



Security for BlackBerry Devices with Bluetooth Wireless Technology

Contents

Audience.....	1
Purpose	1
Bluetooth wireless technology.....	1
BlackBerry devices that are enabled for Bluetooth wireless technology	1
Risks of using Bluetooth wireless technology on mobile devices.....	2
Bluejacking.....	2
Bluesnarfing.....	3
Bluebugging	3
Protecting BlackBerry devices that are enabled for Bluetooth technology	3
Security measures on BlackBerry devices.....	3
BlackBerry Enterprise Server IT policies for Bluetooth technology	4
What can BlackBerry users do to protect their BlackBerry devices?.....	5
What can BlackBerry Enterprise Server administrators do to protect corporate BlackBerry devices?....	6
Summary.....	6
References.....	6
Related resources.....	7
Appendix A: Additional bluejacking information.....	8
Actions to protect BlackBerry devices from bluejacking attacks.....	8
Vulnerability assessment for BlackBerry devices	8
Appendix B: Additional bluesnarfing information	9
Actions to protect BlackBerry devices from bluesnarfing attacks.....	9
Vulnerability assessment for BlackBerry devices	9
Appendix C: Additional bluebugging information.....	10
Actions to protect BlackBerry devices from bluebugging attacks	10
Vulnerability assessment for BlackBerry devices.....	10

Audience

This document is intended for system administrators and system managers and assumes a working knowledge of the following items:

- BlackBerry Enterprise Server™ installation, configuration, and administration
- corporate security issues
- wireless devices and networks
- Bluetooth® wireless technology

Purpose

This document provides information on the following topics:

- Bluetooth wireless technology and its uses with BlackBerry®
- attacks that have exposed potential vulnerabilities in Bluetooth technology
- preventive security measures and strategies that help to protect BlackBerry devices from attacks
- information that you can provide to users about how to reduce the risk of attacks when using Bluetooth technology on BlackBerry
- IT policies that you can set to control how users use Bluetooth technology on BlackBerry

Bluetooth wireless technology

Bluetooth wireless technology uses radio waves to enable mobile devices, such as mobile phones, PDAs and laptops, to establish wireless connections with other devices that are in short range. Bluetooth technology provides user enhancements by ridding devices of the cables that can be cumbersome in a home or office environment and enabling access to mobile technology in areas where it is not normally available.

Unfortunately, wireless networks and devices are not immune to security threats. Security researchers have discovered specific vulnerabilities in Bluetooth that can cause problems for users and IT administrators if they are not understood or if Bluetooth is poorly or improperly implemented.

Research In Motion® (RIM®) is committed to providing corporate system administrators with an end-to-end wireless solution with advanced security features. RIM extends this commitment to BlackBerry devices that use Bluetooth technology. BlackBerry has a number of built-in features and settings that enable BlackBerry users to limit or prevent potential attacks and provide system administrators with the tools to control how users use Bluetooth technology.

BlackBerry devices that are enabled for Bluetooth wireless technology

Bluetooth technology is available on the following BlackBerry wireless devices. These devices support the Bluetooth specification version 1.1 and are Class 2 Bluetooth devices, which means that they work within a 10-meter range.

- BlackBerry 7100 Series
- BlackBerry 7290 Wireless Handheld™
- BlackBerry 7250 Wireless Handheld™
- BlackBerry 7520 Wireless Handheld™

Functionality

BlackBerry devices that are Bluetooth wireless technology enabled can wirelessly connect with car kits, wireless headsets, and other peripherals using a virtual serial port over Bluetooth accessible from the BlackBerry Java

Development Environment (JDE). Using a Bluetooth wireless technology enabled car kit, a BlackBerry user can turn a car stereo into a speakerphone without cables or a special custom hardware installation. Bluetooth wireless technology enabled headsets provide wireless connectivity to BlackBerry devices and enable users to answer phone calls without struggling with cords.

Note: Only one core BlackBerry application is set up to use Bluetooth technology. The phone application uses Bluetooth technology for voice usage with headsets and car kits.

Bluetooth profiles

A Bluetooth profile is a specification that identifies and defines the minimum requirements that the Bluetooth wireless technology enabled device must support to enable interoperability between Bluetooth wireless technology enabled devices. These requirements define the user services, features and procedures that enable Bluetooth devices to communicate wirelessly.

Although many Bluetooth profiles are available for implementation, BlackBerry supports only the following three Bluetooth profiles:

- **Serial port profile:** This profile provides procedures for configuring serial connections between a BlackBerry device and another Bluetooth wireless technology enabled device. This profile is specifically targeted toward supporting third-party peripherals, such as bar code scanners.
- **Headset profile:** This profile supports the connection of a headset to a BlackBerry device. This profile depends on serial port profile availability.
- **Hands free profile:** This profile provides procedures for using Bluetooth technology to connect a BlackBerry device with a hands-free device that can act as an audio input or output device for BlackBerry.

Risks of using Bluetooth wireless technology on mobile devices

According to Adam Laurie of A.L. Digital Ltd., Bluetooth wireless technology enabled devices have three potential areas of vulnerability. First, under the right circumstances, confidential data can be obtained from some Bluetooth wireless technology enabled devices without the user's knowledge or consent. Second, the memory contents of some Bluetooth wireless technology enabled devices can be accessed by a previously trusted (or *paired*) source that has since been removed from the trusted list. Third, access can be gained to higher-level commands and channels such as voice, data, and messaging.

With Bluetooth wireless technology, the security threats can be user or device based.

Type of risk	Description	Example
User-based risk	setting or action that the user makes (or fails to make) that leaves the device vulnerable or open to an attack	bluejacking
Device-based risk	incorrect implementation of Bluetooth technology in the device that leads to a vulnerability where the device is at risk for an attack	bluesnarfing bluebugging

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

- The Bluetooth radio is enabled on the target device.
- The target device is set to discoverable mode.
- The target device is physically located within the range of an attacker.

Bluejacking

Bluejacking is the act of anonymously sending a message to a user of a Bluetooth wireless technology enabled device who has turned on Bluetooth technology and made their device visible (also referred to as discoverable) to other devices. Attackers can target individuals or broadcast anonymous messages to all discoverable devices in

the area. Because Bluetooth wireless technology enabled phones, PDAs, and laptops can search for other devices within a short range, attackers in crowded public areas can easily send anonymous messages without detection.

Bluejacking is a user-based risk.

For more information about bluejacking attacks and BlackBerry, see "Appendix A: Additional bluejacking information" on page 8.

Bluesnarfing

Bluesnarfing occurs when attackers use Bluetooth technology to connect to a target device without notifying the user and access target device information without knowledge or consent. Typically, the attacker accesses the user's contact list, although all object exchange (OBEX)-addressable data that is stored on the device is vulnerable. Revealing sensitive information is the most obvious consequence of this type of attack, but there are other consequences, including sending an SMS message, initiating a phone call, or creating a false phone book entry.

BlackBerry devices should not be vulnerable to bluesnarfing attacks because the OBEX functionality is not implemented on BlackBerry devices. The Bluetooth interface that is implemented by RIM is only plugged into the phone application (for voice usage), which should prevent attackers from accessing core BlackBerry device data.

Bluesnarfing is a device-based risk that occurs because of an incorrect implementation of the specification for Bluetooth wireless technology by device manufacturers.

For more information about bluesnarfing attacks and BlackBerry, see "Appendix B: Additional bluesnarfing information" on page 9.

Bluebugging

Bluebugging involves accessing mobile phone commands using Bluetooth wireless technology without notifying or alerting the user of the target device. This vulnerability enables the attacker to initiate phone calls, send and read SMS messages, access and enter phonebook contacts, eavesdrop on phone conversations, and connect to the Internet all without detection or authorization.

Bluebugging is a device-based risk that occurs because of poor implementation of Bluetooth security mechanisms by device manufacturers.

For more information about bluebugging attacks and BlackBerry, see "Appendix C: Additional bluebugging information" on page 10.

Protecting BlackBerry devices that are enabled for Bluetooth technology

Protecting corporate data, whether it is mobilized wirelessly or not, is a primary concern for many organizations. The following preventive measures and strategies are designed to protect all BlackBerry devices that are enabled for Bluetooth technology.

Security measures on BlackBerry devices

Security measure	Benefit
BlackBerry devices support only a limited number of Bluetooth profiles.	BlackBerry supports only three Bluetooth profiles, which limits the number of ways that devices are vulnerable to attack. See "Bluetooth profiles " on page 2 for a list of profiles that BlackBerry supports.
BlackBerry devices have limited support for the serial port profile. This profile only works with the phone for voice usage with headsets and car kits.	Even though BlackBerry devices support the serial port profile for third-party peripherals and application development, this profile is not set up to work with any other BlackBerry applications.

Security measure	Benefit
By default, BlackBerry devices are set to non-discoverable mode.	Viruses and unwanted messages from Bluetooth wireless technology enabled devices can be sent to devices that are set to discoverable mode. Because BlackBerry devices are set to non-discoverable mode by default, it is more difficult for potential attackers to locate them.
The Bluetooth radio is disabled by default on BlackBerry devices.	When the Bluetooth radio is disabled, Bluetooth technology is not operational and the BlackBerry device is not open attacks.
BlackBerry users must request a connection or pairing with another Bluetooth wireless technology enabled device. BlackBerry devices can pair with a maximum of 20 Bluetooth wireless technology enabled devices.	BlackBerry users control pairing requests and the number of devices with which a user can pair is limited.
BlackBerry users must type a passkey to complete a connection to or pairing with a Bluetooth wireless technology enabled device. Passkey lengths can be anywhere from 1 to 16 characters in length and are dependent on the target peripheral.	The connection is controlled by an encrypted password and the BlackBerry user is aware of the request because the BlackBerry user is the one who makes it.
The BlackBerry device requests a combination key for authentication when devices are paired. ¹	Combination keys prevent the wireless communication between two devices from being intercepted by a third device that had been paired with one of the original two.
By default, the BlackBerry device is prompted each time that a Bluetooth wireless technology enabled device attempts to connect to the BlackBerry device.	BlackBerry users are notified of attempted requests to connect from another device.

BlackBerry Enterprise Server IT policies for Bluetooth technology

BlackBerry Enterprise Server version 4.0 has several IT policies for Bluetooth technology that system administrators can push to BlackBerry devices. System administrators can use these IT policies to simultaneously manage all Bluetooth wireless technology enabled BlackBerry devices or individual BlackBerry devices. System administrators can prevent BlackBerry devices from connecting to Bluetooth wireless technology enabled devices or from connecting to a Bluetooth wireless technology enabled hands-free or wireless device.

Users cannot change or override IT policy settings. The system administrator has complete control over setting and maintaining the IT policies.

Note: IT policies for Bluetooth technology are also available in BlackBerry Enterprise Server version 3.6 Service Pack 3 or later for Microsoft® Exchange.

IT policy	Default setting	Description
DISABLE_BLUETOOTH	FALSE	When set to TRUE, this policy turns off the Bluetooth radio. Use this policy to prevent any Bluetooth wireless technology enabled device on the BlackBerry Enterprise Server from using Bluetooth technology.

¹ If the other Bluetooth wireless technology enabled device requests a unit key, then a unit key is used for the pairing.

IT policy	Default setting	Description
DISABLE_PAIRING	FALSE	<p>When set to TRUE, this policy prevents users from pairing new Bluetooth wireless technology enabled devices with BlackBerry devices. If a user pairs a specific headset make/model with a BlackBerry device, the headset has a unique identifier/MAC address that does not allow other identical make/model headsets to connect with the BlackBerry device.</p> <p>Note: Devices that are paired before the policy is applied can continue to use Bluetooth technology. For example, a system administrator can pair devices with corporate-approved peripherals and then set this IT policy so that only the approved peripheral can be used.</p>
DISABLE_HEADSET_PROFILE	FALSE	<p>When set to TRUE, this policy prevents connections between the BlackBerry device and a Bluetooth wireless technology enabled headset.</p> <p>Headset profile support is required to enable wireless voice capabilities with most headsets and some car kits. Use this profile for wireless voice transmission if the target peripheral does not support the hands-free profile.</p> <p>Note: Some Bluetooth wireless technology enabled headsets use the hands-free profile. See the following IT policy for more information.</p>
DISABLE_HANDSFREE_PROFILE	FALSE	<p>When set to TRUE, this policy prevents connections between the BlackBerry device and Bluetooth wireless technology enabled devices, such as car kits and some headsets.</p> <p>Note: The hands-free profile offers more functionality and performance than the headset profile. Choose the hands-free profile over the headset profile if both are available.</p>
DISABLE_SERIAL_PORT_PROFILE	FALSE	<p>When set to TRUE, this policy prevents connections between the BlackBerry device and third-party Java™ applications using the serial port profile. Use this policy to establish a serial connection between a device and a Bluetooth wireless technology enabled peripheral using a serial port interface. Use the BlackBerry Java Development Environment (JDE) SDK to access the serial port. Visit http://www.blackberry.com/developers for more information.</p> <p>Note: Having the serial port profile enabled does not have an effect unless there is a catcher application on the BlackBerry device. System administrators have complete control in BlackBerry Enterprise Server version 4.0 over what applications are stored on the devices in the organization.</p>

What can BlackBerry users do to protect their BlackBerry devices?

To help prevent against bluebugging, bluesnarfing, and bluebugging attacks, BlackBerry users can perform the following actions:

- Set the BlackBerry device to non-discoverable mode.
- If the BlackBerry device is set to discoverable mode, deny requests to pair with unknown devices.

- When pairing a BlackBerry device with a Bluetooth wireless technology enabled device, set the BlackBerry device to discoverable mode only for as long as it takes to complete the pairing.
- Complete device pairings in private, uncrowded areas.
- Choose to encrypt Bluetooth wireless technology connections with the BlackBerry device. Connection data is encrypted using the passkey (a shared secret key that generates encryption keys) that the BlackBerry device user types. BlackBerry uses Bluetooth Security Mode 3 and the highest encryption key length available on the paired device (minimum = 8 bits/maximum = 128 bits).
- Protect the device name assigned to the BlackBerry device. If an attacker knows the name of a device, it is vulnerable to an attack even when the device is set to non-discoverable mode.

What can BlackBerry Enterprise Server administrators do to protect corporate BlackBerry devices?

To help prevent against attacks, system administrators can perform the following actions:

- Upgrade to BlackBerry Enterprise Server version 4.0 to access the IT policies that control how users use Bluetooth technology on BlackBerry devices. BlackBerry Enterprise Server version 4.0 also supports sending IT policy updates to BlackBerry devices over the wireless network.

Note: IT policies for Bluetooth technology are also available in BlackBerry Enterprise Server version 3.6 Service Pack 3 or later for Microsoft Exchange.

- Create a separate IT policy group on each BlackBerry Enterprise Server that enables Bluetooth technology use. Add users who want to use Bluetooth technology to this group. Disable Bluetooth functionality for all other IT policy groups.
- If you are concerned about unauthorized access to a user's BlackBerry device, but you still want that user to be able to use Bluetooth technology, enable pairing with the target device, then disable the pairing functionality from the user's BlackBerry device. Only the approved target peripheral can pair with the user's BlackBerry device.
- Keep up-to-date on the latest viruses and worms that are identified as threats to mobile devices. Assess whether BlackBerry is vulnerable to the attack, and take the appropriate steps to inform and educate your management, system administrators, and users and protect your corporate devices.
- Educate users about safe usage of Bluetooth technology on BlackBerry devices.

Summary

Bluetooth technology provides valuable mobile user experience enhancements, such as turning a car stereo system into a speakerphone without an expensive custom installation. It also makes users more mobile by enabling them to connect to Bluetooth wireless technology enabled devices without the use of cables. There are some risks to using Bluetooth technology on certain mobile devices. For example, unprotected devices can have information sent to them without consent or even have information altered or stolen from them without warning or consent.

RIM understands the potential risks associated with using Bluetooth and has implemented important security measures on the device, such as making BlackBerry devices non-discoverable (or invisible) by default. In addition, BlackBerry Enterprise Server version 4.0 has many IT policies that enable system administrators to easily control how their users use Bluetooth technology. For example, system administrators can turn off Bluetooth technology over the wireless network. If Bluetooth technology is enabled, system administrators can still control how the device initiates and accepts connections. Administrators can also take steps to protect corporate by educating users about how to use Bluetooth technology more safely on BlackBerry devices.

References

Laurie, Adam and Ben, A.L. Digital Ltd., <http://www.thebunker.net/security/bluetooth.htm>.

The official Bluetooth membership site, <http://www.bluetooth.org/>.

The official Bluetooth web site, <http://www.bluetooth.com/>.

Related resources

Visit

http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8021/7925/736516/How_To_-_Prevent_Bluetooth_device_discovery_when_within_range.html?nodeid=736710&vernum=2 for information about how to make a BlackBerry invisible or non-discoverable.

Visit

http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8021/7925/736516/What_Is_-_Bluetooth.html?nodeid=736517&vernum=1 for information about Bluetooth technology.

Visit

http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8021/7925/736516/What_Is_-_Bluetooth_indicators.html?nodeid=736820&vernum=3 for information about Bluetooth technology indicators on devices.

Visit

http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8021/7925/736516/How_To_-_Pair_Bluetooth_devices.html?nodeid=736798&vernum=2 for information about how to pair Bluetooth wireless technology enabled devices.

Visit <http://www.blackberry.com/knowledgecenterpublic> for information about the BlackBerry Technical Knowledge Center.

Visit

http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8067/645045/7963/7965/729294/729295/Feature_and_Technical_Overview.pdf?nodeid=728592&vernum=0 for information about the BlackBerry Enterprise Server version 4.0 features and enhancements for Microsoft Exchange or http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8067/645045/7963/7965/729294/729295/Administration_Guide.pdf?nodeid=728905&vernum=0 to read the *BlackBerry Enterprise Server for Microsoft Exchange Administration Guide*.

Visit

http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8067/645045/7963/8164/729011/728120/Feature_and_Technical_Overview.pdf?nodeid=729285&vernum=0 for information about the BlackBerry Enterprise Server version 4.0 features and enhancements for IBM® Lotus® Domino® or http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8067/645045/7963/8164/729011/728120/Administration_Guide.pdf?nodeid=729282&vernum=0 to read the *BlackBerry Enterprise Server for IBM Lotus Domino Administration Guide*.

Visit <http://www.blackberry.com> for more information on BlackBerry.

Visit <http://www.rim.com> for more information on Research In Motion.

Appendix A: Additional bluejacking information

The following information describes the actions that BlackBerry users and system administrators can take to protect BlackBerry devices from bluejacking attacks. It also assesses the vulnerability of the BlackBerry device to a bluejack attack.

Actions to protect BlackBerry devices from bluejacking attacks

Person responsible	Action	Reason
User with Bluetooth wireless enabled BlackBerry device	As a best practice, keep the BlackBerry device set to non-discoverable mode, which is the default setting.	This action makes it much more difficult for a potential attacker to find the BlackBerry device.
	If the BlackBerry device is set to discoverable mode, do not accept any unexpected or unwanted message stating <i>Enter passkey for <X></i> where X represents a name of a Bluetooth device that is attempting to pair.	Unexpected messages from unknown sources should <i>always</i> be ignored.
IT administrator	Set IT policy to disable device pairing DISABLE_PAIRING=TRUE	This action provides controlled and safer access to Bluetooth technology. Devices that are paired before the IT policy is set to disallow device-pairings can continue to connect to the BlackBerry device.
	In extreme circumstances, set IT policy to disable Bluetooth functionality DISABLE_BLUETOOTH=TRUE	This action enables system administrators to prevent user access to Bluetooth technology if necessary. In BlackBerry Enterprise Server version 4.0, system administrators can enforce IT policies over the wireless network.

Vulnerability assessment for BlackBerry devices

The following security measures help to protect BlackBerry handhelds from bluejacking attacks.

- BlackBerry devices are, by default, not set to discoverable mode. This makes it much more difficult for potential attackers to send bluejack messages to BlackBerry devices.

Note: An IT policy planned for availability in BlackBerry Enterprise Server version 4.0 Service Pack 1 and BlackBerry Handheld Software version 4.0.2 will allow administrators to force users to keep BlackBerry devices in non-discoverable mode.
- When users set their BlackBerry device to discoverable mode, potential attackers can try to pair with the BlackBerry device, but users are prompted with a message to type the passkey for the device that is attempting to pair. Users should not accept invitations to pair with unknown devices.
- BlackBerry users must type a passkey to complete initial connections with any Bluetooth wireless technology enabled device, and they must manually accept all subsequent connections with that device. Users can only bypass the acceptance prompt by setting the paired device to trusted. This capability is not enabled by default on BlackBerry devices. Even then since there is only access by default without loading third-party software and using peripherals to the phone for voice calls over Bluetooth, potential attackers cannot access any corporate data on BlackBerry. If third-party software is loaded, then system administrators can use the application control IT policies to control whether the software is allowed or disallowed or whether it can access specific APIs on the BlackBerry device.
- If required in extreme circumstances, the system administrator can take control and turn off the Bluetooth radio wirelessly.

Appendix B: Additional bluesnarfing information

The following information describes the actions that BlackBerry users and system administrators can take to protect BlackBerry devices from bluesnarfing attacks. It also assesses the vulnerability of the BlackBerry device to a bluesnarf attack.

Actions to protect BlackBerry devices from bluesnarfing attacks

Person responsible	Action	Reason
User with Bluetooth wireless enabled BlackBerry device	None required.	Because BlackBerry devices do not have OBEX functionality, it is not possible for an attacker to carry out a bluesnarfing attack.
IT administrator	None required.	Same as above.

Vulnerability assessment for BlackBerry devices

BlackBerry devices or handsets should not be vulnerable to bluesnarfing attacks because the OBEX functionality is not implemented on BlackBerry. The Bluetooth interface implemented by RIM is not plugged into the core BlackBerry applications other than the phone application (for voice usage), which should prevent attackers from accessing core BlackBerry device data. This measure is intended to prevent bluesnarfing attacks using Bluetooth wireless technology on a BlackBerry device.

Appendix C: Additional bluebugging information

The following information describes the actions that BlackBerry users and system administrators can take to protect BlackBerry devices from bluebugging attacks. It also assesses the vulnerability of the BlackBerry device to a bluebug attack.

Actions to protect BlackBerry devices from bluebugging attacks

Person responsible	Action	Reason
User with Bluetooth wireless enabled BlackBerry device	As a best practice, keep the BlackBerry device set to non-discoverable mode, which is the default setting.	This action makes the BlackBerry device invisible to most potential attackers and makes bluebug attacks much more difficult.
	When pairing a BlackBerry device with a Bluetooth wireless technology enabled device, set the BlackBerry device to discoverable mode only for as long as it takes to complete the pairing. Return the BlackBerry device to non-discoverable mode when complete.	This action limits the amount of time that the BlackBerry device is vulnerable to potential attackers.
	When the BlackBerry device is set to discoverable mode, do not accept invitations to pair with unknown devices.	This action prevents pairing with potential attackers.
IT administrator	Set IT policy to disable device pairing DISABLE_PAIRING=TRUE	This action provides more controlled and safer access to Bluetooth technology. Devices that are paired before device pairing is disabled can continue to connect to BlackBerry.

Vulnerability assessment for BlackBerry devices

The following security measures help to protect BlackBerry devices from bluebugging attacks:

- BlackBerry devices are, by default, not set to discoverable mode.

Note: An IT policy planned for availability in BlackBerry Enterprise Server version 4.0 Service Pack 1 and BlackBerry Handheld Software version 4.0.2 will allow administrators to force users to keep BlackBerry devices in non-discoverable mode.
- BlackBerry device users must type a passkey to complete initial connections with any Bluetooth wireless technology enabled device, and they must manually accept all subsequent connections. Only by setting the paired device to the status of *trusted* on BlackBerry can users bypass the manual acceptance step. This capability is not enabled by default on the BlackBerry.
- BlackBerry device users cannot compose or send SMS messages remotely using Bluetooth technology.
- BlackBerry device users cannot access the address book remotely using Bluetooth technology.
- BlackBerry device users cannot initiate phone calls (other than a basic redial) using Bluetooth technology.

Security for BlackBerry Devices with Bluetooth Wireless Technology

Appendix C: Additional bluebugging information

Part number: WPS-10007-001

* Certain features outlined in this document require a minimum version of BlackBerry Enterprise Server software, BlackBerry Desktop Software, and/or BlackBerry handheld software and may require additional application development or third party products and/or services for access to corporate applications.

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

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. Microsoft and Exchange are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. IBM, Lotus, and Domino are trademarks of International Business Machines Corporation in the United States, other countries, or both. Java is a trademark or registered trademark of Sun Microsystems, Inc. in the United States or other countries. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

The handheld and/or associated software are protected by copyright, international treaties and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D,445,428; D,433,460; D,416,256. Other patents are registered or pending in various countries around the world. Please visit www.rim.com/patents.shtml for a current listing of applicable patents.

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

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