlackBerry Infrastructure can use the packet format to configure the parameters of the SRP implementation dynamically. Afterwards, the BlackBerry Enterprise Server uses a persistent TCP/IP connection to send data to the BlackBerry Infrastructure. The BlackBerry Infrastructure uses standard protocols to send data to the BlackBerry device.

If the connection between the BlackBerry Enterprise Server and BlackBerry Infrastructure closes, the wireless network can queue up to 5 undelivered messages for up to seven days. If there are more than five undelivered messages, the BlackBerry Enterprise Server stores them in the BlackBerry Configuration Database. The BlackBerry Infrastructure does not store data to send to BlackBerry devices.

If the BlackBerry Infrastructure is not responding, the wireless network discards the undelivered messages. The BlackBerry device does not receive the messages and the BlackBerry Enterprise Server does not receive acknowledgment packets from the BlackBerry device. When the BlackBerry Infrastructure becomes operational again, the BlackBerry Enterprise Server resends messages that it did not receive acknowledgment packets for.

The BlackBerry Infrastructure does not send basic information packets to the BlackBerry Enterprise Server until the BlackBerry Enterprise Server has sent a packet in the same format to the BlackBerry Infrastructure. This permits backward compatibility with previous BlackBerry Enterprise Server versions, which close the SRP connection if they receive unrecognized packets.

Process flow: Authenticating the BlackBerry Infrastructure to the BlackBerry Enterprise Server

1. The BlackBerry® Enterprise Server sends a packet that contains its SRP ID to the BlackBerry® Infrastructure to claim the SRP ID.
2. The BlackBerry Infrastructure sends a random challenge string to the BlackBerry Enterprise Server.

3. When the BlackBerry Enterprise Server receives the random challenge string, it sends a challenge string to the BlackBerry Infrastructure.
4. The BlackBerry Infrastructure hashes the challenge string with the SRP authentication key using the keyed HMAC with SHA-1. The BlackBerry Infrastructure sends the resulting 20-byte value back to the BlackBerry Enterprise Server.
5. The BlackBerry Enterprise Server responds to the BlackBerry Infrastructure challenge string by hashing the challenge string with the shared SRP authentication key, and sending a challenge response to the BlackBerry Infrastructure.
6. The BlackBerry Infrastructure accepts the challenge response and sends a final confirmation to the BlackBerry Enterprise Server to complete the authentication process and configure an authenticated SRP connection between the BlackBerry Infrastructure and BlackBerry Enterprise Server. If the BlackBerry Infrastructure rejects the response, the connection fails and SRP closes the authentication session.

How the BlackBerry Enterprise Server and BlackBerry Infrastructure manage undeliverable messages

When a user sends a message to a BlackBerry® device, the BlackBerry® Infrastructure might not be able to deliver the message to the BlackBerry device immediately in the following scenarios:

Scenario	Result
<p>The BlackBerry device state prevents the BlackBerry device from sending and receiving messages over the wireless network. The user might change the BlackBerry device state by moving in and out of wireless coverage or turning the BlackBerry device on and off.</p>	<ul style="list-style-type: none"> • The message expires if the message remains undelivered after the timeout value specified on the BlackBerry Infrastructure (7 days) elapses or the BlackBerry Infrastructure loses the connection to the BlackBerry® Enterprise Server. The BlackBerry Infrastructure informs the source that the message could not be delivered. • If the BlackBerry Infrastructure cannot deliver a message after trying for 10 minutes, the BlackBerry Infrastructure informs the BlackBerry Enterprise Server and deletes the message. • The BlackBerry Enterprise Server requests a notification message from the BlackBerry Infrastructure when the BlackBerry device state changes. When the BlackBerry device state indicates that it can send and receive messages over the wireless network, the BlackBerry Infrastructure notifies the BlackBerry Enterprise Server and the BlackBerry Enterprise Server sends pending messages to the BlackBerry device.
<p>The connection between the BlackBerry Enterprise Server and the BlackBerry Infrastructure closes.</p>	<ul style="list-style-type: none"> • If the BlackBerry Infrastructure cannot deliver a message after ten minutes, the BlackBerry Infrastructure informs the sender's BlackBerry device and deletes the message. • When the BlackBerry Enterprise Server and BlackBerry Infrastructure reopen the connection, the BlackBerry Enterprise Server resends the undelivered message to the BlackBerry device. If more than 5 messages are pending, the BlackBerry Enterprise Server stores them in the BlackBerry Configuration Database.

BlackBerry Router protocol authentication

When the BlackBerry® Enterprise Server and BlackBerry device use the BlackBerry Router protocol to open a connection between them, the BlackBerry Router is designed to bypass the SRP authenticated connection to the BlackBerry® Infrastructure. The BlackBerry Router can send data to BlackBerry devices that are connected to the BlackBerry® Device Manager through a physical connection to a computer or the BlackBerry Router can send data to BlackBerry devices that are connected over port 4101 to an enterprise Wi-Fi® network. BlackBerry devices and the BlackBerry Dispatcher are designed to compress and encrypt the data that BlackBerry devices and the BlackBerry Router send to each other.

If you want a BlackBerry Router to send data between the BlackBerry Infrastructure and multiple BlackBerry Enterprise Server instances, you can install the BlackBerry Router on a computer that is separate from the computer that hosts the BlackBerry Enterprise Server. The BlackBerry device must authenticate to the BlackBerry Enterprise Server to prove that it knows the master encryption key before the BlackBerry Router sends data to the BlackBerry device. The BlackBerry Enterprise Server and the BlackBerry device use the BlackBerry Router protocol to open an authenticated connection between them. The value of the master encryption key that the BlackBerry device and the BlackBerry Enterprise Server share is not available to the BlackBerry Router.

When the authentication process used by the BlackBerry Router protocol is successful, the BlackBerry device sends data to the BlackBerry Router through the BlackBerry Device Manager or over port 4101 to an enterprise Wi-Fi network, and the BlackBerry Router sends data to the BlackBerry device through the BlackBerry Device Manager or over port 4101 to an enterprise Wi-Fi network. When the user disconnects the BlackBerry device from the computer, closes the BlackBerry Device Manager, or disconnects from the enterprise Wi-Fi network, the BlackBerry device restores the wireless data flow over the SRP connection. The BlackBerry Enterprise Server and the BlackBerry Router use the BlackBerry Router protocol to close the authenticated connection to the BlackBerry device.

Process flow: Authenticating the BlackBerry device with the BlackBerry Enterprise Server using the BlackBerry Router protocol

1. A user connects a BlackBerry® device to a computer that hosts the BlackBerry® Device Manager, or connects a BlackBerry device to an enterprise Wi-Fi® network.
2. The BlackBerry® Enterprise Server and the BlackBerry device use the BlackBerry Router authentication protocol to verify that the BlackBerry device has the correct master encryption key.
3. When the BlackBerry Enterprise Server and BlackBerry device validate each other, they use the same SRP authentication information that the BlackBerry Enterprise Server uses to authenticate with the BlackBerry® Infrastructure.

Related topics

Process flow: Running the masking operation during the initial AES algorithm calculation when content protection is turned on

Authentication during wireless activation

Wireless activation permits a user to associate a BlackBerry® device to the user's email account without a physical connection to a computer.

Wireless activation produces a master encryption key that authenticates a user and secures the communication between the BlackBerry® Enterprise Server and BlackBerry device. To generate the master encryption key, the BlackBerry Enterprise Server and BlackBerry device use an initial key establishment protocol and the activation password. The initial key establishment protocol uses SPEKE as the authentication method. You can generate the activation password when you create the user account using the BlackBerry Administration Service.

The BlackBerry Enterprise Server and the BlackBerry device do not send the master encryption key over the wireless network during the key establishment process, subsequent key generation, or message exchanges.

After the BlackBerry device is activated, the BlackBerry device no longer requires the activation password. Users cannot reuse the activation password to activate other BlackBerry devices.

Process flow: Authenticating the BlackBerry device with the BlackBerry Enterprise Server during wireless activation

1. The user opens the activation application on the BlackBerry® device and types the email address and the activation password.
2. The BlackBerry device sends an activation request to the BlackBerry® Infrastructure using standard BlackBerry protocols. The BlackBerry Infrastructure uses SMTP to send an activation message to the user's email account. This activation message contains BlackBerry device routing information and public keys.
3. The BlackBerry® Enterprise Server sends the BlackBerry device an activation response that contains BlackBerry Enterprise Server routing information and public keys.
4. The BlackBerry Enterprise Server and the BlackBerry device use the initial key establishment protocol to generate a master encryption key and verify it. If the BlackBerry Enterprise Server and the BlackBerry device mutually verify the master encryption key, the activation proceeds, and the BlackBerry Enterprise Server and

BlackBerry device use the master encryption key to encrypt further communication between one another without sending the key over the wireless network.

5. The BlackBerry Enterprise Server sends the appropriate service books to the BlackBerry device. The user can now send messages from and receive messages on the BlackBerry device.
6. If you turn on wireless organizer data synchronization and wireless backup for the user, the BlackBerry Enterprise Server sends the following data to the BlackBerry device:
 - calendar entries
 - contacts, tasks, and memos
 - existing BlackBerry device options (if applicable) that the BlackBerry device backed up using automatic wireless backup

For more information, see the *BlackBerry Wireless Enterprise Activation Technical Overview*.

TCP/IP connection

The TCP/IP connection from the BlackBerry® Enterprise Server to the BlackBerry® Infrastructure is designed to be secure in the following ways:

Security measure	Description
The BlackBerry Enterprise Server sends outbound traffic to the BlackBerry device only through the authenticated connection to the BlackBerry Infrastructure.	You must configure your organization's firewall or proxy server to permit the BlackBerry Enterprise Server to start and maintain an outbound connection to the BlackBerry Infrastructure on TCP port 3101.
The BlackBerry Enterprise Server does not send inbound traffic to the messaging server.	The BlackBerry Enterprise Server discards inbound traffic from any source other than the BlackBerry device (through the BlackBerry Infrastructure or BlackBerry® Desktop Software) or the messaging server.
The BlackBerry Enterprise Solution encrypts data traffic over TCP/IP.	<ul style="list-style-type: none"> • Data remains encrypted with standard BlackBerry encryption from the BlackBerry Enterprise Server to the BlackBerry device or from the BlackBerry device to the BlackBerry Enterprise Server. There is no intermediate point at which the data is decrypted and encrypted again. • No data traffic of any kind can occur between the BlackBerry Enterprise Server and the wireless network or the BlackBerry device unless the BlackBerry Enterprise Server can decrypt the data using the correct, valid master encryption key. Only the BlackBerry device and BlackBerry Enterprise Server have the correct, valid master encryption key.
The BlackBerry Enterprise Server encrypts data between specific components	The BlackBerry Collaboration Service, BlackBerry MDS Connection Service, BlackBerry Policy Service, BlackBerry Synchronization Service, and BlackBerry® Mobile Voice System share a secure communication password. The BlackBerry Messaging Agent and the BlackBerry Dispatcher share a different secure communication password. When one of these components opens a connection to the BlackBerry Dispatcher, the BlackBerry inter-process protocol is designed to use SPEKE to begin a key generation process using the component's secure communication password and establishes a 256-bit AES encryption key (a session key). The BlackBerry Enterprise Server then uses the session key to encrypt data that it sends to any components that store the same secure communication password.
The BlackBerry device opens inbound connections to an enterprise Wi-Fi® network using the BlackBerry Router.	The BlackBerry Router sends the Internet or intranet content requests from the BlackBerry device over port 4101 to the enterprise Wi-Fi network. The BlackBerry Router verifies that the PIN belongs to a BlackBerry device that is registered on the wireless network.

Protecting the connection between the messaging server and the email application

You can configure your organization's messaging server to encrypt BlackBerry® device data that is in transit between the messaging server and the email application on the user's computer.

Messaging server	Data encryption method
IBM® Lotus® Domino®	<ul style="list-style-type: none">The BlackBerry® Enterprise Server and the IBM Lotus Domino server communicate using the same IBM® Lotus Notes® RPC to communicate seamlessly between them.Users that activate BlackBerry devices using physical connections to their computers can encrypt data that is in transit between the IBM Lotus Domino server and their IBM Lotus Notes Inboxes. For more information, see the IBM Lotus Domino help files.
Microsoft® Exchange	<ul style="list-style-type: none">The BlackBerry Enterprise Server and the Microsoft Exchange server communicate using the same Microsoft Exchange server RPC.BlackBerry device users can use 128-bit encryption to encrypt RPC communication over the MAPI connection between the Microsoft Exchange server and Microsoft® Outlook®. For more information about turning on encryption in Windows®, see the Microsoft product documentation.
Novell® GroupWise®	<ul style="list-style-type: none">The BlackBerry® Enterprise Server for Novell® GroupWise® is designed to use a trusted application key to open a connection to the Novell GroupWise server. To generate the trusted application key, the Novell GroupWise administrator runs the trusted application key generator, specifies the location of the Novell GroupWise primary domain database, and specifies the application name that the BlackBerry Enterprise Server uses to connect to the Novell GroupWise server. The trusted application key is a 64-byte ASCII string.The BlackBerry Enterprise Server connects securely to a user's mailbox using the trusted application name and key. The Novell GroupWise server verifies the trusted application name and key and permits the BlackBerry Enterprise Server to establish a connection to the Novell GroupWise database of the user.

Protecting connections between the BlackBerry Desktop Manager and its components

The application loader tool and media manager tool of the BlackBerry Desktop® Manager share a secret password with the BlackBerry Desktop Manager. When the application loader tool or media manager tool opens a connection to BlackBerry® Desktop Software version 4.2 or later, the BlackBerry Desktop Software uses the secure channel technology that Research In Motion developed to create a communication channel. The communication channel is designed to use the shared secret password to secure communication between the BlackBerry Desktop Manager and the application loader tool or media manager tool.

Process flow: Authenticating the application loader tool or the media manager tool with BlackBerry Desktop Software using the communication channel

1. The application loader tool or the media manager tool opens a connection to BlackBerry® Desktop Software version 4.2 or later.
2. The BlackBerry Desktop Software implementation of the secure channel technology uses the shared secret password and the ECDH protocol with a 521-bit curve to create a master encryption key.
3. The secure channel technology uses the master encryption key to create two encryption keys and two HMAC-SHA-256 keys.

4. The secure channel technology uses one of the encryption keys and one of the HMAC keys to encrypt and authenticate data that BlackBerry Desktop Software version 4.2 sends over the communication channel to the components that store the same password.
5. The secure channel technology uses one of the encryption keys and one of the HMAC keys to encrypt and authenticate data that BlackBerry Desktop Software version 4.2 receives over the communication channel from the application loader tool or the media manager tool that opened the connection.

BlackBerry MDS connections

A user can use the BlackBerry® Browser and BlackBerry Java® Applications on the BlackBerry device to access the Internet and your organization's intranet, and to accept and respond to push requests from push applications. The BlackBerry MDS Connection Service uses standard Internet protocols such as HTTP and TCP/IP to access data on the Internet or your organization's intranet, and a BlackBerry MDS security protocol that is Research In Motion proprietary to protect messages that the BlackBerry device sends using the BlackBerry MDS Connection Service. The BlackBerry device uses standard BlackBerry encryption to protect your organization's applications and the online and Internet data that a user receives on the BlackBerry device.

Authenticating data that the BlackBerry device sends to the BlackBerry MDS Integration Service

When the BlackBerry® device sends data using the BlackBerry MDS Integration Service, the BlackBerry MDS security protocol uses HMAC to authenticate part of each BlackBerry MDS message header and payload, and encrypts the MAC of each BlackBerry MDS message header and, if necessary, each BlackBerry MDS message payload.

The BlackBerry MDS security protocol uses a shared session key to authenticate data that the BlackBerry device sends to the BlackBerry MDS Integration Service. The BlackBerry MDS security uses 128-bit AES in CBC mode with PKCS #5 padding to encrypt the shared session key using a database access key, and to encrypt and decrypt data that the BlackBerry device and the BlackBerry MDS Integration Service send between each other.

Requiring secure HTTP connections to the BlackBerry device

By default, the BlackBerry® MDS Integration Service generates a self-signed certificate when it starts after the installation process completes or when it cannot find a certificate in the BlackBerry MDS Integration Service key store. You can replace the self-signed certificate with a signed certificate if the security processes in your organization require it. The certificate permits client authentication between the BlackBerry MDS Integration Service and external web services.

If your organization's BlackBerry® Enterprise Solution uses SSL to communicate with external web services, you must export the certificate to the external web services to authenticate communication with the web services. When BlackBerry devices use SSL to connect to external web services, you can configure the BlackBerry® Enterprise Server to verify that the certificate chains for the certificates that BlackBerry devices use are strong enough. To do so, you can use the Weak Digest Algorithms IT policy rule to identify algorithms that BlackBerry devices and the BlackBerry Enterprise Server should consider weak.

Using a secure connection to push BlackBerry MDS Runtime Applications to BlackBerry devices

After you configure authentication between the BlackBerry® MDS Integration Service and web services, you can permit BlackBerry devices to install the BlackBerry MDS Runtime Applications that use SSL web services only.

Process flow: Registering the BlackBerry device securely with the BlackBerry MDS Integration Service

1. The BlackBerry® device generates the 128-bit AES session key.
2. The BlackBerry device uses 1024-bit RSA with PKCS #1 padding to encrypt the AES session key before the BlackBerry device sends it to the BlackBerry MDS Integration Service and stores it in flash memory.
3. The BlackBerry MDS security protocol uses 128-bit AES in CBC mode with PKCS #5 padding to encrypt a 128-bit AES session key using a 128-bit AES database access key.
4. The BlackBerry MDS Integration Service stores the encrypted 128-bit AES session key in the BlackBerry MDS Integration Service database and stores the 128-bit AES database access key in the database key store.
5. The BlackBerry MDS security protocol uses HMAC with a SHA-1 hash function, in combination with the 128-bit shared secret key, to authenticate data that a BlackBerry device and the BlackBerry MDS Integration Service send between each other.

- The BlackBerry MDS security protocol uses 128-bit AES in CBC mode with PKCS #5 padding to encrypt and decrypt data that a BlackBerry device and the BlackBerry MDS Integration Service send between each other.

Protecting the HTTP connection

If an application on the BlackBerry® device accesses servers on the Internet, you can configure HTTPS to provide additional authentication and security. The BlackBerry device supports HTTPS communication in the following modes:

HTTPS protocol	BlackBerry MDS encryption method	Benefits
proxy mode TLS/SSL	Sun® JSSE 1.4.1 cipher suite components	<ul style="list-style-type: none"> The BlackBerry MDS Connection Service configures the proxy mode TLS/SSL connection for the BlackBerry device. The BlackBerry device does not use proxy mode TLS/SSL to encrypt data over the wireless network. The BlackBerry device uses standard BlackBerry encryption to encrypt the data that it sends to the BlackBerry® Enterprise Server, unless it is behind your organization's firewall. The BlackBerry device experiences faster response times using proxy mode TLS/SSL than it experiences when it uses direct mode TLS/SSL.
direct mode TLS/SSL	TLS and WTLS key establishment algorithms, symmetric ciphers, and hash algorithms that the RIM Cryptographic API currently supports on the BlackBerry device	<ul style="list-style-type: none"> The BlackBerry device uses direct mode TLS/SSL to encrypt data sent to the content server. The BlackBerry MDS Connection Service does not decrypt data sent over the wireless network. You can use direct mode TLS/SSL when only the endpoints of the transaction are trusted (for example, with banking services). BlackBerry devices that are running BlackBerry® Device Software version 3.6.1 or later support direct mode TLS/SSL for connections.

Using two-factor authentication to protect connections to enterprise Wi-Fi networks

The RSA SecurID® Library on a supported BlackBerry® device permits the BlackBerry device to periodically generate software token tokencodes. The BlackBerry device imports and uses random data called a seed to initialize the software token algorithm. The software token algorithm generates the tokencode on the BlackBerry device.

When the user tries to establish a Wi-Fi® or VPN connection that requires two-factor authentication on the BlackBerry device, the BlackBerry device prompts the user to type the software token PIN. The RSA SecurID Library adds the software token PIN to the beginning of the tokencode to create a passcode that the BlackBerry device can use with a two-factor authentication process.

Related topics

Process flow: Generating the tokencode for the RSA SecurID software token

Process flow: Generating the tokencode for the RSA SecurID software token

- The administrator of RSA SecurID® uses the RSA® Authentication Manager to import the seed to the software token database in the form of a soft token file in .asc format.
- The administrator of RSA SecurID uses the RSA Authentication Manager to issue the software token file in .sdtid format. If necessary, the administrator can

- permit the user to specify the software token PIN or have the system automatically generate and send a PIN to the user's BlackBerry® device, or require the user to specify the software token PIN the first time that the user tries to complete two-factor authentication on the BlackBerry device
- bind the seed to a specific BlackBerry device PIN
- specify a password to encrypt the .sdtid file seed

Standard BlackBerry encryption is designed to protect the seed when the BlackBerry® Enterprise Server sends it over the transport layer.

3. You specify the .sdtid file seed for the BlackBerry device in the BlackBerry Administration Service.

If required, you can type the password to decrypt the seed to use it on the BlackBerry device.

4. The BlackBerry Enterprise Server stores the .sdtid file seed in the BlackBerry Configuration Database.
5. The BlackBerry Enterprise Server pushes the .sdtid file seed (and the password, if the administrator of RSA SecurID specified one) to the BlackBerry device during activation of the BlackBerry device and each time the administrator changes the .sdtid file seed for the BlackBerry device.

The BlackBerry device uses Research In Motion proprietary protocols that are designed to be secure to perform all communication necessary to retrieve the seed on behalf of the RSA SecurID Library.

6. The BlackBerry device imports the .sdtid file seed.

If the administrator of RSA SecurID specified a password in the RSA Authentication Manager to encrypt the .sdtid file seed, the BlackBerry device uses the password to decrypt the .sdtid file seed.

If the administrator specified that the .sdtid file seed must bind to a specific BlackBerry device PIN, only the BlackBerry device with that PIN can import the seed.

7. The BlackBerry device stores the .sdtid file seed in flash memory.
8. The BlackBerry device imports a copy of the .sdtid file seed into the RSA SecurID Library on the BlackBerry device. When the BlackBerry device imports the .sdtid file seed into the RSA SecurID Library, the RSA SecurID Library randomly generates a password that the RSA SecurID Library uses to encrypt the .sdtid file seed.
9. The RSA SecurID library authenticates with the RSA authentication server and initializes the software token algorithm once each minute.
10. Each time the BlackBerry device user tries to establish a Wi-Fi® or VPN connection that requires two-factor authentication, the BlackBerry device uses the initialized algorithm to combine the .sdtid file seed with random data based on the BlackBerry device clock and generate a new software token tokencode.

The RSA SecurID Library on the BlackBerry device can decrypt the .sdtid file seed using an optional password if the administrator of RSA SecurID uses RSA Authentication Manager version 6.1 or later to configure the password to issue an encrypted .sdtid file seed to the BlackBerry device user. The RSA SecurID Library uses code signing to prevent third-party applications from altering or reading the information that the RSA SecurID Library stores on the BlackBerry device.

WAP gateway connections

BlackBerry® Device Software version 3.2 SP1 or later supports WTLS, which is designed to provide an extra layer of security when the BlackBerry device connects to a WAP gateway. WTLS requires a WAP gateway to provide standard WAP access to the Internet. For more information about the WAP gateway, see your organization's network operator or wireless service provider.

Instant messaging server connections

The BlackBerry® Collaboration Service is designed to provide a connection between the instant messaging server and the collaboration clients on BlackBerry devices. If your organization's instant messaging server is a Microsoft® Live Communications Server 2005 or Microsoft® Office Communications Server 2007, the BlackBerry Collaboration Service connects to the Microsoft Office Communicator Web Access server using HTTPS or HTTP.

Using a segmented network architecture

To prevent the spread of malware on your organization's network, you can divide your organization's network or LAN into multiple segments that are separated by firewalls to create a segmented network architecture. Each network segment can contain network traffic, which improves the security and performance of the network segment by filtering out data that is not destined for that specific segment. If your organization's security policies enforce the use of segmented network architecture, you can place the BlackBerry® Enterprise Solution components in network segments.

To place the BlackBerry Enterprise Solution in multiple network segments, you must install each BlackBerry Enterprise Solution component on a computer that is separate from the computers that host the other components and then place each computer in its own network segment. When you place the BlackBerry Enterprise Solution components in segmented network architecture, you create an architecture that is designed to prevent the spread of potential attacks from one BlackBerry Enterprise Solution component that exists on one computer to another computer within your organization's LAN. In a segmented network, attacks are isolated and contained on one computer. When each BlackBerry Enterprise Solution component is located in its own network segment, you permit remote communications by opening only the port connections that the BlackBerry Enterprise Solution components use.

Preventing the spread of malware on your organization's Wi-Fi network by using a segmented network architecture

If you have configured an enterprise Wi-Fi® network that uses a VPN solution, when Wi-Fi enabled BlackBerry® devices make connections to the network, they might permit the VPN concentrator, which acts as network gateway, to send data directly over port number 4101 to a BlackBerry® Enterprise Server within the internal network of your organization. The VPN concentrator is the only device that is connected to the enterprise Wi-Fi network in this scenario. You must configure your organization's VPN concentrator to prevent the VPN concentrator from opening unnecessary connections to the internal network.

Protecting BlackBerry Device Software updates over the wireless network

To update the BlackBerry® Device Software over the wireless network, you can use the BlackBerry Administration Service to configure updates, or you can permit your organization's wireless service provider to update the BlackBerry Device Software.

By default, only the BlackBerry® Enterprise Server can send available BlackBerry Device Software updates and request that BlackBerry devices update the BlackBerry Device Software. The wireless service provider cannot send available BlackBerry Device Software updates to BlackBerry devices unless you change the value for the Allow Non Enterprise Upgrade IT policy rule to Yes to turn off exclusive BlackBerry Enterprise Server control of BlackBerry Device Software update requests over the wireless network.

The BlackBerry Enterprise Solution protects the BlackBerry Device Software updates using authentication, IT policies, content protection, and battery requirements.

How the BlackBerry Enterprise Solution authenticates requests for BlackBerry Device Software updates over the wireless network

Request source	Description of authentication method
BlackBerry® Enterprise Server	The BlackBerry Enterprise Server and the BlackBerry device encrypt all communication that they send between each other, including the communication of BlackBerry® Device Software updates, using standard BlackBerry encryption.
<ul style="list-style-type: none">BlackBerry® InfrastructureAdministration web site of the BlackBerry® Provisioning System	The BlackBerry device uses digital signature validation to authenticate the following communication of BlackBerry Device Software updates over the wireless network: <ul style="list-style-type: none">control messages that the BlackBerry device receives from the BlackBerry Infrastructure or the BlackBerry Provisioning System administration siteupdate instructions that the BlackBerry device requests and receives from the BlackBerry Infrastructure or BlackBerry Provisioning System administration site

Process flow: Preparing to send the request for BlackBerry Device Software updates over the wireless network

Before the BlackBerry® Infrastructure sends a BlackBerry® Device Software update to a BlackBerry device, it performs the following actions:

1. The BlackBerry Infrastructure generates an ECDSA key periodically, using ECC over a 521-bit curve.
2. The BlackBerry Infrastructure signs the ECDSA key, using a stored root certificate.
3. The BlackBerry Infrastructure signs the BlackBerry Device Software update that it sends to the BlackBerry device using the digitally signed ECDSA key.

Process flow: Verifying the communication of a BlackBerry Device Software update over the wireless network

When the BlackBerry® device receives the BlackBerry® Device Software update, it performs the following actions:

1. The BlackBerry device verifies the ECDSA key that is using a public key common to all BlackBerry devices that support BlackBerry Device Software updates over the wireless network.
2. The BlackBerry device verifies the digital signature on the ECDSA key, using a stored root certificate.

How a BlackBerry device protects user data during a BlackBerry Device Software update over the wireless network

When you or a user turns on the content protection feature on a BlackBerry® device, the BlackBerry device protects user data as follows:

- the user must type the BlackBerry device password before the BlackBerry® Device Software update process can back up or restore the user data
- the BlackBerry device encrypts stored user data during the BlackBerry Device Software update process

Battery power requirements for BlackBerry Device Software updates over the wireless network

If the battery power level on a BlackBerry® device drops below the required minimum level required (50%) to perform a BlackBerry® Device Software update, the BlackBerry device prompts the user to recharge the battery and start the BlackBerry Device Software update process again. This security measure is designed to protect the BlackBerry device against attacks from users with malicious intent who might try to take advantage of low battery power during a BlackBerry Device Software update.

You can set the Secure Wipe If Low Battery IT policy rule to require that the BlackBerry device delete all user data if the BlackBerry device has insufficient battery power to receive IT policy updates or IT administration commands.

Protecting Wi-Fi connections to the BlackBerry Enterprise Solution

If your organization's wireless solution uses an enterprise Wi-Fi® network to extend your organization's enterprise network, you must protect the enterprise Wi-Fi network from unauthorized use. You must configure all wireless client devices to complete authentication before they can access the enterprise Wi-Fi network and verify that all wireless communications between wireless client devices and the enterprise Wi-Fi network are encrypted.

For details and recommendations about protecting the enterprise Wi-Fi network, see the vendors for your organization's enterprise Wi-Fi network infrastructure.

Security features of the enterprise Wi-Fi network architecture

When you configure the BlackBerry® Enterprise Solution to use an enterprise Wi-Fi® network, you must consider additional network security to protect all message and application data communication between the BlackBerry® Enterprise Server and Wi-Fi enabled BlackBerry devices. Wi-Fi enabled BlackBerry devices are designed to reject incoming connections, to support limited connections in Wi-Fi infrastructure mode only, and to prevent Wi-Fi ad-hoc networking (peer-to-peer) connections.

Wi-Fi enabled BlackBerry devices on an enterprise Wi-Fi network bypass the use of SRP by using the BlackBerry Router to send data between the BlackBerry Enterprise Server and the BlackBerry device. After the BlackBerry Router protocol establishes an authenticated connection, the Wi-Fi enabled BlackBerry device opens a direct connection to the BlackBerry Enterprise Server using the BlackBerry Router instead of SRP connectivity and authentication.

Standard BlackBerry encryption is designed to encrypt messages that the Wi-Fi enabled BlackBerry device and the BlackBerry Enterprise Server send between them after they establish an authenticated connection. Wi-Fi enabled BlackBerry devices also support multiple security methods that are designed to encrypt wireless communications over the enterprise Wi-Fi network between the BlackBerry device and wireless access points or a network firewall on the enterprise Wi-Fi network.

Related topics

BlackBerry Router protocol authentication

Accessing the BlackBerry Infrastructure

Wi-Fi® enabled BlackBerry® devices can connect directly to the BlackBerry® Infrastructure over the Internet for access to voice and data services that a mobile network provider offers, even if UMA is not available. If a user's mobile network provider makes UMA technology (GAN technology) available, and the user subscribes to the UMA feature, a Wi-Fi enabled BlackBerry device is designed to establish an IPSec VPN tunnel over the enterprise Wi-Fi network to the GANC to access the mobile network provider's voice and data services.

The Wi-Fi enabled BlackBerry device and the BlackBerry Infrastructure send all data to each other over the established SSL connection, which encrypts the data using a negotiable algorithm.

The BlackBerry Infrastructure sends its SSL certificate to the BlackBerry device when the BlackBerry device tries to establish the SSL connection to the BlackBerry Infrastructure. The BlackBerry device uses a preloaded root certificate that is encrypted with a 1024 bit key to authenticate the SSL certificate. If the user deletes the root certificate on the BlackBerry device, and the BlackBerry device tries to establish the SSL connection to the BlackBerry Infrastructure, the BlackBerry device prompts the user to trust the SSL certificate.

Related topics

Algorithm suites that the BlackBerry device supports for negotiating SSL connections

Protecting connections from Wi-Fi enabled BlackBerry devices to the BlackBerry Infrastructure

A connection from a Wi-Fi® enabled BlackBerry® device to the BlackBerry® Infrastructure over an SSL connection is designed to provide the same protection that an SRP authenticated connection from the BlackBerry® Enterprise Server to the BlackBerry Infrastructure provides. A user with malicious intent cannot use the connection to send data to or receive data from the BlackBerry device.

If a user with malicious intent tries to impersonate the BlackBerry Infrastructure, the BlackBerry device is designed to prevent the connection when the public key of the SSL certificate of the impersonated BlackBerry Infrastructure does

not match the private key of the root certificate that is preloaded on the BlackBerry device. If a user accepts an invalid certificate, the connection cannot continue unless the BlackBerry device can use the connection to authenticate with a valid BlackBerry Enterprise Server or BlackBerry® Internet Service.

Supported security features of Wi-Fi enabled BlackBerry devices

Wi-Fi® enabled BlackBerry® devices are designed to operate on enterprise Wi-Fi networks that use supported IEEE® 802.11® communication to permit users to access messaging, organizer, and browser-based applications over the wireless network while they are mobile in the physical environment of their organization. Wi-Fi enabled BlackBerry devices provide enterprise Wi-Fi network configuration options that are designed to be compatible with the wireless security policies and environments of most organizations.

Wi-Fi enabled BlackBerry devices support the following categories of enterprise Wi-Fi network security technology:

Enterprise Wi-Fi network security technology	Wi-Fi enabled BlackBerry device support
Enterprise captive portal	Configure authentication with enterprise captive portals (enterprise Wi-Fi networks outside of your organization's network) using a login web page.
Layer 2 security	Configure layer 2 (the IEEE 802.11 link layer) security methods and protocols so that a BlackBerry device and a wireless access point can use the layer 2 methods for encryption, or encryption and user authentication. The BlackBerry device supports the following layer 2 security methods: <ul style="list-style-type: none"> • open (no security method) • 64-bit and 128-bit WEP encryption • PSK • IEEE 802.1X® and EAP authentication framework support (RFC 3748) using LEAP, PEAP, EAP-TTLS, EAP-FAST, EAP-SIM, and EAP-TLS (RFC 2716) • TKIP and AES-CCMP encryption for WPA™-Personal, WPA2™-Personal, WPA-Enterprise, and WPA2-Enterprise
Layer 3 security	Use VPNs (the only layer 3 security method that the BlackBerry device supports) at the IP layer.
Two-factor authentication	Use passcodes to authenticate the user with enterprise Wi-Fi networks using PEAP, EAP-FAST and EAP-TTLS authentication methods and VPNs. The BlackBerry device supports using automatic PAC provisioning with EAP-FAST only.

Related topics

Enterprise Wi-Fi security methods that the BlackBerry device supports

Enterprise Wi-Fi security methods that the BlackBerry device supports

EAP authentication methods that the BlackBerry device supports

The BlackBerry® device supports EAP authentication methods with protected Wi-Fi® networks only.

Authentication method	Description	BlackBerry device implementation
LEAP	<p>Cisco® developed LEAP in response to the weaknesses that were identified in WEP. LEAP uses the IEEE® 802.1X authentication framework.</p> <p>LEAP is designed to significantly improve basic WEP security by providing authentication between the enterprise Wi-Fi network device and the enterprise Wi-Fi network, dynamic generation of WEP keys unique to each client, and automatic WEP key updates throughout the course of a session on the enterprise Wi-Fi network device.</p>	<p>The BlackBerry device supports LEAP authentication based on a user name and password. The BlackBerry device uses a one-way function to encrypt passwords before sending them to the authentication server.</p> <p>LEAP does not provide mutual authentication between the BlackBerry device and the enterprise Wi-Fi network. Specify strong password policies on networks that use LEAP.</p>
PEAP	<p>PEAP is an open standard developed by Microsoft® Corporation, RSA Security®, and Cisco Systems, Inc. PEAP permits supplicant authentication with an authentication server by</p> <ul style="list-style-type: none"> • creating an encrypted tunnel between the supplicant and the authentication server using TLS • using the TLS tunnel to send the supplicant authentication credentials to the authentication server 	<p>The BlackBerry device supports the following versions of PEAP:</p> <ul style="list-style-type: none"> • PEAPv0 • PEAPv1 <p>The BlackBerry device supports EAP-MS-CHAPv2 and EAP-GTC as second-phase protocols that the BlackBerry device can use with PEAP for the exchange of authentication credentials.</p> <p>A root certificate corresponding to the server certificate that the authentication server uses must exist on the BlackBerry device for PEAP authentication to complete.</p>
EAP-TLS	<p>EAP-TLS is defined in RFC 2716. It uses a PKI to permit supplicant authentication with an authentication server by</p> <ul style="list-style-type: none"> • using the TLS protocol to create an encrypted tunnel between the supplicant and the authentication server • using the TLS encrypted tunnel and a client certificate to send authentication credentials to the authentication server 	<p>The Wi-Fi enabled BlackBerry device supports EAP-TLS using certificates that meet specific requirements on the server and the client for authentication.</p> <p>The root certificates of the authentication server certificate and the client certificate must exist on the Wi-Fi enabled BlackBerry device for EAP-TLS authentication to complete.</p>
EAP-TTLS	<p>EAP-TTLS is designed to extend EAP-TLS by permitting authentication from the authentication server to the supplicant. When the authentication server has used its certificate to authenticate to the supplicant and established a secure connection to the BlackBerry device, the server can use an authentication protocol over the secure connection to authenticate the supplicant.</p>	<p>The BlackBerry device supports EAP-MS-CHAPv2 and MS-CHAPv2 as second-phase protocols that the BlackBerry device can use with EAP-TTLS for the exchange of authentication credentials.</p> <p>The root certificates of the authentication server certificate must exist on the Wi-Fi enabled BlackBerry device for EAP-TTLS authentication to complete.</p>

Authentication method	Description	BlackBerry device implementation
EAP-FAST	EAP-FAST is defined in RFC 4851. EAP-FAST uses PAC dynamically to establish a TLS connection to the BlackBerry device and verify the supplicant credentials over the TLS connection.	The BlackBerry device supports EAP-MS-CHAPv2 and EAP-GTC as second-phase protocols that the BlackBerry device can use with EAP-FAST for the exchange of authentication credentials.
EAP-SIM	EAP-SIM is defined in RFC 4186. It uses the GSM SIM for authentication and session key distribution. GSM SIM authentication uses a challenge-response method without mutual authentication.	<p>The BlackBerry device supports using EAP-SIM with the credentials on the GSM SIM only. The user does not need to type or select credentials on the BlackBerry device.</p> <p>The user identity that EAP-SIM uses for authentication on the BlackBerry device is built from the IMSI using the 3GPP® technical specification 3GPP-TS-23.003.</p> <p>The BlackBerry device can receive at least two challenges from the authentication server to provide stronger authentication.</p>

Encryption algorithms that the BlackBerry device supports for use with layer 2 security methods

Protocol	Description	Wi-Fi enabled BlackBerry device implementation
WEP	—	The Wi-Fi® enabled BlackBerry® device supports the use of WEP keys.
TKIP	<p>TKIP is</p> <ul style="list-style-type: none"> • part of the IEEE® 802.11i enterprise Wi-Fi network security standard • designed to address the shortcomings in WEP without requiring replacement of the existing enterprise Wi-Fi network hardware • designed to use the RC4 encryption method (based on improved WEP standards) <p>TKIP is designed to be more robust than WEP in the following ways:</p> <ul style="list-style-type: none"> • uses a key size of 128 bits (compared to 40 bits or 104 bits for WEP) • uses a modified initialization vector, that is designed to increase the difficulty of deriving the WEP key significantly • generates keys dynamically for each session by changing keys for each packet of transmitted data (where WEP uses a fixed key for an entire session) • uses a MIC that fails and discards transmitted packets that are captured, altered, and resent • requires a secure method of distribution to a wireless client device 	<p>The Wi-Fi enabled BlackBerry device supports the use of TKIP with</p> <ul style="list-style-type: none"> • EAP-TLS • EAP-TTLS • EAP-FAST • PEAP • PSK

Protocol	Description	Wi-Fi enabled BlackBerry device implementation
AES-CCMP	<p>AES-CCMP is</p> <ul style="list-style-type: none"> part of the IEEE 802.11i enterprise Wi-Fi network security standard designed to use AES encryption <p>AES-CCMP is designed to provide a robust security protocol similar to TKIP in the following ways:</p> <ul style="list-style-type: none"> uses a key size of 128 bits uses a MIC that fails and discards transmitted packets that are captured, altered, and resent requires a secure method of distribution to a wireless client device 	<p>The Wi-Fi enabled BlackBerry device supports the use of AES-CCMP with</p> <ul style="list-style-type: none"> EAP-TLS EAP-TTLS EAP-FAST PEAP PSK

Related topics

Requiring protected connections to enterprise Wi-Fi networks

EAP authentication methods and encryption algorithms that the BlackBerry device supports the use of CCKM with

EAP authentication methods are designed to provide mutual authentication between supported Wi-Fi® enabled BlackBerry® devices and the enterprise Wi-Fi network. The Wi-Fi enabled BlackBerry device supports the use of CCKM with all EAP authentication methods that the Wi-Fi enabled BlackBerry device supports as well as WEP and TKIP.

The Wi-Fi enabled BlackBerry device does not support the use of CCKM with the Cisco® CKIP encryption algorithm or the AES-CCMP encryption algorithm.

IEEE 802.1X environment components

An IEEE® 802.1X environment includes the following components:

- IEEE 802.1X or EAP client software, also called a supplicant, running on the wireless client device
- IEEE 802.1X software running on the access point, also called an authenticator
- authentication server that authenticates the wireless client devices with the enterprise Wi-Fi® network on behalf of the authenticator and permits the wireless client devices to authenticate the Wi-Fi network

In most cases, the authentication server uses the RADIUS protocol (RFC 2865 and RFC 3579) to communicate with the authenticator on the access point.

The Wi-Fi enabled BlackBerry® device has a built-in IEEE 802.1X supplicant.

How the IEEE 802.1X environment controls access to the enterprise Wi-Fi network

When a wireless client device first associates itself with an access point that you configured for IEEE® 802.1X security, the only communication that the access point permits is IEEE 802.1X authentication. When you configure a negotiated EAP method, the supplicant on the Wi-Fi® enabled BlackBerry® device sends its credentials (typically, a user name and password) to the access point, which forwards the information to the authentication server. The authentication server authenticates the Wi-Fi enabled BlackBerry device on behalf of the access point and instructs the access point to permit or prevent access to the enterprise Wi-Fi network. The authentication server sends Wi-Fi network credentials to the Wi-Fi enabled BlackBerry device to permit it to authenticate with the access point.

After an authentication server permits the Wi-Fi enabled BlackBerry device to access the enterprise Wi-Fi network, the access point and the BlackBerry device use IEEE 802.1X EAPoL-Key messages to establish the WEP, TKIP, or AES-CCMP encryption keys, depending on the EAP method that the BlackBerry device specifies. After the access point and the Wi-Fi enabled BlackBerry device establish encryption keys, the BlackBerry device has encrypted access to the enterprise Wi-Fi network.

If your organization's enterprise Wi-Fi network uses one of the supported EAP authentication methods, you can grant and revoke Wi-Fi enabled BlackBerry devices access to the enterprise Wi-Fi network by updating the central authentication server only. You do not need to update the configuration of each access point.

Managing enterprise Wi-Fi network solution security using IT policy rules and configuration settings

With the BlackBerry® Enterprise Solution, you can monitor and control all BlackBerry devices from the BlackBerry Administration Service using wireless IT commands and IT policy rules. The enterprise Wi-Fi® network solution includes specific IT policy rules and configuration settings for the security of the enterprise Wi-Fi network solution. You can turn Wi-Fi access on and off for Wi-Fi enabled BlackBerry devices on BlackBerry® Enterprise Server version 4.1 SP3 or later, and manage Wi-Fi and VPN configuration settings for user accounts on BlackBerry Enterprise Server version 4.1 SP2 or later.

For more information about using IT policy rules and configuration settings to configure your organization's enterprise Wi-Fi network solution to support Wi-Fi enabled BlackBerry devices, see the *BlackBerry Enterprise Server Administration Guide*.

Requiring protected connections to enterprise Wi-Fi networks

Using WEP encryption to protect connections to enterprise Wi-Fi networks

WEP was designed to bring the same level of security to an enterprise Wi-Fi® network as is available on a wired LAN. WEP uses a matching encryption key at both the access point and the wireless client device to secure wireless communication. This key can be 40 bits (for 64-bit WEP) or 104 bits (for 128-bit WEP) in length.

To use WEP, you must distribute WEP keys to the supported Wi-Fi enabled devices in your organization's enterprise Wi-Fi network. In the BlackBerry® Administration Service, you can define WEP keys for each supported Wi-Fi enabled device using IT policy rules or configuration settings. The BlackBerry® Enterprise Server sends the WEP keys to the Wi-Fi enabled device when a user activates the Wi-Fi enabled device and when you update the IT policy thereafter.

By current industry standards, WEP is not a cryptographically strong security solution. Identified WEP weaknesses include the following scenarios:

- an attacker could capture transmissions over the wireless network and might be able to deduce WEP keys in very little time
- an attacker might be able to use a man-in-the-middle attack to change WEP-encrypted packets

Organizations that use WEP as their preliminary security method to limit access to their enterprise Wi-Fi network can also use a VPN to provide data confidentiality. A VPN can authenticate and encrypt access to their organization's network.

Using IEEE 802.11i to protect connections to enterprise Wi-Fi networks

IEEE® 802.11i defines an enhanced security protocol to protect enterprise Wi-Fi® networks. It uses the IEEE 802.1X standard for authentication and key management. The IEEE 802.1X standard defines a generic authentication framework that wireless client devices and wired or wireless networks can use to authenticate with each other to permit or prevent the wireless client devices from accessing the network. IEEE 802.11i specifies two Wi-Fi network access control methods: one that is based on PSKs and one that is based on IEEE 802.1X, which uses EAP protocols for authentication.

Authentication method	Description	Wi-Fi enabled BlackBerry device implementation
Using IEEE 802.11i with PSK	Small office and home environments, where it is not feasible to configure a server-based authentication infrastructure, might use IEEE 802.1X with the PSK method. The access point and the wireless client device use a PSK (also known as a pass phrase) to mutually derive link layer encryption keys. The PSK method uses TKIP or AES-CCMP algorithms to secure enterprise Wi-Fi network communications, but the PSK method relies on a single, shared pass phrase of up to 256-bits for access control. All access points and wireless client devices must know the pass phrase.	The Wi-Fi® enabled BlackBerry® device is compatible with the WPA™-Personal and WPA2™-Personal specifications. You can specify the pass phrase and distribute it to the Wi-Fi enabled BlackBerry device using the WLAN Preshared Key configuration setting.
Using the IEEE 802.11i with IEEE 802.1X authentication	An IEEE 802.1X framework can use EAP methods to provide authentication. LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, and EAP-FAST authentication methods are designed to provide mutual authentication between the Wi-Fi enabled BlackBerry device and the enterprise Wi-Fi network.	To act as a Wi-Fi supplicant, the Wi-Fi enabled BlackBerry device implements Wi-Fi authentication processes that use EAP methods as specified in RFC 3748 and meet the requirements of RFC 4017. Wi-Fi enabled BlackBerry devices are designed to use EAP authentication methods (for example, EAP-TLS, EAP-TTLS, EAP-FAST, and PEAP) to mutually authenticate to Wi-Fi networks, as defined in the WPA-Enterprise and WPA2-Enterprise specification. Wi-Fi enabled BlackBerry devices use credentials to provide mutual authentication. When the Wi-Fi enabled BlackBerry device sends EAPoL messages, the BlackBerry device uses the encryption and message integrity protection specified by the EAP authentication method. When the BlackBerry device transmits EAPoL-Key messages, the BlackBerry device uses RC4 or AES algorithms to provide message integrity and encryption.

Using certificate-based authentication to protect connections to enterprise Wi-Fi networks

If you use PEAP, EAP-TLS, or EAP-TTLS methods to secure the access points on your organization's enterprise Wi-Fi® network, to connect to the enterprise Wi-Fi network, Wi-Fi enabled BlackBerry® devices must authenticate mutually with an access point using an authentication server. You require a certificate authority to generate the certificates that the Wi-Fi enabled BlackBerry devices and RADIUS server store.

Successful PEAP, EAP-TLS, or EAP-TTLS authentication requires that the Wi-Fi enabled BlackBerry devices trust the certificate of the access authentication server. The certificate binds the authentication server identity to a public and private key pair. Wi-Fi enabled BlackBerry devices do not trust the authentication server certificate automatically. For the Wi-Fi enabled BlackBerry devices to trust the authentication server certificates, the following conditions must exist:

- a certificate authority that the Wi-Fi enabled BlackBerry devices and the authentication server mutually trust must generate the certificate for the authentication server and the certificate for each Wi-Fi enabled BlackBerry device
- the root certificates in the certificate chain to which the certificate of the authentication server belongs must exist on Wi-Fi enabled BlackBerry devices that use PEAP, EAP-TLS, or EAP-TTLS

Each BlackBerry device stores a list of explicitly trusted root certificates that certificate authorities issued.

Caching connection information when using IEEE 802.1X authentication

When using IEEE® 802.11i with IEEE 802.1X authentication, the Wi-Fi® enabled BlackBerry® device and the access point can cache a PMK. The EAP exchange generates keying material which derives the PMK. PMK caching reuses previously established keying material to skip IEEE 802.1X authentication and mutually derive session keys with an access point to which it connects. This helps reduce the roaming latency between access points in an enterprise Wi-Fi network for the Wi-Fi enabled BlackBerry device.

VPN solution on a Wi-Fi enabled BlackBerry device

Wi-Fi® enabled BlackBerry® devices have built-in VPN clients that supports several VPN concentrators. For a list of currently supported VPN concentrators, visit www.blackberry.com/support to read article KB13354.

If a Wi-Fi enabled BlackBerry device has a VPN profile, it logs into the VPN concentrator automatically after it connects to the enterprise Wi-Fi network. To create a VPN profile, you must configure the VPN configuration settings (for example, the IP address of the VPN concentrator, user names and passwords, and cryptographic methods to be used) on the Wi-Fi enabled BlackBerry device or BlackBerry® Enterprise Server. Depending on the security policy of your organization, you or the user can save each user name and password on the Wi-Fi enabled BlackBerry device to prevent the Wi-Fi enabled BlackBerry device from prompting the user for credentials the first time (or each time) that the Wi-Fi enabled BlackBerry device connects to the enterprise Wi-Fi network.

The Wi-Fi enabled BlackBerry device is also compatible with VPN environments that use two-factor authentication using hardware tokens or software tokens for user credentials. When the Wi-Fi enabled BlackBerry device tries to log in to the VPN, the Wi-Fi enabled BlackBerry device uses, with the hardware token or software token, credentials that are generated automatically or provided by the user.

Using VPNs to protect connections to enterprise Wi-Fi networks

Your organization's environment might include VPNs, such as IPSec VPNs, that provide remote users with secure access to an enterprise Wi-Fi® network. A VPN provides a strongly encrypted tunnel between the wireless client device and your organization's network. Unlike other supported security methods for enterprise Wi-Fi networks, a VPN does not involve the access point in data encryption.

An enterprise Wi-Fi VPN solution consists of the following components:

- a VPN client on the Wi-Fi enabled BlackBerry® device which the BlackBerry device uses to gain access to the network
- a VPN concentrator, which acts as the gateway to the enterprise Wi-Fi network

When your organization uses a VPN to protect access to the enterprise Wi-Fi network, by default, the enterprise Wi-Fi network configuration also uses a Wi-Fi authentication or encryption method to provide an access-control mechanism for the enterprise Wi-Fi network itself, and uses VPN to provide the secure access method. In this scenario, you can configure the enterprise Wi-Fi network as an untrusted network, and only connect the VPN concentrator to the enterprise Wi-Fi network.

The VPN client on a Wi-Fi enabled BlackBerry device is designed to perform the following actions:

- use strong encryption to authenticate itself with the VPN concentrator
- create an encrypted tunnel between the Wi-Fi enabled BlackBerry device and the VPN concentrator through which the Wi-Fi enabled BlackBerry device and Wi-Fi enterprise network can direct their communication

Using captive portals to protect connections to enterprise Wi-Fi networks or Wi-Fi hotspots

A captive portal is a web-based authentication mechanism that permits access to an enterprise Wi-Fi® network or Wi-Fi hotspot. Wi-Fi enabled BlackBerry® devices can use a captive portal to gain access to an IP filtered segment of the enterprise Wi-Fi network or hotspot. After the BlackBerry device uses a captive portal to connect to an enterprise Wi-Fi network or hotspot, the user can send a browser request for a web site from the Wi-Fi enabled BlackBerry device to an HTML login page, which permits the enterprise Wi-Fi network or hotspot to authenticate with the BlackBerry device before permitting it access to the web site.

If your organization has a captive portal, you can permit users to access the captive portal using the WLAN Login application on the BlackBerry device. Users must authenticate with the WLAN Login application browser using login credentials that you provide.

When the BlackBerry device authenticates with the captive portal, the user can use the BlackBerry® Browser on the BlackBerry device to access other web sites and data services that are available on the Wi-Fi network. The BlackBerry device is designed to support web browsing using the BlackBerry MDS Connection Service.

Authenticating a user

When a user activates a BlackBerry® device, the BlackBerry® Enterprise Solution uses a wired or wireless method to generate the master encryption key so that it can authenticate the user and the BlackBerry device with the BlackBerry® Enterprise Server. The user must have a valid email address so that the BlackBerry device can activate and register with the wireless network.

Authenticating a user using a password

When you associate a BlackBerry® device with a BlackBerry® Enterprise Server, you can require a user to authenticate with the BlackBerry device using a security password. You can use IT policy rules to configure password requirements such as duration, length, and strength, to specify password patterns, and to forbid specific passwords. For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

If a user activates the BlackBerry device over the wireless network, the user must contact you for a temporary activation password that the BlackBerry device uses to generate the master encryption key. You can specify an activation password and communicate it to the user.

The activation password has the following characteristics:

- applies to the user's email account
- is not valid after five unsuccessful activation attempts
- expires if the user does not activate the BlackBerry device within the default period (48 hours), or a period of up to 720 hours that you can specify when you create the activation password
- is deleted from the BlackBerry Enterprise Server when the BlackBerry device activates successfully

Using the BlackBerry Smart Card Reader

To require users to prove their identities to their BlackBerry® device, you can configure two-factor authentication using a smart card. You can use what users have (the smart card) and what users know (the smart card password).

The BlackBerry® Smart Card Reader integrates smart card use with the BlackBerry® Enterprise Solution, permitting users who authenticate with their smart cards to log in to certain Bluetooth® enabled BlackBerry devices.

The BlackBerry Smart Card Reader

- creates a reliable two-factor authentication environment for granting users access to BlackBerry and PKI applications
- is designed to permit the wireless digital signing and encryption of wireless email messages using the S/MIME Support Package for BlackBerry® smartphones
- stores all encryption keys in RAM only and never writes the keys to flash memory

For more information, see the *BlackBerry Smart Card Reader Security Technical Overview*.

Binding the smart card to the BlackBerry device

If a user has a smart card authenticator, smart card driver, and smart card reader driver installed on the BlackBerry® device, you or the user can start two-factor authentication on the BlackBerry device to bind the BlackBerry device to the installed smart card. After the BlackBerry device binds to the smart card, it requires that smart card to authenticate the user.

You can configure the Force Smart Card Two-Factor Authentication IT policy rule in the BlackBerry Administration Service to require that a user authenticates with the BlackBerry device using a smart card. If you do not require the user to authenticate with the BlackBerry device using a smart card, the user can turn two-factor authentication on and off with the smart card when they configure in the BlackBerry device options, in the Security Options screen, the User Authenticator field..

Process flow: Turning on two-factor authentication with a smart card

When you or the user turns on two-factor authentication, the following events occur:

1. The BlackBerry® device locks.
2. When a user tries to unlock the BlackBerry device, the BlackBerry device prompts the user to type the BlackBerry device password. If the user has not yet specified a BlackBerry device password, the BlackBerry device requires them to specify one.
3. The BlackBerry device prompts the user to type the user authenticator (smart card) password to turn on two-factor authentication with the installed smart card.
4. The BlackBerry device binds to the installed smart card by storing the following binding information in a special BlackBerry device NV store location that a user cannot access:
 - the name of a Java® class that the BlackBerry® Smart Card Reader requires
 - the binding information format
 - the smart card type (for the Common Access Card, this string is "GSA CAC".)
 - the name of a Java class that the smart card code requires
 - a unique 64-bit identifier that the smart card provides
 - a smart card label that the smart card provides (for example, "GRAHAM.JOHN.1234567890")
5. The BlackBerry device pushes the current IT policy to the BlackBerry Smart Card Reader.

Confirming that the BlackBerry device binds to the correct smart card

After a user turns on two-factor authentication, the BlackBerry® device prompts the user to insert the smart card into the BlackBerry® Smart Card Reader, and the BlackBerry device prompt indicates the label and the card type of the correct (bound) smart card. If the BlackBerry device is running BlackBerry® Device Software version 3.6 with the S/MIME Support Package version 1.5 for BlackBerry® smartphones installed or without the S/MIME Support Package for BlackBerry smartphones installed, the information in the prompt is the only indication that a smart card is bound to the BlackBerry device.

If the BlackBerry device is running BlackBerry Device Software version 4.0 or later (S/MIME Support Package for BlackBerry smartphones optional), the user can also view smart card information in the BlackBerry device options, in the Security Options screen.

Field	Description
Name	This field indicates the type of the installed smart card software.
Initialized	This field indicates whether the BlackBerry device authenticated with and is bound to the smart card.

Controlling BlackBerry devices

In the BlackBerry® Enterprise Solution, you can control all BlackBerry devices over the wireless network from the BlackBerry Administration Service.

Controlling BlackBerry devices using IT policy rules

You can use IT policies to control BlackBerry® devices and the BlackBerry® Desktop Software in your organization's environment. The Default IT policy includes all IT policy rules configured to default values to reflect the default behavior of BlackBerry devices or BlackBerry Desktop Software. By default, after users activate their BlackBerry devices on the BlackBerry® Enterprise Server, the BlackBerry Enterprise Server pushes the Default IT policy to their BlackBerry devices automatically. For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Changing the default behavior of BlackBerry devices and BlackBerry Desktop Software

An IT policy rule permits you to customize and control the following actions of the BlackBerry® device and BlackBerry® Desktop Software:

- changing the value for an IT policy rule to Yes or No
- typing a string, which turns on an IT policy rule and provides the parameters for its use at the same time
- selecting a predefined value to assign to an IT policy rule

You cannot use all IT policy rules to control all BlackBerry device types. The BlackBerry Device Software version must support the IT policy rule that you configure. For example, you cannot use the Disable Camera IT policy rule to control whether a user can access the camera on the BlackBerry device if the BlackBerry Device Software version does not support the IT policy rule. For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

The BlackBerry Administration Service groups the IT policy rules by common properties or by application. Most IT policy rules are designed so that you can assign them to multiple user accounts.

If you delete an IT policy that you assigned user accounts to, the BlackBerry® Enterprise Server reassigns the user accounts to the Default IT policy and resends the Default IT policy to the BlackBerry device, enforcing the default values.

Creating IT policy rules to control custom applications

You can create IT policy rules to control custom applications that your organization develops to run on BlackBerry® devices. After you create an IT policy rule, you can add it to any IT policy and assign a value to it. Only the custom applications can use IT policy rules that you create. You cannot create IT policy rules to control standard BlackBerry device applications and features.

Enforcing IT policy changes over the wireless network

You can send IT policies over the wireless network to enforce IT policy rule additions, deletions, or changes on C++ based BlackBerry® devices that are running BlackBerry® Device Software version 2.5 or later and on Java® based BlackBerry devices that are running BlackBerry Device Software version 3.6 or later. When a BlackBerry device receives an updated IT policy or a new IT policy, the BlackBerry device and the BlackBerry® Desktop Software apply the configuration changes.

The BlackBerry® Enterprise Server must resend a changed IT policy to the BlackBerry device to update the behavior of the BlackBerry device and the BlackBerry Desktop Software over the wireless network. By default, the BlackBerry Enterprise Server is designed to resend the IT policy to the BlackBerry devices within a short period of time after you update the IT policy.

You can also resend an IT policy to a user manually. You can configure the BlackBerry Enterprise Server to resend IT policies to BlackBerry devices that you associated with a specific BlackBerry Enterprise Server at a scheduled interval regardless of whether you changed the IT policies.

Enforcing BlackBerry device and BlackBerry Desktop Software security

The BlackBerry® Enterprise Solution offers a different security settings for the BlackBerry device and BlackBerry® Desktop Software. For example, you can specify one or more IT policy rules to enforce the following features to meet your organization's security requirements:

- Enforce encryption (for example, encryption of user data and messages that the BlackBerry® Enterprise Server forwards to the message recipient) and encryption strength
- Enforce password or pass phrase use
- Enforce a strong password or pass phrase
- Secure Bluetooth® connections
- Protect user data on a BlackBerry device
- Protect master encryption keys on a BlackBerry device
- Restrict application use on a BlackBerry device
- Restrict BlackBerry device resources that are available to third-party applications

Controlling BlackBerry device access to the BlackBerry Enterprise Server

You can turn on the Enterprise Service Policy to control which BlackBerry® devices can connect to the BlackBerry® Enterprise Server. After you turn on the Enterprise Service Policy, the BlackBerry Enterprise Server still permits connections from BlackBerry devices and BlackBerry enabled devices that you previously associated with the BlackBerry Enterprise Server, but, by default, it prevents connections from BlackBerry devices that you associate after you turn on the Enterprise Service Policy.

You can define BlackBerry device criteria in an allowed list to turn on and turn off BlackBerry Enterprise Server access for BlackBerry devices. BlackBerry devices that meet the allowed list criteria can complete wireless activation on that BlackBerry Enterprise Server.

You can define the following types of criteria:

- specific, permitted BlackBerry device PINs as a string
- a permitted range of BlackBerry device PINs

You can also control access to the BlackBerry Enterprise Server based on specific manufacturers and models of BlackBerry devices. The BlackBerry Administration Service includes lists of permitted manufacturers and models based on the properties of BlackBerry devices that you already associated with the BlackBerry Enterprise Server. You can clear items on these lists to control further connections from BlackBerry devices of a specific manufacturer or model.

You can permit a specific user to override the Enterprise Service Policy. If you then configure the allowed list with criteria that excludes that BlackBerry device or BlackBerry enabled device, the user can still connect to the BlackBerry Enterprise Server.

For more information, see the *BlackBerry Enterprise Server Administration Guide*.

Protecting Bluetooth connections on BlackBerry devices

Bluetooth® wireless technology permits Bluetooth enabled BlackBerry® devices to establish a wireless connection with other Bluetooth devices that are within a 10-meter range (for example, a hands-free car kit or wireless headset).

Bluetooth profiles specify how applications on Bluetooth enabled BlackBerry devices and on other Bluetooth devices connect and interoperate. Bluetooth enabled BlackBerry devices implement their Bluetooth serial port profiles to establish serial connections to Bluetooth peripherals using virtual serial ports. The Bluetooth software on the BlackBerry device accesses the serial port through the BlackBerry SDK.

You can use IT policies to manage all Bluetooth enabled BlackBerry devices at the same time. By default, Bluetooth enabled BlackBerry devices that are running BlackBerry® Device Software version 4.0 or later include the following security measures:

- You or the user can turn off the Bluetooth wireless technology for the BlackBerry device.

- Users must request a connection or pairing on the BlackBerry device with another Bluetooth device. Users must also type a shared secret key (called a passkey) to complete the pairing.
- Users can specify whether to encrypt data to and from the BlackBerry device over Bluetooth connections. The BlackBerry® Enterprise Solution uses the passkey to generate encryption keys.
- The BlackBerry device prompts the user each time a Bluetooth device tries to connect to the BlackBerry device.

For more information, see *Security for BlackBerry Devices with Bluetooth Wireless Technology*.

Using Bluetooth CHAP password authorization on the BlackBerry device

Bluetooth® enabled BlackBerry® devices support using CHAP as described in RFC 1994. CHAP is a protocol designed to authenticate the Bluetooth client using a challenge that is combined with a secret (for example, the BlackBerry device password).

BlackBerry devices that use CHAP can establish a Bluetooth connection to the BlackBerry® Desktop Software so that the BlackBerry device never sends its password over an unprotected connection. BlackBerry devices and the BlackBerry Desktop Software can use CHAP to send a challenge and subsequently use the SHA-1 algorithm to calculate a response to the challenge or validate the response of the other party, depending on which party started the Bluetooth link establishment process.

Controlling location-based services on the BlackBerry device

By default, third-party applications and preloaded BlackBerry® applications on BlackBerry devices that support the GPS feature can use it. For example, BlackBerry® Maps is a preloaded application that uses the GPS feature on BlackBerry devices to permit users to locate their global positions. The BlackBerry® Enterprise Server includes the following options to permit you to control the GPS feature and the location-based services:

Option	Description
Turn off the GPS feature.	The following measures prevent third-party applications and preloaded BlackBerry applications from accessing the global position of the BlackBerry device: <ul style="list-style-type: none"> • You can change the value of the Disable GPS IT policy rule to Yes to prevent the BlackBerry device from permitting third-party applications or preloaded BlackBerry applications from accessing the GPS feature. • You can change the value of the Device GPS application control policy rule to Not Permitted in the default application control policy to prevent all third-party applications from using the GPS feature.
Control whether specific third-party applications on the BlackBerry device can use the GPS feature.	You can change the value of the Device GPS application control policy rule to Not Permitted in a specific application control policy to prevent specific third-party applications from using the GPS feature.
Prevent the BlackBerry device from reporting its location to the BlackBerry Enterprise Server.	By default, the value for the Enable Enterprise Location Tracking IT policy rule is No to prevent the BlackBerry device from using the GPS feature to report its location to the BlackBerry Enterprise Server at regular intervals. You can turn on Enterprise Location Tracking, specify a message that the BlackBerry device displays to notify the user when you turn on Enterprise Location Tracking, and configure the interval after which a BlackBerry device reports its location to the BlackBerry Enterprise Server.
Turn off the BlackBerry Maps application.	You can use the Disable BlackBerry Maps IT policy rule to specify whether the BlackBerry Maps application is turned off.

How the BlackBerry device protects its operating system and the BlackBerry Device Software

Each time a user turns on the BlackBerry® device, specific components on the BlackBerry device automatically check the authenticity of the operating system and the integrity of the BlackBerry® Device Software. The BlackBerry Device Software must pass these security tests before users can run the BlackBerry Device Software on the BlackBerry device and BlackBerry Device Software updates over the wireless network can occur.

BootROM authentication and processor binding during the preboot process on BlackBerry devices

The BlackBerry® device processor provides an authentication mechanism that is designed to verify that the preinstalled Research In Motion bootROM code that is located in flash memory is permitted to run on BlackBerry devices. The internal ROM code of the processor is the root of trust on BlackBerry devices. The processor stores the digital signature and the hash of the public key or the entire RSA public key that the RIM signing authority system uses to sign the bootROM code digitally within the bootROM. The RIM signing authority system stores the private RSA keys that it uses to sign the BlackBerry device processors digitally. For example, it stores keys from VeriSign® and uses them to sign Qualcomm® processors digitally.

When a user turns on a BlackBerry device, the BlackBerry device processor runs internal ROM code that reads the RIM bootROM from flash memory and verifies the digital signature of the bootROM code using the public keys that the processor stores. If the verification process is successful, the bootROM is permitted to run on the BlackBerry device. If the verification process fails, the processor stops running.

The process of binding a processor that stores an entire public key to that specific public key can occur during processor manufacturing, or as a step in BlackBerry device manufacturing, during BlackBerry® Device Software configuration, depending on the manufacturer and model number of the processor. Binding a processor involves selecting the specific public key to use or programming a custom key. If the binding process does not occur during the manufacturing of the processor, the BlackBerry device is still permitted to complete the boot process. If the binding process does not occur during the BlackBerry Device Software configuration, the BlackBerry device is not permitted to complete the boot process.

Protecting the BlackBerry device against malware

The BlackBerry® Enterprise Solution includes tools that are designed to permit you to control the manual or automatic installation of third-party applications and limit the access of untrusted applications to the BlackBerry device and its resources. These resources help contain malware attacks on the BlackBerry device.

The BlackBerry Enterprise Solution is designed to use IT policies, application control policies, and code signing to control third-party application access to the BlackBerry device resources and applications. These containment methods are designed to prevent malware that might gain access to the BlackBerry device from causing damage to the BlackBerry device, applications and data, or your organization's network.

You can use BlackBerry Enterprise Solution tools to help prevent opportunities for attackers to use malware to access your organization's network and BlackBerry devices.

For more information, see *Protecting the BlackBerry Device Platform Against Malware*.

Developing third-party wireless applications for BlackBerry devices

Java® based BlackBerry® devices are designed to provide an open platform for third-party wireless enterprise application development. Using BlackBerry® MDS Studio and the BlackBerry® Java® Development Environment, the BlackBerry® Enterprise Solution permits software developers to create third-party applications for BlackBerry devices. BlackBerry JDE developers can create more powerful, sophisticated applications than are created using the standard Java® Platform, ME. A third-party BlackBerry application can perform the following tasks on the BlackBerry device:

- communicate and share persistent storage with other third-party applications
- interact with other BlackBerry applications
- access user data such as calendar entries, email messages, and contacts

By default, Java based BlackBerry devices can download a third-party application over the wireless network using the BlackBerry® Browser. You can also send third-party applications to BlackBerry devices over the wireless network, and install them on BlackBerry devices.

Malware

Malware, or malicious software, is a third-party application that a user with malicious intent creates to cause harm to or exploit computer systems.

Type of malware	Description
virus	<ul style="list-style-type: none">• replicates itself by attaching to legitimate applications on a computer• characterized by both its propagation, or the delivery method and action that it performs• might require a trigger to run
trojan horse	<ul style="list-style-type: none">• disguises or embeds itself within a seemingly innocuous or trusted application• depends on the action of the user to succeed, and requires successful use of social engineering rather than the ability to exploit flaws in the security design or configuration of the target
worm	<ul style="list-style-type: none">• replicates itself to spread across networks and potentially overwhelm computer systems• self-contained, and does not need to be a part of another application to spread itself
spyware	<ul style="list-style-type: none">• designed to log user activities and personal data• sends data to the user with malicious intent

The BlackBerry® Enterprise Solution focuses on containing malicious applications and is designed to help prevent malicious applications from causing damage after they appear on a computer system.

Preventing and detecting malware

On computers, malware prevention requires processes that both detect and contain malware attacks. Effective malware detection requires a comprehensive and frequently-updated local database or a constant connection to a similarly qualified online database. While computers might have access to these databases, current mobile devices do not have enough storage space for a malware database and cannot guarantee a constant connection to the Internet.

Using IT policy rules to contain malware on the BlackBerry device

The BlackBerry® Enterprise Server version 4.1 SP2 or later includes IT policy rules that are designed to permit the following actions:

- prevent BlackBerry devices from downloading third-party applications over the wireless network
- specify whether applications, including third-party applications, on the BlackBerry device can open specific types of connections

You cannot use an IT policy to permit users or prevent users from downloading specific applications on the BlackBerry device. You can do this using one or more application control policies.

Using application control policy rules to contain malware on the BlackBerry device

You can use application control policy rules to permit or prevent the installation of specific third-party applications on the BlackBerry® device and to limit the permissions of third-party applications. You can permit or prevent the following items:

- which items that third-party applications can access on the BlackBerry device (for example, messaging, phone, and BlackBerry device key store)
- which types of connections that a third-party application running on the BlackBerry device can establish (for example, local, internal, and external connections)

- whether an application can access the user authenticator framework API, which permits the registration of drivers to provide two-factor authentication to unlock the BlackBerry device

For example, to control connections to your organization's internal servers from third-party applications on the BlackBerry device, you can create an application control policy that prevents the application from making internal connections. When you assign the application control policy to a software configuration for a user account or one or more groups, users might not be able to use all the features of any third-party application that you assign the application control policy to. For example, applications might not be able to send and receive data from internal servers. When you specify application policy rules for groups, the BlackBerry® Enterprise Server limits permitted application behavior to a small subset of trusted users.

IT policy rule values override application control policy rule values. For example, if you change the value for the Allow Internal Connections IT policy rule (the default value is Yes) and you also configure an application control policy that permits a specific application to make internal connections, the IT policy rule value overrides the application control policy rule value and the application cannot make internal connections.

The BlackBerry device resets if the permissions for the application that you apply the application control policy to become more restrictive. BlackBerry devices that run BlackBerry® Device Software version 4.1 or later permit users to make application permissions more, but never less, restrictive than what you specify.

Using code signing to contain malware on the BlackBerry device

Research In Motion does not inspect or verify third-party applications that run on BlackBerry® devices. However, RIM controls the use of BlackBerry device APIs that include sensitive packages, classes, or methods to prevent unauthorized applications from accessing data on the BlackBerry device. Each third-party application requires authorization to run on the BlackBerry device.

Before you or a user can run a third-party application that uses the RIM controlled APIs on the BlackBerry device, the RIM signing authority system must use public key cryptography to authorize and authenticate the application code. The third-party application developer must visit www.blackberry.com/developers/downloads/jde/api.shtml to register with the RIM signing authority system for access to the controlled APIs and use the BlackBerry Signature Tool, which is a component of the BlackBerry® Java Development Environment, to request, receive, and verify a digital signature from RIM for the application.

Third party application developers who create controlled access third-party APIs can act as a signing authority for those APIs. The application developer can download and install the BlackBerry® Signing Authority Tool to permit other developers to register for access to the application developer's controlled APIs. Registered developers can use the BlackBerry Signature Tool to request, receive, and verify digital signatures from the application developer's BlackBerry Signing Authority Tool for their applications.

MIDlets (also known as applications that use standard MIDP and CLDC APIs only) cannot write to memory on a BlackBerry device, access the memory of other applications, or access the persistent data of other MIDlets unless they are digitally signed by RIM's signing authority system. For more information about code signing and third-party applications, see the *BlackBerry Signing Authority Tool Administrator Guide*.

Using code signing on BlackBerry MDS Runtime Applications

Developers in your organization can digitally sign BlackBerry® MDS Runtime Applications that they create using BlackBerry® MDS Studio, before the developers publish these applications to the BlackBerry MDS Application Repository. BlackBerry devices support using a private key with a corresponding certificate in X.509 syntax to digitally sign BlackBerry MDS Runtime Applications.

BlackBerry MDS Runtime Applications communicate with your organization's content and application servers through the BlackBerry MDS Integration Service. The BlackBerry MDS Integration Service verifies the digital signature on the BlackBerry MDS Runtime Application code before it sends the application to BlackBerry devices over the wireless network. When a BlackBerry device receives the BlackBerry MDS Runtime Application, it displays the certificate subject details as the code signer identity, and prompts the user to accept or reject the application.

The BlackBerry device does not display the code signer identity to the user, and does not install the application if any of the following conditions are true:

- the application is signed with an untrusted certificate
- the signature is invalid

- the value for the Allow Unsigned Applications option is False for the BlackBerry MDS Integration Service, and the application is not digitally signed

Protecting lost, stolen, or replaced BlackBerry devices

You can send IT administration commands over the wireless network to immediately protect confidential data on BlackBerry® devices.

IT administration command	Description
Set Password and Lock Handheld	This command creates a new password and locks a lost BlackBerry device remotely. You can communicate the new password to the user verbally when the user locates the BlackBerry device. When the user unlocks the BlackBerry device, the BlackBerry device prompts the user to accept or reject the new password.
Erase Data and Disable Handheld	This command remotely erases all user information and application data that the BlackBerry device stores. You can also configure the following options: <ul style="list-style-type: none">• configure a delay, in hours, before the BlackBerry device starts the process of deleting all its user information and application data if a BlackBerry device is lost and might be recovered by the user• require the BlackBerry device to return to factory default settings when it receives this command• specify whether to permit the user to stop the process of erasing data from and making the BlackBerry device unavailable during the delay period You can use this command to prepare a BlackBerry device for transfer between users in your organization.

For more information, see the *BlackBerry Enterprise Server Administration Guide*.

Related topics

Remotely erasing data from BlackBerry device memory and making the BlackBerry device unavailable

Remotely resetting the password of a BlackBerry device that is content protected

The remote password reset cryptographic protocol is designed to permit you to specify the BlackBerry® device password remotely, even if you or the user turns on content protection. The BlackBerry device does not prompt the user for the old BlackBerry device password.

The cryptographic protocol for resetting the password remotely on a BlackBerry device that is content protected is designed to provide the following features:

- permits the BlackBerry device to re-encrypt the content protection key with the new password, without knowing the old password
- prevents a hardware-based attack on the BlackBerry device from recovering the content protection key without knowing either the BlackBerry device password or the IT policy private key of the IT policy public and private key pair that the BlackBerry® Enterprise Server generates for the BlackBerry device
- prevents a small subgroup containment attack through the use of elliptic curve cryptography
- prevents the BlackBerry Enterprise Server from learning anything that an attacker could use to recover the content protection key

You should send the Set a Password and Lock Handheld IT administration command to a content-protected BlackBerry device that is in the possession of the BlackBerry device user only. If you send this command to a BlackBerry device in the possession of an attacker, an attacker that uses a hardware-based attack to recover the key pair that the BlackBerry device creates when it receives the IT policy from flash memory, and thereby decrypt all the data on the BlackBerry device.

Related topics

Protocol that you use to reset the password on a content-protected BlackBerry device from the BlackBerry Enterprise Server

Deleting all device data

When you or a user deletes all device data, the BlackBerry® device is designed to delete all data in internal memory and overwrite that memory with zeroes.

Method	Description
Deleting all device data using the default factory method	You can start this method of deleting BlackBerry device data remotely by using the Remote Wipe Reset to Factory Defaults IT policy rule.
security wipe of data (standard security wipe)	You can delete BlackBerry device data remotely, or a user can delete data locally on the BlackBerry device.
security wipe of data and third-party applications (standard security wipe with "Include third party applications" option selected on the BlackBerry device)	A user can remove BlackBerry device data locally on the BlackBerry device. You can achieve the same result by performing a factory default device wipe.
security wipe of data on a content-protected device (standard security wipe on a BlackBerry device that is content protected)	If you or a user turned on content protection, during a security wipe the BlackBerry device uses a memory scrub process to overwrite the flash memory file system of the BlackBerry device. The BlackBerry memory scrub process complies with United States government requirements for deleting sensitive user data, including <i>Department of Defense directive 5220.22-M</i> and <i>National Institute of Standards and Technology Special Publication 800-88</i> .

For more information, see *Erasing File Systems on BlackBerry Devices Technical Overview*.

Related topics

Removing third-party applications when a user starts a security wipe

Remotely erasing data from BlackBerry device memory and making the BlackBerry device unavailable

BlackBerry device actions when deleting all device data

The BlackBerry® device performs the following actions, depending on the method used to delete the internal device memory:

Action	Description
deletes user data	The BlackBerry device permanently deletes all user data in memory.
deletes your organization's PIN encryption key	The BlackBerry device permanently deletes its references to your organization's PIN encryption key in memory.
deletes the master encryption key of the BlackBerry device	The BlackBerry device permanently deletes its references to the master encryption key in memory.
unbinds the smart card (if applicable)	The BlackBerry device permanently deletes the smart card binding information from the NV store so that a user can authenticate with the BlackBerry device using a new smart card.
unbinds the IT policy	The BlackBerry device permanently deletes the IT policy public key from its NV store so that it can receive a new IT policy and IT policy public key from a BlackBerry® Enterprise Server.
deletes password history	The BlackBerry device permanently deletes its references to past BlackBerry device password hashes in memory.
deletes stored IT policy	The BlackBerry device permanently deletes its stored IT policy.
deletes third-party applications	The BlackBerry device permanently deletes all third-party applications stored on the BlackBerry device.

Action	Description
overwrites BlackBerry device memory if you or a BlackBerry device user turns on content protection	The BlackBerry device uses a memory scrub process to overwrite the file system of the BlackBerry device flash memory.

Process flow: Deleting all device data from the BlackBerry device

A BlackBerry® device process is designed to delete and overwrite the BlackBerry device memory.

1. The BlackBerry device specifies a Device Under Attack flag in the NV store.
If a user removes the battery or the battery power drops to zero before the BlackBerry device data wipe ends, when the user replaces the battery, the BlackBerry device wipe process continues because the Device Under Attack flag is still present.
2. If you or a user turned on content protection of master encryption keys, the BlackBerry device overwrites the copy of the grand master key in RAM with zeroes.
3. The BlackBerry device deletes its binding with the BlackBerry® Enterprise Server by deleting the IT policy public key from the NV store. This permits the BlackBerry device to bind to a new BlackBerry Enterprise Server.
The IT policy public key does not undergo memory scrubbing because it is not a protected or hidden value.
4. If applicable, the BlackBerry device deletes the smart card binding information from the NV store. This permits the BlackBerry device to bind to a new smart card.
5. The BlackBerry device wireless transceiver turns off.
6. The BlackBerry device deletes data in the persistent store in flash memory, including references to the master encryption key.
7. The BlackBerry device overwrites flash memory with zeroes.
8. The BlackBerry device memory scrub process overwrites the BlackBerry device heap in RAM, changing the state of each bit four times.
9. The BlackBerry device deletes the BlackBerry device password from the NV store.
10. The BlackBerry device formats the external memory file system if it exists on the BlackBerry device.
11. If you or a user turned on content protection, the BlackBerry device memory scrub process overwrites the file system of the BlackBerry device flash memory.
12. If you or a user turned on content protection, the BlackBerry device memory scrub process overwrites the external memory file system if it exists on the BlackBerry device.
13. The BlackBerry device deletes the Device Under Attack flag from the NV store.
14. The BlackBerry device restarts.

Related topics

Unbinding the smart card from the BlackBerry device

Process flow: Scrubbing the memory on BlackBerry devices

Memory scrub processes for flash memory on BlackBerry devices

Remotely erasing data from BlackBerry device memory and making the BlackBerry device unavailable

A BlackBerry® device that a user has not physically connected to a computer is designed to permanently delete its user and application data when any of the following events occur:

- The user clicks Wipe Handheld in the Security Options screen on the BlackBerry device.
- The user types the password incorrectly more times than the Set Maximum Password Attempts IT policy rule permits on the BlackBerry device. The default is ten tries.

- You send the Erase Data and Disable Handheld IT administration command to the BlackBerry device from the BlackBerry Administration Service.
- You send the Erase Data and Disable Handheld IT administration command with a delay (in hours, up to 168 hours) to the BlackBerry device from the BlackBerry Administration Service.

Removing third-party applications when a user starts a security wipe

When the user clicks Wipe Handheld in the Security Options screen on the BlackBerry® device, the user can select the Include third party applications option at the same time. If the user selects this option, when the BlackBerry device permanently deletes its stored user data during the device wipe, it will also remove all its third-party applications and application data.

Requiring a delay when deleting all user data on remote BlackBerry devices

You can configure the following IT policy rules to require that a BlackBerry® device automatically deletes its user and application data.

IT policy rule	Description
Secure Wipe Delay After IT Policy Received	Configure this IT policy rule to a period of time, in hours. If the BlackBerry device has not received IT policy updates or IT administration commands before this time expires, the BlackBerry device permanently deletes its user and application data.
Secure Wipe Delay After Lock	Configure this IT policy rule to a period of time, in hours. If the user has not unlocked the BlackBerry device before this time expires, the BlackBerry device permanently deletes its user and application data.
Secure Wipe if Low Battery	Configure this IT policy rule to require that, if the BlackBerry device battery power is insufficient to receive IT policy updates or IT administration commands, the BlackBerry device permanently deletes its user and application data.

Remotely resetting a BlackBerry device to factory default settings

You can use the Remote Wipe Reset to Factory Defaults IT policy rule to require the BlackBerry® device to return to factory default settings when it receives the Erase Data and Disable Handheld IT administration command over the wireless network. When you change the value for this rule to Yes and send the Erase Data and Disable Handheld IT administration command to the BlackBerry device from the BlackBerry Administration Service, the BlackBerry device returns to its factory default settings and permanently deletes all the following items:

- user data
- your organization's PIN encryption key
- master encryption key of the BlackBerry device
- smart card binding information
- password history
- record of time elapsed since the BlackBerry device was last turned on
- stored IT policy
- third-party applications and application data

When the BlackBerry device returns to its factory default settings, it overwrites BlackBerry device internal memory and, if you or a BlackBerry device user turns on content protection, performs a scrub of BlackBerry device memory.

Deleting data from BlackBerry device memory and making the BlackBerry device unavailable using the standard security wipe process

A BlackBerry® device that a user has not physically connected to a computer is designed to permanently delete its user and application data when any of the following events occur:

- The user clicks Wipe Handheld in the Security Options screen on the BlackBerry device.
- The user types the password incorrectly more times than the Set Maximum Password Attempts IT policy rule allows on the BlackBerry device. (The default is ten tries.)
- You send the Erase Data and Disable Handheld IT administration command to the BlackBerry device from the BlackBerry Administration Service.
- You send the Erase Data and Disable Handheld IT administration command with a delay (in hours, up to 168 hours) to the BlackBerry device from the BlackBerry Administration Service.

A BlackBerry device is designed to erase its user and application data and all applications when a user physically connects it to a computer and any of the following events occur:

- The user runs the application loader tool of the BlackBerry® Desktop Software and types the password incorrectly more times than the Set Maximum Password Attempts IT policy rule allows in the application loader tool prompt. (The default is ten tries.)

The user can also use the application loader tool of the BlackBerry Desktop Software to erase all user and application data on the BlackBerry device, but choose not to erase the BlackBerry device applications.

- You click Remove user data from current device in the BlackBerry Administration Service when the BlackBerry device is connected to the BlackBerry Administration Service. This option deletes all data and applications from the BlackBerry device even if service books do not exist on the BlackBerry device.

Removing third-party applications when a user starts a security wipe

When the user clicks Wipe Handheld in the Security Options on the BlackBerry® device, the user can select the Include third party applications option at the same time. If the user selects this option, when the BlackBerry device permanently deletes its stored user data during the BlackBerry device wipe, it will also remove all its third-party applications and application data.

Requiring a delay on remote BlackBerry device wipes

You can configure the following IT policy rules to require that the remote BlackBerry® device automatically delete its user and application data.

IT policy rule	Description
Secure Wipe Delay After IT Policy Received	Configure this IT policy rule to a period of time, in hours. If the BlackBerry device has not successfully received IT policy updates or IT administration commands before this time expires, the BlackBerry device permanently deletes its user and application data.
Secure Wipe Delay After Lock	Configure this IT policy rule to a period of time, in hours. The user has not unlocked the BlackBerry device before this time expires, the BlackBerry device permanently deletes its user and application data.
Secure Wipe if Low Battery	Configure this IT policy rule to require that, if the BlackBerry device battery power is insufficient to receive IT policy updates or IT administration commands, the BlackBerry device permanently deletes its user and application data.

Process flow: Scrubbing the memory on BlackBerry devices

To overwrite the BlackBerry® device heap in RAM by changing the state of each bit four times, the BlackBerry device memory scrub process performs the following actions:

1. Writes 0x33 to each byte (0011 0011₂).
2. Deletes all bytes to 0x00 (0000 0000₂).
3. Writes 0xCC to each byte (1100 1100₂).
4. Deletes all bytes to 0x00 (0000 0000₂).
5. Writes 0x55 to each byte (0101 0101₂).

6. Deletes all bytes to 0x00 (0000 0000₂).
7. Writes 0xAA to each byte (1010 1010₂).

Memory scrub processes for flash memory on BlackBerry devices

Process flow: Scrubbing the flash memory on BlackBerry devices that are running BlackBerry Device Software version 4.6 and later

If you or a user turned on content protection, during a BlackBerry® device wipe, the BlackBerry device runs the BlackBerry device memory scrub process. The memory scrub process overwrites the BlackBerry device NAND flash memory by writing a single character before it deletes the data.

1. The memory scrub process writes or programs 0x00 to each byte (0000 0000₂).
2. The memory scrub process deletes all blocks, changing all bytes to 0xFF (1111 1111₂).

Process flow: Scrubbing the flash memory on BlackBerry devices running BlackBerry Device Software versions earlier than 4.6

If you or a user turned on content protection, during a BlackBerry® device wipe, the BlackBerry device runs the BlackBerry device memory scrub process. The memory scrub process overwrites the BlackBerry device NOR flash memory by changing the state of each bit four times.

1. The memory scrub process writes 0x33 to each byte (0011 0011₂).
2. The memory scrub process deletes all bytes to 0xFF to each byte (1111 1111₂).
3. The memory scrub process writes 0xCC to each byte (0x1100 1100₂).
4. The memory scrub process deletes all bytes to 0xFF (1111 1111₂).
5. The memory scrub process writes 0x55 to each byte (0x0101 0101₂).
6. The memory scrub process deletes all bytes to 0xFF (1111 1111₂).
7. The memory scrub process writes 0xAA to each byte (0x1010 1010₂).
8. The memory scrub process deletes all bytes to 0xFF (1111 1111₂).

Process flow: Scrubbing the flash memory that stores user-saved files on BlackBerry devices

If you or a user turned on content protection, during a BlackBerry® device wipe, the BlackBerry device runs the BlackBerry device memory scrub process. If the BlackBerry device supports a partition of flash memory to store user-saved files using an internal memory card file system, the memory scrub process overwrites that section of the BlackBerry device memory by writing a single character before the memory scrub process deletes the data.

1. The memory scrub process writes or programs 0x55 to each byte (0101 0101₂).
2. The memory scrub process writes or programs 0xAA to each byte (1010 1010₂).
3. The memory scrub process deletes all blocks, changing all bytes to 0xFF (1111 1111₂) or 0x00 (0000 0000₂).

Unbinding the smart card from the BlackBerry device

When you or the user starts a BlackBerry® device wipe, which causes the BlackBerry device to erase its stored user and application data, the BlackBerry device permanently deletes the smart card binding information from the NV store so that a user can authenticate with the BlackBerry device using a new smart card.

You can delete the smart card binding information permanently from the BlackBerry device in the following ways.

- Send the Erase Data and Disable Handheld IT administration command to the BlackBerry device to delete the binding between a user's current smart card and the BlackBerry device permanently.
- When the user turns off two-factor authentication, the BlackBerry device turns off two-factor authentication with the installed smart card and deletes the smart card binding information from the BlackBerry device permanently.

RIM Cryptographic API

The RIM Cryptographic API on the BlackBerry® device and in the BlackBerry® Java® Development Environment consists of a Java interface and an encryption algorithm, a key agreement scheme, a signature scheme, a key generation protocol, message authentication, message digest, and a hash code.

Developers can use the Java interface of the BlackBerry JDE to access the RIM Cryptographic API encryption algorithms and other code to create solutions. Developers are not required to modify or directly access the encryption code because all calls to the native C++ encryption code are sent through the Java code.

RIM uses code signing to authorize running secure applications on the BlackBerry device and to control third-party application access to the RIM Cryptographic API.

Cryptographic features that the RIM Cryptographic API provides

The RIM Cryptographic API on the BlackBerry® device provides a toolkit of cryptographic algorithms and support tools.

Symmetric block algorithms

Algorithm (uses PKCS#5 for padding)	Key length (bits)	Modes (implemented separately from the block encryption algorithms)
AES	128, 192, and 256	ECB, CBC, CFB, OFB, X
DES	56	ECB, CBC, CFB, OFB, X
RC2	8 to 1024	ECB, CBC, CFB, OFB, X
RC5	0 to 2040	ECB, CBC, CFB, OFB, X
Skipjack	80	ECB, CBC, CFB, OFB, X
Triple DES	112 and 168	ECB, CBC, CFB, OFB, X
CAST5-128	128	ECB, CBC, CFB, OFB, X

Symmetric stream encryption algorithms

Algorithm	Key length (bits)
ARC4	Unlimited

Asymmetric stream encryption algorithms

Algorithm	Key length (bits)
ECIES	unlimited (160 to 571 for seeding)

Asymmetric encryption algorithms

Algorithm	Key length (bits)	Type
RSA raw	512 to 4096	integer factorization
RSA with PKCS #1 formatting (version 1.5 and 2.0)	512 to 4096	integer factorization
RSA with OAEP formatting	512 to 4096	integer factorization
El Gamal	512 to 4096	discrete logarithm

Key agreement scheme algorithms

Algorithm	Key length (bits)	Type
Diffie-Hellman	512 to 4096	discrete logarithm

Algorithm	Key length (bits)	Type
KEA	1024	discrete logarithm
ECDH	160 to 571	(EC) discrete logarithm
ECMQV	160 to 571	(EC) discrete logarithm

Signature scheme algorithms

Algorithm	Key length (bits)	Type
DSA	512 to 1024	discrete logarithm
RSA using PKCS #1 (version 1.5 and 2.0)	512 to 4096	integer factorization
RSA using ANSI X9.31 ANSI® X9.31 uses one of the following algorithms for the required message digest code: SHA-1, SHA-256, SHA-384 or SHA-512, or RIPEMD-160.	512 to 4096	integer factorization
RSA using PSS	512 to 4096	integer factorization
ECDSA	160 to 571	(EC) discrete logarithm
ECNR	160 to 571	(EC) discrete logarithm

Key generation algorithms

Algorithm	Key length (bits)	Type
RSA	512 to 2048	integer factorization
Diffie-Hellman	512 to 4096	discrete logarithm
DSA	512 to 1024	discrete logarithm
EC	160 to 571	(EC) discrete logarithm

Message authentication codes

Code	Key length (bits)
CBC MAC	variable (block cipher key length)
HMAC	variable

Message digest codes

Code	Digest length (bits)
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	160, 224, 256, 384, 512
MD2	128
MD4	128
MD5	128
RIPEMD-128, 160	128, 160

TLS and WTLS standards that the RIM Cryptographic API supports

The RIM Cryptographic API on the BlackBerry® device supports the TLS and WTLS protocol cipher suite components that apply to WTLS and handheld (direct) mode TLS/SSL only.

Key establishment algorithm cipher suites that the RIM Cryptographic API supports

Direct mode SSL	Direct mode TLS	WTLS
RSA_EXPORT	RSA_EXPORT	RSA_anon
DH_anon_EXPORT	DH_anon_EXPORT	RSA_anon_512
DHE_DSS_EXPORT	DHE_DSS_EXPORT	RSA_anon_768
RSA	RSA	RSA
DHE_DSS	DHE_DSS	RSA_512
DH_anon	DH_anon	RSA_768
		DH_anon
		DH_anon_512
		DH_anon_768

Symmetric algorithms that the RIM Cryptographic API supports

Direct mode SSL	Direct mode TLS	WTLS
RC4 40	RC4 40	RC5 40
DES 40	RC4 56	RC5 56
DES	RC4 128	RC5 64
Triple DES	DES 40	RC5
RC4 128	DES	RC5 128
	Triple DES	DES 40
	AES 128	DES
	AES 256	Triple DES
	RC4 128	

Hash algorithms that the RIM Cryptographic API supports

Direct mode SSL	Direct mode TLS	WTLS
MD5	MD5	SHA
SHA-1	SHA-1	SHA-40
		SHA-80
		MD5
		MD5 40
		MD5 80

Limitations of RIM Cryptographic API support for key establishment algorithm cipher suites

The RIM Cryptographic API implementation of the TLS and WTLS protocols supports the use of RSA® and DSA public key algorithms and the Diffie-Hellman key exchange algorithm, with the following limitations:

Cipher suite type	Typical component limitation (in bits)
export	<ul style="list-style-type: none"> RSA and Diffie-Hellman: 1024 bytes or less

	<ul style="list-style-type: none">• EC: 163 bytes or less
non export (limitations due to computational constraints on the BlackBerry® device)	<ul style="list-style-type: none">• non elliptic curve operations: 4096 bytes• elliptic curve operations: 571 bytes

Power and electromagnetic side-channel attacks and countermeasures

The BlackBerry® device implementation of AES is designed to protect user data and encryption keys from traditional and side-channel attacks.

Attack type	Description
Traditional	<ul style="list-style-type: none">attacks data that the cryptographic system stores or transmitstries to determine the user's encryption key or the plain text data by exploiting a weakness in the design of the cryptographic algorithm or protocol
side-channel	<ul style="list-style-type: none">tries to exploit physical properties of the algorithm implementation using power analysis (for example, SPA and DPA) and electromagnetic analysis (for example, SEMA and DEMA)tries to determine the encryption keys that a device uses by measuring and analyzing the power consumption, or electromagnetic radiation that the device emits during cryptographic operations

The BlackBerry device uses a masking operation, table splitting, and an application of random masks to help protect the cryptographic keys and plain text data against side-channel attacks at all points during the BlackBerry device encryption and decryption operations.

Process flow: Running the masking operation during the initial AES algorithm calculation when content protection is turned on

During the initial AES algorithm calculation, if you or a user turned on content protection, the following actions occur:

1. The BlackBerry® device completes the masking operation by performing the following actions:
 - creating a mask table (M), where each table entry is a random value
 - creating a masked version of the S-Box table (S') used within AES
 - periodically and randomly permuting all table entries
2. The BlackBerry device runs the input through both M and S'.
3. The BlackBerry device combines the output from M and S'.
4. The BlackBerry device deletes the mask and produces the AES output.

Process flow: Running the masking operation during subsequent AES algorithm calculations when content protection is turned on

1. The BlackBerry® device performs the masking operation by periodically and randomly permuting all table entries in every calculation.
2. The BlackBerry device runs the input through both M and S'.
3. The BlackBerry device combines the output from M and S'.
4. The BlackBerry device deletes the mask and produces the AES output.

Process flow: Running the masking operation uses when content protection is turned off

The AES algorithm calculation that BlackBerry® devices use when content protection is turned off consists of the following stages:

1. The BlackBerry device masks the output from the round key.

2. The BlackBerry device masks the AES S-Box input.
3. The BlackBerry device masks the AES S-Box output.

How the AES algorithm creates S-Box tables and uses round keys and masks

The BlackBerry® device permutes each AES S-Box entry randomly and masks each entry with a random value.

The BlackBerry device masks the round keys (subkeys that the key schedule calculates for each round of encryption) with random values and any S-Box masks that the AES algorithm requires to work.

The BlackBerry device changes the random masks periodically and uses extra S-Box data to make identification of the S-Box table difficult, whether the BlackBerry device uses the S-Box table in the encryption, decryption, or key schedule process.

BlackBerry Router protocol

When the BlackBerry® Enterprise Server and BlackBerry device use the BlackBerry Router protocol to open a connection between each other, the BlackBerry Router protocol is designed to use its unique authentication protocol to verify that the BlackBerry device has the correct master encryption key while preventing the BlackBerry Router from knowing the value of the master encryption key. To accomplish this, the BlackBerry Router protocol uses two runs of the elliptic curve version of the Schnorr identification scheme to provide mutual authentication between the BlackBerry device and the BlackBerry Enterprise Server.

The BlackBerry Enterprise Server and BlackBerry Router also use the BlackBerry Router protocol to close an authenticated connection to the BlackBerry device. The BlackBerry Router protocol is designed to permit only an authenticated party to close the connection by using one run of the Schnorr identification scheme to authenticate the close command that the BlackBerry Enterprise Server sends to the BlackBerry Router.

The BlackBerry Router, BlackBerry Enterprise Server, and BlackBerry device are designed to share the following cryptosystem parameters when using the BlackBerry Router protocol:

Parameter	Description
$E(Fq)$	the NIST-approved 521-bit random elliptic curve over Fq , which has a cofactor of 1; the BlackBerry Router authentication protocol does all math operations in the group $E(Fq)$ and Z_p
Fq	a finite field of prime order q
P	a point of E that generates a prime subgroup of $E(Fq)$ of order p
xR	a representation of elliptic curve scalar multiplication, where x is the scalar and R is a point on $E(Fq)$
s	the master encryption key value
h	the SHA-512 hash of s

How the BlackBerry Router protocol uses the Schnorr identification scheme

The implementation of the Schnorr identification scheme in the BlackBerry® Router protocol uses a group of large prime order, the additive group of elliptic curve points for a prime p .

The BlackBerry Router protocol is designed to use the perform the following security actions:

- use the NIST recommended 521 bit elliptic curve group
- verify that points supplied by the parties involved in the communication are members of the Elliptic Curve group
- verify that R_D does not equal R_B , to prevent recovery of h by an attacker
- verify that e does not equal 0, to prevent recovery of h by an attacker
- verify that R does not equal the point at infinity, to verify that R is a valid public key
- verify that R does not equal the point at infinity, to verify that R is a valid public key
- reset any malformed data that it finds to a random value so that the protocol can proceed past the point that it detects malformed data at, which permits the protocol to fail at completion only; this measure is designed to prevent various types of timing attacks

Examples of attacks that the BlackBerry Router protocol is designed to prevent

Impersonating a BlackBerry device

An impersonation of the BlackBerry® device occurs when a user with malicious intent sends messages to the BlackBerry® Enterprise Server so that the BlackBerry Enterprise Server believes it is communicating with the BlackBerry device. The user with malicious intent must send the master encryption key value (s) to the BlackBerry Enterprise Server, which requires the user to solve the discrete log problem to determine s or the hash of s .

Impersonating a BlackBerry Enterprise Server

An impersonation of the BlackBerry® Enterprise Server occurs when a user with malicious intent sends messages to the BlackBerry device so that the BlackBerry device believes it is communicating with the BlackBerry Enterprise Server. The user with malicious intent must send the master encryption key value (s) to the BlackBerry device, which requires the user to solve the discrete log problem to determine s or the hash of s .

Process flow: Using the BlackBerry Router protocol to open an authenticated connection

1. The BlackBerry device® and BlackBerry® Enterprise Server both hash the current master encryption key using SHA-512.
2. The BlackBerry device selects a random value r_D , where $1 < r_D < p - 1$ and calculates $R_D = r_D P$.
3. The BlackBerry device sends R_D and a master encryption key identifier (*KeyID*), to the BlackBerry Enterprise Server.
4. The BlackBerry Router observes the data that the BlackBerry device sends and confirms that the value R_D is not the point at infinity. If R_D is the point at infinity, the BlackBerry Router configures R_D to a random value.
5. The BlackBerry Router forwards R_D and *KeyID* to the BlackBerry Enterprise Server.
6. The BlackBerry Enterprise Server calculates that as R_D approaches the point at infinity, R_D is random.
7. The BlackBerry Enterprise Server selects a random value r_B , where $1 < r_B < p - 1$ and calculates $R_B = r_B P$.
If R_D equals R_B , the BlackBerry Enterprise Server calculates another value of R_B .
8. The BlackBerry Enterprise Server selects a random value e_D , where $1 < e_D < p - 1$.
9. The BlackBerry Enterprise Server sends R_B , e_D , and *KeyID* to the BlackBerry device.
10. The BlackBerry Router observes the data that the BlackBerry Enterprise Server sends and confirms the following calculations:
 - The BlackBerry Router checks that when the value R_B approaches the point at infinity or R_D equals R_B , the value R_B is random.
 - The BlackBerry Router checks that when the value e_D equals 0, the value e_D is random.
11. The BlackBerry Router forwards R_B , e_D , and *KeyID* to the BlackBerry device.
12. The BlackBerry device performs the following calculations:
 - The BlackBerry device checks that when the value R_B approaches the point at infinity or R_D equals R_B , the value R_B is random.
 - The BlackBerry checks that when the value e_D equals 0, the value e_D is random.
 - The BlackBerry computes $y_D = h - e_D r_D \text{ mod } p$.
13. The BlackBerry device selects a random value e_B , where $1 < e_B < p - 1$.
14. The BlackBerry device sends y_D and e_B to the BlackBerry Enterprise Server.
15. The BlackBerry Router observes the data that the BlackBerry device sends and confirms that if e_B equals 0 or e_B equals e_D , the value e_B is random.
16. The BlackBerry Router forwards y_D and e_B to the BlackBerry Enterprise Server.
17. The BlackBerry Enterprise Server performs the following calculations:
 - The BlackBerry Enterprise Server checks that when the value e_D equals e_B , the value e_B is random.
 - The BlackBerry Enterprise Server checks that when the value e_D equals 0, the value e_D is random.
 - The BlackBerry Enterprise Server computes $y_B = h - e_B r_B \text{ (mod } p)$.
18. The BlackBerry Enterprise Server sends y_B to the BlackBerry device.
19. The BlackBerry device receives y_B .

If the BlackBerry device accepts y_B , the BlackBerry Enterprise Server and BlackBerry device open an authenticated connection between each other.

If the BlackBerry device calculates that $y_B P + e_B R_B \neq hP$, the BlackBerry device rejects the connection attempt. The BlackBerry Enterprise Server and BlackBerry device do not open an authenticated connection between each other.

If the BlackBerry Router calculates that $y_B P + e_B R_B \neq y_D P + e_D R_D$, the BlackBerry Router rejects the connection attempt.

If the BlackBerry Enterprise Server calculates that $y_D P + e_D R_D \neq hP$, the BlackBerry Enterprise Server rejects the connection attempt.

20. The BlackBerry Router stores $R_D, R_B, y_D P + e_D R_D, e_D$, and e_B .
21. The BlackBerry Enterprise Server stores R_D, R_B, e_D, e_B , and h .
22. The BlackBerry Router overwrites y_B and y_D in memory with zeroes.
23. The BlackBerry Enterprise Server overwrites y_B, y_D , and r_B in memory with zeroes.
24. The BlackBerry device overwrites y_B, y_D , and r_D in memory with zeroes.

Process flow: Using the BlackBerry Router protocol to close an authenticated connection

1. The BlackBerry® Enterprise Server selects a random value r_C where $1 < r_C < p - 1$.
2. The BlackBerry Enterprise Server calculates $R_C = r_C P$.
If R_C equals R_B or R_C equals R_D the BlackBerry Enterprise Server calculates another R_C value.
3. The BlackBerry Enterprise Server sends the value R_C to the BlackBerry Router to begin connection closure.
4. The BlackBerry Router performs the following calculations:
 - The BlackBerry Router checks that when the value R_C approaches the point at infinity, the value R_C is random.
 - The BlackBerry Router checks that when the value R_C equals R_B or R_C equals R_D , the value R_C is random.
5. The BlackBerry Router selects a random value e_C where $1 < e_C < p - 1$.
If e_C equals e_D or e_C equals e_B the BlackBerry Router calculates another e_C value.
6. The BlackBerry Router sends the value e_C to the BlackBerry Enterprise Server.
7. The BlackBerry Enterprise Server performs the following calculations:
 - The BlackBerry Enterprise Server checks that when the value e_C equals 0, the value e_C is random.
 - The BlackBerry Enterprise Server checks that when the value e_C equals e_B or e_C equals e_D , the value e_C is random.
8. The BlackBerry Enterprise Server calculates $y_C = h - e_C r_C \text{ mod } p$.
9. The BlackBerry Enterprise Server sends the value y_C to the BlackBerry Router.

If the BlackBerry Router accepts y_C , the BlackBerry Router closes the authenticated connection to the BlackBerry device for the BlackBerry Enterprise Server.

If the BlackBerry Router calculates that $y_C P + e_C R_C \neq y_D P + e_D R_D$, the BlackBerry Router rejects the connection close attempt. The BlackBerry Router does not close the authenticated connection to the BlackBerry device.

Algorithm suites that the BlackBerry device supports for negotiating SSL connections

Wi-Fi® enabled BlackBerry® devices support the following direct mode TLS algorithm suites for negotiating SSL connections to the BlackBerry® Infrastructure:

- DH_anon_WITH_3DES_EDE_CBC_SHA
- DH_anon_WITH_AES_128_CBC_SHA
- DH_anon_WITH_AES_256_CBC_SHA
- DH_anon_WITH_DES_CBC_SHA
- DH_anon_WITH_RC4_128_MD5
- DH_anon_EXPORT_WITH_DES40_CBC_SHA
- DH_anon_EXPORT_WITH_RC4_40_MD5
- DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- DHE_DSS_WITH_3DES_EDE_CBC_SHA
- DHE_DSS_WITH_AES_128_CBC_SHA
- DHE_DSS_WITH_AES_256_CBC_SHA
- DHE_DSS_WITH_DES_CBC_SHA
- DHE_RSA_WITH_AES_128_CBC_SHA
- DHE_RSA_WITH_AES_256_CBC_SHA
- DHE_RSA_WITH_3DES_EDE_CBC_SHA
- DHE_RSA_WITH_DES_CBC_SHA
- RSA_EXPORT_WITH_RC4_40_MD5
- RSA_EXPORT_WITH_DES40_CBC_SHA
- RSA_WITH_DES_CBC_SHA
- RSA_WITH_RC4_128_SHA
- RSA_WITH_RC4_128_MD5
- RSA_WITH_3DES_EDE_CBC_SHA
- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_AES_256_CBC_SHA
- TLS

Protocol that you use to reset the password on a content-protected BlackBerry device from the BlackBerry Enterprise Server

If you or a user turn on content protection for a BlackBerry® device, you can reset the BlackBerry device password from the BlackBerry® Enterprise Server. To reset the password, the BlackBerry Enterprise Server uses elliptic curve cryptography to generate an encryption key. The BlackBerry Enterprise Server uses the encryption key and the new BlackBerry device password (which is also encrypted) to encrypt the content protection key. The BlackBerry Enterprise Server generates the encryption key from the NIST recommended 521 bit elliptic curve over a prime field and from the IT policy public key for the BlackBerry device.

The BlackBerry Enterprise Server sends the data required to reconstruct the encryption key to the BlackBerry device. The process is designed so that the BlackBerry Enterprise Server cannot reconstruct the encryption key at a later time.

Cryptosystem parameters

The BlackBerry® Enterprise Server and BlackBerry device are designed to share the following cryptosystem parameters when they use the protocol for resetting the password on a content-protected BlackBerry device remotely.

Parameter	Description
$E(F_q)$	the NIST-approved 521-bit random elliptic curve over F_q , which has a cofactor of 1
F_q	a finite field of prime order q
P	a point of E that generates a prime subgroup of $E(F_q)$ of order p
$B = bP$	the long-term IT policy public and private key pair that the BlackBerry Enterprise Server generates for the BlackBerry device; the BlackBerry Enterprise Server stores b in the BlackBerry Configuration Database, and sends B to the BlackBerry device in the IT policy
$D = dP$	the key pair that the BlackBerry device creates when it receives B ; the BlackBerry device stores D but deletes d to prevent a hardware-based attack from recovering d and B , and then calculating $K = dB$
$K = dB$	the encryption key that the BlackBerry device uses to encrypt the content protection key
r	a short term random number that the BlackBerry device stores in RAM
$D' = rD$	a blinded version of D
$K' = bD' = brD = rK$	a blinded version of K

Uppercase letters represent elliptic curve points. Lowercase letters represent scalars. The elliptic curve group operations are additive.

Process flow: Sending the Set a Password and Lock Handheld IT administration commands

When you send the Set a Password and Lock Handheld IT administration commands to a BlackBerry® device that you or a user turned on content protection for, the following actions occur:

1. You type the new BlackBerry device password in the BlackBerry Administration Service.
2. The BlackBerry® Enterprise Server sends the Set a Password and Lock Handheld IT administration command and the new BlackBerry device password to the BlackBerry device.
3. The BlackBerry device performs the following actions:
 - selects r randomly
 - stores r in RAM
 - calculates $D' = rD = rdP$
 - calculates $h = \text{SHA-1}(B)$
4. The BlackBerry device sends D' and h to the BlackBerry Enterprise Server.
5. The BlackBerry Enterprise Server receives D' and h , and performs the following actions:
 - uses h to determine which B the BlackBerry device used, and hence which b to use
 - verifies that D' is a valid public key
 - calculates $K' = bD' = brdP = rdB = rK$ (the BlackBerry Enterprise Server knows only rK , and cannot calculate K without r .)
 - calculates $h = \text{SHA-1}(D')$
6. The BlackBerry Enterprise Server sends the new BlackBerry device password, K' and h to the BlackBerry device.
7. The BlackBerry device receives the new BlackBerry device password, K' and h , and performs the following actions:
 - uses h to verify that K' is associated with D' and r
 - verifies K' is a valid public key
 - calculates $r^{-1}K' = r^{-1}rK = K$
 - permanently deletes r
 - uses K to decrypt the content protection key
 - permanently deletes K
8. The BlackBerry device performs the following actions:
 - selects d randomly
 - calculates $D = dP$
 - store D in flash memory
 - calculates $K = dB$.
9. The BlackBerry device uses K to encrypt the new BlackBerry device password.
10. The BlackBerry device uses the encrypted new password to encrypt the content protection key.

Related resources

Resource	Information
<i>BlackBerry Enterprise Server Feature and Technical Overview</i>	<ul style="list-style-type: none"> • BlackBerry® Enterprise Server architecture
<i>BlackBerry Enterprise Server Installation Guide</i>	<ul style="list-style-type: none"> • network environment settings • messaging environment settings • database environment settings
<i>BlackBerry Enterprise Server Administration Guide</i>	<ul style="list-style-type: none"> • generating and changing master encryption keys of BlackBerry devices • enabling encryption • managing security
<i>BlackBerry Signing Authority Tool Administrator Guide</i>	<ul style="list-style-type: none"> • the BlackBerry® Signing Authority Tool implementation of public key cryptography • installing, configuring, and managing the BlackBerry Signing Authority Tool • restricting access to APIs
<i>BlackBerry Java Development Environment Fundamentals Guide</i>	<ul style="list-style-type: none"> • BlackBerry APIs in the BlackBerry® JDE • APIs, classes, and methods with limited access • retrieving custom IT policy rules from the IT policy API • installing applications using the BlackBerry® Desktop Software • publishing applications over the wireless network
<i>BlackBerry Java Development Environment Development Guide</i>	<ul style="list-style-type: none"> • using controlled APIs • code signatures
<i>BlackBerry Smart Card Reader Security Technical Overview</i>	<ul style="list-style-type: none"> • secure pairing between the BlackBerry device and the BlackBerry® Smart Card Reader • initial key establishment protocol • connection key establishment protocol
<i>BlackBerry Wireless Enterprise Activation Technical Overview</i>	<ul style="list-style-type: none"> • wireless activation process • wireless master encryption key generation • initial key establishment protocol • key rollover protocol
<i>Enforcing Encryption of Internal and External File Systems on BlackBerry Devices Technical Overview</i>	<ul style="list-style-type: none"> • list of data items that BlackBerry devices encrypt by default • using encryption to protect stored files in internal and external memory on BlackBerry devices
<i>Erasing File Systems on BlackBerry Devices Technical Overview</i>	<ul style="list-style-type: none"> • list of data items that is deleted from BlackBerry device memory during BlackBerry device wipes • performing different types of remote BlackBerry device wipes

Resource	Information
<i>Garbage Collection in the BlackBerry Java Development Environment</i>	<ul style="list-style-type: none"> • cleaning the BlackBerry device memory
<i>BlackBerry Enterprise Server Policy Reference Guide</i>	<ul style="list-style-type: none"> • list of BlackBerry Enterprise Server IT policy rules and application control policy rules • using IT policies and application control policies
<i>PGP Support Package for BlackBerry devices Security Technical Overview</i>	<ul style="list-style-type: none"> • PGP® security and encryption • using PGP® Universal Server to store and manage PGP keys • searching for and validating PGP keys • sending and receiving PGP messages
<i>PGP Support Package User Guide Supplement</i>	<ul style="list-style-type: none"> • installing the PGP® Support Package for BlackBerry® smartphones • managing PGP keys on the BlackBerry device • specifying PGP options for digitally signing and encrypting messages
<i>Protecting the BlackBerry Device Platform Against Malware</i>	<ul style="list-style-type: none"> • understanding the BlackBerry device application platform default behavior • understanding malware vulnerabilities on the BlackBerry device • managing the risk of malware attacks • using BlackBerry® Enterprise Solution tools to contain malware on the BlackBerry device
<i>S/MIME Support Package for BlackBerry devices Technical Overview</i>	<ul style="list-style-type: none"> • S/MIME security and encryption • managing S/MIME certificates on the BlackBerry device and computer
<i>S/MIME Support Package User Guide Supplement</i>	<ul style="list-style-type: none"> • installing the S/MIME Support Package for BlackBerry® smartphones • managing certificates on the BlackBerry device and computer • specifying S/MIME options for digitally signing and encrypting messages • sending and receiving S/MIME messages
<i>Security for BlackBerry Devices with Bluetooth Wireless Technology</i>	<ul style="list-style-type: none"> • Bluetooth® wireless technology overview • using and protecting Bluetooth enabled BlackBerry devices • risks of using Bluetooth wireless technology on mobile devices
www.blackberry.com/security	<ul style="list-style-type: none"> • information about BlackBerry Enterprise Solution security

Glossary

3GPP

Third Generation Partnership Project

ACL

An access control list (ACL) is a list of permissions that are associated with an object, such as a file, directory, or other network resource. It specifies which users or components have permission to perform specific operations on an object.

AES

Advanced Encryption Standard

AES-CCMP

Advanced Encryption Standard Counter Mode CBCMAC Protocol

API

application programming interface

ARC4

Alleged Rivest Cipher 4

ASCII

American Standard Code for Information Interchange

BlackBerry MDS

BlackBerry® Mobile Data System

BlackBerry MVS

BlackBerry® Mobile Voice System

CAC

Common Access Card

CAST

Carlisle Adams - Stafford Tavares

CBC

cipher block chaining

CBC MAC

cipher block chaining message authentication code

CCKM

Cisco® Centralized Key Management

CFB

cipher feedback

CHAP

Challenge Handshake Authentication Protocol

CLDC

Connected Limited Device Configuration

CRL

certificate revocation list

DEMA

Differential Electro-Magnetic Analysis

DoS

denial of service

DPA

Differential Power Analysis

DSA PRNG

Digital Signature Algorithm pseudo-random number generator

DSS

Digital Signature Standard

EAP

Extensible Authentication Protocol

EAPPoL

Extensible Authentication Protocol over LAN

EAP-FAST

Extensible Authentication Protocol Flexible Authentication via Secure Tunneling

EAP-GTC

Extensible Authentication Protocol Generic Token Card

EAP-MS-CHAPv2

Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2

EAP-SIM

Extensible Authentication Protocol Subscriber Identity Module

EAP-TLS

Extensible Authentication Protocol Transport Layer Security

EAP-TTLS

Extensible Authentication Protocol Tunneled Transport Layer Security

ECB

electronic codebook

ECC

Elliptic Curve Cryptography

ECDH

Elliptic Curve Diffie-Hellman

ECDSA

Elliptic Curve Digital Signature Algorithm

ECIES

Elliptic Curve Integrated Encryption Standard

ECMQV

Elliptic Curve Menezes-Qu-Vanstone

ECNR

Elliptic Curve Nyberg Rueppel

EFS

Encrypting File System

FAT

File Allocation Table

FIPS

Federal Information Processing Standards

GAN

generic access network

GANC

generic access network controller

GPS

Global Positioning System

HMAC

keyed-hash message authentication code

HTTP

Hypertext Transfer Protocol

HTTPS

Hypertext Transfer Protocol over Secure Sockets Layer

IEEE

Institute of Electrical and Electronics Engineers

IMSI

International Mobile Subscriber Identity

JSSE

Java Secure Socket Extension

KEA

Key Exchange Algorithm

LAN

local area network

LDAP

Lightweight Directory Access Protocol

LDAPS

Lightweight Directory Access Protocol over Secure Sockets Layer

LEAP

Lightweight Extensible Authentication Protocol

MAC

message authentication code

MAPI

Messaging Application Programming Interface

MD5

Message-Digest Algorithm, version 5

messaging server

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

MIC

Message Integrity Check

MIDP

Mobile Information Device Profile

MMS

Multimedia Messaging Service

MSCAPI

Microsoft® Cryptographic Application Programming Interface

MS-CHAPv2

Microsoft Challenge Handshake Authentication Protocol version 2

NIST

National Institute of Standards and Technology

NTFS

New Technology File System

NV

nonvolatile

OAEP

Optimal Asymmetric Encryption Padding

OCSP

Online Certificate Status Protocol

OFB

output feedback

PAC

Protected Access Credential

PEAP

Protected Extensible Authentication Protocol

PGP/MIME

PGP® Multipurpose Internet Mail Extensions

PIN

personal identification number

PKCS

Public-Key Cryptography Standards

PKI

Public Key Infrastructure

PMK

pairwise master key

PSK

pre-shared key

PSS

Probabilistic Signature Scheme

RADIUS

Remote Authentication Dial In User Service

RC2

Rivest's Cipher, version 2

RC5

Rivest's Cipher, version 5

RFC

Request for Comments

RIPMD

RACE (Research and Development in Advanced Communications Technologies in Europe) Integrity Primitives Evaluation Message Digest 160

RPC

remote procedure call

RSA

Rivest Shamir Adleman

S/MIME

Secure Multipurpose Internet Mail Extensions

SEMA

Simple Electro-Magnetic Analysis

SHA

Secure Hash Algorithm

SIM

Subscriber Identity Module

SMS

Short Message Service

SMTP

Simple Mail Transfer Protocol

SPA

Simple Power Analysis

SPEKE

Simple Password-authenticated Exponential Key Exchange

SQL

Structured Query Language

SRP

Server Routing Protocol

SSL

Secure Sockets Layer

TCP

Transmission Control Protocol

TKIP

Temporal Key Integrity Protocol

TLS

Transport Layer Security

Triple DES

Triple Data Encryption Standard

UDP

User Datagram Protocol

UID

unique identifier

UMA

Unlicensed Mobile Access

VPN

virtual private network

WAP

Wireless Application Protocol

WEP

Wired Equivalent Privacy

WLAN

wireless local area network

WPA

Wi-Fi Protected Access

WTLS

Wireless Transport Layer Security

Provide feedback

To provide feedback on this deliverable, visit www.blackberry.com/docsfeedback.

Legal notice

Document ID: 23391575 version 3

©2009 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType® and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used as trademarks in the U.S., Canada, and countries around the world.

Bluetooth is a trademark of Bluetooth SIG. Cisco is a trademark of Cisco Systems, Inc. Entrust Authority is a trademark of Entrust, Inc. IBM, Domino, Lotus, and Lotus Notes are trademarks of IBM Corporation. IEEE is a trademark of the Institute of Electrical and Electronics Engineers, Inc. Microsoft, PowerPoint, SQL Server, Outlook, and Windows are trademarks of Microsoft Corporation. Netscape is a trademark of Netscape Communication Corporation. Novell and GroupWise are trademarks of Novell, Inc. PGP is a trademark of PGP Corporation. Qualcomm is a trademark of Qualcomm Incorporated. RSA, RSA Security, and SecurID are trademarks of RSA Security. Sun and Java are trademarks of Sun Microsystems, Inc. VeriSign is a trademark of VeriSign, Inc. Wi-Fi, Wi-Fi Protected Access, WPA, and WPA2 are trademarks of the Wi-Fi Alliance. All other trademarks are the properties of their respective owners.

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

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

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

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

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

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

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

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

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a

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

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

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

Research In Motion Limited

295 Phillip Street

Waterloo, ON N2L 3W8

Canada

Research In Motion UK Limited

200 Bath Road

Slough, Berkshire SL1 3XE

United Kingdom

Published in Canada