FIPS 140-2 Security Policy

BlackBerry Smartcard Reader

Firmware Version 3.8.5.51

Hardware Revision 2.0

Document Version 2.1

Security Certifications Team

www.blackberry.com

Research In Motion (RIM)

Document and Contact Information

Version	Date	Author	Description
1.0	05 January 2009	Sean Sandrock	Document creation.
1.1	22 June 2009	Sean Sandrock	Multiple additions including module picture, module architecture, and strength of authentication functions.
1.2	09 September 2009	Sean Sandrock	Multiple additions including zeroization service, information flows, and key information.
1.3	18 September 2009	Sean Sandrock	Minor changes.
1.4	23 September 2009	Sean Sandrock	Responded to lab comments.
1.5	23 September 2009	Sean Sandrock	Responded to lab comments.
1.6	23 September 2009	Sean Sandrock	Responded to lab comments.
1.7	20 April 2010	Sean Sandrock	Responded to lab comments.
1.8	21 April 2010	Sean Sandrock	Responded to lab comments. Included Crypto Officer guidance.
1.9	04 May 2010	Sean Sandrock	Responded to lab comments. Removed irrelevant material.
2.0	05 October 2010	Sean Sandrock	Responded to CMVP comments.
2.1	January 25, 2011	Randy Eyamie	Responded to CMVP comments.

Contact	Corporate Office
Security Certifications Team certifications@rim.com (519) 888-7465 ext. 72921	**Research In Motion** 295 Phillip Street Waterloo, Ontario Canada N2L 3W8 www.rim.com www.blackberry.com

Contents

Introduction 1
Cryptographic Module Specification 3
Cryptographic Module Ports and Interfaces 7
Roles, Services, and Authentication 8
Physical Security 11
Cryptographic Keys and Critical Security Parameters 12
Self-Tests 13
Mitigation of Other Attacks 14
Glossary 15

List of Tables

Table 1. Module Security Functions 3
Table 2. Implementation of FIPS 140-2 Interfaces 7
Table 3. Module Services 8
Table 4 - Strength of Authentication Mechanisms 9
Table 5. Role Selection by Module Service 10
Table 6. Cryptographic Keys and CSPs 12
Table 7. Module Self-Tests 13
Table 8. Attack Types 14

List of Figures

Figure 1. BlackBerry Solution Architecture 1
Figure 2 - BlackBerry Smartcard Reader Architecture 2
Figure 3. Cryptographic Module Boundary 5
Figure 4. Hardware Revision Examples 5
Figure 5 - Front and Back Sides of Module 11

Introduction

BlackBerry® is the leading wireless solution that allows users to stay connected to a full suite of applications, including email, phone, enterprise applications, Internet, SMS, and organiser information. The *BlackBerry Enterprise Solution* is a totally integrated package that includes innovative software, advanced BlackBerry wireless devices and wireless network service, providing a seamless emulsion. The BlackBerry architecture is shown in the following figure.

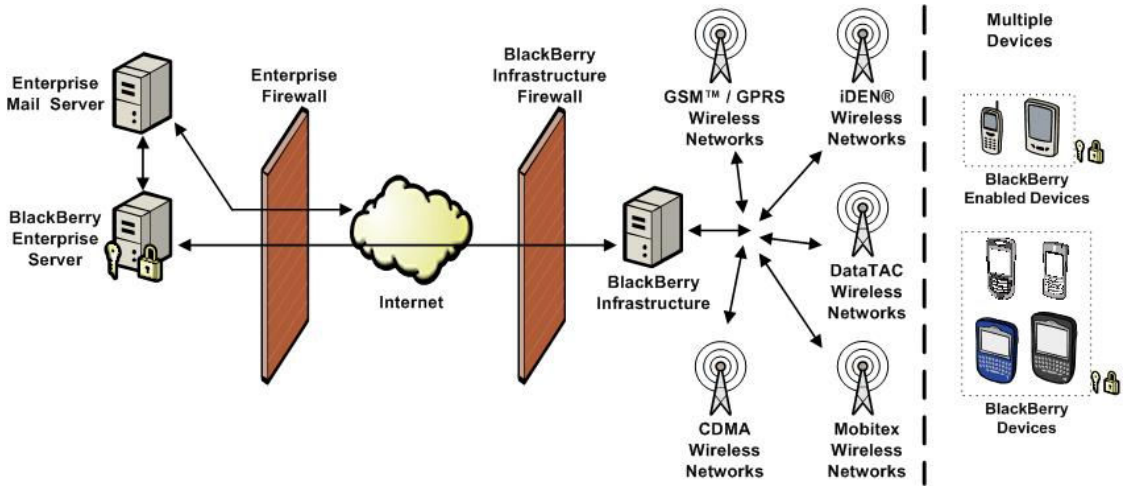

Figure 1. BlackBerry Solution Architecture

The BlackBerry Smart Card Reader for BlackBerry devices is an accessory that, when used in proximity to certain Bluetooth® enabled BlackBerry devices and computers, integrates smart card use with the *BlackBerry Enterprise Solution*, letting users authenticate with their smart cards to log in to Bluetooth enabled BlackBerry devices and computers.

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

- communicate over the wireless network with Bluetooth wireless technology version 1.1 or later–enabled BlackBerry devices and computers using the AES 256 encryption method (by default) on the application layer
- create a reliable two factor authentication environment for granting users access to BlackBerry and PKI applications
- enable the wireless digital signing and encryption of wireless email messages sent from the BlackBerry device using the S/MIME Support Package
- store all encryption keys in RAM only and never write the keys to flash memory
- only stores smartcard data on the conjoining device or computer to be authenticated to

BlackBerry Smartcard Reader contains the BlackBerry Cryptographic Kernel, a firmware Kernel currently deployed in all BlackBerry Smartphones. While the Kernel provides the cryptographic functionality required for basic operation of the device, the cryptographic module will be considered the entire Smartcard Reader hardware and firmware. The BlackBerry Smartcard Reader, hereafter referred to as *cryptographic module* or *module*, provides the following cryptographic services:

- Data encryption and decryption

- Message digest and authentication code generation
- Random data generation
- Elliptic curve key agreement

The BlackBerry Smartcard reader architecture is described by the following:

Figure 2 - BlackBerry Smartcard Reader Architecture

More information on the BlackBerry Smartcard Reader solution is available from: http://na.blackberry.com/eng/ataglance/security/products/smartcardreader/.

Cryptographic Module Specification

Security Functions

The cryptographic module is a Hardware module that implements the following FIPS-Approved or Allowed security functions[1]:

Table 1. Module Security Functions

Algorithm	Description	Certificate Number
AES-256	Encrypt and Decrypt, as specified in FIPS 197. The implementation supports the CBC and ECB modes of operation.	# 1172
SHA-1 **SHA-256** & **SHA-512**	as specified in FIPS 180-3.	# 1084
HMAC-SHA-1, **HMAC-SHA-256** & **HMAC-SHA-512**	as specified in FIPS 198.	# 672
FIPS 186-2 RNG	as specified in FIPS 186-2. The implementation uses SHA-1 as the function *G*	# 648
RSA PKCS#1	Signature verification, as specified in PKCS #1, version 2.1	# 555
ECMQV	Key agreement, key establishment methodology provides 256 bits of encryption strength	As specified in IEEE P1363 Draft 13.

[1] A security function is FIPS-Approved if it is explicitly listed in *FIPS 140-2 Annex A: Approved Security Functions for FIPS PUB 140-2*.

ECDH	Key agreement, key establishment methodology provides 256 bits of encryption strength	As specified in IEEE P1363 Draft 13.
ECDSA	Signature verification, as specified in FIPS 186-2 and ANSI X9.62. The implementation supports elliptic curve K-571.	# 140

Modes of Operation

The module does not have a non-Approved mode of operation and, consequently, always operates in a FIPS-Approved mode of operation once securely initiated. Module initiation is achieved via the following steps:

- Remove the module from its original packaging
- Power the module battery for approximately 20 minutes. During this time there is no module functionality and the following notifications are provided:
    - Temporary orange LED Indicator and “Low Battery” message within LCD.
    - When the battery is sufficiently charged the module will automatically initiate startup with the message “Booting” displayed.
    - During booting, the module will begin initiating firmware accompanied by the LED flashing multiple colours, a display of application and platform versions and the self-test result.
    - With a successful startup, the module will remain in the ‘Off’ position, essentially disabling the Bluetooth radio.
    - Bluetooth Pair the module with a computer or BlackBerry device as per the ***Getting Started Guide***.
    - Secure Channel Pair the module with the same computer or BlackBerry device as per the ***Getting Started Guide***.
    - Successfully enter a minimum 4-character password when requested.
    - FIPS mode is achieved when the module display’s the message “On Conn:#” within the display output.

Conformance Testing and FIPS-Compliance

For the purposes of FIPS 140-2 conformance testing, the module utilized was a BlackBerry SmartCard Reader version 2.0.

Cryptographic Boundary

The module is a light-weight, portable, contact smartcard reader designed to be worn as a lanyard with the intent of providing two factor authentication to BlackBerry devices and/or General Purpose Computers.

The physical and cryptographic boundary of the module is the physical boundary of the BlackBerry Smartcard Reader that executes the BlackBerry Cryptographic Kernel and is the exterior of the Reader shown in the following figure. An additional security layer is provided via a potted and canned chip interior. Consequently, the embodiment of the module is multiple-chip standalone intended to meet FIPS 140-2 Level 3 requirements.

Figure 3. Cryptographic Module Boundary

Determining the Module Version

The operator may determine the version of the module on a BlackBerry Smartcard Reader by performing the following operations:

1. Ensure the operator possesses **hardware revision 2.0** of the module. This can be determined by ensuring the module appears as follows with a larger two-line LCD display versus preceding one line revisions. Any BlackBerry Smartcard readers preceding hardware revision 2.0 possess:
    i. A removable battery (see Figure 4)
    ii. A one line LCD. (see Figure 4)

Figure 4. Hardware Revision Examples

Revision 2.0 Hardware Example on Left – Preceding Versions Example on Right with Removable Battery and One-Line LCD.

2. Locate both the **Action** (side) and **Backlight** (top) buttons and depress for approximately 5 seconds.
3. The module will reset and post the module version while booting, i.e. “Module Version 3.8.5.51”.

Cryptographic Module Ports and Interfaces

The following table describes the module ports and interfaces.

Table 2. Implementation of FIPS 140-2 Interfaces

FIPS 140-2 Interface	Module Ports
Data Input	USB port, smartcard contact, Bluetooth® wireless radio
Data Output	USB port, Bluetooth wireless radio
Control Input	Action button, backlight button, smartcard contact
Status Output	Primary LCD screen, LED
Power Input	USB port

Roles, Services, and Authentication

Roles

The module supports a User and Crypto Officer role. The module does not support a maintenance role. The module does not support multiple or concurrent operators and is intended for use by a single operator, thus it always operates in a single-user mode of operation.

Services

The services described in the following table are available to the operator.

Table 3. Module Services

Service	Description
Zeroization	Zeroizes device keys and user data present on the device. May be accomplished via a Module reset accommodated by pressing the **backlight + action** key combination.
View Status	Displays the status of the module.
Perform Key Agreement	Creates a new Secure Connection Key and uses it to replace the existing Secure Connection Key. The new Keys are created cooperatively by performing key agreement via ECDH with a BlackBerry device or GPC loaded with compatible device drivers.
Encrypt Data	Encrypts data that is to be sent from the device. A Secure Connection Key is automatically generated via the Generate Secure Connection Key service and is used to encrypt the data.
Decrypt Data	Decrypts data that has been received by the device. The Session Key is used to decrypt the data. This service is performed automatically on behalf of the operator.
Perform Self-Tests	Executes the module self-tests.
Bluetooth Pairing	Creates a Bluetooth paired connection between the Module and a corresponding BlackBerry or GPC.
Secure RIM Pairing	Creates an AES encrypted tunnel between the Module and a Bluetooth paired BlackBerry Smartphone or GPC to securely transmit data sent and received via Bluetooth.
Retrieve Smartcard Data	Retrieves Application Protocol Data Units from the card and forwards the units to the corresponding BlackBerry device or GPC.
Change Password	Changes the module password.

Authentication

The Module supports identity-based operator authentication. Roles are explicitly selected based on authentication mechanisms performed by the operator. Explicit role selection is summarised in the following table, as are the keys and critical security parameters (CSPs) that are affected by each service. Operator authentication requires the following steps:

1.) The operator presses the module's action button identifying the Module operator ID and requests the operator to enter the same ID into the BlackBerry or GPC which is obscured with an asterisk.
2.) Upon successful entry, the Module will produce a random 8-character alphanumeric PIN to initiate Bluetooth pairing. The operator must enter the PIN into the corresponding device or GPC which is obscured with an asterisk. At this point, the Bluetooth connection is achieved.

3.) The operator is then presented with another random 8-character alphanumeric PIN, to identify the Crypto Officer, which is entered into the corresponding device or GPC. The PIN entry is again obscured with an asterisk, and confirmed by the Module for secure pairing. This process initiates the generation of an AES 256-bit shared connection key (Session Key) by ECDH to further secure the connection. At this point, there is an encrypted channel overlaying the Bluetooth encryption by AES encryption and the Crypto Officer is further authenticated by means of an AES 256-bit key (Secure Connection Key) shared between the Module and corresponding secure pairing device or GPC (something the operator has).
4.) The operator is then instructed to enter a minimum 4-character password (something the operator knows) to further identify the operator as a User role and complete the identity based authentication. The data entered is obscured by the replacement of characters entered by the asterisk character. This password is transmitted via a trusted path to the module by AES encryption as is all authentication data entering the Module.

Power cycling the module ensures the previous authentication results are removed from memory.

Strength of Authentication Mechanisms

Table 4 - Strength of Authentication Mechanisms

Role	*Type of Authentication*	*Authentication Data*
Crypto Officer	Password	Randomly generated 8 character password. The Module accepts 93 different characters for a password and the probability that a random password attempt will succeed with a minimum 4 character password and the potential characters defined is **1 in 93^8** or **1 in 5.596×10^{15}**. An operator has only one attempt at entering this password. A failed attempt will result in loss of the Bluetooth connection, and the process for creating a session is restarted, requiring the operator to press the action button to re-initiate the secure pairing sequence.
	AES 256 bit key.	Successful random access to the Module would require **1.1×10^{77}** potential key combinations. Given that the only possible way of accessing the Module through this method is by previously engaging a Bluetooth connection with a properly configured second party (i.e. BlackBerry Device or Windows workstation loaded with the correct drivers installed), the possibility of attempting to access the module through this means would only allow for approximately 20 attempts within a one minute period and a probability of **5.5^{77}** of successfully replicating the key.
User	Password	User generated 4 character password. The Module accepts 93 different characters for a password and the probability that a random password attempt will succeed with a minimum 4 character password and the potential characters

Role	*Type of Authentication*	*Authentication Data*
		defined is **1 in 93**[4] or **1 in 74,805,201**. A failed login is accompanied by a 1 second delay allowing for no more than 10 attempts for authentication. If these 10 attempts are failed sequentially the module is instructed to zeroize all data including key and CSP data.

Crypto Officer Guidance Defining Procedures to Administer the Module

Overview: The Module is designed and manufactured entirely within Research In Motion secure facilities. All devices are shipped via standard secure shipping procedures and should be contained within a sealed package upon procurement.

To administer the module:

1. Ensure the Module is fully charged before continuing.
2. Complete Steps 1-4 within the Authentication section.

Table 5. Role Selection by Module Service

Service	Role Explicitly Selected	Affected Keys and CSPs	Access to Type
View Status	Crypto Officer/User	N/A	N/A
Perform Key Agreement	Crypto Officer	ECC Key Pair	Execute
Secure RIM Pairing	Crypto Officer	ECC Key Pair	Execute
		Random 8 character password	Write/Execute
		Secure Connection Key	Write/Execute
	User	Minimum 4 character password	Write/Execute
Encrypt Data	User	Session Key	Execute
Decrypt Data	User	Session Key	Execute
Retrieve Smartcard Data	User	N/A	N/A
Change Password	User	Session Key	Execute
Perform Self-Tests	Crypto Officer/User	Firmware Integrity Key	Execute

Unauthenticated Services:

- Zeroization Service: Zeroizes device keys and user data present on the device. May be accomplished via a Module reset accommodated by pressing the **backlight + action** key combination
- Bluetooth Pairing: transmits and receives Bluetooth pairing keys and authentication materials to establish a Bluetooth encrypted session via the Bluetooth port.

Physical Security

The Module is manufactured using industry standard integrated circuits and production-grade components that includes standard passivation techniques and meets the FIPS 140-2 Level 3 physical security requirements.

The Module consists of an ultrasonically welded plastic exterior (SABIC GE Cycoloy C1200HF resin) with no means of accessing internal components via doors or removable covers. To penetrate the Module, an attacker must break the ultrasonic weld along the Module seam which causes several fractures and markings indicating tampering. The following figure demonstrates the front and backsides of the Module and the opaqueness of the Reader. Additionally, attempts at accessing the internal Module components triggers a tamper response mechanism to disconnect the battery causing a tamper condition and the removal of all CSP's held within RAM. The module is void of slits or holes for ventilation or otherwise.

To further ensure physical security compliance, the chip embodiment containing Module cryptographic Firmware and memory, including associated circuitry, is encased using an opaque potting epoxy which, when breached, will result in a high-probability of module failure.

Figure 5 - Front and Back Sides of Module

Cryptographic Keys and Critical Security Parameters

The following table describes the cryptographic keys, key components, and CSPs utilised by the module.

Table 6. Cryptographic Keys and CSPs

Key / CSP	Description
Secure Connection Key	An AES-256 key used established utilizing ECDH.
User Password	Operator generated password of 4-characters minimum.
Crypto Officer Password	Randomly generated 8-character password
Session Key	An AES-256 key used to encrypt and decrypt data. The module generates Session Keys using the implemented FIPS 186-2 RNG.
Firmware Integrity Key	A RSA public key used to verify the integrity of the module firmware.
ECC Key Pair	A key pair used to perform key agreement over elliptic curves.
Bluetooth PIN	A random numeric or alphanumeric identifier to initiate Bluetooth pairing of at least eight characters in length.
Secure Pairing PIN	A random numeric or alphanumeric identifier which initiates Secure pairing of at least eight characters in length.
HMAC Key	A key used to calculate a message authentication code using the HMAC algorithm.

Key Zeroization

Key Zeroization is accomplished via a Module reset accommodated by pressing the **backlight + action** key combination

Protected Key Storage

To help limit the risk of key disclosure, the BlackBerry Smart Card Reader is designed to store all keys in its RAM only and does not write keys to its flash memory. The Module boundary is designed so that if breached, keys stored in RAM will be zeroized.

Self-Tests

The module implements the self-tests described in the following table.

Table 7. Module Self-Tests

Test	Description
Firmware Integrity Test	The module implements an integrity test for the module firmware by verifying its 1024-bit RSA signature. The firmware integrity test passes if and only if the signature verifies successfully using the Firmware Integrity Key.
AES-256 KAT	The module implements a Known Answer Test (KAT) for AES-256. The KAT passes if and only if the calculated output equals the expected output.
SHA-1 KAT	The module implements a KAT for SHA-1. The KAT passes if and only if the calculated output equals the expected output.
SHA-256 KAT	The module implements a KAT for SHA-256. The KAT passes if and only if the calculated output equals the expected output.
SHA-512 KAT	The module implements a KAT for SHA-512. The KAT passes if and only if the calculated output equals the expected output.
HMAC SHA-1 KAT	The module implements a KAT for HMAC SHA-1. The KAT passes if and only if the calculated output equals the expected output.
HMAC SHA-256 KAT	The module implements a KAT for HMAC SHA-256. The KAT passes if and only if the calculated output equals the expected output.
HMAC SHA-512 KAT	The module implements a KAT for HMAC SHA-512. The KAT passes if and only if the calculated output equals the expected output.
RSA Verify KAT	The module implements a KAT for RSA signature verification. The test passes if and only if the calculated output equals the expected output.
FIPS 186-2 RNG KAT	The module implements a KAT for the FIPS 186-2 RNG. The KAT passes if and only if the calculated output equals the expected output.
Continuous RNG Test	The module implements a continuous RNG test, as specified in FIPS 140-2, for the implemented FIPS 186-2 RNG.

All self-tests, except the Continuous RNG Test, are executed during power-up without requiring operator input or action. The Firmware Integrity Test is the first self-test executed during power-up.

Invoking the Self-Tests

Both the Crypto Officer and the User roles may invoke the power-up self-tests by resetting the module via the Reset service. This may be accomplished by locating both the **Action** (side) and **Backlight** (top) buttons and depressing the keys for approximately 5 seconds.

Mitigation of Other Attacks

The module is designed to mitigate multiple side-channel attacks specific to the AES algorithm. Mitigation of these attacks is accomplished through the execution of table masking, splitting, and stirring manoeuvres designed to aid in the protection of cryptographic keys and plain text data at all points during the encryption, decryption, and self-test operations.

The following table describes the types of attacks the module mitigates.

Table 8. Attack Types

Attack type	Description
Side-Channel	• attempts to exploit physical properties of the algorithm implementation using Power Analysis (for example, SPA and DPA) and Electro-Magnetic Analysis (for example, SEMA and DEMA) • attempts to determine the encryption keys that a device uses by measuring and analyzing the power consumption, or electro-magnetic radiation, emitted by the device during cryptographic operations

Glossary

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CBC	Cipher block chaining
CSP	Critical security parameter
DES	Data Encryption Standard
EC	Elliptic curve
ECC	Elliptic curve cryptography
ECDSA	Elliptic curve Digital Signature Algorithm
ECMQV	Elliptic curve Menezes, Qu, Vanstone
FIPS	Federal Information Processing Standard
HMAC	Keyed-hashed message authentication code
IEEE	Institute of Electrical and Electronics Engineers
KAT	Known answer test
LCD	Liquid crystal display
LED	Light emitting diode
PIN	Personal identification number
PKCS	Public Key Cryptography Standard
PUB	Publication
RIM	Research In Motion
RNG	Random number generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SMS	Short Messaging Service
URL	Uniform resource locator
USB	Universal serial bus