# Research In Motion (RIM)

---

## Blackberry™ Cryptographic Kernel Versions 3.6.1, 3.7.0, and 3.7.1

## FIPS 140-2 Non-Proprietary Security Policy
**Version 1.1**

**Level 1 Validation**

**November 3, 2003**

© Copyright 2003 Research In Motion
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

## TABLE OF CONTENTS




© Copyright 2003 Research In Motion
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

# 1 INTRODUCTION

## *1.1 Purpose*

This is a non-proprietary Cryptographic Module Security Policy for the Blackberry™ Cryptographic Kernel from Research In Motion (RIM). This security policy describes how the Kernel meets the security requirements of FIPS 140-2 and how to run the Kernel in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 certification of the Blackberry™ Cryptographic Kernel.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

## *1.2 References*

This document deals only with operations and capabilities of the Kernel in the technical terms of a FIPS 140-2 cryptographic module security policy. More information on Research In Motion products can be found from the following sources:

- The Research In Motion website (http://www.rim.com) and the BlackBerry™ website (http://www.blackberry.net): contain information on the full line of products from RIM
- The NIST Validated Modules website (http://csrc.ncsl.nist.gov/cryptval/): contains contact information for answers to technical or sales-related questions for the Cryptographic Kernel

© Copyright 2003 Research In Motion
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

# 2 BLACKBERRY™ CRYPTOGRAPHIC KERNEL

## *2.1 Overview*

BlackBerry™ is the leading wireless enterprise solution that allows users to stay connected with secure, wireless access to email, corporate data, phone, web and organizer features. BlackBerry™ is a totally integrated package that includes hardware, software and service, providing a complete end-to-end solution. The BlackBerry™ Cryptographic Kernel is the software module that provides the basic cryptographic functionality for the BlackBerry™.

## *2.2 Cryptographic Modules*

The cryptographic module being tested is a software module designed to run on RIM BlackBerry™ devices. For the purposes of this FIPS 140-2 validation, the physical boundary of the module is the outer case of the BlackBerry™ handheld device. The FIPS 140-2 cryptographic boundary includes the cryptographic components of the BlackBerry™ Cryptographic Kernel and the cryptographic components of the RIM-proprietary BlackBerry™ operating system. The cryptographic module is being tested as a level 1 software module. The module's interfaces are documented in section 2.3 of this document.

There are two sets of software components that comprise the Cryptographic Kernel (and thus, are included within cryptographic boundary). The first set of components is the Native Files. These files make up the low-level cryptographic routines implemented within the BlackBerry™ operating system. The second set of components is the Java Files, which forms the Cryptographic Kernel. The two sets of components together comprise the entire set of tested software within the cryptographic boundary of the module.

## *2.3 Module Interfaces*

The BlackBerry™ Cryptographic Kernel is tested as a multi-chip standalone module. The Cryptographic Kernel uses the interfaces located on the BlackBerry™ handheld. All of these physical interfaces are separated into the logical interfaces specified in FIPS 140-2 and are described in Table 1 below.

| Logical Interface | Physical Interface Mapping |
|---|---|
| Data Input Interface | keyboard, serial port, internal radio modem |
| Data Output Interface | serial port, internal radio modem, LCD |
| Control Input Interface | keyboard, serial port, thumbwheel |
| Status Output Interface | LED, LCD |
| Power Interface | serial port |

© Copyright 2003 Research In Motion

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

**Table 1 – Logical and Physical Interfaces**

## *2.4 Roles and Services*

An operator assuming the User role can perform the following functions of the cryptographic kernel: encrypting and decrypting services, running self tests, and generating session keys. The Crypto Officer role performs all the above and also has the ability to reboot the module with the reset function. Operators assume the roles implicitly by the services they access on the module. The table below illustrates the services available to the operator:

| Service | Role | CSP | Type of Access to CSP |
|---|---|---|---|
| Encrypt | Crypto Officer, User | 3DES, SHA-1 | Read Only |
| Decrypt | Crypto Officer, User | 3DES | Read Only |
| Run Self Tests | Crypto Officer, User | N/A | N/A |
| Generate Session Keys | Crypto Officer, User | 3DES, SHA-1 | Read, Write |
| Input Master Key | Crypto Officer, User | 3DES | Write |
| Reboot Module | Crypto Officer, User | N/A | N/A |

**Table 2 – Roles and Services**

## *2.5 Physical Security*

The BlackBerry™ Cryptographic Kernel is a software module, thus the FIPS 140-2 physical security requirements are not applicable.

## *2.6 Operational Environment*

The BlackBerry™ operating system, upon which the module resides, is a Limited Operational Environment in the context of FIPS 140-2. Thus the FIPS 140-2 Operating System Requirements are not applicable.

## *2.7 Cryptographic Key Management*

The module supports the following FIPS-Approved algorithms:

- 3DES (With the following modes: CBC, ECB, OFB, CFB8, CFB 64) (FIPS 46-3, *Data Encryption Standard*)
- SHA-1 (FIPS 180-1, Secure Hash Standard)
- HMAC SHA-1
- RSA (PKCS #1) for signature verification of the module only

© Copyright 2003 Research In Motion

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

The handheld device uses the following keys and Critical Security Parameters in the module:

| Key | Key type | Generation | Storage | Use |
|---|---|---|---|---|
| Master Keys | 3DES(CBC encryption) | Generated outside the cryptographic boundary | Flash memory | Encrypt session keys |
| Session Keys | 3DES(CBC encryption) | FIPS approved RNG | RAM | Secure encrypted emails |
| OS Integrity Verification Key | RSA public key | Generated outside the cryptographic boundary | Flash Memory | Integrity of self tests |
| HMAC Key | HMAC | Generated outside of the crypto boundary | N/A | HMAC Generation |
| PIN-to-PIN Master Key | 3DES(CBC encryption) | Generated outside the cryptographic boundary | Flash memory | Allows BlackBerry™ to BlackBerry™ communication over wireless network. |

**Table 3 – Keys and Critical Security Parameters**

The Master Keys are generated outside the cryptographic boundary of the device by the BlackBerry™ Desktop Manager, an external management tool used to generate master keys, backup/restore data, and synchronize current information with the handheld by communicating over the serial port. The Master keys are used for encrypting the session keys for outgoing messages and are stored in plaintext in the flash memory. These keys are input into the device during initialization via the serial port from the cradle.

There are 3 types of Master Keys: a Current Key, Pending Key, and a Past Key. The Current Key resides in the module with an intended lifetime of 30 days. After 30 days, the BlackBerry™ Desktop Manager will prompt the user to create a new Pending Key for insertion into the module However, a new Pending Key can be generated at anytime with the BlackBerry™ Desktop Manager and stored in the BlackBerry™ Desktop Manager until the device is set in the cradle. Once a new Pending Key is inserted into the Module, it becomes the Current Key, and the previous Current Key becomes the Past Key with a lifetime of 7 days before it is deleted from the module. The BlackBerry Cryptographic Kernel only contains the current and past keys within the cryptographic boundary at any one time.

The module has key output functionality. Session keys are output in encrypted form by the Triple DES Master Key. Session keys are generated by the handheld for each e-mail message fragment that is sent out. These session keys are used to encrypt and decrypt e-mail message

© Copyright 2003 Research In Motion

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

fragments (each of approximately 2 kilobytes length), and are deleted after each ingoing or outgoing message has finished processing.

The module implements HMAC SHA-1 and provides it for use to other BlackBerry™ applications through the API.

The OS Integrity Verification Key is a RSA public key that is hard-coded in the source code of the Cryptographic Kernel. The key is used to ensure the integrity of the software image upon startup.

The default PIN-to-PIN Master Key is a Triple DES key that is embedded within the Kernel source code. It is used in instances where the corporate e-mail network is bypassed (in the event it was disabled), and communication occurs over the wireless communication stations from BlackBerry™ device to BlackBerry™ device. Similar to the e-mail scenario, the PIN-to-PIN Master Key is used to wrap session keys for the PIN-to-PIN messages. A new, externally generated PIN-to-PIN Master Key can be used to replace the default key, but only BlackBerry™ devices with the same PIN-to-PIN Master Key can communicate via PIN-to-PIN messaging. The PIN-to-PIN Master Key is zeroized when the zeroize command is issued.

### *2.7.1 Random Number Generator*

The module implements the random number generator (RNG) specified in FIPS 186-2 Appendix 3.3.

### *2.7.2 Key Storage*

One copy of the Master Key is stored in a special database in flash memory (the keystore) of the BlackBerry™ handheld.

The other copy of this key is stored outside the module in the module operator's secure corporate messaging environment.

### *2.7.3 Key Zeroization*

Every 30 days, the operator is prompted by the Desktop Manager to generate a new Master Key when docking the BlackBerry™ in its cradle. Operators can additionally request generation of a new Master Key at any time using the Desktop Manager. The old Master Key becomes the Past Key, which resides in the handheld and the e-mail server for seven days, allowing for any delayed email messages to be received. The Past Key is then deleted after this seven-day period.

To limit access to data on the device, and use of the Master Key, the BlackBerry™ has a device password. The device password is unique for each device and is set by the operator. With the password set, a lock

© Copyright 2003 Research In Motion

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

screen appears after a set period of inactivity; the lock screen can be customized to display the operator's contact information. Once the password is set, a lock function is made available to the operator that causes the immediate appearance of the lock screen. When the lock screen appears, access to data on the handheld, through both the keyboard and the serial port, is prevented until the operator enters the correct password.

If an incorrect password is entered more than ten times, the handheld's memory will automatically be erased, destroying all key material and user specific data.

Session keys that are created per datagram are destroyed after each e-mail fragment is sent.

PIN-to-PIN Master Keys are zeroized when the module is zeroized.

## *2.8 EMI/EMC*

The module conforms to FCC Part 15 Class B requirements for home use.

## *2.9 Self-Tests*

The BlackBerry™ Cryptographic Kernel includes self-tests required for a FIPS 140-2 validation. More detail about the specific self-tests implement is listed below.

### *2.9.1 POWER-UP TESTS*

The module consists of the following power-up tests:

1. 3DES Known Answer Test
2. SHA-1 Known Answer Test
3. RSA Known Answer Test for Encrypt Only
4. HMAC-SHA-1 Known Answer Test
5. Software Integrity Test
6. Statistical RNG Tests

### *2.9.2 RANDOM NUMBER GENERATOR TESTS*

The module includes a continuous test on the output from the FIPS-Approved RNG. The module compares the output of the RNG with the previous output to ensure the RNG has not failed to a constant value. The module also implements statistical random number generator tests (monobit, runs, and poker) at startup. If any of these self-tests fail, the module enters an error state.

© Copyright 2003 Research In Motion

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

### *2.9.3 INVOKING SELF-TESTS*

The operator can invoke the power-up tests by resetting the module. Additionally the operator can invoke all of the power-up tests, except the software integrity test, by performing the following operations:

1. Select the Options icon in the main screen.
2. Select “Security” from the Options menu.
3. Click the thumbwheel and select “Verify Security Software”.

## *2.10 Mitigation of Other Attacks*

The BlackBerry™ Cryptographic Kernel does not employ technology that claims to mitigate specialized attacks.

© Copyright 2003 Research In Motion
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

# 3 SECURE OPERATION OF THE BLACKBERRY™ CRYPTOGRAPHIC KERNEL

The instructions provided in this section must be followed in order to place the BlackBerry™ Cryptographic Kernel in a FIPS-Approved mode of operation.

## *3.1 Password Configuration*

During initial configuration of the BlackBerry™ device, the Crypto Officer or User must configure a device password. To configure the password, the operator must perform the following steps:

1. Select the Options icon in the main screen.
2. Select “Security” from the Options menu.
3. Set the “Password” option to “Enabled”.
4. Set the “Security Timeout” option to a value no greater than 10 minutes.
5. Click the thumbwheel and select “Save”.
6. Enter the device password in the “New Password” dialog that appears.
7. Re-enter the device password in the “Verify New Password” dialog that appears.

© Copyright 2003 Research In Motion
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

# 4 TERMS AND DEFINITIONS

The following table lists the terms discussed in this security policy and their respective definitions

| Term | Definition |
|---|---|
| 3DES | Triple Data Encryption Standard |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| FCC | Federal Communication Commission |
| FIPS | Federal Information Processing Standard |
| HMAC | Hash Message Authentication Code |
| LCD | Liquid Crystal Display |
| LED | Light Emitting Diode |
| NIST | National Institute of Standards and Technology |
| RIM | Research In Motion |
| RNG | Random Number Generator |
| RSA | Rivest, Shamir and Adleman |
| SCM | Software Configuration Management |
| SHA1 | Secure Hash Algorithm |

**Table 4 – Terms and Definitions**

© Copyright 2003 Research In Motion
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.