



BlackBerry Security

White Paper

Release 4.0

Contents

Wireless security.....	1
Confidentiality.....	1
Integrity and authenticity.....	1
BlackBerry security.....	1
Messaging Server.....	2
Microsoft Exchange Server.....	2
IBM Lotus Domino Server.....	3
Novell GroupWise Server.....	3
BlackBerry Enterprise Server.....	3
Corporate firewall or proxy.....	5
BlackBerry Router authentication protocol.....	5
Server Routing Protocol authentication.....	6
BlackBerry Mobile Data Service.....	7
IT policies and IT commands.....	8
BlackBerry device.....	9
Java-based BlackBerry devices.....	10
Bluetooth support on BlackBerry devices.....	10
Content protection.....	11
Application control.....	13
Deleting BlackBerry device data.....	13
Password keeper.....	14
BlackBerry wireless messaging.....	14
Wireless enterprise activation.....	14
Sending an email message from the BlackBerry device.....	15
Receiving an email message on the BlackBerry device.....	16
PIN and SMS messaging.....	16
BlackBerry encryption.....	17
Advanced Encryption Standard.....	17
Triple-DES Encryption Standard.....	18
BlackBerry compatibility.....	18
Running the downgrade utility.....	18
Triple-DES IT policy.....	19
Key-under-key encryption.....	19

Master encryption keys.....	19
Message keys.....	22
BlackBerry with the S/MIME Support Package	22
Private and public keys.....	22
Certificates and certificate authorities.....	23
Public Key Infrastructure compatibility.....	23
Related resources.....	24
Appendix A: Cryptographic Application Programming Interface.....	25
Cryptographic functionality provided by the API.....	25
Appendix B: Supported standards.....	28
Key establishment algorithms.....	28
Symmetric ciphers	29
Hash algorithms	29
Appendix C: Memory scrubbing.....	30
Memory scrub process	30

This document explores the security features of the BlackBerry® Enterprise Solution™ and provides an overview of the BlackBerry® security architecture.

Wireless security

Many companies are realizing significant return on investments and productivity gains by extending their enterprise information to mobile employees. With increased demand for mobile content and the threat of information theft, companies have security at the top of their list when evaluating wireless solutions. Without an effective security model, sensitive corporate data could be exposed with financial and legal implications.

A wireless data solution is considered to be effectively "secure" if it encompasses the following cryptographic concepts:

Confidentiality

A message is considered confidential if only the intended recipient can view the contents of a message. Confidentiality is typically achieved using encryption, which is the scrambling of data based on a key. An encryption algorithm is designed so that only the parties that know the secret key can decrypt the encrypted data or cipher text.

The BlackBerry Enterprise Solution uses a symmetric key algorithm, which is designed to provide strong security and complete confidentiality of sensitive user information. BlackBerry devices are designed to compress and encrypt the message using a key that is unique to that device. When receiving a message from the BlackBerry device, the BlackBerry Enterprise Server™ is designed to decompress and decrypt the message using the device's unique key. The BlackBerry Enterprise Server and the BlackBerry device should be the only parties that know the value of the master encryption key.

Integrity and authenticity

Integrity enables a recipient to detect if a message has been tampered with in transit. Authenticity allows the recipient to identify the sender and trust that the sender actually did send the message.

The BlackBerry Enterprise Solution relies on its encryption mechanism to provide integrity and authenticity based on a known message format. The decrypted and decompressed message must conform to a known message format. If it does not conform, the recipient knows that the message has been altered in transit because only the BlackBerry Enterprise Server and the BlackBerry device know the value of the symmetric encryption key. The BlackBerry device is designed to automatically reject any messages that do not produce the known message format upon decryption.

BlackBerry security

The BlackBerry Enterprise Solution™ (consisting of a BlackBerry device, BlackBerry Handheld Software, and the BlackBerry Enterprise Server software) is designed so that users can send and receive email and access corporate data wirelessly, while seamlessly protecting data against attack. The BlackBerry Enterprise Solution uses Advanced Encryption Standard (AES) or Triple Data Encryption Standard (Triple-DES) encryption methods to encrypt data in transit. The BlackBerry Enterprise Solution is designed so that data remains encrypted during transit and is not decrypted between the BlackBerry Enterprise Server and the BlackBerry device. See "BlackBerry encryption" on page 17 for more information.

The BlackBerry Enterprise Solution was created with corporate data security in mind. By encrypting data using a strong encryption algorithm and verifying that data remains encrypted in transit between the BlackBerry Enterprise Server and the BlackBerry device, the BlackBerry Enterprise Solution is designed to preserve the integrity, confidentiality, and authenticity of your corporate data.

The BlackBerry Enterprise Solution is designed to prevent the decryption of information at an intermediate point between the BlackBerry device and the BlackBerry Enterprise Server or company LAN. That is, only the BlackBerry

Enterprise Server and BlackBerry device user have access to the information sent between them. In particular, the BlackBerry Enterprise Solution is designed to prevent service providers from accessing potentially sensitive company information in a decrypted format. Also, since the exchange of the master encryption key (see page 17 for more information) is allowed only when the BlackBerry device is connected to the user's desktop, or during wireless enterprise activation, there is an authenticated link for exchanging the key.

In addition to providing effective corporate security, the BlackBerry Enterprise Solution provides system administrators with an effective way to manage their BlackBerry users. The BlackBerry Enterprise Solution enables system administrators to manage security settings for all BlackBerry devices associated with a given BlackBerry Enterprise Server from inside the organization at a central location instead of on individual computers. Through the BlackBerry Enterprise Server, system administrators can create and send wireless commands that enable and disable BlackBerry device functionality, such as changing device passwords and locking or deleting information from lost devices. Groups of users can be created and managed using IT policies to customize security settings. See "IT policies and IT commands" on page 8 for more information.

New in this release

Feature	Description
Content protection	BlackBerry device data (for example, email messages, contacts, and appointments) can be encrypted with AES.
Application control	This feature enables system administrators to restrict privileges of each third-party application, for example, restricting interprocess communication and network access.
Wireless enterprise activation	Users can activate a BlackBerry device on the BlackBerry Enterprise Server without a cradle or without connecting the device to a USB port. Users open the Enterprise Activation program on the BlackBerry device and type their shared secret password. An AES or Triple-DES encryption key is created, which enables users to send and receive email.
Advanced Encryption Standard	Data that is exchanged between the BlackBerry device and the BlackBerry Enterprise Server can be encrypted using the AES encryption algorithm.

Messaging Server

The BlackBerry Enterprise Solution is designed to interoperate with the Messaging Server and does not alter the normal functionality of the Messaging Server. The Messaging Server continues to receive, deliver, and store all corporate email messages, while the BlackBerry Enterprise Server acts as a conduit to transfer these messages to and from the BlackBerry device. The Messaging Server still performs all message storage, so that no mail is stored on the BlackBerry Enterprise Server.

Microsoft Exchange Server

The BlackBerry Enterprise Server is designed to leverage existing Microsoft® Exchange Server security by using hidden folders in the Microsoft Exchange mailboxes to store important BlackBerry user-related information. Therefore, the BlackBerry administration account must have an enabled mailbox. This mailbox stores BlackBerry administrative information such as BlackBerry Enterprise Server names, BlackBerry user lists, the SRP ID (network connection information), and authentication keys.

Microsoft Exchange mailboxes that are associated with BlackBerry users store individual BlackBerry information, including individual BlackBerry user statistics, the personal identification number (PIN) of the user's BlackBerry device, and the master encryption key for encrypting and decrypting the user's messages. See "Key storage" on page 21 for more information on encryption key storage.

IBM Lotus Domino Server

The IBM® Lotus® Domino® databases that are used by the BlackBerry Enterprise Server are created within the IBM Lotus Domino environment and leverage existing Lotus Domino security features. Specifically, the security for individual databases is controlled by the database access control list (ACL). Also, some fields that require more security are encrypted within the database.

The following IBM Lotus Domino databases are created and used for managing email messages:

Database	Description
BlackBerry outbox	This database acts as an outbound queue for wireless email. It tracks all messages that are delivered to the wireless network and verifies that the messages reach their destination. This database stores message information that is contained in the header of messages (for example, message ID, date, and message status) that are sent by the BlackBerry Enterprise Server.
BlackBerry profiles	This database stores important configuration information for each BlackBerry user, including BlackBerry device identification information, device's encryption key, link to the user's BlackBerry state database, and other information that is used to manage the flow of messages to and from the user's device.
BlackBerry state	This database stores an entry that establishes a connection between the original message in the 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 that stores tracking information for each message.

The BlackBerry Enterprise Server and IBM Lotus Domino Server communicate using the same Remote Procedure Call (RPC) that is contained within IBM Lotus Notes. The IBM Lotus Notes RPC enables seamless communication between the BlackBerry Enterprise Server, BlackBerry-related IBM Lotus Domino databases, and the IBM Lotus Domino Server.

Novell GroupWise Server

The BlackBerry Enterprise Server is designed to use a trusted application key to open a connection to the Novell® GroupWise® server. To generate the trusted application key, the GroupWise administrator runs the trusted application key generator by specifying the primary domain location. The trusted key is a 65-byte string that is created based on the trusted application name that the administrator submits to the GroupWise server.

The BlackBerry Enterprise Server is designed to connect to a user's online mailbox after the administrator enters the trusted application name and key during installation of the BlackBerry Enterprise Server. The GroupWise server verifies the trusted application credentials for the BlackBerry Enterprise Server and permits the BlackBerry Enterprise Server to establish a connection to the user's GroupWise database.

Information such as BlackBerry Enterprise Server names, BlackBerry user lists, the SRP ID (network connection information), authentication keys, personal identification number (PIN) of the user's BlackBerry device, and the master encryption key for encrypting and decrypting the user's messages is stored in the BlackBerry Enterprise Server configuration database.

BlackBerry Enterprise Server

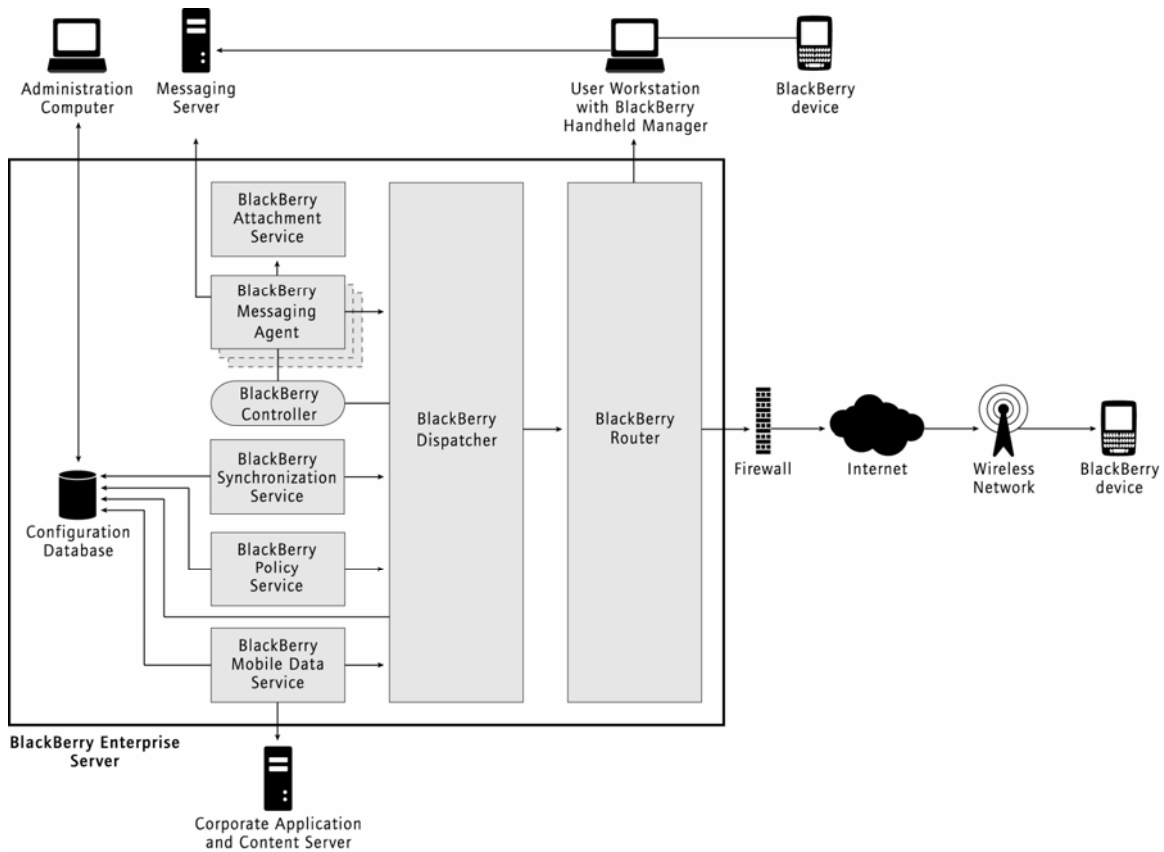
The BlackBerry Enterprise Server is designed to establish a secure, two-way link between the user's Messaging Server account and the user's BlackBerry device. The BlackBerry Enterprise Server provides security features and helps to preserve the confidentiality, integrity, and authenticity of your corporate data.

After communication with the Messaging Server is established, the BlackBerry Enterprise Server instructs the Messaging Server to monitor BlackBerry user mailboxes for new mail items. When BlackBerry users receive a new message in their mailbox, the Messaging Server notifies the BlackBerry Enterprise Server. The BlackBerry Enterprise Server retrieves a text copy of the message and compares the message to the IT-defined filters and user-defined filters. If the message meets the criteria for delivery, the message is compressed, encrypted, and sent to the BlackBerry device.

The BlackBerry Enterprise Server does not duplicate or change messages that are stored on the Messaging Server; it simply forwards messages from the user's mailbox.

Before sending a message to the BlackBerry device, the BlackBerry Enterprise Server compresses and encrypts the message using a key that is unique to that device. When receiving a message from the BlackBerry device, the BlackBerry Enterprise Server decompresses and decrypts the message using the device's unique key. After the message is decrypted, the Messaging Server places it in the user's mailbox for delivery. See "Key-under-key encryption" on page 19 for more information.

The BlackBerry device supports attachments through the BlackBerry Attachment Service. The BlackBerry Attachment Service supports Microsoft Excel, Microsoft PowerPoint®, Corel® WordPerfect®, Adobe® PDF, and text documents.



BlackBerry Enterprise Server architecture

By encrypting and decrypting messages within the protection of the corporate firewall, the BlackBerry Enterprise Server is designed to keep messages encrypted from the sender via the BlackBerry Enterprise Server to a co-worker's BlackBerry device.

See the *BlackBerry Enterprise Server Feature and Technical Overview* for more information on the BlackBerry Enterprise Server.

Corporate firewall or proxy

After the initial connection to the BlackBerry Infrastructure is established (over the Internet), a persistent TCP/IP connection is used to send traffic between the BlackBerry Enterprise Server and the BlackBerry device.

To establish the initial connection, the BlackBerry Enterprise Server contacts the BlackBerry Infrastructure using SRP. An authentication handshake is performed when the connection is established. If the authentication fails, the connection will not be established. See "SRP authentication between the BlackBerry Enterprise Server and the wireless network" on page 6 for more information.

To maintain an outbound-initiated TCP/IP connection from the BlackBerry Enterprise Server, a configuration change at the firewall is required to allow an outgoing connection on TCP port 3101.

Outbound traffic from the BlackBerry Enterprise Server has no destination other than the BlackBerry device through the wireless network. Inbound traffic to the BlackBerry Enterprise Server from any source other than the device (through the BlackBerry Infrastructure or BlackBerry Desktop Software) or the Messaging Server is discarded.

The TCP connection through port 3101 is designed to be secure in the following ways:

- The connection to the wireless network is outbound-initiated by the BlackBerry Enterprise Server and must be authenticated. No inbound-initiated traffic is permitted.
- All data traffic between the BlackBerry Enterprise Server and the user's BlackBerry device is encrypted using AES or Triple-DES encryption. All data remains encrypted along the entire path from the BlackBerry Enterprise Server to the BlackBerry device or from the BlackBerry device to the BlackBerry Enterprise Server. There is no staging location in which the data is decrypted and encrypted again. Therefore, all communications between the BlackBerry Enterprise Server and the BlackBerry device are protected by encryption from all unauthorized parties.
- The BlackBerry Enterprise Server only accepts data that it can decrypt using a valid encryption key. No communication of any kind can occur between the BlackBerry Enterprise Server and wireless network or BlackBerry device unless this condition is met. Because only the BlackBerry device and BlackBerry Enterprise Server have a valid encryption key, no datagrams are accepted from any outside source.

BlackBerry Router authentication protocol

The BlackBerry Router connects to the BlackBerry Enterprise Server and is designed to route data to BlackBerry devices that are connected to the BlackBerry Handheld Manager through a serial/USB port. The BlackBerry Router can be installed on a remote computer to route BlackBerry traffic to and from the BlackBerry Infrastructure for one or more BlackBerry Enterprise Servers. The BlackBerry device must authenticate itself to the BlackBerry Enterprise Server before the BlackBerry Router can send data to the device.

1. **User connects the BlackBerry device:** The user connects the BlackBerry device to a desktop computer that is running the BlackBerry Handheld Manager.
2. **BlackBerry device is authenticated:** The BlackBerry Router uses a unique authentication protocol to verify that the user is a valid user. The authentication sequence uses the authentication information that the BlackBerry Enterprise Server and the BlackBerry device use to validate each other to determine whether the connection is valid. The BlackBerry Router does not learn the value of the master encryption key that passes between the BlackBerry device and the BlackBerry Enterprise Server.
3. **Data bypasses the wireless network:** The BlackBerry Router and the BlackBerry Handheld Manager manage all data flow to and from the BlackBerry device through the physical connection.
 - Data from the BlackBerry device is sent to the BlackBerry Router through the BlackBerry Handheld Manager.
 - Data to the BlackBerry device is sent from the BlackBerry Router to the device through the BlackBerry Handheld Manager.

All data between the BlackBerry device and the BlackBerry Enterprise Server is compressed and encrypted. When the user disconnects the BlackBerry device or closes the BlackBerry Handheld Manager, the wireless data flow is restored.

Server Routing Protocol authentication

The BlackBerry Infrastructure is designed to communicate with the BlackBerry Enterprise Server using a Research In Motion (RIM) proprietary protocol called Server Routing Protocol (SRP). SRP is a point-to-point protocol that runs over TCP/IP. All BlackBerry Enterprise Servers are designed to communicate with the BlackBerry Infrastructure using SRP. SRP is designed to perform the following actions:

- SRP establishes the connectivity between the BlackBerry Enterprise Server and the BlackBerry Infrastructure.
- SRP authenticates the BlackBerry Infrastructure to the BlackBerry Enterprise Server and the BlackBerry Enterprise Server to the BlackBerry Infrastructure.

The BlackBerry Infrastructure and the BlackBerry Enterprise Server must be authenticated with each other before data can be transferred. The authentication sequence depends on a shared secret encryption key (the authentication key), which is configured on both the BlackBerry Enterprise Server and the BlackBerry Infrastructure. If at any point in the process the authentication fails, the connection is terminated.

- SRP exchanges configuration information between the BlackBerry Enterprise Server and the BlackBerry Infrastructure.

To allow the BlackBerry Enterprise Server and the BlackBerry Infrastructure to tune the parameters of the SRP protocol implementations dynamically, some packet formats are defined. To support backwards compatibility with older versions of the BlackBerry Enterprise Server software, which terminate the connection if unrecognized packets are received, the BlackBerry Infrastructure does not send these packets to the BlackBerry Enterprise Server unless it has previously sent a packet to the BlackBerry Infrastructure. The BlackBerry Enterprise Server should send a basic information packet to the BlackBerry Infrastructure immediately following the authentication process.

- SRP sends and receives transactions between the BlackBerry Enterprise Server and the BlackBerry Infrastructure.

The BlackBerry Infrastructure acts as a temporary storage for data that is to be sent to BlackBerry devices. Whenever the connection between the BlackBerry Enterprise Server and the BlackBerry Infrastructure is broken, the data that is sent to the BlackBerry Infrastructure is stored. The BlackBerry Enterprise Server can request confirmation that the BlackBerry Infrastructure stored the message in its message store. If this confirmation is received, the message does not have to be re-submitted when the connection is re-established.

SRP authentication between the BlackBerry Enterprise Server and the wireless network

1. SRP sends UID to BlackBerry Infrastructure:

The BlackBerry Enterprise Server claims the Unique Identifier (UID) with which it has been configured. A packet is sent to the BlackBerry Infrastructure claiming the UID.

When the customer purchases the BlackBerry Enterprise Solution, the UID is included in the package along with the authentication key. The authentication key is a 20-byte shared secret assigned by RIM to the BlackBerry Enterprise Server.

RIM can also generate new UIDs and keys and provide them to customers as necessary.

2. **BlackBerry Infrastructure sends a challenge string to BlackBerry Enterprise Server:**

The BlackBerry Infrastructure sends a random challenge string to the BlackBerry Enterprise Server.

3. **BlackBerry Enterprise Server sends a challenge string to BlackBerry Infrastructure:**

When the BlackBerry Enterprise Server receives the BlackBerry Infrastructure challenge string, it sends a challenge to the BlackBerry Infrastructure.

4. BlackBerry Infrastructure sends a challenge response to BlackBerry Enterprise Server:

The BlackBerry Enterprise Server challenge is hashed with the authentication key using the HMAC SHA-1. The resulting 20-byte value is sent back to the BlackBerry Enterprise Server.

5. BlackBerry Enterprise Server sends a challenge response to BlackBerry Infrastructure:

The BlackBerry Enterprise Server responds to the BlackBerry Infrastructure challenge by hashing the challenge with the shared authentication key.

6. BlackBerry Infrastructure sends an acceptance to BlackBerry Enterprise Server:

If the BlackBerry Infrastructure accepts the response, it sends a final confirmation to the BlackBerry Enterprise Server. The authentication process is now complete. In practice, only a success result is returned. If the BlackBerry Infrastructure rejects the response, the connection fails and the session is ended.

BlackBerry Mobile Data Service

The BlackBerry Mobile Data Service is an integrated part of the BlackBerry Enterprise Server that is designed to provide the BlackBerry Browser and third-party Java™ applications with access to the Internet and online corporate data and applications. The BlackBerry Enterprise Server and the BlackBerry Mobile Data Service are designed to perform the following key functions:

- provide BlackBerry device applications with access to the intranet and Internet
- transcodes content from the origin server for optimal display on the BlackBerry device
- accept and respond to push requests from server-side push applications

See the *BlackBerry Application Platform Technical Overview* for more information on the Mobile Data Service.

Security architecture

Users can use the BlackBerry Browser to access data on the Internet or corporate intranet and can use third-party applications that require secure access behind the firewall. The BlackBerry Mobile Data Service uses a standard Internet protocol such as HTTP or TCP/IP. The same encryption that protects data that is sent to or from users' BlackBerry devices is used to protect data from the Internet, and online corporate data and applications.

See the *BlackBerry Browser Technical Reference Guide* for more information on using the BlackBerry Browser.

An HTTP connection can be set up over SSL/TLS (Hypertext Transfer Protocol over Secure Sockets, or HTTPS) to provide additional authentication and security if an application accesses servers on the Internet. The BlackBerry device supports HTTPS communication in one of the following modes, depending on corporate security requirements:

- Proxy mode SSL/TLS: The BlackBerry Mobile Data Service sets up the SSL/TLS connection on behalf of the BlackBerry device. Communication over the wireless network between the BlackBerry device and BlackBerry Enterprise Server is not encrypted using SSL/TLS, but it is still AES or Triple-DES encrypted. A point exists behind the corporate firewall where data is not encrypted.
- BlackBerry device direct mode SSL/TLS: Data is encrypted over SSL/TLS for the entire connection between the BlackBerry device and the origin server. This type of connection is considered to be more secure than proxy mode because data remains encrypted and is not decrypted at the BlackBerry Mobile Data Service.

In proxy mode SSL, the user experiences faster response times, but the system administrator must be trusted with the data. BlackBerry device direct mode SSL/TLS is appropriate when only the endpoints of the transaction are trusted (for example, with banking services).

Note: BlackBerry device direct mode SSL is supported on BlackBerry devices with BlackBerry Handheld Software version 3.6.1 or later.

Wireless Transport Layer Security

BlackBerry supports Wireless Transport Layer Security (WTLS), which is designed to provide an extra layer of security when connecting to a Wireless Application Protocol (WAP) gateway. WTLS requires a WAP gateway to provide standard WAP access to the Internet. To use a WAP gateway, a company must work with the network operator or service provider. WTLS is supported in BlackBerry Handheld Software version 3.2.1 or later.

IT policies and IT commands

In the past, personal devices, such as mobile phones and personal digital assistants (PDAs), were difficult if not impossible for system administrators to manage. Even if system administrators deployed them, devices seldom contained the technology to track or monitor them effectively. With the advent of powerful new devices that can access and store more sensitive corporate data, controlling the security of these devices becomes a much more important issue. In the wrong hands, roaming devices with remote access to sensitive data could be dangerous.

With the BlackBerry Enterprise Solution, a system administrator can monitor and control all BlackBerry devices from the BlackBerry Enterprise Server Management console. With BlackBerry Enterprise Server software version 4.0, BlackBerry Enterprise Solution incorporates a high level of wireless IT control. This control is accomplished using wireless IT commands and IT policies.

Wireless IT commands

System administrators can control BlackBerry devices remotely using wireless IT commands. These commands are most commonly used on lost or stolen BlackBerry devices. The following wireless IT commands are available to system administrators:

- **Kill Handheld:** This command is designed to erase all user and application data that is stored on the BlackBerry device. If a BlackBerry device has been stolen or cannot be found, the system administrator can erase all information and application data remotely.
- **Set a Password and Lock the Handheld:** This command is designed to enable the system administrator to create a new password and lock the BlackBerry device remotely. If the user is uncertain of the BlackBerry device location, the system administrator can set a password (if one has not been set) and lock the device. The system administrator can then verbally communicate the new password to the user when the device is found. The user is prompted on the device to accept or reject the new password change.
- **Reset the Password and Lock the Handheld:** If the user has forgotten the BlackBerry device password, this command enables a system administrator to reset the password remotely and communicate the new password to the user.

Note: If content protection is enabled, the administrator will not be able to reset the user's password remotely.

Wireless IT commands enable system administrators to immediately respond to a lost or stolen BlackBerry device and protect confidential enterprise information.

IT policies for security settings

IT policies enable system administrators to customize the features such as password, mail forwarding, and browser options that are common to all BlackBerry device users on a given BlackBerry Enterprise Server. IT policies provide an efficient method for managing many different users simultaneously.

With wireless IT policy, custom settings can be enabled from the BlackBerry Enterprise Server and immediately enforced on C++-based BlackBerry devices running handheld software version 2.5 or later and Java-based BlackBerry devices running BlackBerry Handheld Software version 3.6 or later.

Using the BlackBerry Enterprise Server, system administrators can set specific IT policies to define how users use the security settings that are included on BlackBerry devices and in the BlackBerry Desktop Manager.

- IT policies for security: The BlackBerry Enterprise Solution offers users many different security settings for the BlackBerry device and BlackBerry Desktop Manager. All BlackBerry user security settings can be defined by system administrators. For example, system administrators specify whether a password is required, the length of time that a password can exist before it becomes invalid, and the length and composition of a password. Encryption key details can also be specified using an IT policy.
- Wireless policy deployment: All IT policies, including security settings, can be immediately applied wirelessly. This innovative feature is extremely important, because many BlackBerry device users are mobile workers who rarely synchronize their devices with the enterprise network. To accomplish wireless delivery of new policies and immediate user adoption, IT policy settings are automatically written to the user configurations. To verify that the settings are always current, the BlackBerry Enterprise Server periodically transmits BlackBerry device settings to the device wirelessly.
- Continuous updating of IT policies: All IT policies, including security settings, are updated regularly. The BlackBerry device is updated periodically through wireless policy deployment. With continuous updating, it enables BlackBerry device users to quickly adopt new IT policies, including security settings.
- Group policies: The IT policy feature enables a system administrator to define a policy for a group and apply it to all users in the group instead of creating a policy for each user. For example, a system administrator can create a policy for executives, and assign each executive to the group policy.

See the security and IT policy appendices in the *BlackBerry Enterprise Server Administration Guide* for more information.

BlackBerry device

The BlackBerry Enterprise Solution is designed to use either the AES or Triple-DES encryption algorithm to protect data while it is in transit between the BlackBerry Device and BlackBerry Enterprise Server. All messages that the BlackBerry Device sends or receives are AES or Triple-DES encrypted. This encryption verifies that a BlackBerry message remains protected in transit to the BlackBerry Enterprise Server while it is outside the corporate firewall.

Users can use a password to lock the BlackBerry device when it is not in use. The BlackBerry device password is an important feature for securing device data, and it can be forced by system administrators through the use of an IT policy. When creating a password, the user must create a strong password without using repetition or excessive simplicity. Passwords that consist of a natural sequence (such as 1, 2, 3, 4, and 5) or identical characters are rejected by the BlackBerry device.

A counter is incremented each time the user enters an incorrect password. If the password is incorrectly entered five times, the user must type "blackberry" at the prompt in order to continue attempting to unlock the BlackBerry device. After the user's fifth attempt, the user's password appears in text on the screen as it is typed. (**Note:** Make sure the Suppress Password Echo IT policy rule is set to False.) At the eighth attempt, the user is prompted again and must type "blackberry" to continue. If the user does not enter "blackberry" when prompted, the counter on the BlackBerry device will stop incrementing and all subsequent password attempts will be ignored. The counter will not increment again until the user types "blackberry" at the prompt.

By default, a user is limited to ten password attempts on the BlackBerry device. The data on the BlackBerry device is designed to be deleted after ten incorrect password attempts. If users have a current backup of the BlackBerry device data on the desktop, they can use the backup and restore tool in the BlackBerry Desktop Software to replace the data on the device. System administrators can change the value of the password setting through an IT policy. See the security and IT policy appendices in the *BlackBerry Enterprise Server Administration Guide* for more information.

The BlackBerry device only stores a SHA-1 hash of the password. A hash is a function that takes a variable-length input string and converts it into a fixed-length numerical representation of the original value. The hash is known as a one-way function because it cannot be reversed easily to reveal the password value.

The user can also specify a security timeout, which indicates the number of idle minutes that occur before the BlackBerry device locks so that data stored on the device can remain safe in the event of a theft or loss. When the BlackBerry device locks, either from a security timeout or from a user command, the owner information is immediately displayed and access to data through the keyboard or serial/USB port is prevented until the user types the correct password. In version 3.6 or later of the BlackBerry Handheld Software, users can set the BlackBerry device to lock whenever it is inserted in the holster. This locking can also be set through an IT policy. See the security and IT policy appendices in the *BlackBerry Enterprise Server Administration Guide* for more information.

Java-based BlackBerry devices

Java™-based BlackBerry devices are designed to provide an open platform for third-party application development. With the Mobile Data Service feature of the BlackBerry Enterprise Server and the BlackBerry Java Development Environment (JDE), the BlackBerry Enterprise Solution enables the creation of wireless enterprise applications that give users access to corporate data.

BlackBerry Handheld Software version 3.6 or later enables users to download Java applications wirelessly using the BlackBerry Browser. The BlackBerry Enterprise Solution includes features to protect corporate data on the BlackBerry device and on the network, and additional security features are designed to minimize the potential risk from adding third-party applications to the BlackBerry device.

The BlackBerry JDE enables developers to create more powerful, sophisticated applications than are possible with standard Java 2 Micro Edition™ (J2ME™). Third-party BlackBerry applications can communicate with each other, share persistent storage, interact with native BlackBerry applications, and access user data such as calendar appointments, email messages, and contacts. This open and flexible framework for application development can increase security concerns. Security concerns for application development on the BlackBerry JDE are addressed in the following ways:

- Third-party applications can only access persistent storage or user data, or communicate with other applications, through specific application programming interfaces (APIs).
- Applications that use these sensitive APIs must be digitally signed by RIM.
- Administrators can restrict privileges of each third-party application. See "Application control" on page 13 for more information.

To prevent malicious applications from accessing data on the BlackBerry device, sensitive APIs on the BlackBerry device are controlled by "code signing"; third-party applications that use these APIs must be digitally signed by RIM before they can be installed and run on a BlackBerry device. Code signing provides an audit trail of applications that use sensitive APIs. RIM does not inspect or in any way verify third-party applications. However, system administrators can use an IT policy to block third-party applications from being loaded on the BlackBerry device.

Java-based BlackBerry devices are designed to prevent applications from causing problems, either accidentally or maliciously, in other applications or on the device itself. Applications that are based on the Mobile Information Device Profile (MIDP), called MIDlets, cannot write to memory on a BlackBerry device. MIDlets cannot access the memory of other applications or the persistent data of another MIDlet application.

Bluetooth support on BlackBerry devices

Bluetooth® wireless technology enables Bluetooth enabled BlackBerry devices to establish a wireless connection with other devices that are within a 10-meter range of these BlackBerry devices. These particular BlackBerry devices can connect to other Bluetooth wireless technology enabled devices such as a hands free car kit or wireless headset.

Bluetooth profiles specify how applications on the Bluetooth enabled BlackBerry devices and on other Bluetooth devices connect and are interoperable. The Bluetooth Serial Port Profile (SPP) is implemented on Bluetooth enabled BlackBerry devices to establish a serial connection between the device and a Bluetooth peripheral using a serial port interface. The Bluetooth peripheral accesses the serial port through the BlackBerry Software Development Kit (SDK).

The following security measures are applied on BlackBerry devices that are Bluetooth wireless technology enabled and running BlackBerry Handheld Software version 4.0 or later:

- By default, the Bluetooth radio is disabled on the BlackBerry device.
- Users must request a connection or pairing on the BlackBerry device with another Bluetooth device. Users must also type a password ("passkey") to complete the pairing.
- By default, the BlackBerry device is prompted each time a Bluetooth device attempts to connect to the device.
- Users can specify whether Bluetooth connections with the BlackBerry device are encrypted. Data is encrypted using the passkey that the user enters. The passkey is a shared secret key that is used to generate encryption keys.

Administrators can also use IT policies to simultaneously manage all BlackBerry devices that are Bluetooth wireless technology enabled. Administrators can prevent BlackBerry devices from establishing a connection to another Bluetooth wireless technology enabled device, or from connecting to a Bluetooth wireless technology enabled handsfree or wireless device.

Content protection

Content protection is designed to encrypt data that is stored on the BlackBerry device using 256-bit AES. The BlackBerry device also encrypts email messages and meeting requests that it receives when it is locked.

The following items on the BlackBerry device are encrypted with content protection:

BlackBerry device application	User data
Email	<ul style="list-style-type: none">• subject• email addresses• message body• attachments
Calendar	<ul style="list-style-type: none">• subject• location• organizer• attendees• notes included in the appointment or meeting request
MemoPad	<ul style="list-style-type: none">• title• information included in the body of the note
Tasks	<ul style="list-style-type: none">• subject• information included in the body of the task
Contacts	<ul style="list-style-type: none">• all information except for title and category
Auto Text	<ul style="list-style-type: none">• all entries that the original text is replaced with

BlackBerry device application	User data
BlackBerry Browser	<ul style="list-style-type: none"> • content that is pushed to the BlackBerry device • web sites that are saved on the BlackBerry device • browser cache

Note: Third-party developers can write applications that use content protection. Applications must be modified to use content protection.

Enabling content protection

When content protection is enabled, a padlock icon appears at the top of the locked screen. Users can enable content protection in the BlackBerry device options, on the Security screen. See the *BlackBerry Wireless Handheld User Guide* for more information. When a locked padlock is displayed at the top of the locked screen, the BlackBerry device is finished encrypting the data.

Note: Secure garbage collection is enabled on the BlackBerry device when content protection is enabled, a program uses the Cryptographic Application Programming Interface (Crypto API) to create a private or symmetric key, a third-party application enables secure garbage collection or the BlackBerry with the S/MIME Support Package is installed. See the *Garbage Collection in the BlackBerry Java Development Environment White Paper* for more information.

Content protection key

When the user enables content protection for the first time, a 256-bit AES bulk key and the Elliptic curve cryptography (ECC) key pair are randomly generated.¹ The AES bulk key and the ECC private key are each encrypted with another ephemeral 256-bit key that is derived from the BlackBerry device password.² Encrypted versions of the content protection keys are stored on the BlackBerry device in flash memory.

The ECC public key is used to encrypt data on the BlackBerry device when it is locked instead of the AES symmetric encryption key that encrypts data when the device is unlocked. Using an asymmetric key to protect data while the BlackBerry device is locked is designed to prevent other users from extracting the symmetric encryption key from the device's flash memory and decrypting the user's data. Depending on the content protection IT policy strength, the following ECC key pairs can be used to encrypt content on the BlackBerry device when the device is locked: 160-bit, 283-bit, and 571-bit keys. See the *BlackBerry Enterprise Server Administration Guide* for more information on IT policies.

Note: If a content protection strength is selected for this IT policy rule, content protection is enabled on the BlackBerry device.

Content protection keys in encrypted form are stored in the non-volatile (NV) store, a protected section of the BlackBerry device's flash memory, which is designed to eliminate the risk of backing up the keys on the desktop when users backup and restore their device data. The NV store cannot be accessed by third-party applications.

Encrypting user data

1. **Content protection is enabled on the BlackBerry device:** User enables content protection in the BlackBerry device options, on the Security screen. Alternatively, the administrator can enable content protection on BlackBerry devices using the content protection strength IT policy rule.
2. **Keys are randomly generated:** The 256-bit AES bulk key and the ECC key pair are randomly generated on the BlackBerry device.

¹ National Institute of Standards and Technology (NIST) approved the pseudo-random number generator (PRNG) that is used to generate the bulk key. See Federal Information Processing Standard – FIPS PUB 186-2 change1 for more information.

² RSA Security – Public Key Cryptography Standards (PKCS) #5.

3. **Randomly generated content protection keys are encrypted:** The AES bulk key and the ECC private key are each encrypted with another 256-bit ephemeral key derived from the BlackBerry device password. Content protection keys in encrypted form are stored on the BlackBerry device in flash memory.
4. **User data is encrypted:** User data is encrypted in the following scenarios:
 - **BlackBerry device is locked:** The first time the BlackBerry device is locked after content protection is enabled, user data (see table above) from the Message, Calendar, MemoPad, Tasks, Contacts, Auto Text and BlackBerry Browser programs is automatically encrypted. Since the decrypted form of the AES bulk key and ECC private key are erased when the BlackBerry device locks, user data is encrypted with the ECC public key. Messages and data received when the BlackBerry device is already locked are encrypted with the ECC public key.
 - **BlackBerry device is unlocked:** When the user, for example, composes a message on the BlackBerry device or receives a message, the user data is encrypted with the AES bulk key.

Decrypting user data

Since content protection decryption keys are erased when the BlackBerry device locks, user data is only decrypted when the device is unlocked. When the BlackBerry device is unlocked, the device password is used to decrypt the AES bulk key and the ECC private key, which were each previously encrypted by the 256-bit ephemeral key and stored on the device in flash memory.

When the user opens an encrypted entry, the user data is decrypted with the 256-bit AES bulk key. If the user attempts to open an entry that was encrypted by the BlackBerry device while it was locked, the user data is decrypted with the ECC private key.

Application control

Administrators can control third-party applications in the BlackBerry Manager Handheld Configuration Tool by performing the following actions:

- Allow or disallow third-party applications from being downloaded onto BlackBerry devices.
- Create application control policies that define which resources (for example, email, phone, and BlackBerry device key store) third-party applications can access on the BlackBerry device. System administrators can also create policies that define the types of connections that a third-party application deployed on the BlackBerry device can establish (for example, opening network connections inside the firewall).
- Assign application control policies, which specify the third-party applications that are downloaded to a BlackBerry device.
- Send third-party applications to BlackBerry devices wirelessly. Applications that are required for a particular user are pushed wirelessly to the BlackBerry device and are automatically installed.

See the *BlackBerry Enterprise Server Handheld Management Guide* for more information.

Deleting BlackBerry device data

Users can delete data on their BlackBerry device in the device options, on the Security screen. See the *BlackBerry Wireless Handheld User Guide* for more information. This is a useful feature for transferring BlackBerry devices between users in the same organization. BlackBerry device data is automatically deleted from the device after ten incorrect password attempts (default IT policy setting).

Note: When you delete data from the BlackBerry device, master encryption keys, content protection keys, and passwords are also deleted from the device. IT policies are not deleted from the BlackBerry device.

Password keeper

Users can use the password keeper to create and store all their passwords. The first time that users open the password keeper, they must create a password keeper password. Information in the password keeper is encrypted with 256-bit AES. Information that is stored in the password keeper is only decrypted when users type the password keeper password.

Users can also generate random passwords and copy passwords to the clipboard in the password keeper. BlackBerry device data is automatically deleted from the device if the password keeper password is entered incorrectly ten times.

See the *BlackBerry Wireless Handheld User Guide* for more information on the password keeper.

BlackBerry wireless messaging

The BlackBerry Enterprise Solution is designed with advanced security features to enable users to send and receive email while on the go. The BlackBerry Enterprise Server and BlackBerry Device are designed to work seamlessly with existing corporate networks. A corporate network handles an email message sent from a BlackBerry device the same way that it handles a traditional email message, by routing messages through the Messaging Server and forwarding them to the user's device or desktop computer. Email remains encrypted at all points between the BlackBerry device and the BlackBerry Enterprise Server.

Wireless enterprise activation

Wireless enterprise activation enables users to activate a BlackBerry device on the BlackBerry Enterprise Server without a cradle. Wireless enterprise activation produces a master encryption key, which authenticates the user and secures the communication between the BlackBerry Enterprise Server and the BlackBerry device.

Wireless enterprise activation can be used to deploy a large quantity of BlackBerry devices. When users purchase or replace a BlackBerry device, they can phone their system administrator. The system administrator provides the activation password over the phone. Users can open the enterprise activation program on their BlackBerry device and enter the activation password and their corporate email address. After the BlackBerry system begins the activation protocol, users are authenticated, the BlackBerry security parameters are negotiated, and users can send and receive email messages.

Using the BlackBerry Manager, the system administrator sets the activation password for the user. The activation password is only used once. After the user is successfully activated on the BlackBerry Enterprise Server, the password is no longer required. More importantly, the password cannot be re-used to establish another activation.

Enabling wireless enterprise activation

1. **New BlackBerry device:** A user receives or purchases a new BlackBerry and contacts a system administrator to activate it.
2. **System administrator creates the password:** In the BlackBerry Manager, on the General tab, the system administrator sets the password for the user's account. The system administrator then communicates the password to the user.

The password applies to the user's account only. The password is invalid after five unsuccessful activation attempts. If the user does not activate the BlackBerry device within 48 hours after the password is created, the password expires and cannot be used. When the BlackBerry device is activated successfully, the password is removed from the BlackBerry Enterprise Server.

3. **User initiates wireless enterprise activation:** The user opens the enterprise activation program on the BlackBerry device and types the appropriate corporate email address and activation password.

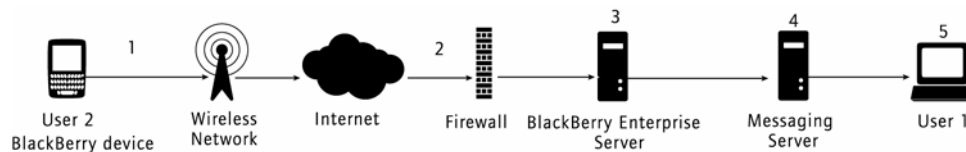
4. **BlackBerry device sends activation request:** The BlackBerry device sends an activation request email message to the user's corporate email account. This email contains BlackBerry device information such as routing information and the device activation public keys.
5. **BlackBerry Enterprise Server sends activation response:** The BlackBerry Enterprise Server sends the BlackBerry device an activation email response that contains BlackBerry Enterprise Server routing information and public keys.
6. **BlackBerry Enterprise Server and BlackBerry device establish and verify keys:** The BlackBerry Enterprise Server and the BlackBerry device establish a master encryption key. Both the BlackBerry Enterprise Server and the BlackBerry device verify their knowledge of the master key to each other. If key confirmation succeeds, the activation proceeds and further communication is encrypted.
7. **BlackBerry Enterprise Server sends service books:** The BlackBerry Enterprise Server sends the appropriate service books to the BlackBerry device. The user can now send and receive messages on the BlackBerry device.
8. **BlackBerry Enterprise Server sends data to BlackBerry device:** If the user is configured for wireless personal information management (PIM) synchronization and wireless backup, the BlackBerry Enterprise Server sends the following data to the user's BlackBerry device: calendar entries, contacts, tasks, memos and existing BlackBerry device options (if applicable) that were backed up through automatic wireless backup.

To perform wireless data synchronization between the BlackBerry Enterprise Server and the BlackBerry device, the system administrator must enable **Wireless Synchronization** and **Automatic Wireless Backup** on the user's account in the BlackBerry Manager.

See the *BlackBerry Wireless Enterprise Activation Technical Overview* for more information.

Sending an email message from the BlackBerry device

The Messaging Server manages an email message that is sent from a BlackBerry device the same way that it manages an email message that is sent from a desktop computer on the corporate network.



BlackBerry messaging: device to desktop

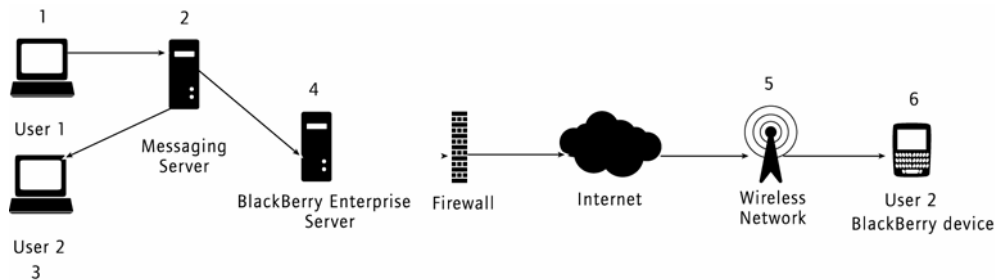
1. A message is created and sent from a BlackBerry device.
In this case, User 2 responds to User 1's message by composing an email on the BlackBerry device. The message is compressed, encrypted, and then sent over the wireless network. All messages that are created from a user's BlackBerry device contain the necessary BlackBerry Enterprise Server routing information for the wireless network, making sure that the item is correctly delivered to the user's BlackBerry Enterprise Server.
2. The encrypted message is routed through the TCP connection on port 3101 to the BlackBerry Enterprise Server on which the user is enabled.

The connection from the BlackBerry Enterprise Server to the BlackBerry Infrastructure is a two-way TCP connection. Messages are directed to this connection by the BlackBerry Infrastructure through the routing information in the message.

3. The BlackBerry Enterprise Server receives the message and decrypts it using the unique AES or Triple-DES encryption key. The BlackBerry Enterprise Server does not store a copy of the message.
4. After it is decrypted, the message is decompressed and sent to the Messaging Server for delivery.
5. The message is delivered to User 1's desktop computer.

Note: The BlackBerry Enterprise Solution also supports PIN and short message service (SMS) messaging. See "PIN and SMS messaging" on page 16 for more information on PIN and SMS messaging security.

Receiving an email message on the BlackBerry device



BlackBerry messaging: desktop to device

1. User 1 sends a message to User 2 from a desktop computer. In this scenario, User 1 and User 2 both work at the same company.
2. The message is received by the Messaging Server, which notifies the BlackBerry Enterprise Server that the message has arrived.
3. The Messaging Server delivers the message to the recipient's (User 2) desktop computer.
4. The BlackBerry Enterprise Server retrieves the message from the Messaging Server. The BlackBerry Enterprise Server then queries the Messaging Server for user preferences to determine whether or not to forward the message to the user's BlackBerry device. The message is compressed, encrypted using the user's unique encryption key, and placed in the outgoing queue.

The BlackBerry Enterprise Server is designed to maintain a constant, direct TCP/IP connection to the wireless network over the Internet through the firewall on port TCP/3101, which allows efficient, continuous delivery of data to and from the BlackBerry device.

5. The wireless network routes and then delivers the encrypted message to User 2's BlackBerry device.
6. The BlackBerry device receives the encrypted message. The message is then decrypted and displayed on the BlackBerry device.

See the *BlackBerry Enterprise Server Feature and Technical Overview* for more information on PIM and mobile data flow.

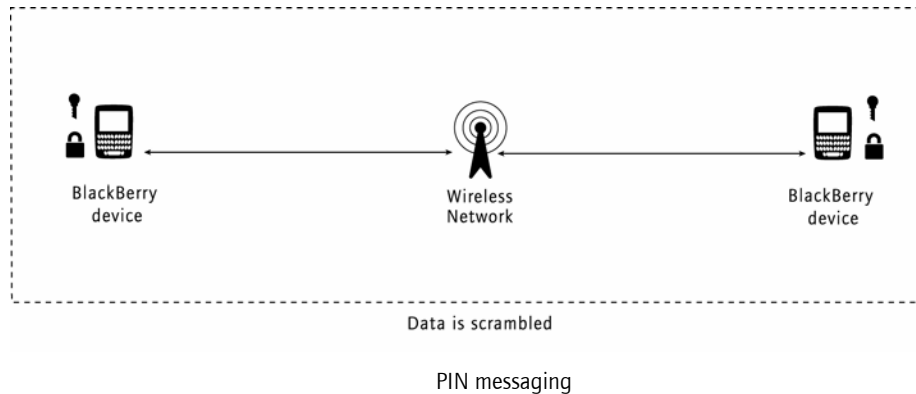
PIN and SMS messaging

PIN communication uses the BlackBerry device PIN as a means of device identification. Instead of sending a message to an email address, the message is sent directly to the BlackBerry device's PIN, bypassing the BlackBerry Enterprise Server and the corporate network.

In the PIN-messaging model, all BlackBerry devices share a common encryption key that is loaded during manufacturing. Because the same key is found on every BlackBerry device, the key is not considered to be secret.

PIN messages are encrypted with Triple-DES; however, the key to decrypt the message is available to everyone with a BlackBerry device. Therefore, PIN messages should be considered scrambled, but not encrypted.

Administrators should generate a new peer-to-peer encryption key if the current key is known to be compromised. Administrators can update and resend the peer-to-peer encryption key for users in the BlackBerry Manager. See "Managing Users" in the *BlackBerry Enterprise Server Administration Guide* for more information.



Disabling PIN and SMS messaging

Some organizations might want to track all communications for security or for other purposes. To address this concern, system administrators can disable the PIN functionality for BlackBerry Enterprise Server software version 3.5 or later using the appropriate wireless IT policy. The wireless IT policy can disable PIN communication, which disables the transmission of PIN messages from the BlackBerry device; however users can still receive PIN email messages.

SMS messaging is available on some BlackBerry devices. System administrators can also disable SMS communications using the appropriate wireless IT policy. By disabling PIN and SMS communication, system administrators can make sure that all BlackBerry device communication travels through the enterprise-messaging environment.

BlackBerry encryption

BlackBerry uses symmetric key cryptography to protect the confidentiality of the data that is sent between the BlackBerry Enterprise Server and the BlackBerry device. Before sending a message, the BlackBerry device encrypts the message using a key that is unique to that device, called the master encryption key. When receiving a message from the BlackBerry device, the BlackBerry Enterprise Server decrypts and decompresses the message using the master encryption key. The BlackBerry device, the user's mailbox, and the BlackBerry Enterprise Server configuration database each store the master encryption key.

Data that is sent between the BlackBerry device and the BlackBerry Enterprise Server is encrypted using the AES or the Triple-DES algorithm. Administrators can enable data encryption using either an AES or a Triple-DES encryption key.

Users can create a master encryption key in the BlackBerry Desktop Software, on the Security tab. Users can also generate a master key wirelessly. See the *BlackBerry Wireless Enterprise Activation Technical Overview* for more information on generating a master encryption key wirelessly. System administrators can create a master encryption key in the BlackBerry Manager, on the Security tab.

Advanced Encryption Standard

The Advanced Encryption Standard (AES) was developed to replace the Data Encryption Standard (DES). It provides a better combination of security and performance than DES or Triple-DES. AES can provide greater security against brute-force attacks by offering a larger key size. The BlackBerry Enterprise Solution uses 256-bit

keys in cipher block chaining (CBC) mode to encrypt data that is sent between the BlackBerry Enterprise Server and the BlackBerry device.

Triple-DES Encryption Standard

BlackBerry uses three iterations of the Data Encryption Standard (DES) algorithm with two 56-bit keys, in outer cipher block chaining (CBC)³ mode, for an overall key length of 112-bits. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. With Triple-DES, the data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the first key.

Note: In version 3.6 or later of the BlackBerry Enterprise Server, Triple-DES is enabled by default.

BlackBerry compatibility

Using BlackBerry Enterprise Server software version 4.0 or later, system administrators can encrypt data using a Triple-DES encryption key by selecting one of the following options in the BlackBerry Manager:

- 3DES Only
- Both 3DES & AES

Using BlackBerry Enterprise Server version 4.0, system administrators can encrypt data using an AES encryption key by selecting one of the following options in the BlackBerry Manager:

- AES Only
- Both 3DES & AES

If system administrators have enabled both Triple-DES and AES on the BlackBerry Enterprise Server and users are running an earlier version (a version earlier than 4.0) of the BlackBerry Handheld Software, BlackBerry Desktop Software, or the BlackBerry Enterprise Server software, the BlackBerry Desktop Manager generates a Triple-DES encryption key. When the user inserts the BlackBerry device into the cradle or connects the device to a USB port, its capabilities, including the encryption keys it uses, are transferred to the desktop manager.

If system administrators have enabled the AES option on the BlackBerry Enterprise Server, and users are running an earlier version (a version earlier than 4.0) of the BlackBerry Handheld Software, BlackBerry Desktop Software, or the BlackBerry Enterprise Server software, system administrators must upgrade all components to version 4.0 to use AES encryption.

Running the downgrade utility

Before system administrators run the downgrade utility on the BlackBerry Enterprise Server, AES must be enabled, and the BlackBerry Enterprise Server, BlackBerry Desktop Software, and the BlackBerry device must be running version 4.0 software. Alternatively, instead of running the downgrade utility, system administrators can disable AES on the BlackBerry Enterprise Server before performing a downgrade.

The downgrade utility removes AES encryption keys from the BlackBerry Enterprise Server so that data can be encrypted and decrypted using Triple-DES. The BlackBerry Desktop Software is designed to detect the BlackBerry Enterprise Server software version 3.6 or earlier capabilities and generates a Triple-DES encryption key based on this detection.

If users' data was previously encrypted with AES, an 'X' appears beside messages that they attempted to send from the BlackBerry device. Users must insert their BlackBerry devices into the cradle to send and receive messages again.

³ See Federal Information Processing Standard - FIPS PUB 81 [3] for more information.

Note: If either the BlackBerry device or the BlackBerry Desktop Manager is downgraded, a Triple-DES key is used to encrypt data.

Triple-DES IT policy

Set the Triple-DES IT policy to encrypt data from the BlackBerry Enterprise Server to the BlackBerry device using AES.

Perform one of the following actions:

Action	Procedure
Enable AES encryption for an environment that is running version 4.0 BlackBerry Handheld Software, version 4.0 BlackBerry Desktop Software, and the version 4.0 BlackBerry Enterprise Server software.	<ul style="list-style-type: none">Set the Disable 3DES Transport Crypto policy rule to TRUE. <p>Note: If the rule is set to TRUE, the BlackBerry device does not accept Triple-DES encrypted messages. Instead, communications for all BlackBerry devices are encrypted using AES.</p>
Disable AES encryption for an environment that is running a version of the BlackBerry Handheld Software, BlackBerry Desktop Software, or the BlackBerry Enterprise Server software that is earlier than version 4.0.	<ul style="list-style-type: none">Set the Disable 3DES Transport Crypto policy rule to FALSE.

See the *BlackBerry Enterprise Server Administration Guide* for more information on IT policies.

Key-under-key encryption

In the key-under-key encryption algorithm, the key that is used to encrypt the message data (message key) is encrypted with a second key that is unique to the BlackBerry device, called a master encryption key. The encrypted data and the cipher key that encrypted it are sent together to the recipient.

The key-under-key encryption algorithm provides the following benefits:

- Because the encryption key encrypts a relatively small amount of data when it encrypts the message key, and because the message key contains only random bits, the only known method of attack is by exhaustive key search or brute force.
- If a message key is compromised, only the corresponding message cipher text can be decrypted.

Master encryption keys

The master encryption key is created by the BlackBerry Desktop Software. When the user connects the BlackBerry device to the computer, the key is sent through the corporate LAN to the device and Messaging Server. The cradle or USB port connection to the desktop computer is designed to provide a secure connection because it uses the serial port of a trusted computer, which connects to the corporate LAN.

Alternatively, users can generate a master encryption key wirelessly. Wireless enterprise activation enables a user to remotely activate a BlackBerry device on the BlackBerry Enterprise Server without a physical network connection. During wireless enterprise activation, the BlackBerry Enterprise Server and the BlackBerry device negotiate and generate the master encryption key. See "Wireless enterprise activation" on page 14 for more information.

In addition, users can regenerate a master encryption key wirelessly. After a user requests a new key from the BlackBerry device, the key request is sent to the BlackBerry Enterprise Server. Administrators can also initiate key regeneration on the user's behalf from the BlackBerry Enterprise Server.

The master encryption key is stored on the Messaging Server, on the BlackBerry device, and in the BlackBerry Enterprise Server configuration database. To send and receive messages, the keys on the Messaging Server and the BlackBerry device must match. If the keys do not match, the email message is discarded and any attempts to communicate fail.

Wired key generation

In BlackBerry Enterprise Server software version 4.0, the data used to create the encryption key must be random so that the key cannot be recreated or duplicated.

The BlackBerry Enterprise Server is designed to create a message key by obtaining random data from the user. The BlackBerry Enterprise Server harvests system events and resources, all messages and keys are mixed into the state array. Using a technique derived from the initialization function of the ARC4 (Alleged Rivest Cipher Four) encryption algorithm, these data items are gathered and used to permute the contents of a 256-byte (2048-bit) long array.

Each new message key is created from the first 16-bytes (for Triple-DES) or 32-bytes (for AES) that are generated by a DSA pseudo-random number generator function (PRNG). The DSA pseudo-random number generator is used to generate pseudo-random bits for the creation of keys. Next, 521-bytes are drawn from the ARC4 state array, with each byte of the array used at least twice. Using SHA-512, this value is hashed to 64-bytes, which is used to seed the Digital Signature Algorithm (DSA) PRNG. The 16-byte output (for Triple-DES) or 32-bytes (for AES) generated by the DSA PRNG is used to form the message key.

If the user has Microsoft Cryptographic Application Programming Interface (MSCAPI) installed on the computer running the BlackBerry Enterprise Server software, and to avoid two or more requests for random data that yield the same output, 512 bits of randomness are requested from it to mix up the state array even further. The state array is then input into the permutation ARC4 algorithm to further randomize the array. A copy of the current seed is stored in a file. When the BlackBerry Enterprise Server is restarted, this seed is read from the file and XOR'ed with the existing seed.

Note: For Triple-DES, both message keys and master encryption keys contain 112-bits (16 bytes) of key data and 16-bits of parity data, which are stored as a 128-bit long binary string. Each parity bit is stored in the least significant bit of each of the 8 bytes of key data. For AES, both types of keys contain 256-bits of key data.

In versions of BlackBerry Enterprise Server software prior to version 4.0, each time the key generation function is called, the C language's `srand` function is seeded with the current time. Entropy is then gathered from the mouse movement in the following manner:

1. When the mouse is moved, the lowest twelve bits of the x and y axes of the new location are examined. If they are different than the previous sample, they are stored, which generates 3 bytes of randomness. If they are the same, no sample is taken.
2. The algorithm sleeps for a random interval between 50 and 150 milliseconds and then samples again.
3. The algorithm loops until 384 bytes are gathered.
4. 384 bytes of randomness are then retrieved from the MSCAPI.
5. The randomness from the mouse and the randomness from MSCAPI are hashed with SHA-512 to produce 32 bytes of data.
6. In the case of AES, the resulting 32 bytes are used as the shared key. In the case of Triple-DES, the high 16 bytes are used as the key.

See the *BlackBerry Wireless Enterprise Activation Technical Overview* for information on wireless key generation.

Wireless key generation

In wireless enterprise activation, the initial key establishment protocol is used to establish the initial master key. The initial key establishment protocol enables a BlackBerry device user to establish a strong, cryptographically protected connection with a BlackBerry Enterprise Server by bootstrapping from the activation password. The BlackBerry device and the BlackBerry Enterprise Server negotiate a common key in such a way that an unauthorized party cannot calculate the same key.

When the key is regenerated wirelessly, the key rollover protocol is used to renegotiate and generate the encryption key. The key rollover protocol uses an existing master encryption key to establish a new master encryption key. Perfect forward secrecy is achieved since the new master key is independent of the previous key, and knowledge of the previous master key will not enable an attacker to learn the new master encryption key.

The initial key establishment protocol and the key rollover protocol both provide strong authentication. Only an authorized BlackBerry device can initiate wireless enterprise activation and key generation. See the *BlackBerry Wireless Enterprise Activation Technical Overview* for more information on the key establishment protocols and the associated security benefits.

Key storage

The encryption keys are stored as clear text in the following states in the NV store:

- The **previous key** is the encryption key that is used before the current key is used. The previous key is stored in case a message that was encrypted with it is received after it has been replaced. This situation usually only occurs when delivery of a message is delayed and the encryption key is updated in the meantime.

The BlackBerry Device stores the previous key in flash memory for 7 days. The corresponding previous key is also stored on the BlackBerry Enterprise Server. This is the maximum amount of time that a message can be queued on the BlackBerry Enterprise Server for delivery.

On the BlackBerry device, multiple previous keys can remain in memory for up to 7 days. Multiple keys are stored on the BlackBerry device in case a user creates a new key multiple times while messages are still queued on the BlackBerry Enterprise Server.

- The **current key** is the encryption key currently used to encrypt and decrypt message keys.
Like the previous key, the BlackBerry device stores the current key in flash memory. The corresponding current key is also stored on the BlackBerry Enterprise Server.
- The **pending key** is a key that is generated by the system administrator or the user to replace the current encryption key. A pending key becomes the new current key the next time that the user inserts the BlackBerry device into the cradle or connects the device to a USB port. The current key becomes the new previous key.

The pending key is stored only on the BlackBerry Enterprise Server; it is sent to the BlackBerry device when the user inserts the device into the cradle or connects the device to a USB port.

The encryption keys are stored in the following locations:

- Messaging Server

Platform	Storage location
Microsoft Exchange Server	user mailbox
Lotus Domino Server	BlackBerry profiles database
Novell GroupWise Server	configuration database

- BlackBerry device key store (stored in a database in flash memory)
- BlackBerry Enterprise Server configuration database

Deleting a key

When the encryption key is destroyed on the BlackBerry device, the program releases its references to the object and the object is deleted from memory by secure garbage collection. (See the *Garbage Collection in the BlackBerry Java Development Environment White Paper* for more information.) When the user inserts the BlackBerry device into the cradle or connects the device to a USB port, the BlackBerry system recognizes the pending key. If a pending key exists, the current key becomes a previous key and the pending key replaces the current key. Previous keys are kept for 7 days before they are released for destruction. See "Key storage" on page 21 for more information on key states (previous, current and pending keys).

If a pending key exists on the BlackBerry Enterprise Server, it becomes the new current key the next time that the user inserts the BlackBerry device into the cradle or connects the device to a USB port. This process causes the current key to replace the previous key and the pending key to replace the current key. The pending key property is then marked as unused, indicating to the system that no pending key exists.

Message keys

The message key is used to encrypt data each time a new message is sent from the BlackBerry device or is sent outbound through the BlackBerry Enterprise Server. The BlackBerry Enterprise Server generates a message key for each message sent. After the message key is created, it is used to encrypt data, which is then encrypted with the master encryption key and sent to the intended recipient. The recipient then uses its copy of the master encryption key to decrypt the message key. The message key decrypts the original message and is not used again and, as such, is not stored persistently.

The message key itself is comprised of a small amount of random information, which makes it difficult for an outside party to decrypt. The message key is designed to protect the integrity of data such as short keys or large messages. If a message contains several datagrams and exceeds 2 KB, a unique message key is generated for each new datagram.

BlackBerry with the S/MIME Support Package

Secure Multipurpose Internet Mail Extensions (S/MIME) technology offers an additional layer of security between the sender and recipient of an email message. S/MIME technology enables sender-to-recipient authentication and confidentiality and preserves the integrity of the data from the time that the sender of a message sends it over the wireless network to the time that it is decoded and read by the message recipient.

BlackBerry with the S/MIME Support Package enables users who are already sending and receiving S/MIME messages on their desktop to send and receive S/MIME messages on the BlackBerry device.

BlackBerry with the S/MIME Support Package is designed to include the following features:

- certificate and private key management tools in the BlackBerry Desktop Manager that facilitate an extended synchronization process that includes certificates and private key synchronization whenever a BlackBerry device is connected to the computer
- modifications to the BlackBerry email client that include support for encrypting and decrypting messages (including PIN messages), verifying signatures, and digitally signing outgoing messages
- wireless support for certificate fetching and retrieving certificate revocation status from the BlackBerry device

Note: BlackBerry with the S/MIME Support Package is supported on the BlackBerry Enterprise Server software for Microsoft Exchange version 3.6 or later.

Private and public keys

S/MIME uses public key cryptography to provide security for messages. The sender's private key is used to sign messages. Private key information is never made public, whereas public key information can be shared. The public key is typically distributed in a certificate, which validates the authenticity of the public key. The sender

uses the recipient's public key to encrypt a message, which can then be decrypted only using the recipient's private key.

Certificates and certificate authorities

Certificate Authorities (CAs) issue a digital document, called a certificate, which binds the association between a user and a public key and, essentially, provides a level of trust in the authenticity of the association. For the certificate to be trusted, its issuing Certificate Authority must be trusted. This relationship is indicated in a certificate chain. Certificates can be downloaded from several sources:

- Windows certificate store
- Lightweight Directory Access Protocol (LDAP) certificate server
- Entrust desktop security store (*.epf) and the Entrust Address Book
- supported smart card reader

Certificates are typically included in S/MIME messages and contain information about the certificate holder.

Public Key Infrastructure compatibility

BlackBerry is designed to support the following Public Key Infrastructure (PKI) protocols:

- **Lightweight Directory Access Protocol (LDAP)**: LDAP supports wireless and desktop manager certificate searches and downloads from LDAP servers.
- **Online Certificate Status Protocol (OCSP)**: OCSP supports wireless and desktop manager verification of certificate revocation status from OCSP servers.
- **Certificate Revocation List (CRL)**: CRL supports automatic certificate revocation status verification from CRL servers.

See the *BlackBerry with the S/MIME Support Package White Paper* for more information.

Related resources

Guide	Information
BlackBerry Enterprise Server Administration Guide	<ul style="list-style-type: none">• Generating and changing master encryption keys• Enabling S/MIME encryption• IT policies• Security best practices
BlackBerry Handheld Management Guide	<ul style="list-style-type: none">• Controlling third-party software applications• Application control IT policies
BlackBerry with the S/MIME Support Package User Guide BlackBerry with the S/MIME Support Package White Paper	<ul style="list-style-type: none">• Installing the S/MIME Support Package• Managing certificates on the BlackBerry device and desktop• Setting S/MIME options for signing and encrypting messages• Sending and receiving S/MIME messages

Note: BlackBerry with the S/MIME Support Package is supported on the BlackBerry Enterprise Server software for Microsoft Exchange version 3.6 or later.

Appendix A: Cryptographic Application Programming Interface

The Research In Motion (RIM) cryptographic application programming interface (Crypto API) provides developers with a toolkit of cryptographic algorithms and support tools.

The Crypto API is included on the BlackBerry device and in the Java Development Environment (JDE). Using the API, it enables developers to create secure applications such as financial software and other business connectivity. RIM uses code signing to control access to the Crypto API and authorization to run secure applications on the BlackBerry device.

The Crypto API consists of a Java interface and encryption algorithm code. Developers can use the JDE Java interface to access the various components of the Crypto API and to create simple solutions using the encryption algorithms. Developers do not need to modify or directly access the encryption code because all calls to the native C++ encryption code are routed through the JDE Java code.

The following algorithms are available on the BlackBerry device and Java Development Environment.

See the BlackBerry JDE Javadocs for more information on the RIM Crypto API.

Cryptographic functionality provided by the API

Symmetric Block Algorithms*

Algorithm	Key length (bits)	Modes**
AES	128, 192 and 256	ECB, CBC, CFB, OFB, X, CTR
DES	56	ECB, CBC, CFB, OFB, X, CTR
RC2	8 to 1024	ECB, CBC, CFB, OFB, X, CTR
RC5	0 to 2040	ECB, CBC, CFB, OFB, X, CTR
Skipjack	80	ECB, CBC, CFB, OFB, X, CTR
Triple-DES	112 and 168	ECB, CBC, CFB, OFB, X, CTR
CAST5-128	128	ECB, CBC, CFB, OFB, X, CTR

* All listed symmetric block encryption algorithms use PKCS#5 for padding.

** All listed cryptographic modes of operation are implemented separately from the block encryption algorithms themselves.

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)
RSA raw	512 to 4096
RSA with PKCS1 formatting (version 1.5 and 2.0)	512 to 4096
RSA with OAEP formatting	512 to 4096
El Gamal	512 to 4096

Key Agreement Schemes

Algorithm	Key length (bits)	Type
DH	512 to 4096	Discrete Logarithm
KEA	1024	Discrete Logarithm
ECDH	160 to 571	Elliptic Curve
ECMQV	160 to 571	Elliptic Curve

Signature Schemes

Algorithm	Key length (bits)	Type
DSA	512 to 1024	Discrete Log
RSA using PKCS1 (version 1.5 and 2.0)	512 to 4096	Integer Factorisation
RSA using ANSI X9.31 *	512 to 4096	Integer Factorisation
RSA using PSS	512 to 4096	Integer Factorisation
ECDSA	160 to 571	Elliptic Curve
ECNR	160 to 571	Elliptic Curve

* ANSI X9.31 uses one of the following algorithms for the required MDC: SHA-1, SHA-256, SHA-384, SHA-512, or RIPEMD-160.

Key generation

Algorithm	Key length (bits)	Type
RSA	512 to 2048	Integer Factorisation
DH	512 to 4096	Discrete Log
DSA	512 to 1024	Discrete Log
EC	160 to 571	Elliptic Curve

Message Authentication Codes

Codes	Key length (bits)
CBC MAC	variable (block cipher key length)

HMAC	variable
------	----------

Message Digest Codes

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

Appendix B: Supported standards

The following section lists the TLS and WTLS standards that are currently supported by the RIM Crypto API. Because the RIM Crypto API exists on the BlackBerry device, these cipher suite components apply only to WTLS and direct mode TLS/SSL. Proxy mode TLS/SSL uses the cipher suite components provided by the Sun® JSSE 1.4.1 on the Mobile Data Service.

Key establishment algorithms

The RIM Crypto API implementation of the TLS/WTLS protocol supports the use of Rivest Shamir Adelman (RSA), Digital Signature Algorithm (DSA), and Diffie Helman (DH).

The following table lists the key establishment algorithms that are currently supported by the RIM Crypto API:

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

Export cipher suite components are typically limited to 1024 bits or less for RSA and DH and 163 bits or less for EC. Non-export cipher suite components are not normally limited; however, because of computational constraints on the BlackBerry device, all Non-Elliptic Curve operations are limited to 4096 bits or less. Elliptic Curve operations are limited to 571 bits.

Symmetric ciphers

The following table lists the symmetric cipher algorithms that are currently supported by the RIM Crypto API:

Direct mode SSL	Direct mode TLS	WTLS
RC4_40	RC4_40	RC5_40
DES_40	RC4_56	RC5_56
DES	RC4_128	RC5_64
TripleDES	DES_40	RC5
RC4_128	DES	DES_40
	TripleDES	DES
	AES_128	TripleDES
	AES_256	
	RC4_128	

Hash algorithms

The following table lists the hash algorithms that are currently supported by the RIM Crypto API:

Direct mode SSL	Direct mode TLS	WTLS
MD5	MD5	SHA
SHA1	SHA1	SHA_40
		SHA_80
		MD5
		MD5_40
		MD5_80

Appendix C: Memory scrubbing

Memory scrubbing on the BlackBerry device occurs when content protection is enabled. If content protection is enabled, the virtual machine (VM) overwrites the memory with a value of '0' after it undergoes secure garbage collection (GC).

The BlackBerry device initiates a comprehensive memory scrub in the following situations:

- A user types the password incorrectly more times than the IT policy allows. (The default is ten attempts.)
- A user manually initiates a BlackBerry device wipe (**Security > Wipe Handheld**).
- A system administrator sends a wireless command to wipe the BlackBerry device.

Memory scrub process

During a memory scrub, the following actions are performed:

1. The radio is turned off.
2. A 'device under attack' flag is set in the NV Store. If the battery is removed and the BlackBerry device wipe is ended, when power is restored, the scrub continues because the flag is present.
3. BlackBerry device data in flash memory (the persistent store) is deleted.
4. The BlackBerry device heap in Random Access Memory (RAM) is overwritten in eight passes. Each bit changes state four times.
 1. Each byte has 0x33 written to it (0011 0011₂).
 2. All bytes are cleared to 0x00 (0000 0000₂).
 3. Each byte has 0xCC written to it (1100 1100₂).
 4. All bytes are cleared to 0x00 (0000 0000₂).
 5. Each byte has 0x55 written to it (0101 0101₂).
 6. All bytes are cleared to 0x00 (0000 0000₂).
 7. Each byte has 0xAA written to it (1010 1010₂).
5. The BlackBerry device flash memory file system is overwritten in eight passes. Each bit changes state at least two times. This step only occurs if content protection is enabled.
 1. The flash memory is erased, and each byte is set to 0xFF (1111 1111₂)⁴.
 2. Each byte is logically ANDed with 0x33 (0011 0011₂). This is the equivalent of writing that value IF no other data is present in that byte.
 3. Each byte is cleared to 0xFF (1111 1111₂).
 4. Each byte has 0xCC logically ANDed to it (0x1100 1100₂).
 5. Each byte is cleared to 0xFF (1111 1111₂).
 6. Each byte has 0x55 logically ANDed to it (0x0101 0101₂).
 7. Each byte is cleared to 0xFF (1111 1111₂).
 8. Each byte has 0xAA logically ANDed to it (0x1010 1010₂).

⁴ The flash memory runs negative logic, which means that 0xFF is equivalent to a logical '0' state for a byte.

-
9. Each byte is cleared to 0xFF (1111 1111₂).
 6. The BlackBerry device password is cleared from the NVStore.
 7. The BlackBerry device data space in RAM is cleared four times.
 8. The BlackBerry device is restarted.

Part number: SWD_X_BES-002.000

© 2005 Research In Motion Limited. All Rights Reserved. The BlackBerry and RIM families of related marks, images and symbols are the exclusive properties of Research In Motion Limited. RIM, Research In Motion, "Always On, Always Connected", the "envelope in motion" symbol and BlackBerry are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

Microsoft and PowerPoint are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. IBM, Lotus, Domino, and Lotus Notes are registered trademarks of IBM in the United States and/or other countries. Novell and GroupWise are either registered trademarks or trademarks of Novell, Inc., in the United States and other countries. The Bluetooth® word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by Research In Motion Limited is under license. Corel and WordPerfect are trademarks or registered trademarks of Corel Corporation and its subsidiaries in Canada, the United States and/or other countries. Adobe is either a registered trademark or trademark of Adobe Systems Incorporated in the United States and/or other countries. Sun, Java and J2ME are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

The handheld 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; D,445,428; D,433,460; D,416,256. Other patents are registered or pending in various countries around the world. Please visit www.rim.net/patents.shtml for a current listing of applicable patents.

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

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

Check with airtime service provider for availability, roaming arrangements, features and service plans. Certain features outlined in this document require a minimum version of BlackBerry Enterprise Server Software, BlackBerry Desktop Software, BlackBerry Desktop Manager and/or BlackBerry device software and may require additional development or third party products and/or services for access to corporate applications.