

# BlackBerry PlayBook Tablet

Version: 1.0

## Security Technical Overview



Published: 2011-09-08  
SWD-1674396-0316050254-001

# Contents

1	Revision history.....	4
2	Tablet security features.....	6
3	System requirements: tablet.....	7
4	Opening an encrypted and authenticated connection between a tablet and smartphone.....	8
	The Bluetooth pairing process.....	8
	The BlackBerry Bridge pairing key.....	9
	Generating an initial pairing key during the BlackBerry Bridge pairing process.....	9
	Process flow: Generating an initial pairing key.....	10
	Cryptosystem parameters that the BlackBerry Bridge pairing process uses to generate an initial pairing key.....	11
	Generating a BlackBerry Bridge pairing key during the BlackBerry Bridge pairing process.....	11
	Process flow: Generating a BlackBerry Bridge pairing key.....	12
	Connecting a tablet to a smartphone that is activated on the BlackBerry Enterprise Server or BlackBerry Internet Service.....	13
	Process flow: Generating a BlackBerry Bridge work key.....	13
	Reconnecting a tablet to a smartphone.....	13
	Deleting a tablet and smartphone connection.....	13
	Bluetooth security features on the tablet and smartphone.....	14
	Using IT policy rules to manage Bluetooth technology on smartphones.....	15
	Specifying Bluetooth connections that third-party applications can access.....	16
	Bluetooth profiles that the tablet supports.....	17
5	Securing tablets in your organization's environment for work use.....	18
	How a tablet distinguishes between work data and personal data.....	18
	How a tablet protects work data.....	19
	What happens when a user updates or creates work files on a tablet.....	20
	How a tablet controls whether an application is a work application or a personal application.....	20
	Determining which applications are work applications or personal applications.....	20
	Comparison of work applications and personal applications.....	21
	Access rights for work data and personal data that the BlackBerry Tablet OS grants to applications.....	22
	Using the Bridge Browser.....	22
	Running the Files application in work mode.....	23
	Taking screen shots on a tablet.....	23
	When a tablet prevents a user from accessing work data or work applications.....	23
	Connecting a tablet to an enterprise Wi-Fi network.....	24

IT policy rules that apply to a tablet.....	24
<b>6 The BlackBerry Tablet OS.....</b>	<b>25</b>
The tablet file system.....	25
How the BlackBerry Tablet OS uses sandboxing to protect application data.....	26
How the BlackBerry Tablet OS manages the resources on the tablet.....	26
How the tablet manages permissions for applications.....	26
How the tablet verifies the boot ROM code.....	27
How the tablet manages software updates.....	27
<b>7 Protecting user information.....</b>	<b>28</b>
Using the smartphone password to help protect access to the tablet.....	28
Using the tablet password.....	28
Deleting data from the tablet memory.....	29
What happens to work data on the tablet when it is connected to a smartphone that deletes all smartphone data.....	29
<b>8 Cryptographic algorithms, codes, protocols, and APIs that the tablet supports.....</b>	<b>31</b>
Symmetric encryption algorithms.....	31
Asymmetric encryption algorithms.....	31
Hash algorithms.....	32
Message authentication codes.....	32
Signature scheme algorithms.....	32
Key agreement schemes.....	32
Cryptographic protocols.....	33
Cryptographic APIs.....	33
VPN cryptographic support.....	33
Wi-Fi cryptographic support.....	33
<b>9 Attacks that the BlackBerry Bridge pairing process is designed to prevent.....</b>	<b>35</b>
Brute-force attack.....	35
Online dictionary attack.....	35
Eavesdropping.....	35
Impersonating a smartphone.....	36
Man-in-the-middle attack.....	36
Small subgroup attack.....	36
<b>10 Glossary.....</b>	<b>37</b>
<b>11 Provide feedback.....</b>	<b>41</b>

12 Legal notice.....	42
----------------------	----

# Revision history

1

Date	Description
15 July 2011	<p>Added the following topics:</p> <ul style="list-style-type: none"> <li>• The Bluetooth pairing process</li> <li>• Generating an initial pairing key during the BlackBerry Bridge pairing process</li> <li>• Process flow: Generating an initial pairing key</li> <li>• Cryptosystem parameters that the BlackBerry Bridge pairing process uses to generate an initial pairing key</li> <li>• Generating a BlackBerry Bridge pairing key during the BlackBerry Bridge pairing process</li> <li>• Process flow: Generating a BlackBerry Bridge pairing key</li> <li>• Process flow: Generating a BlackBerry Bridge work key</li> <li>• Bluetooth security features on the tablet and smartphone</li> <li>• Using IT policy rules to manage Bluetooth technology on smartphones</li> <li>• Specifying Bluetooth connections that third-party applications can access</li> <li>• Bluetooth profiles that the tablet supports</li> <li>• Taking screen shots on a tablet</li> <li>• What happens to work data on the tablet when it is connected to a smartphone that deletes all smartphone data</li> </ul> <p>Updated the following topics:</p> <ul style="list-style-type: none"> <li>• Tablet security features</li> <li>• Opening an encrypted and authenticated connection between a tablet and smartphone</li> <li>• The BlackBerry Bridge pairing key</li> <li>• Connecting a tablet to a smartphone that is activated on the BlackBerry Enterprise Server or BlackBerry Internet Service</li> <li>• Reconnecting a tablet to a smartphone</li> <li>• How a tablet distinguishes between work data and personal data</li> <li>• How a tablet protects work data</li> <li>• Determining which applications are work applications or personal applications</li> <li>• Running the web browser in work mode (changed to "Using the Bridge Browser")</li> <li>• Running the Files application in work mode</li> <li>• When a tablet prevents a user from accessing work data or work application</li> </ul>

Date	Description
	<ul style="list-style-type: none"><li>• Using the tablet password</li><li>• The tablet file system</li><li>• Using the smartphone password to help protect access to the tablet</li><li>• Deleting data from the tablet memory</li><li>• Symmetric encryption algorithms</li></ul>
4 April 2011	Initial version

# Tablet security features

2

Feature	Description
Encrypted and authenticated connection between a BlackBerry PlayBook tablet and BlackBerry smartphone	<ul style="list-style-type: none"> <li>• A tablet and smartphone perform two pairing processes to open an encrypted and authenticated connection between each other: a Bluetooth pairing process and a BlackBerry Bridge pairing process that is designed to enhance the level of encryption for the connection.</li> <li>• The BlackBerry Bridge uses the ECDH algorithm to negotiate a key and AES-256 to encrypt the connection.</li> </ul>
Protection of work data on a tablet	<ul style="list-style-type: none"> <li>• The tablet is designed to isolate the work file system and work applications from the personal file system and personal applications.</li> <li>• The tablet classifies applications as work applications and allows them to access work data.</li> <li>• The tablet helps protect work data using XTS-AES-256 encryption.</li> <li>• The tablet does not store local copies of work data permanently, the tablet uses the BlackBerry smartphone file system to store work data.</li> </ul>
Protection of BlackBerry PlayBook tablet user information	The tablet is designed to allow a user to delete all user information and application data from the tablet memory.
Protection of BlackBerry Tablet OS	<ul style="list-style-type: none"> <li>• When the BlackBerry Tablet OS starts, it completes integrity tests to detect damage to the kernel.</li> <li>• The BlackBerry Tablet OS can restart a process that stops responding without negatively affecting other processes.</li> <li>• The BlackBerry Tablet OS validates requests that applications make for resources on the tablet.</li> </ul>
Protection of the user spaces that applications run in	<p>The BlackBerry Tablet OS runs each process in a user space on the tablet.</p> <p>To help protect a user space, the BlackBerry Tablet OS is designed to evaluate the requests that processes make for memory outside of the user space. The BlackBerry Tablet OS is designed to permit a process to access only the memory that it has permissions for at a specific time.</p>
Protection of resources	The BlackBerry Tablet OS uses adaptive partitioning to allocate resources that are not used by applications during typical operating conditions and to make sure that resources are available to applications during times of peak operating conditions.
Management of permissions to access capabilities	The BlackBerry Tablet OS evaluates every request that an application makes to access a capability on the tablet.
Verification of the boot ROM code	The tablet verifies that the boot ROM code is permitted to run on the tablet.



## System requirements: tablet

3

Item	Requirement
BlackBerry Enterprise Server version	<p>To use IT policy rules to control settings for the BlackBerry Bridge and BlackBerry PlayBook tablet, your organization's environment must include BlackBerry Enterprise Server 4.0 or later and the IT policy rules included in KB26294 imported into the BlackBerry Enterprise Server.</p> <p>For more information about importing the IT policy rules to control settings for the BlackBerry Bridge and tablet, visit <a href="http://www.blackberry.com/go/kbhelp">www.blackberry.com/go/kbhelp</a> to read KB26294.</p>
smartphone	<p>BlackBerry PlayBook tablet users who want to use the BlackBerry Bridge must have a BlackBerry smartphone that is running one of the following:</p> <ul style="list-style-type: none"> <li>• BlackBerry Device Software 5.0</li> <li>• BlackBerry 6</li> <li>• BlackBerry 7</li> </ul> <p>Users whose smartphones are running BlackBerry Device Software 5.0 and BlackBerry 6, must install BlackBerry Bridge from the BlackBerry App World storefront. The BlackBerry Bridge is pre-installed on smartphones that are running BlackBerry 7.</p>
operating system	<p>Users who want to install and run BlackBerry Desktop Software to manage the tablet using their computers must have one of the following operating systems running on a computer:</p> <ul style="list-style-type: none"> <li>• Windows XP SP3 or later</li> <li>• Windows Vista</li> <li>• Windows 7</li> <li>• Mac OS X 10.5.7 or later</li> </ul>
BlackBerry Desktop Software	<p>Users who want to manage the tablet using their computers must install one of the following:</p> <ul style="list-style-type: none"> <li>• BlackBerry Desktop Software (Windows) 6.0.2 or later</li> <li>• BlackBerry Desktop Software (Mac) 2.0.0 or later</li> </ul>

# Opening an encrypted and authenticated connection between a tablet and smartphone

## 4

A BlackBerry PlayBook tablet and BlackBerry smartphone perform two pairing processes to open an encrypted and authenticated connection between each other:

- Bluetooth pairing process to open a Bluetooth connection
- BlackBerry Bridge pairing process to provide a level of security that is greater than what the Bluetooth pairing process provides

During the Bluetooth pairing process, the tablet and smartphone share a Bluetooth key to encrypt and decrypt data that is sent between the tablet and smartphone.

During the BlackBerry Bridge pairing process, the tablet and smartphone share a BlackBerry Bridge pairing key to authenticate the connection and encrypt and decrypt data that is sent between the tablet and smartphone. During the BlackBerry Bridge pairing process, the tablet and smartphone also share the BlackBerry Bridge work key if the smartphone was activated on a BlackBerry Enterprise Server. The tablet uses the 512-bit BlackBerry Bridge work key and XTS-AES-256 to encrypt the keys that encrypt and decrypt the work data that the tablet stores.

A user can start a Bluetooth pairing process and BlackBerry Bridge pairing process on a tablet or smartphone in one step. To start the pairing processes, the user can add a smartphone in the Paired Device options on the tablet or in the BlackBerry Bridge application on the device.

If the BlackBerry PlayBook tablet user presses and holds the power key to reset the tablet, the tablet erases the BlackBerry Bridge work key from memory.

## The Bluetooth pairing process

Bluetooth technology permits a BlackBerry PlayBook tablet and a BlackBerry smartphone to open a wireless connection between each other.

Bluetooth profiles on the tablet and smartphone specify how Bluetooth enabled applications can connect and run. The Bluetooth Serial Port Profile that is on the tablet and smartphone specifies how the tablet and smartphone can open a serial connection between each other using a virtual serial port.

By default, a tablet and smartphone include the following Bluetooth security features:

- A user can turn off the Bluetooth technology for the tablet or smartphone. You can turn off the Bluetooth technology for the smartphone using IT policies.
- A user must request a connection, or pairing, between the tablet and smartphone. A user can connect a tablet and smartphone by scanning a barcode or manually configuring the connection (and typing a shared secret to complete the pairing).
- If a user connects or reconnects a tablet to a smartphone that requires a password, the user must type the smartphone password on the tablet.
- A user can delete a Bluetooth connection between a tablet and smartphone in the Bluetooth settings on a tablet.

- The tablet and smartphone use AES-256 encryption to encrypt and decrypt data that is sent between each other. The tablet and smartphone use SHA-256 to authenticate the connection between each other.
- The smartphone prompts the user each time a Bluetooth device tries to connect to the smartphone.

## The BlackBerry Bridge pairing key

The first time that a BlackBerry PlayBook tablet connects to a BlackBerry smartphone, the tablet connects with the smartphone using Bluetooth technology and generates a BlackBerry Bridge pairing key. The BlackBerry Bridge pairing key is designed to protect data as it travels between the tablet and smartphone.

A BlackBerry PlayBook tablet user can connect a tablet and smartphone by scanning a barcode or manually configuring the connection. When the user connects a tablet and smartphone, the connection creates a shared secret to use in the key agreement protocol. The shared secret contains 128 bits of randomness when the user scans a barcode and 32 bits of randomness when the user manually configures the connection. To discover the shared secret by eavesdropping during the key agreement protocol, a potentially malicious user must perform an online dictionary attack. The tablet is designed to prevent an online dictionary attack by permitting the potentially malicious user only one guess at the shared secret. If the guess is incorrect, the user must restart the pairing process, which then creates a new shared secret.

The BlackBerry Bridge uses the shared secret and ECDH with a 521-bit Random Curve to perform a password-authenticated key agreement and create an initial pairing key. The BlackBerry Bridge uses the initial pairing key to generate the BlackBerry Bridge pairing key. The BlackBerry Bridge uses the BlackBerry Bridge pairing key and AES-256 encryption to encrypt and decrypt data that is sent between the tablet and the smartphone. The BlackBerry Bridge uses the BlackBerry Bridge pairing key and SHA-256 to authenticate the connection between the tablet and smartphone.

## Generating an initial pairing key during the BlackBerry Bridge pairing process

The initial key establishment protocol uses ECDH with the 521-bit Random Curve and the SPEKE authentication method with the shared secret (the shared secret parameter is "s") to generate a long-term symmetric initial pairing key. The BlackBerry Bridge pairing key establishment protocol uses the initial pairing key to generate the BlackBerry Bridge pairing key.

If you delete a BlackBerry PlayBook tablet and BlackBerry smartphone connection in the Bluetooth settings on a tablet, the next time you connect the tablet to the smartphone, the BlackBerry Bridge pairing process uses the initial key establishment protocol to create a new initial pairing key.

The initial key establishment protocol negotiates algorithms and parameters that are used in subsequent BlackBerry Bridge pairing key exchanges, including the following:

- Elliptic curve used by future ECDH exchanges
- Encryption algorithm and hash algorithm used by the BlackBerry Bridge

The initial key establishment protocol is designed to negotiate so that the tablet and smartphone can use the 521-bit Random Curve, AES-256, and SHA-256 for application layer encryption and authentication, and SHA-512 for IT policy authentication.

#### Related topics

[Cryptosystem parameters that the BlackBerry Bridge pairing process uses to generate an initial pairing key, 11](#)

## Process flow: Generating an initial pairing key

1. The BlackBerry smartphone sends an initial echo of the value 0xC1F34151520CC9C2 to the BlackBerry PlayBook tablet to confirm that a Bluetooth connection to the tablet exists and to verify that the smartphone and tablet both understand the protocol.
2. The tablet receives the initial echo and replies with an echo transmission of the same value.
3. The smartphone receives the echo and replies to the tablet with a request for a list of supported algorithms.
4. The tablet creates a list of all the algorithms and elliptic curves that it supports and sends the list to the smartphone.
5. The smartphone searches the list for matches with algorithms and elliptic curves that the smartphone supports.
  - If a match is not available, the smartphone sends an error to the tablet and stops processing the list.
  - If a match exists, the smartphone begins the key establishment process by sending a pairing request using the selected algorithms, the selected elliptic curve, and a 64-byte seed to the tablet.
6. The tablet verifies the selected algorithms and elliptic curve.
7. The tablet performs the following calculation to select a short-term key (Y):
  - Selects random  $y$ ,  $1 < y < r - 1$
  - Calculates  $Y = yS$
8. The tablet sends Y to the smartphone.
9. The smartphone performs the following calculations to select a short-term key (X):
  - Selects random  $x$ ,  $1 < x < r - 1$
  - Calculates  $X = xS$
  - Calculates the initial pairing key (MK) using the following information:

Parameter	Value
K	$xY = xyS$
H1	SHA-512 (sent data packets)
H2	SHA-512 (received data packets)

- Calculates  $H = H1 + H2$
  - Calculates  $MK = \text{SHA-256}(H || K)$
10. The smartphone sends X to the tablet.
  11. The tablet calculates MK using the following information:

Parameter	Value
K	$yX = yxS$

Parameter	Value
H1	SHA-512 (sent data packets)
H2	SHA-512 (received data packets)
H	H1 + H2
MK	SHA-256 ( H    K )

The smartphone and the tablet share an initial pairing key.

#### Related topics

[Cryptosystem parameters that the BlackBerry Bridge pairing process uses to generate an initial pairing key, 11](#)

## Cryptosystem parameters that the BlackBerry Bridge pairing process uses to generate an initial pairing key

A BlackBerry PlayBook tablet and BlackBerry smartphone are designed to share the following cryptosystem parameters.

Parameter	Description
E(Fq)	This parameter is the NIST-approved 521-bit random elliptic curve over Fq, which has a cofactor of 1.  The initial key establishment protocol performs all mathematical operations in the group E(Fq).
Fq	This parameter is a finite field of prime order q.
P	This parameter is a point of E that generates a subgroup of E(Fq) of prime order r.
xR	This parameter is a representation of elliptic curve scalar multiplication, where x is the scalar and R is a point on E(Fq).
s	This parameter is the shared secret that appears on the tablet screen.  The shared secret must be known only to the authorized user of the smartphone and the tablet until the protocol completes.
S	This parameter is the shared secret converted to a point on E(Fq).

## Generating a BlackBerry Bridge pairing key during the BlackBerry Bridge pairing process

If the initial key establishment protocol process is successful, the BlackBerry PlayBook tablet and the BlackBerry smartphone share an initial pairing key. The tablet and smartphone use the initial pairing key to generate a BlackBerry Bridge pairing key. The BlackBerry Bridge pairing key is used to encrypt and authenticate the data that the tablet and smartphone send between each other.

The BlackBerry Bridge pairing key establishment protocol uses ECDH and the elliptic curve that the initial key establishment protocol negotiates. The ECDH algorithm provides PFS, which prevents the protocol from deriving previous or subsequent encryption keys. Each run of the BlackBerry Bridge pairing key establishment protocol

uses a unique, random, ephemeral key pair to create the new BlackBerry Bridge pairing key. The tablet discards the ephemeral key pair after generating the BlackBerry Bridge pairing key. Even if the ephemeral private keys from a specific protocol run of the ECDH algorithm are compromised, the BlackBerry Bridge pairing keys from other runs of the same protocol remain uncompromised.

## Process flow: Generating a BlackBerry Bridge pairing key

1. The BlackBerry smartphone sends an initial echo of the value 0xC1F34151520CC9C2 to the BlackBerry PlayBook tablet to confirm that a Bluetooth connection to the tablet exists and to verify that both the smartphone and tablet understand the protocol.
2. The tablet receives the initial echo and replies with an echo transmission of the same value.
3. The smartphone receives the echo and uses the algorithm that the initial key establishment protocol negotiated to send the selected algorithms, the selected elliptic curve, and a seed to the tablet.
4. The tablet performs the following calculation to select a short-term key (Y):
  - Selects random  $y$ ,  $1 < y < r - 1$
  - Calculates  $Y = yP$ , where  $P$  is a fixed point on the selected elliptic curve that generates a subgroup of prime order
5. The tablet sends  $Y$  to the smartphone.
6. The smartphone performs the following calculation to select a short-term key (X):
  - Selects random  $x$ ,  $1 < x < r - 1$
  - Calculates  $X = xP$
  - Calculates the BlackBerry Bridge pairing key (CK) using the following information:

Parameter	Value
K	$xY = xyP$
H1	SHA-512 (sent data packets)
H2	SHA-512 (received data packets)
H	$H1 + H2$
CK	SHA-256 ( MK    H    MK    K )

7. The smartphone sends  $X$  to the tablet.
8. The tablet calculates the BlackBerry Bridge pairing key (CK) using the following information:

Parameter	Value
K	$yX = yxP$
H1	SHA-512 (sent data packets)
H2	SHA-512 (received data packets)
H	$H1 + H2$
CK	SHA-256( MK    H    MK    K )

The smartphone and tablet share a BlackBerry Bridge pairing key.

## Connecting a tablet to a smartphone that is activated on the BlackBerry Enterprise Server or BlackBerry Internet Service

If a BlackBerry PlayBook tablet connects to a BlackBerry smartphone that was activated on a BlackBerry Enterprise Server, the data that the smartphone stores on the tablet is classified as work data. Work data is stored separately from personal data and is protected using the BlackBerry Bridge work key. During the BlackBerry Bridge pairing process, the tablet and smartphone share the BlackBerry Bridge work key. The BlackBerry Bridge work key encrypts the keys that encrypt and decrypt data that is stored on the tablet.

If a tablet connects to a smartphone that was activated on the BlackBerry Internet Service only, then the data that the smartphone stores on the tablet is considered personal data. Personal data that is stored on the tablet is not encrypted.

### Process flow: Generating a BlackBerry Bridge work key

1. During the BlackBerry Bridge pairing process, the BlackBerry smartphone generates a random 256-bit key and sends it to the BlackBerry PlayBook tablet.
2. The tablet uses SHA-512 to hash the key that it receives from the smartphone with the tablet system key to produce the BlackBerry Bridge work key.

The tablet system key is created during the manufacturing process and is the SHA-512 hash of a hardware ID and a 512-bit random key.

## Reconnecting a tablet to a smartphone

The BlackBerry PlayBook tablet is designed to reconnect automatically to a BlackBerry smartphone that it was previously connected to if the tablet did not delete the Bluetooth key or BlackBerry Bridge pairing key.

If you reconnect a tablet to a smartphone that requires a password, you must type the smartphone password on the tablet. The tablet and smartphone then perform the Bluetooth pairing process and BlackBerry Bridge pairing process. The smartphone uses the previous BlackBerry Bridge work key to decrypt the keys that were used to encrypt the data that the smartphone stored on the tablet when the tablet and smartphone were previously connected. The previous BlackBerry Bridge work key is stored in the memory of the smartphone.

## Deleting a tablet and smartphone connection

You can delete a BlackBerry PlayBook tablet and BlackBerry smartphone connection in the Bluetooth settings on a tablet. If you delete a tablet and smartphone connection on a tablet, the tablet performs the following actions:

- Closes all work applications
- Erases the Bluetooth key and BlackBerry Bridge pairing key from memory
- Deletes the work file system and erases the BlackBerry Bridge work key from memory

- Removes the Bluetooth connection with the smartphone

## Bluetooth security features on the tablet and smartphone

The following security features on the BlackBerry PlayBook tablet and BlackBerry smartphone enhance the existing protection for Bluetooth technology on the tablet and smartphone.

You can use the BlackBerry Enterprise Server to set IT policy rules in the Bluetooth policy group that are designed to control the behaviour of Bluetooth enabled smartphones. For more information about the IT policy rules, see the *BlackBerry Enterprise Server Policy Reference Guide*. For more information about configuring IT policy rules, see the *BlackBerry Enterprise Server Administration Guide*.

Security feature	Description
Limit paired Bluetooth enabled devices	<p>You can use the Disable Pairing IT policy rule to prevent a BlackBerry smartphone user from pairing a smartphone with a Bluetooth enabled device other than their tablet. After the smartphone pairs with the tablet, you can use this rule to prevent the smartphone from pairing with other Bluetooth enabled devices.</p> <p>You can also use application control policy rules to prevent third-party applications from accessing Bluetooth technology on smartphones.</p>
Limited use of serial port profiles	<p>The tablet uses the Bluetooth Serial Port Profile only, which allows you to use application control policy rules to turn off all the other profiles on the smartphone and prevent third-party applications from using the smartphone or tablet.</p> <p>Smartphones support only seven of the available Bluetooth profiles. The user can control pairing requests and the number of Bluetooth enabled devices that the user can pair with is limited.</p>
Use of Bluetooth pairing process to help prevent passive attack	<p>During the Bluetooth pairing process, the tablet uses a random key (unlike the hard-coded keys that headsets and other Bluetooth enabled smartphones use).</p> <p>A user starts the Bluetooth pairing process from the tablet or smartphone. If a message prompts the user to type a pairing password when the user did not start a pairing process, the user knows that another Bluetooth enabled device, which the user might not want to connect to, started the pairing process. The Bluetooth pairing process is designed to help prevent a passive attack where a potentially malicious user tries to search for the smartphone PIN or tablet PIN.</p>
Protection of the Bluetooth encryption key	<p>After the user resets the tablet, a smartphone can perform the Bluetooth pairing process and BlackBerry Bridge pairing process to reconnect to the tablet. If the smartphone was the last smartphone to connect to the</p>



Security feature	Description
	tablet before the user reset the tablet, the tablet restores the backed-up Bluetooth encryption key for the Bluetooth connection and opens the Bluetooth connection to the smartphone automatically.
Use of the discoverable mode option	<p>By default, the discoverable mode option on a smartphone and tablet is turned off. The smartphones are not visible to other Bluetooth enabled smartphones. The tablet or smartphone does not enter into discoverable mode unless the user turns on the discoverable mode option. Potentially malicious users cannot locate tablets or smartphones easily and compromise them.</p> <p>You can also set the Limit Discoverable Time IT policy rule to True to allow the user to turn on the discoverable mode option on the smartphone for 2 minutes only. The smartphone is discoverable for a very limited time to allow pairing with another Bluetooth enabled device.</p>
Control the Bluetooth wireless transceiver	<p>By default, the Bluetooth wireless transceiver on tablets and smartphones is turned off. When the Bluetooth wireless transceiver is turned off, Bluetooth technology is not operational on the tablet or smartphone, and the tablet or smartphone are not open to potentially malicious users using the Bluetooth technology.</p> <p>You can also use the Disable Bluetooth IT policy rule to control the Bluetooth wireless transceiver on smartphones.</p>
Protect data over a Bluetooth connection	The tablet and smartphone use AES-256 encryption to encrypt and decrypt data that is sent between each other. The tablet and smartphone use SHA-256 to authenticate the connection between each other.

## Using IT policy rules to manage Bluetooth technology on smartphones

You can use the BlackBerry Enterprise Server to set IT policy rules that are designed to control the behaviour of Bluetooth enabled BlackBerry smartphones. For example, you can configure the following IT policy rules in the Bluetooth policy group to manage Bluetooth settings on smartphones.

For more information about the IT policy rules, see the *BlackBerry Enterprise Server Policy Reference Guide*. For more information about configuring IT policy rules, see the *BlackBerry Enterprise Server Administration Guide*.

Action	IT policy rule
Opening a Bluetooth connection with a BlackBerry PlayBook tablet	<ul style="list-style-type: none"> <li>• Disable Bluetooth</li> <li>• Disable Pairing</li> </ul>
Turning on the discoverable mode option	<ul style="list-style-type: none"> <li>• Disable Discoverable Mode</li> </ul>

Action	IT policy rule
Setting the discoverable mode option to have no time limit	<ul style="list-style-type: none"> <li>Limit Discoverable Time</li> </ul>
Using the Bluetooth profiles that tablet and smartphone support	<ul style="list-style-type: none"> <li>Disable Advanced Audio Distribution Profile</li> <li>Disable Audio/Video Remote Control Profile</li> <li>Disable Dial-Up Networking</li> <li>Disable Handsfree Profile</li> <li>Disable Headset Profile</li> <li>Disable Message Access Profile</li> <li>Disable Serial Port Profile</li> <li>Disable SIM Access Profile</li> </ul>
Using wireless bypass over a Bluetooth connection	<ul style="list-style-type: none"> <li>Disable Wireless Bypass</li> </ul>
Exchanging files with supported Bluetooth OBEX devices	<ul style="list-style-type: none"> <li>Disable File Transfer</li> </ul>
Sending or receiving address book information over a Bluetooth connection	<ul style="list-style-type: none"> <li>Disable Address Book Transfer</li> </ul>
Making calls over a Bluetooth connection	<ul style="list-style-type: none"> <li>Allow Outgoing Calls</li> </ul>
Using Bluetooth encryption on all Bluetooth connections	<ul style="list-style-type: none"> <li>Require Encryption</li> </ul>
Flashing the LED light when the smartphone is connected to another Bluetooth enabled device	<ul style="list-style-type: none"> <li>Require LED Connection Indicator</li> </ul>
Prompting users to type their smartphone passwords to turn on Bluetooth support	<ul style="list-style-type: none"> <li>Require Password for Enabling Bluetooth Support</li> </ul>
Prompting users to type their smartphone passwords to turn on discoverable mode	<ul style="list-style-type: none"> <li>Require Password for Discoverable Mode</li> </ul>

## Specifying Bluetooth connections that third-party applications can access

You can use application control policy rules to limit the use of Bluetooth technology and the Bluetooth profiles to specific, permitted third-party applications. You can use the BlackBerry Enterprise Server to configure application control policy rules to control which applications can access resources on the BlackBerry smartphone. For example, you can use application control policy rules to make all Bluetooth profiles unavailable for applications by default and to turn on the Bluetooth Serial Port Profile for the BlackBerry PlayBook tablet driver only. If you configure these settings, only specific applications are allowed to use the tablet driver.

The following table lists the application control policy rules and the result that you can achieve by configuring them.

Action	Application control policy rule
Permit or prevent a BlackBerry smartphone user from downloading third-party applications	<ul style="list-style-type: none"> <li>Disposition</li> </ul>
Specify the features (for example, the email application, the phone application, and the smartphone key store) that third-party applications can access	<ul style="list-style-type: none"> <li>Is Access to the Email API Allowed</li> <li>Is Access to the Phone API Allowed</li> <li>Is Access to the Handheld Key Store Allowed</li> <li>Is Access to the PIM API Allowed</li> <li>Is Access to the Screen, Microphone, and Video Capturing APIs</li> </ul>
Specify the types of connections that a third-party application can open (for example, opening network connections inside the firewall)	<ul style="list-style-type: none"> <li>Are External Network Connections Allowed</li> <li>Are Internal Network Connections Allowed</li> <li>Are Local Connections Allowed</li> </ul>

## Bluetooth profiles that the tablet supports

A BlackBerry PlayBook tablet uses Bluetooth profiles to communicate with BlackBerry smartphones and other types of Bluetooth enabled devices. The tablet supports the following Bluetooth profiles.

Profile	Description
Dial-up Networking (DUN)	The tablet uses this profile to connect to a tethered smartphone or other Internet-enabled device to access the Internet connection.
Human Interface Device (HID)	The tablet uses this profile to connect to a wireless keyboard or mouse.
Serial Port Profile (SPP)	The tablet uses this profile to connect to a smartphone through the BlackBerry Bridge.

# Securing tablets in your organization's environment for work use

5

Your organization can permit a BlackBerry PlayBook tablet user to connect a BlackBerry PlayBook tablet to a BlackBerry smartphone that is associated with a BlackBerry Enterprise Server and use the tablet for work purposes. Security features on the tablet can control how the tablet helps protect your organization's data and applications. The security features provide the following benefits:

- Control access to your organization's data on the tablet
- Help prevent your organization's data from being compromised
- Provide one experience for users, regardless of whether they access work data or personal data
- Make your organization's data on the tablet inaccessible when the connection to the smartphone closes

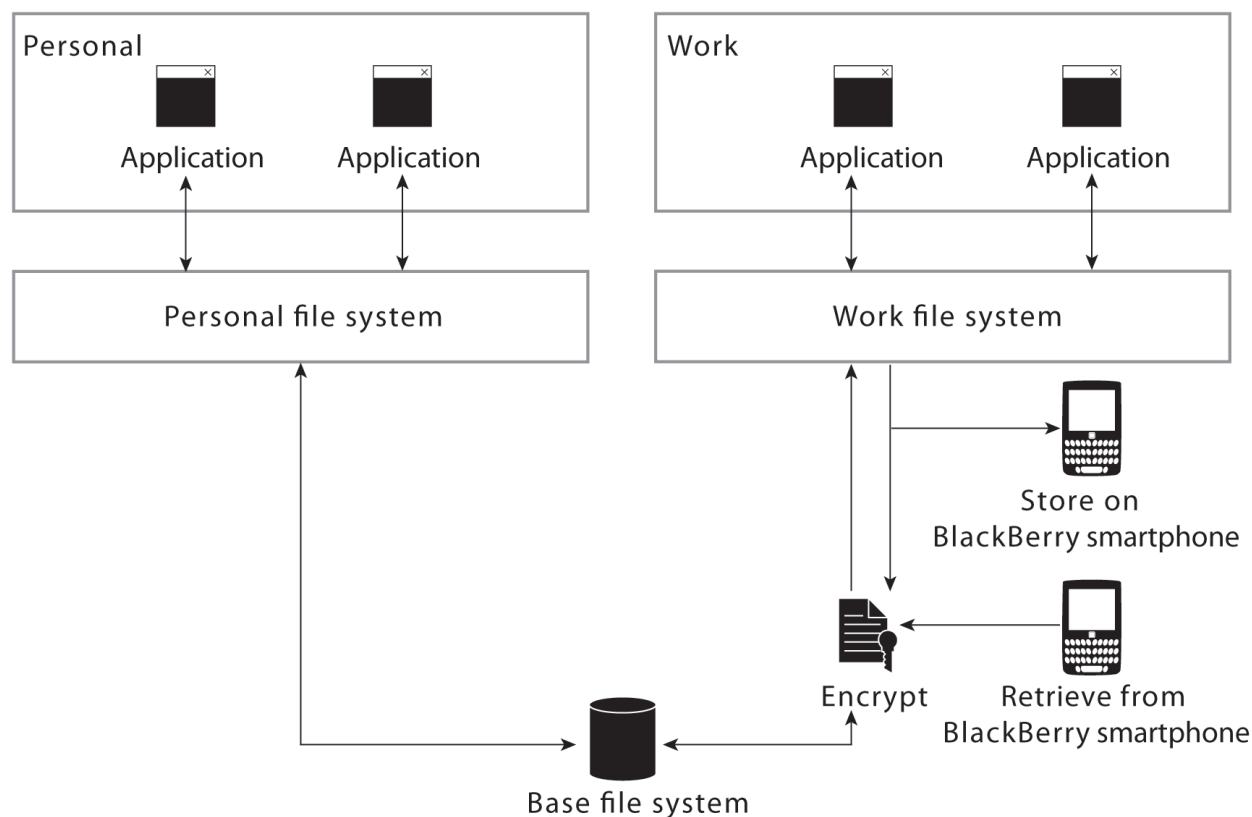
These security features are not available when the user connects the tablet to a smartphone that is activated on the BlackBerry Internet Service. If the user connects the tablet to a smartphone that is activated on a BlackBerry Internet Service, the tablet specifies that all data and applications on the tablet are for personal use.

## How a tablet distinguishes between work data and personal data

Work data consists of all email messages, calendar entries, and attachments that a BlackBerry Enterprise Server and a BlackBerry smartphone send between each other and any data that is associated with work applications (for example, metadata). If a BlackBerry PlayBook tablet user connects a BlackBerry PlayBook tablet to a smartphone that is activated on a BlackBerry Enterprise Server, the tablet permits the user to view and interact with work data. A media card must be inserted in the smartphone to permit the user to interact with work data (for example, open attachments on the tablet or save updates to files).

To help protect work data, the tablet automatically creates a work file system in the BlackBerry Tablet OS that isolates work data and work applications from personal data and personal applications. The tablet encrypts the work file system using XTS-AES-256 encryption.

The tablet is designed to prevent the user from seeing or accessing the work file system directly on the tablet by clicking on an icon for the work file system. The tablet is designed to allow the user to access work data and work applications when the user connects the tablet to the smartphone using the BlackBerry Bridge. When the user connects the tablet to the smartphone, the tablet displays the BlackBerry Bridge panel. The user can use the BlackBerry Bridge to access work applications.



## How a tablet protects work data

The BlackBerry PlayBook tablet is designed to prevent work data from persisting in flash memory in cleartext form.

When the tablet is connected to a BlackBerry smartphone, the tablet caches work data locally in the work file system. The tablet encrypts the work data using XTS-AES-256 before it caches the work data.

The tablet uses a randomly generated 512-bit file encryption key to encrypt the contents of a file. The file encryption process creates a security record for the encrypted file that consists of a 512-bit random salt, the file encryption key, and several attributes of the file. The tablet encrypts the file security record using the domain key, which is a 512-bit randomly generated key.

The tablet uses the domain key to encrypt all file security records in the work file system. The domain key is stored in a security record that is similar to the file security record. The domain security record is encrypted using the BlackBerry Bridge work key. The BlackBerry Bridge work key is stored in RAM and is never written to persistent storage on the tablet. Only the smartphone stores the BlackBerry Bridge work key in persistent memory.

The tablet does not encrypt the BlackBerry PlayBook tablet user's personal data.

## What happens when a user updates or creates work files on a tablet

The BlackBerry PlayBook tablet helps protect work data when a BlackBerry PlayBook tablet user performs the following actions:

Action	Description
Open a file to view or update it	<p>When the user opens a work file such as an email message or an attachment, the tablet starts the application in work mode.</p> <p>When the user updates a work file using Documents To Go, the tablet automatically saves the changes that the user makes. The tablet queues any work file updates for back up to the media card that is inserted in the BlackBerry smartphone and sends the updates to the smartphone frequently.</p>
Copy and paste data to a work file	<p>The tablet does not permit the user to move data from the work file system to the personal file system. The user cannot cut, copy, or paste data from a work file to a personal file.</p> <p>The tablet does permit a user to move data from the personal file system to the work file system. The user cannot cut, copy, or paste personal data into a work file. The user can attach a personal file to a work email message or work calendar entry.</p>

## How a tablet controls whether an application is a work application or a personal application

Applications on a BlackBerry PlayBook tablet can run in work mode, personal mode, or both, depending on the metadata that is associated with them. By default, all applications on the tablet run in personal mode. After a BlackBerry PlayBook tablet user connects a tablet to a BlackBerry smartphone that is activated on a BlackBerry Enterprise Server, an application can run in work mode.

Some applications such as Documents To Go can run in work mode and personal mode. If the user opens an attachment in a work email message or work calendar entry, Documents To Go runs in work mode. You cannot add applications to a tablet and classify them as work applications.

When applications are running, work applications and personal applications cannot share files or memory, or synchronize objects with each other.

## Determining which applications are work applications or personal applications

The BlackBerry PlayBook tablet permits the following applications to run in work mode only:

- BlackBerry Messenger

- Bridge Browser

The tablet permits the following applications to run in work mode or personal mode:

- BlackBerry Bridge
- Photo viewer
- Media player
- Email application
- Calendar application
- Contacts application
- Document viewers such as Documents To Go or Adobe Reader
- Files application

The tablet permits the following applications to run in personal mode only:

- Applications that a BlackBerry PlayBook tablet user downloads and installs on the tablet
- Browser
- Maps application
- YouTube
- Facebook
- Twitter

## Comparison of work applications and personal applications

Work applications	Personal applications
Work applications can access work data; they can view but not change personal data.	Personal applications cannot access work data but they can access personal data.
Work applications can attach personal files to work email messages or work calendar entries (for example, a BlackBerry PlayBook tablet user can attach a picture that the user took using the BlackBerry PlayBook tablet camera to a work email message).	Personal applications cannot attach work files to personal email messages or personal calendar entries.
Work applications can access your organization's network using the BlackBerry Bridge.	Personal applications cannot access your organization's network using the BlackBerry Bridge.
A user can access work applications only when the tablet is connected to a BlackBerry smartphone (for example, if a user opens a .pdf file attachment in a work email message, the Adobe Reader work application can open the file).	A user can access personal applications regardless of whether the tablet is connected to the smartphone.
The tablet upgrades work applications when the BlackBerry Tablet OS is upgraded.	The tablet upgrades preinstalled personal applications when the BlackBerry Tablet OS is upgraded and the user can upgrade the personal applications that the user installs at any time.

## Access rights for work data and personal data that the BlackBerry Tablet OS grants to applications

The following table displays the access rights that applications have to work data or personal data.

Access right	Work application A	Work application B	Personal application C	Personal application D
Access a work file that a work application saves	Read-write access	Read-write access	No access	No access
Access a personal file that a personal application saves	Read-only	Read-only	Read-write access	Read-write access
Access the private data of Work application A	Read-write access	No access	No access	No access
Access the private data of Work application B	No access	Read-write access	No access	No access

## Using the Bridge Browser

If the Allow Browser IT policy rule is set to Yes and you configure the BlackBerry MDS Connection Service to connect a BlackBerry smartphone to the Internet and intranet, a BlackBerry PlayBook tablet that is connected to the smartphone can use the Bridge Browser to browse the Internet or intranet in work mode.

The Bridge Browser does not use the Wi-Fi connection to connect to the Internet or intranet. Instead, the Bridge Browser connects to the Internet or your organization's intranet using the smartphone's connection to the BlackBerry MDS Connection Service. The tablet encrypts any cached data that is stored on the tablet using randomly generated file encryption keys that are encrypted using the BlackBerry Bridge work key.

A BlackBerry PlayBook tablet user can access the Bridge Browser on the tablet by clicking the Bridge Browser icon on the BlackBerry Bridge panel. By default, when a user clicks a link in a work application (for example, a link in work email messages, work calendar entries, the contact list, tasks, memos, or BlackBerry Messenger messages), the tablet opens the link in personal mode using the browser. The tablet opens the link in work mode using the Bridge Browser if any of the following conditions exist:

- The link is to an address that is not routable on the public Internet, such as a private IP address as specified in RFC 1918 or an address that does not contain periods.
- The link is to a domain that is included in the MDS Browser Domains IT policy rule that applies to the smartphone that the tablet is connected to.
- The Wi-Fi Internet Access Path IT policy rule that applies to the smartphone that the tablet is connected to is set to "Access through BlackBerry MDS Connection Service".



- No Wi-Fi connection is available.

To open a link using the Bridge Browser, the tablet must be able to access the BlackBerry MDS Connection Service.

## Running the Files application in work mode

When a BlackBerry PlayBook tablet runs the Files application in work mode, a BlackBerry PlayBook tablet user can access the files that are stored on the media card that is inserted in the BlackBerry smartphone. The tablet opens the files using work applications and classifies the files as work data.

If the user opens and updates files that are stored on the media card, the tablet does not store any content locally, and encrypts any data it caches using XTS-AES-256 encryption.

## Taking screen shots on a tablet

The BlackBerry PlayBook tablet allows a BlackBerry PlayBook tablet user to take a screen shot of the current screen by holding the Volume Up key and Volume Down key at the same time.

The user can take screen shots when the tablet is running in personal mode only. The tablet saves screen shots in the Camera application and displays them in the Photo viewer application. The tablet treats screen shots as personal files.

The tablet prevents the user from taking screen shots of work data when a work application is open and unlocked.

## When a tablet prevents a user from accessing work data or work applications

A BlackBerry PlayBook tablet user can access work data and work applications when the BlackBerry PlayBook tablet is connected to a BlackBerry smartphone. The tablet does not permit the user to access work data or work applications when any of the following events occur:

- User stops interacting with the tablet for a time period that is longer than the smartphone-timeout period
- Tablet resets or loses power
- Bluetooth connection to the smartphone closes
- You or the user deletes all smartphone data

If one of these events occurs, the tablet locks all work applications and deletes the BlackBerry Bridge work key so that local cache data is not recoverable.

If the user connects the tablet to another smartphone or the user types the smartphone password incorrectly more times than the Set Maximum Password Attempts IT policy rule or the password option on the smartphone permits, the tablet performs the following actions:

- Deletes the work file system
- Closes all work applications
- Deletes the BlackBerry Bridge work key from the tablet memory

Personal data and personal applications are not affected by the actions that the tablet performs to prevent the user from accessing work data and work applications.

When the tablet reconnects to the smartphone, the tablet restores the user's access to the work data and work applications.

## Connecting a tablet to an enterprise Wi-Fi network

The first time that a BlackBerry PlayBook tablet and a BlackBerry smartphone connect to each other, the tablet retrieves the Wi-Fi profiles that the BlackBerry smartphone user configured on the smartphone, but the tablet does not retrieve the Wi-Fi profiles that administrators assigned to the smartphone. The tablet also does not retrieve any client certificates that the Wi-Fi profiles require; however, the tablet can retrieve root certificates when the tablet and smartphone connect for the first time.

The tablet retrieves Wi-Fi profiles using the encrypted and authenticated connection between the tablet and the smartphone. While the tablet and the smartphone are connected, the tablet can use the Wi-Fi profiles to access BlackBerry services over a Wi-Fi network. The tablet uses the same method and security to access the Wi-Fi network that the smartphone uses.

If the user wants to use a Wi-Fi profile on the tablet and the Wi-Fi profile requires a client certificate, the user must connect the tablet to a computer and import the certificate on the tablet.

If your organization's environment includes VPNs, you can configure the tablet to authenticate with a VPN connector so that the tablet can access a Wi-Fi network.

For more information about how Wi-Fi enabled BlackBerry smartphones connect to an enterprise Wi-Fi network, see "Wi-Fi enabled BlackBerry smartphones" in the *BlackBerry Enterprise Server Security Technical Overview*.

## IT policy rules that apply to a tablet

The following IT policy rules apply to a BlackBerry PlayBook tablet:

IT policy group	IT policy rule
Companion devices	<ul style="list-style-type: none"> <li>BlackBerry PlayBook Log Submission</li> </ul>
BlackBerry Bridge	<ul style="list-style-type: none"> <li>Enable BlackBerry Bridge</li> </ul>

A BlackBerry smartphone that is running specific bundles of BlackBerry 6 can distinguish between work data and personal data after you configure specific IT policy rules. The IT policy rules that you can configure for the smartphone do not apply to the tablet. The tablet can automatically distinguish between work data and personal data if a smartphone that is activated on a BlackBerry Enterprise Server connects to the tablet and treats all data that the smartphone sends as work data. For more information about configuring a smartphone to distinguish what is work data and personal data, see the *Securing Devices for Personal Use and Work Use Security Note*.

# The BlackBerry Tablet OS

## 6

The BlackBerry Tablet OS is the microkernel operating system of the BlackBerry PlayBook tablet. Microkernel operating systems implement the minimum amount of software in the kernel and run other processes in the user space that is outside of the kernel.

Microkernel operating systems are designed to contain less code in the kernel than other operating systems. The reduced amount of code helps the kernel to avoid the vulnerabilities that are associated with complex code and to make verification easier. Verification is the process of evaluating a system for programming errors. Many of the processes that run in the kernel in a conventional operating system run in the user space of the BlackBerry Tablet OS.

The BlackBerry Tablet OS is designed to be tamper resistant. The kernel performs an integrity test when the BlackBerry Tablet OS starts and if the integrity test detects damage to the kernel, the tablet does not start.

The BlackBerry Tablet OS is designed to be resilient. The kernel is designed isolate a process in its user space if it stops responding and to restart the process without negatively affecting other processes. In addition, the kernel uses adaptive partitioning to allocate resources to specific processes during overload conditions.

The BlackBerry Tablet OS is designed to be highly secure. The kernel validates requests for resources and an authorization manager controls how applications access the capabilities of the tablet.

## The tablet file system

The BlackBerry PlayBook tablet file system runs outside of the kernel and is designed to keep work data highly secure and separate from personal data. The BlackBerry Tablet OS divides the file system into three areas:

1. Base file system
2. Personal file system
3. Work file system

The base file system is read-only and contains system files. Because the base file system is read-only, the BlackBerry Tablet OS can check the integrity of the base file system and mitigate the damage that a potentially malicious user who changes the file system can cause.

The personal file system contains the applications that run in personal mode and personal application data. Applications that a BlackBerry PlayBook tablet user installs on the tablet are located in the personal file system.

The work file system contains the applications that run in work mode and work application data. The tablet encrypts the work file system. The key that the tablet uses to decrypt the work file system is stored on the BlackBerry smartphone that is connected to the tablet to prevent access to work data when the tablet and the smartphone are not connected.

## How the BlackBerry Tablet OS uses sandboxing to protect application data

The BlackBerry Tablet OS uses a security mechanism called sandboxing to separate and restrict the capabilities and permissions of applications that run on the BlackBerry PlayBook tablet. Each application process runs in its own sandbox, which is a virtual container that consists of the memory and the part of the file system that the application process has access to at a specific time.

The BlackBerry Tablet OS evaluates the requests that an application's process makes for memory outside of its sandbox. If a process tries to access memory outside of its sandbox without approval from the BlackBerry Tablet OS, the BlackBerry Tablet OS is designed to end the process, reclaim all of the memory that the process is using, and restart the process without negatively affecting other processes.

When the BlackBerry Tablet OS is installed, it assigns a unique group ID to each application. Two applications cannot share the same group ID, and the BlackBerry Tablet OS does not reuse group IDs after applications are removed. An application's group ID remains the same when the application is upgraded.

By default, each application stores its private data in its own data directory. The BlackBerry Tablet OS prevents applications from accessing file system locations that are not associated with the application's group ID.

An application can also store and access data in a shared directory, which is a data directory that is available to any application that has access to it. When an application that wants to store or access files in the shared directory starts for the first time, the application prompts the user to grant access.

## How the BlackBerry Tablet OS manages the resources on the tablet

The BlackBerry Tablet OS is designed to manage the BlackBerry PlayBook tablet resources so that an application cannot take resources from another application. The BlackBerry Tablet OS uses adaptive partitioning to reallocate unused resources to applications during typical operating conditions and enhance the availability of the resources to specific applications during peak operating conditions.

## How the tablet manages permissions for applications

The authorization manager is the part of the BlackBerry Tablet OS that evaluates requests from applications to access the capabilities of the BlackBerry PlayBook tablet. Capabilities include taking a photograph and recording audio. The BlackBerry Tablet OS invokes the authorization manager when an application starts to set the permissions for the capabilities that the application uses. When an application starts, it might prompt the BlackBerry PlayBook tablet user to allow access to a capability. The authorization manager can store permission that the user grants access to and apply the permission the next time that the application starts.

## How the tablet verifies the boot ROM code

The BlackBerry PlayBook tablet uses an authentication method that is designed to verify that the boot ROM code is permitted to run on the tablet. The manufacturing process installs the boot ROM code in the memory on the tablet and the RIM signing authority system uses an RSA public key to sign the boot ROM code. The tablet stores information that it can use to verify the digital signature of the boot ROM code.

When a BlackBerry PlayBook tablet user turns on a tablet, it runs internal ROM code that reads the boot ROM from memory and verifies the digital signature of the boot ROM code using the RSA public key. If the verification process completes, the boot ROM is permitted to run on the tablet. If the verification process cannot complete, the tablet stops running.

## How the tablet manages software updates

Applications that a BlackBerry PlayBook tablet user installs on the BlackBerry PlayBook tablet are located in the personal file system and the applications can only operate in personal mode. Only the user can update applications that operate in personal mode; the user cannot change the applications to make them operate in work mode. An administrator cannot update applications that operate in personal mode.

## Protecting user information

7

The BlackBerry PlayBook tablet is designed to allow a BlackBerry PlayBook tablet user to delete all user information and application data from the tablet memory.

The user can use the Security Wipe option in the Security settings on the tablet to delete all data from the personal file system. If a user deletes all data from the personal file system, all of the user's personal information is permanently removed from the tablet and other users cannot access the personal information if they use the tablet in the future.

## Using the smartphone password to help protect access to the tablet

After a BlackBerry PlayBook tablet user connects the BlackBerry PlayBook tablet to a BlackBerry smartphone that requires a password, the tablet automatically requires that the user provides the smartphone password when the tablet accesses any smartphone data. Smartphone data can include email messages, calendar entries, tasks, memos, BlackBerry Messenger messages, intranet content, files, or attachments that the user views on the tablet.

The tablet requires that the user provide the smartphone password regardless of whether the applications are running in work mode or personal mode.

All password features that apply to the smartphone are extended to the tablet. For example, the tablet uses the same security timeout as the smartphone that it is connected to.

If you permit a user to connect a tablet to a smartphone that is associated with a BlackBerry Enterprise Server, you can use IT policy rules to control the password security level on the smartphone and tablet. If you send the Specify new device password and lock device IT administration command to the smartphone, the tablet requires the user to provide the new smartphone password when the tablet accesses any smartphone data. For more information about IT policy rules and configuring smartphone passwords, see the *BlackBerry Enterprise Server Security Technical Overview*.

## Using the tablet password

The BlackBerry PlayBook tablet permits the BlackBerry PlayBook tablet user to set a tablet password. If the user sets a tablet password, the user must provide the password to log in to the tablet. The user can configure the tablet password and timeout options using the Password option in the Security settings on the tablet.

If the user types the tablet password incorrectly more than 10 times, the tablet deletes all data from the personal file system.

For more information about setting the tablet password, see the tablet help.

### Related topics

[Deleting data from the tablet memory, 29](#)

## Deleting data from the tablet memory

A BlackBerry PlayBook tablet user can permanently delete the following data from the BlackBerry PlayBook tablet memory using the Security Wipe option in the Security settings on the tablet. The tablet also deletes the following data if the user types the tablet password incorrectly more than 10 times.

- Personal files
- Personal videos, music, photos, and voice notes
- Personal applications that a user downloaded and installed on the tablet
- Personal data that is associated with personal applications on the tablet (for example, game scores, saved maps, and the browser cache)
- Wi-Fi profiles
- VPN profiles
- Tablet password

If the tablet is connected to a BlackBerry smartphone when the user uses the Security Wipe option to delete tablet data, the tablet also deletes the following data:

- Encrypted work data from the local cache on the tablet
- BlackBerry Bridge work key from the tablet memory
- Bluetooth pairing with the smartphone
- Bluetooth key and BlackBerry Bridge pairing key from the tablet memory

### Related topics

[Securing tablets in your organization's environment for work use, 18](#)

## What happens to work data on the tablet when it is connected to a smartphone that deletes all smartphone data

When a BlackBerry smartphone that is connected to a BlackBerry PlayBook tablet deletes all smartphone data, the smartphone deletes its copy of the BlackBerry Bridge work key and the Bluetooth connection to the tablet closes. The tablet locks all work applications and deletes its copy of the BlackBerry Bridge work key, which is stored only in RAM.

The tablet encrypts all work data with keys that are encrypted using the BlackBerry Bridge work key. When the Bluetooth connection closes and the smartphone and tablet delete their copies of the BlackBerry Bridge work key, the keys that encrypt the work data cannot be decrypted so the work data cannot be decrypted.

The smartphone is designed to delete all smartphone data from memory when any of the following events occurs:

- The user clicks Security Wipe in the security options on the smartphone.
- The user types the smartphone password incorrectly more times than the Set Maximum Password Attempts IT policy rule or the password option on the smartphone permits. The default value is ten attempts.
- The user runs the application loader tool and types the smartphone password incorrectly more times than the Set Maximum Password Attempts IT policy rule permits.

- The user uses the application loader tool to delete all user data and application data on the smartphone. The user can choose not to delete the smartphone applications.
- You send the Delete all device data and remove device IT administration command to the smartphone with or without a delay (in hours), to the smartphone. The maximum delay is 168 hours (7 days).
- You click the Remove user data from current device option in the BlackBerry Administration Service after you connect the smartphone to the BlackBerry Administration Service. This option deletes all data and applications from the smartphone even if service books do not exist on the smartphone.



# Cryptographic algorithms, codes, protocols, and APIs that the tablet supports

8

The BlackBerry PlayBook tablet supports the following types of cryptographic algorithms, codes, protocols, and APIs:

- Symmetric encryption algorithms
- Asymmetric encryption algorithms
- Hash algorithms
- Message authentication codes
- Signature scheme algorithms
- Key agreement scheme algorithms
- Cryptographic protocols
- Cryptographic APIs
- VPN cryptographic support
- Wi-Fi cryptographic support

## Symmetric encryption algorithms

Algorithm	Key length (in bits)	Modes
AES	128, 192, and 256	CBC, ECB, CTR
AES	512	XTS
Blowfish	40 to 448	CBC, CFB, ECB, OFB
Camellia	128 to 256	CBC
Camellia	256	ECB
CAST	40 to 128	CBC, CFB, ECB, OFB
CCMP	128	—
DES	56	CBC, CFB, ECB, EDE, OFB
RC4	128	—
Skipjack	80	—
Triple DES	168	EDE, CBC, CFB, OFB
Twofish	128 to 256	CBC

## Asymmetric encryption algorithms

Algorithm	Key length (in bits)
ECC	163, 192, 256, 283, 384, and 512
RSA	a minimum of 512

## Hash algorithms

Algorithm	Digest size (in bits)
MD2	128
MD4	128
MD5	128
MDC-2	128
RIPEMD-160	160
SHA-1	160
SHA-2	224, 256, 384, 512

## Message authentication codes

Codes	Use with	Key length (in bits)
AES-XCBC-MAC	—	128
HMAC	MD5	128
HMAC	SHA-1	160
HMAC	RIPEMD-160	160

## Signature scheme algorithms

Algorithm	Key length (in bits)	Type
ECDSA	521	Elliptic Curve (curve secp521r1)
RSA	512, 1024, 2048, and 4096	Integer factorization

## Key agreement schemes

Scheme	Key length (in bits)	Type
RSA	512, 1024, 2048, and 4096	Integer factorization
Diffie-Hellman	Maximum of 1024	Discrete logarithm
ECDH	256	(Elliptic curve) discrete logarithm
EC-SPEKE	256	(Elliptic curve) discrete logarithm
ECMQV	256	(Elliptic curve) discrete logarithm

## Cryptographic protocols

- SSL
- TLS
- IPSec
- WEP
- WPA
- WPA2

## Cryptographic APIs

- libeap
- libipsec
- PF-Key
- Security Builder® Crypto™-C
- OpenSSL

## VPN cryptographic support

Protocol	Authentication types	IKE IPSec DH group	IKE IPSec cipher	IKE IPSec hash	IKE PRF
IKE	PSK, PKI, XAUTH-PSK, XAUTH-PKI	1, 2, 5, 7 to 26	DES (56-bit key), Triple DES (168-bit key), AES (128, 192, 256-bit keys)	AES-XCBC, MD5, SHA-1, SHA-256, SHA-384, SHA-512	HMAC
IKEv2	PSK, PKI, EAP-TLS, EAP-MS-CHAPv2	1, 2, 5, 7 to 26	DES (56-bit key), Triple DES (168-bit key), AES (128, 192, 256-bit key)	AES-XCBC, MD5, SHA-1, SHA-256, SHA-384, SHA-512	AES-XCBC, HMAC-MD5, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512

## Wi-Fi cryptographic support

Cryptographic protocol	Encryption protocol	EAP outer method	EAP inner method
WEP	RC4	—	—
WPA	TKIP	PEAP, EAP-TTLS, EAP-FAST, EAP-TLS	MSCHAPv2, EAP-GTC

<b>Cryptographic protocol</b>	<b>Encryption protocol</b>	<b>EAP outer method</b>	<b>EAP inner method</b>
WPA2	TKIP, CCMP (AES)	PEAP, EAP-TTLS, EAP-FAST, EAP-TLS	MSCHAPv2, EAP-GTC

# Attacks that the BlackBerry Bridge pairing process is designed to prevent

The BlackBerry Bridge pairing process is designed to help protect the connection between the BlackBerry PlayBook tablet and BlackBerry smartphone from the following types of attacks:

- Brute-force attack
- Online dictionary attack
- Eavesdropping
- Impersonating a smartphone
- Man-in-the-middle attack
- Small subgroup attack

## Brute-force attack

A brute-force attack occurs when a potentially malicious user tries all possible keys and guesses what the encryption key is. The BlackBerry Bridge pairing key is 256 bits long, which makes a brute-force attack computationally infeasible.

## Online dictionary attack

An online dictionary attack occurs when a potentially malicious user uses feedback to determine the correct password. For example, during the key agreement protocol, the potentially malicious user might try to guess the shared secret between the BlackBerry PlayBook tablet and BlackBerry smartphone.

The ECDH protocol permits the potentially malicious user to only guess the shared secret one time. If the guess is incorrect, the BlackBerry PlayBook tablet user must restart the pairing process, which creates a new shared secret before the potentially malicious user guesses again.

## Eavesdropping

An eavesdropping event occurs when a potentially malicious user monitors the communication that occurs between a BlackBerry PlayBook tablet and BlackBerry smartphone. The goal of the potentially malicious user is to determine the BlackBerry Bridge pairing key on the tablet and smartphone and then use the key to decrypt the data that the tablet and smartphone send between each other.

Because the BlackBerry Bridge uses the ECDH algorithm to generate the BlackBerry Bridge pairing key, a potentially malicious user must solve the ECDH problem to compute the key. Solving this problem is equivalent to solving the DH problem, which is considered computationally infeasible.

## Impersonating a smartphone

An impersonation event against a BlackBerry PlayBook tablet occurs when a potentially malicious user sends data to a tablet so that the tablet believes it is communicating with a BlackBerry smartphone. A potentially malicious user must know the BlackBerry Bridge pairing key to impersonate a smartphone.

Because the BlackBerry Bridge uses the ECDH algorithm to generate the BlackBerry Bridge pairing key, a potentially malicious user must solve the ECDH problem to compute the key. Solving this problem is equivalent to solving the DH problem, which is considered computationally infeasible.

## Man-in-the-middle attack

A man-in-the-middle attack occurs when a potentially malicious user intercepts and changes messages that are in transit between a BlackBerry PlayBook tablet and BlackBerry smartphone. When a potentially malicious user makes a successful man-in-the-middle attack, the BlackBerry PlayBook tablet user does not know that the user is monitoring and changing data traffic.

For a man-in-the-middle attack to occur, the potentially malicious user must link the flow of data between the tablet and the smartphone permanently, not just for the duration of the key agreement protocol. For a potentially malicious user to start a man-in-the-middle attack, the potentially malicious user must know either the BlackBerry Bridge pairing key or the shared secret between the tablet and smartphone.

Because BlackBerry Bridge uses the ECDH algorithm to generate the BlackBerry Bridge pairing key, a potentially malicious user must solve the ECDH problem to compute the key. Solving this problem is equivalent to solving the DH problem, which is considered computationally infeasible.

The ECDH protocol only permits the potentially malicious user to guess the shared secret one time. If the guess is incorrect, the BlackBerry PlayBook tablet user must restart the pairing process, which creates a new shared secret before the potentially malicious user can guess again.

## Small subgroup attack

A small subgroup attack occurs when a potentially malicious user tries to limit the key agreement protocol between the BlackBerry PlayBook tablet and BlackBerry smartphone to generate BlackBerry Bridge pairing keys from a small subset of keys. If the BlackBerry Bridge pairing key is generated from a small subset of keys, it is easier for the potentially malicious user to guess the BlackBerry Bridge pairing key.

The BlackBerry PlayBook security protocols are designed to use ECDH operations to prevent a small subgroup attack.

# Glossary

10

**AES**

Advanced Encryption Standard

**AES-CCMP**

Advanced Encryption Standard Counter Mode CBCMAC Protocol

**AES-XCBC-MAC**

Advanced Encryption Standard extended cipher block chaining message authentication code

**API**

application programming interface

**CAST**

Carlisle Adams Stafford Tavares

**CBC**

cipher block chaining

**CFB**

cipher feedback

**CTR**

Counter

**DES**

Data Encryption Standard

**DH**

Diffie-Hellman

**EAP-FAST**

Extensible Authentication Protocol Flexible Authentication via Secure Tunneling

**EAP-GTC**

Extensible Authentication Protocol Generic Token Card

**EAP-TLS**

Extensible Authentication Protocol Transport Layer Security

**EAP-TTLS**

Extensible Authentication Protocol Tunneled Transport Layer Security

**ECB**

electronic code book

**ECC**

Elliptic Curve Cryptography

**ECDH**

Elliptic Curve Diffie-Hellman

**ECDSA**

Elliptic Curve Digital Signature Algorithm

**EDE**

Encryption-Decryption-Encryption

**HMAC**

keyed-hash message authentication code

**HTML**

Hypertext Markup Language

**IKE**

Internet Key Exchange

**IPsec**

Internet Protocol Security

**IT policy**

An IT policy consists of various IT policy rules that control the security features and behavior of BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerryWeb Desktop Manager.

**IT policy rule**

An IT policy rule permits you to customize and control the actions that BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager can perform.

**MD**

Message Digest Algorithm

**MDC**

Modification Detection Code

**MS-CHAP**

Microsoft Challenge Handshake Authentication Protocol



**OFB**

output feedback

**PEAP**

Protected Extensible Authentication Protocol

**PFS**

Perfect Forward Secrecy

**PKI**

Public Key Infrastructure

**PSK**

pre-shared key

**RACE**

Research and Development in Advanced Communications Technologies in Europe

**RC**

Rivest's Cipher

**RFC**

Request for Comments

**RIM signing authority system**

The RIM signing authority system is used by third-party developers to cryptographically sign their applications.

**RIPEMD**

RACE Integrity Primitives Evaluation Message Digest

**SHA**

Secure Hash Algorithm

**SSL**

Secure Sockets Layer

**TCP**

Transmission Control Protocol

**TCP MD5**

Transmission Control Protocol message digest algorithm 5

**TKIP**

Temporal Key Integrity Protocol

**TLS**

Transport Layer Security

**Triple DES**

Triple Data Encryption Standard

**VPN**

virtual private network

**WAP**

Wireless Application Protocol

**WEP**

Wired Equivalent Privacy

**WPA**

Wi-Fi Protected Access

**XEX**

Xor-Encrypt-Xor

**XTS**

XEX-based Tweaked CodeBook mode with CipherText Stealing

# Provide feedback

11

To provide feedback on this deliverable, visit [www.blackberry.com/docsfeedback](http://www.blackberry.com/docsfeedback).

## Legal notice

12

©2012 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

Adobe and Reader are trademarks of Adobe Systems Incorporated. Bluetooth is a trademark of Bluetooth SIG. Documents To Go is a trademark of Dataviz, Inc. Facebook is a trademark of Facebook, Inc. Mac and Mac OS are trademarks of Apple Inc. RSA is a trademark of RSA Security. Security Builder is a trademark of Certicom Corp. Twitter is a trademark of Twitter, Inc. Wi-Fi, WPA, and WPA2 are trademarks of the Wi-Fi Alliance. Windows and Windows Vista are trademarks of Microsoft Corporation. YouTube is a trademark of Google Inc. All other trademarks are the property of their respective owners.

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada