



# **Security Technical Overview**

## **BlackBerry Devices with Bluetooth Technology**



# Contents

<b>1 BlackBerry Enterprise Solution security</b>	<b>3</b>
<b>2 Bluetooth technology</b>	<b>5</b>
Bluetooth profiles	5
Bluetooth profiles that BlackBerry devices support	5
<b>3 Risks of using Bluetooth technology on wireless devices</b>	<b>7</b>
Bluejacking	7
Bluesnarfing	7
Bluebugging	8
<b>4 Managing Bluetooth enabled BlackBerry devices</b>	<b>9</b>
Bluetooth technology security measures on BlackBerry devices	9
Using IT policy to manage Bluetooth technology on BlackBerry devices	11
IT policy rules that control Bluetooth technology on BlackBerry devices	11
Educating users about how to protect their Bluetooth enabled BlackBerry devices	20
<b>5 Glossary</b>	<b>21</b>
<b>6 Legal notice</b>	<b>23</b>



# BlackBerry Enterprise Solution security

# 1

The BlackBerry® Enterprise Solution is designed to encrypt data in transit at all points between the BlackBerry device and the BlackBerry® Enterprise Server to protect your organization from data loss or alteration. Only the BlackBerry Enterprise Server and the BlackBerry device can access the data that they send between them. If events that threaten the wireless security of your organization occur, third parties, including wireless service providers, cannot access your organization's potentially sensitive information in a decrypted format.

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

Criteria	Description
confidentiality	The BlackBerry Enterprise Solution uses encryption to make sure that only the intended message recipients can view the contents of the message.
integrity	<p>The BlackBerry Enterprise Solution protects each message that the BlackBerry device sends with one or more message keys. To prevent third-party decryption or alteration of the message data, the message keys are designed to consist of random data.</p> <p>Only the BlackBerry Enterprise Server and the BlackBerry device know the value of the master encryption key, recognize the format of the decrypted and decompressed message, and automatically reject a message that is not encrypted with the correct master encryption key.</p>
authenticity	The BlackBerry device authenticates itself to the BlackBerry Enterprise Server to prove that it knows the master encryption key before the BlackBerry Enterprise Server can send data to the BlackBerry device.



## Bluetooth technology

## 2

Bluetooth® technology is a standard for short-range wireless technology. It enables two devices to communicate using radio waves that operate at 2.4 GHz. A BlackBerry® device that uses Bluetooth technology can open a wireless connection with other Bluetooth enabled devices, such as hands-free car kits or headsets, that are within a 10 m range.

The wireless industry considers Bluetooth technology to be a nonsecure channel. If Bluetooth technology is implemented incorrectly, using it might introduce security vulnerabilities into your organization's network.

### Bluetooth profiles

Bluetooth® profiles specify how applications on BlackBerry® devices and on Bluetooth enabled devices connect and are interoperable. Bluetooth profiles provide use-case scenarios and information about how to configure applications that are interoperable. Many Bluetooth profiles are available for implementation.

### Bluetooth profiles that BlackBerry devices support

Bluetooth® enabled BlackBerry® devices currently support Bluetooth profiles and provide specific IT policy rules to control their use.

Profile	Description
A2DP	<p>This profile defines how a BlackBerry device can send and receive audio in an audio stream format for two-channel stereo over a Bluetooth connection to another Bluetooth enabled device.</p> <p>You can use the Disable Advanced Audio Distribution Profile IT policy rule to specify whether to prevent the BlackBerry device from using this profile.</p>
AVRCP	<p>This profile defines how a Bluetooth enabled device controls audio/video functionality on a BlackBerry device.</p> <p>You can use the Disable Audio/Video Remote Control Profile IT policy rule to specify whether to prevent the BlackBerry device from using this profile.</p>
DUN	<p>This profile is based on the SPP and allows a BlackBerry device to access dial-up services, such as the Internet, using Bluetooth technology.</p> <p>You can use the Disable Dial-up Networking IT policy rule to specify whether to prevent the BlackBerry device from using this profile.</p>

Profile	Description
HFP	<p>This profile works with the SPP to enable wireless voice capabilities with most headsets and some car kits. If both the HSP and HFP are available, consider using the HFP because it offers more functionality and performance than the HSP. For example, the HFP can support wireless transfer of contact lists for car kits that use commands that control modems.</p> <p>You can use the Disable Handsfree Profile IT policy rule to specify whether to prevent the BlackBerry device from using this profile.</p>
HSP	<p>This profile works with the SPP to enable wireless voice capabilities with most headsets and some car kits. You use the HSP for wireless voice transmission only if the target peripheral does not support the HFP.</p> <p>You can use the Disable Headset Profile IT policy rule to specify whether to prevent the BlackBerry device from using this profile.</p>
SPP	<p>This profile provides procedures that describe how to configure serial connections between a BlackBerry device and a Bluetooth enabled peripheral that uses a virtual serial port. The Bluetooth enabled peripheral accesses the serial port through the BlackBerry Software Development Kit.</p> <p>You can use the Disable Serial Port Profile IT policy rule to specify whether to prevent the BlackBerry device from using this profile.</p>
SIM Access Profile	<p>This profile allows another Bluetooth enabled device to control the SIM card on a BlackBerry device. For example, a car kit could use the SIM card to control its own GSM communication. This might be useful if functioning of the BlackBerry device degrades significantly inside a high-end car because the car is well insulated. When the car controls the SIM card, the BlackBerry device prevents any applications that might use the SIM card from running on the device.</p>

## Risks of using Bluetooth technology on wireless devices

### 3

The wireless industry considers that Bluetooth® enabled devices have the following potential areas of vulnerability:

- Users with malicious intent can obtain confidential data from Bluetooth enabled devices without the knowledge or consent of the authorized users.
- A previously trusted (or paired) source that has been removed from the Trusted list can access the memory contents of some Bluetooth enabled devices.
- Users with malicious intent can gain access to higher-level commands and to voice, data, and messaging channels.

Security threats to Bluetooth wireless technology can be user based or device based.

Type of threat	Description	Examples
user based	User-based threats occur when users change settings or perform (or fail to perform) actions that leave their devices vulnerable or open to attacks.	bluejacking
device based	Device-based threats are the result of incorrect implementation of Bluetooth wireless technology on devices, which leave the devices vulnerable or open to attacks.	bluesnarfing and bluebugging

Any Bluetooth enabled device is at risk for attack when all of the following conditions are present:

- The Bluetooth wireless transceiver is turned on.
- The device is set to use discoverable (visible) mode.
- The device is physically located within range of a user with malicious intent.

### Bluejacking

Bluejacking is a user-based threat that occurs when users with malicious intent send text messages anonymously to Bluetooth® enabled devices that are set to use discoverable mode and are physically located within 10 m of the attacking devices. Users with malicious intent can target individuals or they can broadcast anonymous messages to all discoverable devices in the area. Bluetooth enabled phones, personal device assistants, and laptops can search for other devices within a short range, so users with malicious intent who are located in crowded public areas can send anonymous messages easily and without detection.

### Bluesnarfing

Bluesnarfing is a device-based threat that occurs when device manufacturers implement the specification for Bluetooth® technology incorrectly, allowing users with malicious intent to use Bluetooth technology to connect to devices without notifying the authorized users, and access device information without the knowledge or consent of the authorized users.

Typically, users with malicious intent gain access to the device users' contact lists although all OBEX-addressable data that is stored on the devices is vulnerable. During bluesnarfing attacks, users with malicious intent can obtain sensitive information, such as the unique network identifier of a device. They might also send text messages, make calls, or create false address book entries.

By default, on BlackBerry devices, the ability to exchange files with supported OBEX devices is turned off, which helps to protect the devices against bluesnarfing attacks by preventing users with malicious intent from using the OBEX implementation to access core BlackBerry device data.

## Bluebugging

Bluebugging is a device-based threat that occurs when device manufacturers implement security mechanisms for Bluetooth® technology improperly. Bluebugging also occurs when users with malicious intent use Bluetooth technology to access phone commands on devices without notifying or alerting the authorized users. This vulnerability enables the users with malicious intent to make calls, send and read text messages, access and add contacts to contact lists, eavesdrop on phone conversations, and connect to the Internet, all without detection or authorization.

## Managing Bluetooth enabled BlackBerry devices

# 4

Using BlackBerry® Enterprise Server version 4.0 or later, you can set IT policy rules that are designed to control the behavior of Bluetooth® enabled BlackBerry devices. For example, you can use IT policy rules to prevent users from performing the following actions on their BlackBerry devices:

- opening a Bluetooth connection with another Bluetooth enabled BlackBerry device, another Bluetooth enabled device, or the BlackBerry® Desktop Software
- turning on the discoverable mode option
- setting the discoverable mode option to have no time limit
- using the Bluetooth profiles that the BlackBerry devices support
- using wireless bypass over a Bluetooth connection
- exchanging files with supported Bluetooth OBEX devices
- sending or receiving address book information over a Bluetooth connection
- making calls over a Bluetooth connection

You can also use IT policy rules to require the following behavior on BlackBerry devices:

- using Bluetooth encryption on all Bluetooth connections
- using CHAP authentication on all Bluetooth serial connections to computers
- flashing the LED light when connected to another Bluetooth enabled device
- prompting users to type their BlackBerry device passwords to turn on Bluetooth support
- prompting users to type their BlackBerry device passwords to turn on discoverable mode

### Bluetooth technology security measures on BlackBerry devices

The following measures are designed to protect Bluetooth® enabled BlackBerry® devices.

Security measure	Benefit
BlackBerry devices support only seven of the available Bluetooth profiles.	This measure limits the ways that BlackBerry devices are vulnerable to attacks.
BlackBerry devices have limited support for the Bluetooth SPP. This profile works only with the BlackBerry phone application to provide voice capability using Bluetooth enabled headsets and car kits. Even though BlackBerry devices support the Bluetooth SPP for third-party peripheral devices and application development, this profile is not set up to work with other BlackBerry applications.	BlackBerry device users can control pairing requests. The number of devices that users can pair with is limited.

Security measure	Benefit
By default, the discoverable mode option on BlackBerry devices is turned off. The devices are not visible to other Bluetooth enabled devices. A BlackBerry device never enters into discoverable mode unless the user turns on that feature.	Potential users with malicious intent cannot locate BlackBerry devices easily and compromise them.
You can set the Limit Discoverable Time IT policy rule to True to allow users to turn on the discoverable mode option for 2 minutes only.	The BlackBerry devices are discoverable for a very limited time to allow pairing with another device.
You can use the Disable Bluetooth IT policy rule to control the Bluetooth wireless transceiver on BlackBerry devices. By default, the Bluetooth wireless transceiver on BlackBerry devices is turned off.	When the Bluetooth wireless transceiver is turned off, Bluetooth wireless technology is not operational on the BlackBerry devices, and the devices are not open to malicious use of their Bluetooth technology.
Users must request connections between their BlackBerry devices and other Bluetooth enabled devices. They must type a password called a passkey, which is a shared secret key, to complete a connection or pairing with another Bluetooth enabled device. A user's passkey must be between one and 16 characters long, and it is dependent on the target peripheral device.	Users are aware of attempts to connect or pair with Bluetooth enabled devices because their BlackBerry devices prompt them for a passkey.
Users can specify whether their BlackBerry devices use a passkey to encrypt data that the users send over a Bluetooth connection. You can use the Require Encryption IT policy rule to require that Bluetooth enabled BlackBerry devices use encryption over all Bluetooth connections.	Communication over the Bluetooth connection is protected.
When BlackBerry devices try to pair with other Bluetooth enabled devices, the BlackBerry devices request a combination key for authentication. The combination key is unique to a BlackBerry device and the Bluetooth enabled device that it is paired with.	Combination keys are designed to prevent the interception of wireless communication between two devices by a third device that was previously paired with one of the devices.
The BlackBerry devices prompt the users each time that other Bluetooth enabled devices try to connect to them.	BlackBerry device users can decline connection requests from Bluetooth enabled devices.

Security measure	Benefit
You can set the Disable Desktop Connectivity IT policy rule to True to prevent connections between the BlackBerry device and the BlackBerry® Desktop Manager using Bluetooth wireless technology.	The BlackBerry Desktop Manager does not open the BlackBerry based virtual serial port at regular intervals to try to open a connection with a BlackBerry device that is within range. This security measure is designed to reduce the risk of unauthorized access to a BlackBerry device through the open port.
You can set the Disable Wireless Bypass IT policy rule to True to require BlackBerry devices to use a serial port to exchange information with the BlackBerry® Enterprise Server, instead of using a virtual serial port and a wireless connection.	The BlackBerry® Device Manager does not open the Bluetooth based virtual serial port at regular intervals to try to open a connection with a BlackBerry device that is within range. This security measure is designed to reduce the risk of unauthorized access to a BlackBerry device through the open port.

## Using IT policy to manage Bluetooth technology on BlackBerry devices

IT policy rules that control the use of Bluetooth® wireless technology on BlackBerry devices are available in BlackBerry® Enterprise Server version 4.0 and later. These versions of the BlackBerry Enterprise Server support sending updates to IT policies to BlackBerry devices over the wireless network. IT policy rules for Bluetooth wireless technology are also available in BlackBerry Enterprise Server version 3.6 SP3 or later for Microsoft® Exchange.

You can manage all Bluetooth enabled BlackBerry devices simultaneously, or you can manage individual Bluetooth enabled BlackBerry devices. With BlackBerry Enterprise Server version 4.1 and later, you can create a separate IT policy for users who must use Bluetooth wireless technology, and set the Disable Bluetooth IT policy rule to True to turn off Bluetooth functionality in all other IT policies. For more information about assigning IT policies to groups, see the *BlackBerry Enterprise Server Administration Guide*.

### IT policy rules that control Bluetooth technology on BlackBerry devices

The BlackBerry® Manager lists all of the IT policy rules for managing Bluetooth® technology on BlackBerry devices in the Bluetooth policy group.

For more information about IT policy rules, see the *Policy Reference Guide*.

#### Allow Outgoing Calls IT policy rule

##### Description

This rule specifies whether the user can place outgoing calls from a BlackBerry® device using Bluetooth® technology.

**Default setting**

The default setting is always.

**Usage**

Set this IT policy rule to always, never, or only when the BlackBerry device is unlocked.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.0.2
- BlackBerry® Enterprise Server Version 4.0 SP2

**Disable Address Book Transfer IT policy rule****Description**

This rule specifies whether to prevent the BlackBerry® device from exchanging address book data with supported Bluetooth® enabled devices.

**Default setting**

The default setting is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.1
- BlackBerry® Enterprise Server Version 4.0 SP3

**Disable Advanced Audio Distribution Profile IT policy rule****Description**

This rule specifies whether a Bluetooth® enabled BlackBerry® device can use the Bluetooth A2DP.

**Default setting**

The default setting is False.

**Usage**

Set this IT policy rule to True to turn off the ability to stream audio using Bluetooth technology.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.2.2
- BlackBerry® Enterprise Server Version 4.1 SP4

## **Disable Audio/Video Remote Control Profile IT policy rule**

### **Description**

This rule specifies whether a Bluetooth® enabled BlackBerry® device can use the Bluetooth AVRCP.

### **Default setting**

The default setting is False.

### **Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.2.2
- BlackBerry® Enterprise Server Version 4.1 SP4

## **Disable Bluetooth IT policy rule**

### **Description**

This rule specifies whether support for Bluetooth® technology is turned off.

### **Default setting**

The default setting is False.

### **Usage**

If Bluetooth technology is turned on when the BlackBerry® device receives this IT policy rule, the BlackBerry device must be reset for the change to take effect.

### **Minimum requirement**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 3.8
- BlackBerry® Enterprise Server Version 4.0
- BlackBerry® Connect™ Transport Stack Version 4.0

### **Exceptions**

The BlackBerry Enterprise Server for Novell® GroupWise® supports this IT policy rule in BlackBerry Device Software Version 4.0 and later.

## **Disable Desktop Connectivity IT policy rule**

### **Description**

This rule specifies whether to prevent the BlackBerry® device from using Bluetooth® technology to connect to the BlackBerry® Desktop Software.

### **Default setting**

The default setting is True.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.1
- BlackBerry® Enterprise Server Version 4.0 SP3

**Disable Dial-Up Networking IT policy rule****Description**

This rule specifies whether to prevent the BlackBerry® device from using the Bluetooth® DUN profile.

**Default setting**

The default setting is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.2
- BlackBerry® Enterprise Server Version 4.0 SP6

**Disable Discoverable Mode IT policy rule****Description**

This rule specifies whether to prevent BlackBerry® device users from making their BlackBerry devices discoverable.

A BlackBerry device that is discoverable can be found by other Bluetooth® enabled devices in range of the BlackBerry device.

**Default setting**

The default setting is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.0.2
- BlackBerry® Enterprise Server Version 4.0 SP2

**Disable File Transfer IT policy rule****Description**

This rule specifies whether to prevent the BlackBerry® device from exchanging files with supported Bluetooth OBEX devices.

**Default setting**

The default setting is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.2
- BlackBerry® Enterprise Server Version 4.0 SP6

**Disable Handsfree Profile IT policy rule****Description**

This rule specifies whether the BlackBerry® device can use the Bluetooth HFP.

**Default setting**

The default setting is False.

**Usage**

The BlackBerry device uses the Bluetooth HFP to connect to most car kits and some headsets.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 3.8
- BlackBerry® Enterprise Server Version 4.0
- BlackBerry® Connect™ Transport Stack Version 4.0

**Exceptions**

The BlackBerry Enterprise Server for Novell® GroupWise® supports this IT policy rule in BlackBerry Device Software Version 4.0 and later.

**Disable Headset Profile IT policy rule****Description**

This rule specifies whether the BlackBerry® device can use the Bluetooth® HSP.

**Default setting**

The default setting is False.

**Usage**

The BlackBerry device uses the Bluetooth HSP to connect to most headsets and some car kits.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 3.8
- BlackBerry® Enterprise Server Version 4.0

- BlackBerry® Connect™ Transport Stack Version 4.0

**Exceptions**

The BlackBerry Enterprise Server for Novell® GroupWise® supports this IT policy rule in BlackBerry Device Software Version 4.0 and later.

**Disable Pairing IT policy rule****Description**

This rule specifies whether the BlackBerry® device can pair with a Bluetooth® enabled device.

**Default setting**

The default setting is False.

**Usage**

After the BlackBerry device pairs with a supported Bluetooth enabled device, you can use this IT policy rule to prevent the BlackBerry device from pairing with other Bluetooth enabled devices.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 3.8
- BlackBerry® Enterprise Server Version 4.0
- BlackBerry® Connect™ Transport Stack Version 4.0

**Exceptions**

The BlackBerry Enterprise Server for Novell® GroupWise® supports this IT policy rule in BlackBerry Device Software Version 4.0 and later.

**Disable Serial Port Profile IT policy rule****Description**

This rule specifies whether the BlackBerry® device can use the Bluetooth® SPP.

**Default setting**

The default setting is False.

**Usage**

The BlackBerry device uses the Bluetooth SPP to establish a serial connection between the BlackBerry device and a Bluetooth enabled device that uses a serial port interface.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 3.8

- BlackBerry® Enterprise Server Version 4.0
- BlackBerry® Connect™ Transport Stack Version 4.0

**Exceptions**

The BlackBerry Enterprise Server for Novell® GroupWise® supports this IT policy rule in BlackBerry Device Software Version 4.0 and later.

**Disable Wireless Bypass IT policy rule****Description**

This rule specifies whether to prevent the BlackBerry® device from using wireless bypass using Bluetooth® technology.

**Default setting**

The default setting is True.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.1
- BlackBerry® Enterprise Server Version 4.0 SP3

**Force CHAP Authentication on Bluetooth Link IT Policy rule****Description**

This rule specifies whether the BlackBerry® device must use CHAP authentication to connect to a computer using a Bluetooth® serial connection.

**Default setting**

The default setting is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.2.2
- BlackBerry® Enterprise Server Version 4.1 SP4

**Limit Discoverable Time IT policy rule****Description**

This rule specifies whether BlackBerry® device users can set the Bluetooth® discoverable mode option to have no time limit.

**Default setting**

The default setting is False.

### Usage

Set this rule to True to permit users to set the Bluetooth discoverable mode option to have a time limit of 2 minutes or to turn off Bluetooth discoverable mode.

### Dependencies

The BlackBerry device uses this IT policy rule only if the Disable Discovery Mode IT policy rule is set to False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.5
- BlackBerry® Enterprise Server Version 4.1 SP5

## Minimum Encryption Key Length IT policy rule

### Description

This rule specifies the minimum encryption key length (in bytes) that the BlackBerry® device uses to encrypt Bluetooth® connections.

### Default setting

The default setting is 1 byte.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.5
- BlackBerry® Enterprise Server Version 4.1 SP5

## Require Encryption IT policy rule

### Description

This rule specifies whether the BlackBerry® device uses Bluetooth® encryption for all connections.

### Default setting

The default setting is False.

### Usage

If you set this IT policy rule to True to require Bluetooth encryption for all connections, you might restrict compatibility with some Bluetooth enabled devices.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.1

- BlackBerry® Enterprise Server Version 4.0 SP4

### **Require LED Connection Indicator IT policy rule**

#### **Description**

This rule specifies whether the LED must flash when the BlackBerry® device is connected to a Bluetooth® enabled device.

#### **Default setting**

The default setting is False.

#### **Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.2
- BlackBerry® Enterprise Server Version 4.0 SP6

### **Require Password for Discoverable Mode IT policy rule**

#### **Description**

This rule specifies whether it is mandatory for the user to type the BlackBerry® device password before the BlackBerry device can be discovered by Bluetooth® enabled devices.

#### **Default setting**

The default setting is False.

#### **Dependencies**

The BlackBerry device uses this IT policy rule only if the Password Required IT policy rule is set to True.

#### **Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.1
- BlackBerry® Enterprise Server Version 4.0 SP3

### **Require Password for Enabling Bluetooth Support IT policy rule**

#### **Description**

This rule specifies whether it is mandatory for the user to type the BlackBerry® device password to turn on Bluetooth® technology.

#### **Default setting**

The default setting is False.

#### **Dependencies**

The BlackBerry device uses this IT policy rule only if the Password Required IT policy rule is set to True.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.1
- BlackBerry® Enterprise Server Version 4.0 SP3

## Educating users about how to protect their Bluetooth enabled BlackBerry devices

You can educate users in your organization about how to use Bluetooth® technology on their BlackBerry® devices safely. To help users protect their devices against Bluetooth based attacks, instruct them to perform the following actions:

- Leave the Discoverable option on the BlackBerry device set to No.
- If the Discoverable option on the BlackBerry device is set to Yes, deny requests to pair with unknown Bluetooth enabled devices.
- When pairing a BlackBerry device with another Bluetooth enabled device, set the Discoverable option to 2 Minutes. The BlackBerry device is discoverable for two minutes, as long as it should take to complete the pairing.
- Complete device pairings in private, uncrowded areas only.
- Choose to encrypt Bluetooth data traffic both to and from the BlackBerry device. The BlackBerry® Enterprise Solution uses the Bluetooth passkey to generate encryption keys. BlackBerry devices use Bluetooth Security Mode 3 and the highest encryption key length that is available on the paired device (minimum = 8 bits, maximum = 128 bits).
- Protect the assigned name of a BlackBerry device. If a user with malicious intent knows the name of the BlackBerry device, the device is vulnerable to an attack, even when it is not discoverable.

# Glossary

# 5

**A2DP**

Advanced Audio Distribution Profile

**AVRCP**

Audio/Video Remote Control Profile

**DUN**

Dial-up Networking

**GSM**

Global System for Mobile communications

**HFP**

Hands-Free Profile

**HSP**

Headset Profile

**LED**

light-emitting diode

**OBEX**

Object Exchange

**SIM**

Subscriber Identity Module

**SPP**

Serial Port Profile



## Legal notice

## 6

©2008 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType® and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used as trademarks in the U.S., Canada, and countries around the world.

Bluetooth is a trademark of Bluetooth SIG. The Bluetooth word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by Research In Motion is under license. Novell and GroupWise are trademarks of Novell, Inc. All other trademarks are the properties of their respective owners.

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

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at [www.blackberry.com/go/docs](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, MERCHANTABILITY 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. 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.

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

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

Research In Motion UK Limited  
200 Bath Road  
Slough, Berkshire SL1 3XE  
United Kingdom

Published in Canada