BlackBerry Internet Service

Security Technical Overview

Version: 4.0

BlackBerry

Contents

Overview

The BlackBerry® Internet Service is designed to provide subscribers with automatic delivery of email messages, mobile access to attachments, and convenient access to Internet content.

The BlackBerry Internet Service uses the security of the wireless network that it connects to. Email messages that are sent between the BlackBerry Internet Service and the BlackBerry device are not encrypted. However, email messages that are sent between the BlackBerry Internet Service and the messaging server can be encrypted using SSL encryption. SSL encryption can also be used by the BlackBerry® Browser and other applications on the BlackBerry device to help protect data when subscribers connect to the Internet (for example, while shopping and banking online). Subscribers can also set up a BlackBerry device to help protect it from theft, viruses, and spyware.

Security features

BlackBerry Internet Service security features

Feature	Description
protection for online transactions	The BlackBerry® Internet Service uses SSL to increase the security of the connection to mobile shopping and mobile banking web sites for BlackBerry devices.
email message encryption for integrated email accounts	The BlackBerry Internet Service encrypts email messages that it sends and receives using SSL if the external messaging server (POP over SSL, IMAP over SSL, or Microsoft® Outlook® Web Access) supports SSL encryption. External messaging servers use a standard TCP connection if an SSL connection is not supported.
instant messaging encryption	If the instant messaging server supports SSL encryption, the BlackBerry Internet Service encrypts instant messages that the subscriber sends and receives over the SSL connection that the BlackBerry device uses to connect to the instant messaging server.
encryption of login credentials and changes to personal information or login credentials	Subscribers with a user name and password protect their data with a password when they log in to the BlackBerry Internet Service web site. The BlackBerry Internet Service is designed to encrypt login credential information from the BlackBerry Internet Service login web page using SSL and sends it using HTTPS. This encryption is designed to protect user names, passwords, and other BlackBerry Internet Service account information from unauthorized access. This encryption applies to login credential changes that the subscriber submits after logging in to the BlackBerry Internet Service web site.

Protecting messages and data using SSL

When subscribers log in to the BlackBerry® Internet Service on the BlackBerry device, their login credentials are transmitted over the wireless network to the BlackBerry Internet Service using an SSL connection over an HTTP connection (HTTPS), the available network security model. This proven model for data protection can also apply to all of the subscribers' email and instant messaging data, and to browser operations that support using SSL connections.

Subscribers can determine whether SSL encryption is helping to protect data that they send or receive using the BlackBerry® Browser. When the connection uses SSL encryption, a closed lock icon appears in the upper-right corner of the browser screen. When the connection does not use SSL encryption, an open lock icon appears.

Note: The external messaging server must support using POP over SSL, IMAP over SSL, or Microsoft® Outlook® Web Access for the email messages that subscribers send and receive on the BlackBerry device to be protected using HTTPS.

Connection type	Description	Minimum BlackBerry Device Software version required
HTTP connections	If an application on the BlackBerry device accesses servers on the Internet, the device can use an HTTPS connection to provide additional authentication and security. The device uses SSL encryption to create a highly secure connection to application servers that also support SSL. The device may list a Proxy option for TLS connections (also known as SSL connections) that is disabled because it requires the device to be activated on a BlackBerry® Enterprise Server.	3.6.1
Direct TCP connections	When creating an HTTPS connection using a direct TCP connection, data is encrypted between the BlackBerry device and the origin server (if the server supports HTTPS), and is not decrypted at any point in transit.	4.0
WAP gateway connections	The BlackBerry device can use WTLS, which is designed to provide an extra layer of security when connecting to a WAP gateway. WTLS requires a WAP gateway to provide standard WAP access to the Internet. WAP 2.0 supports HTTPS, which secures the connection end-to-end. Support for HTTPS connections through a WAP gateway may depend on the wireless service provider. Wireless service providers can provide details on connections permitted using the WAP gateway.	3.2 SP1

Types of messages that are not protected using SSL

Message type	Description
PIN	All BlackBerry® devices can use the unique PINs of other BlackBerry devices to send them PIN-to-PIN messages (including BlackBerry® Messenger messages). A PIN message bypasses the BlackBerry® Internet Service, making it useful in the event that the BlackBerry Internet Service is temporarily unavailable to process emails. The user may add a contact to BlackBerry Messenger using the contact's unique PIN if the contact is also using a BlackBerry device. Instant messages that are sent using the PIN of the contact's device also use the PIN message scrambling model.

Message type	Description
	Note: Due to its direct peer-to-peer messaging model, PIN messages use a low strength data scrambling model. Every BlackBerry device uses the same key to scramble PIN messages it sends and unscramble PIN messages it receives. This means that if a BlackBerry device user other than the intended recipient receives a PIN message, that user can decrypt and read the PIN message automatically.
Text (SMS, MMS) and instant messaging	Supported BlackBerry devices can send text messages over the wireless network to any other device or device with a phone number that is registered on a wireless network, using the standard network protection offered by the wireless service provider. BlackBerry device users can use supported instant messaging applications to send instant messages to their contacts. Third-party instant messaging applications may allow the user to add the contact to the instant messaging application using the contact's phone number. Instant messages that are sent using the device phone number also use the standard network protection offered by the wireless service provider.

Attachments

The BlackBerry® device does not run applications that subscribers receive as attachments in email messages. The BlackBerry® Internet Service processes attachments and renders them in a format that is designed to protect subscribers from potentially damaging attachment code such as macros.

To protect the received attachments that the BlackBerry device stores, subscribers can turn on the content protection feature.

Spam email messages

The BlackBerry® Internet Service has an anti-spam system that is designed to block spam email messages that are sent to a subscriber's BlackBerry email address. This feature helps to protect subscribers against the inconvenience and potential privacy threat of email messages that are not intended specifically for them.

For additional control of spam email messages, a subscriber can create email message filters to prevent unwanted email messages from being delivered to the BlackBerry device.

Security options

Security options on the BlackBerry device

Subscribers can set additional security options on their BlackBerry® devices to help protect against an attack intended to steal data from their devices.

Option	Description
Using passwords	Subscribers are advised to protect their devices with a password that must be typed to unlock and use the device. Subscribers can set password protection in the security options on the device. The device can be set to lock automatically at specified time intervals (for example, every 30 minutes) or to lock when it is inserted in a holster. By default, password authentication is limited to ten attempts, after which the device memory is erased, including all user data. Subscribers can also use the Password Keeper to protect all of the passwords that are used to access applications and websites on the device. For more information, see Protecting passwords that a BlackBerry device stores, 7.
Using encryption to protect stored data	The device is designed to use encryption, with symmetric and asymmetric encryption algorithms and encryption keys, to protect stored user data. If the subscriber turns on the content protection feature, the device encrypts the data (for example, messages, contact entries, calendar entries, memos, and tasks). If a potentially malicious user attempts to access the data by stealing it directly from the internal device hardware, that person cannot decrypt and read the data without knowing the device password. For more information, see Encrypting BlackBerry device data, 7.
Email message encryption for email addresses that subscribers add to the device	The BlackBerry® Internet Service encrypts email messages that it sends and receives using SSL if the external messaging server (POP over SSL, IMAP over SSL, or Microsoft® Outlook® Web Access) supports SSL. External messaging servers use a standard Internet connection (using TCP/IP) if they do not support SSL connections, and therefore email messages are not encrypted.
Storing data on a media card	The device is designed to support encrypting specific files on the external media card. For more information, see Encrypting files that a BlackBerry device stores on a media card, 9.

Option	Description
Using Bluetooth® connections to other Bluetooth enabled devices	Subscribers can help protect Bluetooth connections to and from the BlackBerry device. For more information, see Protecting Bluetooth connections, 9.
Using GPS data	Subscribers can help protect the GPS co-ordinates of the BlackBerry device when they use the GPS feature. For more information, see Protecting GPS location information, 10.
Downloading applications	Subscribers can help protect the device against untrusted downloaded applications. For more information, see Controlling downloaded applications, 10.
Using Wi-Fi® connections to the Internet	Subscribers can help protect Wi-Fi connections on the device. For more information, see Protecting Wi-Fi connections, 11.
Cleaning data from the device	Subscribers can manually clean sensitive data from the device memory, and enhance the security of the automatic memory cleaning that occurs. For more information, see Cleaning memory, 12.

Protecting passwords that a BlackBerry device stores

Subscribers can use the Password Keeper to store all passwords that they use to access applications and websites from a BlackBerry® device. The Password Keeper is designed to protect the passwords with a Password Keeper password. The subscriber is required to remember only the Password Keeper password.

The first time that the subscriber opens the Password Keeper on the device, the subscriber must create the Password Keeper password. The Password Keeper encrypts the information that it stores using AES-256 encryption, and uses the Password Keeper password to decrypt the information when the subscriber types the Password Keeper password. The device deletes all Password Keeper data if a subscriber exceeds the number of allowed password attempts in the Password Keeper.

In the Password Keeper, a subscriber can perform the following actions:

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

Encrypting BlackBerry device data

When subscribers set up encryption of their BlackBerry® device data using the content protection feature, the device is designed to be protected against potentially malicious users who could attempt to steal data directly from the internal hardware. No one can read subscribers' encrypted data without their device password.

In the Security Options, subscribers can set the Content Protection Strength level. The device then encrypts their data (for example, messages, contact entries, and tasks). The Content Protection Strength level optimizes either the encryption strength or the decryption time. When the device decrypts a message that it received while locked, the device uses an encryption key. More encryption strength means a longer decryption process.

If subscribers set the content protection strength to Stronger, they should use a minimum length of 12 characters for the device password. If subscribers set the content protection strength to Strongest, they should use a minimum length of 21 characters. These password lengths maximize the encryption strength that these settings are designed to provide.

Types of data protected by encryption

If a subscriber turns on content protection, the subscriber can configure a locked BlackBerry® device to encrypt stored user data and data that the locked device receives. When a subscriber turns on content protection, a locked device is designed to use AES-256 encryption to encrypt stored data and an ECC public key to encrypt data that the locked device receives.

For example, the locked device uses content protection to encrypt the following items:

Item	Description
AutoText	all text that replaces the text automatically that the subscriber types on the device
BlackBerry Browser	• content that websites or third-party applications push to the device • any websites that the subscriber saves on the device • the browser cache
calendar	• subject • location • organizer • attendees • notes in all appointments or meeting invitations
contacts (in the Contacts application)	all contact information in the Contacts application except for the contact title and category **Note:** The device permits the Caller ID and Bluetooth® Address Book transfer features to work when content protection is turned on and the device is locked.
email	• subject • email addresses of intended recipients • message body • attachments
memos	• title • information that is included in the body of a memo
tasks	• subject

Item	Description
	• information that is included in the body of a task
third-party application data	all data that is associated with third-party applications that a subscriber installs on the device

Encrypting files that a BlackBerry device stores on a media card

The BlackBerry® device is designed to encrypt media files that subscribers store on a media card according to the Encrypt Media Files option in the device options.

This encryption does not apply to files that subscribers manually transfer to a media card (for example, from a storage device using mass storage mode).

When subscribers store a file on a media card for the first time after they turn on mass storage mode, the BlackBerry device decrypts the encryption key for the external memory file and uses it to automatically encrypt the stored file.

For more information about encrypting media card files, visit www.blackberry.com/support to read article KB16088.

Protecting Bluetooth connections

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

The BlackBerry device creates a Bluetooth profile, which specifies how applications on the BlackBerry device and on other Bluetooth devices connect and communicate. The BlackBerry device uses the Bluetooth profile to open serial connections to Bluetooth enabled devices using virtual serial ports.

By default, a Bluetooth enabled BlackBerry device that runs BlackBerry® Desktop Software 4.0 or later includes the following security measures:

- Subscribers can turn off the Bluetooth wireless technology for the BlackBerry device.
- Subscribers must request a connection or pairing on the BlackBerry device with another Bluetooth device and type a passkey (also known as a shared secret key) to complete the pairing.
- Subscribers can specify whether to encrypt data sent to and from the BlackBerry device over a Bluetooth connection.
- The BlackBerry device prompts the subscriber each time a Bluetooth device tries to connect to the BlackBerry device.

Using password authorization for Bluetooth connections

A Bluetooth® enabled BlackBerry® device can use CHAP to open a Bluetooth connection to the BlackBerry® Desktop Software. To open a Bluetooth connection, the BlackBerry device or BlackBerry Desktop Software can use CHAP to send a challenge. The BlackBerry device or BlackBerry Desktop Software can subsequently use the SHA-1 algorithm to calculate a response to the challenge or to validate the response of the other party, depending on which party started the process to open the Bluetooth connection.

When the BlackBerry device uses CHAP, the BlackBerry device never sends the BlackBerry device password over an unprotected connection. The BlackBerry device combines the challenge with the BlackBerry device password to authenticate with the BlackBerry Desktop Software.

Protecting GPS location information

The BlackBerry® device stores GPS location information. Third-party applications and preloaded BlackBerry device applications that support location-based services can use that GPS location information. For example, subscribers can use BlackBerry® Maps to get the GPS location of their device. However, third-party applications cannot access their GPS location information automatically.

When applications have access to subscribers' GPS location information, they could potentially track their location or report their location back to a server. To prevent applications from using the GPS location of the device, subscribers can perform any of the following actions:

- Block specific third-party applications from using the GPS location information.
- Block all third-party applications from using location-based services.
- Turn off GPS technology on the device.
- Delete BlackBerry Maps from the device.

Controlling downloaded applications

Subscribers can download third-party applications for the BlackBerry® device over the wireless network by using the BlackBerry® Browser. A third-party application can communicate and share data with other third-party applications and BlackBerry device applications. Third-party applications can also access a subscriber's calendar entries, email messages, and contacts.

BlackBerry device applications include inherent virus protection and spyware protection that is designed to contain and prevent the spread of viruses and spyware to other applications.

When subscribers download an application, they are prompted to confirm that they trust the source. If subscribers trust the application, the application is installed on their device. Subscribers can proactively protect their device from viruses and spyware by only downloading applications from trustworthy sources.

Subscribers can use the application controls on the device to prevent the installation of specific third-party applications and to limit the permissions of third-party applications, including the following items:

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

Protecting Wi-Fi connections

If made available by the wireless service provider, supported Wi-Fi® enabled BlackBerry® devices can access the BlackBerry Infrastructure using a reliable and highly secure transport when using Wi-Fi connections.

When the subscriber connects to a Wi-Fi network on the device, an SSL tunnel is created between the device and the BlackBerry® Infrastructure, helping to protect the communication throughout the unprotected networks. Wi-Fi enabled BlackBerry devices support negotiating SSL connections to the BlackBerry® Infrastructure to establish a browsing connection to the Internet over a Wi-Fi connection. Supported Wi-Fi enabled BlackBerry devices also support multiple security methods that are designed to encrypt wireless communications over the Wi-Fi network between the device and either the wireless access points or a network firewall. Wi-Fi enabled BlackBerry devices are designed to reject incoming connections, to support limited connections in Wi-Fi infrastructure mode only, and to prevent Wi-Fi ad-hoc networking (peer-to-peer) connections.

For more information about Wi-Fi enabled BlackBerry devices, visit http://na.blackberry.com/eng/ataglance/networks/#tab_ddetail_subtab_wifi.

BlackBerry device storage

The BlackBerry® device consists of various sections that store user data and sensitive information such as keys. Third-party applications that are installed on a device cannot write to or access the sections that store sensitive information.

Section	Description
application storage	The application storage is a file system that is internal to the device. The application storage stores application data and user data. Subscribers cannot physically remove the application storage from the device. Sections of application storage can store files that a subscriber downloads or saves.
built-in media storage	The built-in media storage stores files that a subscriber saves on a device. The device uses and exposes the built-in media storage similarly to the way that the device uses and exposes a media card. When a subscriber permanently deletes all device data, the device deletes the files from the built-in media storage, except for the system storage partition, which includes sample pictures and sample songs.

Section	Description
NV store	The NV store persists in application storage, and only the operating system of the device can write to it. Third-party application code cannot write to the NV store.
media card storage	The media card stores files that a subscriber saves using a device. A subscriber can save, access, and encrypt files on the media card from the device. When a subscriber permanently deletes device data, the device does not delete the files from the media card unless the device is running BlackBerry® Device Software 5.0 or later.

Cleaning memory

By default, the BlackBerry® device continually cleans temporary memory to remove sensitive data that is no longer being used.

The device can perform the following additional cleaning actions:

- Overwrite memory
- Periodically run the memory cleaning application, which causes applications to empty any caches, free memory, and automatically overwrite the freed memory

The device performs additional cleaning actions during any of the following situations:

- When subscribers turn on the content protection feature
- When a third-party application that a subscriber has downloaded registers with the memory cleaning application

Subscribers can set the memory cleaning application to run when they insert their device into the holster or when their device remains idle for a specified period of time. Subscribers can also manually run the memory cleaning application on their device, run specific registered memory cleaners in the Security Options on their device, and turn on or turn off memory cleaning.

Deleting all BlackBerry device data

The BlackBerry® device is designed to permanently delete subscribers' stored data and application data when they type their device password incorrectly more than 10 times or when they perform a Security Wipe (in the Security Options). When subscribers delete all device data, they can also select the Include third party applications option to remove all third-party applications and application data from the device.

Before subscribers resell a device, they should consider using one of the preceding methods to delete all of their data so that the person that buys the device cannot access the original owner's personal information. For more information about preparing a device for resale, visit www.blackberry.com/support to read article KB05099.

A device is designed to permanently delete the following data from the NV store, application storage, and built-in media storage:

- All user data

- Any references to the device transport key
- If applicable, authentication information (for example, the binding information of the smart card)
- If the subscriber is resetting the device to the factory default settings, any references to past hashes of the device password
- Record of time elapsed since the device was last turned on
- If specified, all third-party applications and application data
- If the subscriber turns on content protection, the device uses a memory-scrubbing process to overwrite the application storage on the device and the built-in media storage.

BlackBerry Smart Card Reader

The BlackBerry® Smart Card Reader is an accessory that, when used in proximity to a Bluetooth® enabled BlackBerry device or a Bluetooth enabled computer, permits a user to authenticate with a smart card and log in to the BlackBerry device or computer.

The BlackBerry Smart Card Reader is designed to perform the following actions:

- Communicate with BlackBerry devices and computers using Bluetooth technology 1.1 or later and, by default, use AES-256 encryption on the application layer
- Permit a user to use two-factor authentication to access BlackBerry services and PKI applications
- Store all encryption keys in RAM only and never write the keys to application storage

The BlackBerry Smart Card Reader permits a user to prove the user's identity to the BlackBerry device or a computer using what the user has (smart card) and what the user knows (smart card password).

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

Glossary

AES
Advanced Encryption Standard

CHAP
Challenge Handshake Authentication Protocol

ECC
Elliptic Curve Cryptography

GPS
Global Positioning System

HTTP
Hypertext Transfer Protocol

HTTPS
Hypertext Transfer Protocol over Secure Sockets Layer

IMAP
Internet Message Access Protocol

MMS
Multimedia Messaging Service

NV store
The NV store is a nonvolatile store that persists in application storage on a BlackBerry device. Only the operating system of the BlackBerry device can write to it. Third-party applications cannot write to the NV store.

PIN
personal identification number

PKI
Public Key Infrastructure

POP
Post Office Protocol

SHA
Secure Hash Algorithm

SMS
Short Message Service

SSL
Secure Sockets Layer

TCP
Transmission Control Protocol

TLS
Transmitting Subscriber Identification

WAP
Wireless Application Protocol

WTLS
Wireless Transport Layer Security

Legal notice

ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

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

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

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

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

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

Research In Motion UK Limited
Centrum House
36 Station Road

Egham, Surrey TW20 9LF
United Kingdom

Published in Canada