FIPS 140-2 Security Policy

BlackBerry Cryptographic Kernel Version 3.8.6.5

Document Version 1.3

BlackBerry Security Certifications, Research In Motion

Document and Contact Information

Version	Date	Description
1.0	May 25, 2010	Document creation
1.1	June 28, 2010	Added Certificate numbers from the CAVP
1.2	June 29, 2010	Updated with comments received from DOMUS
1.3	November 11, 2010	Updated policy with comments received from CMVP

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

List of Tables

List of Figures

1 Introduction

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

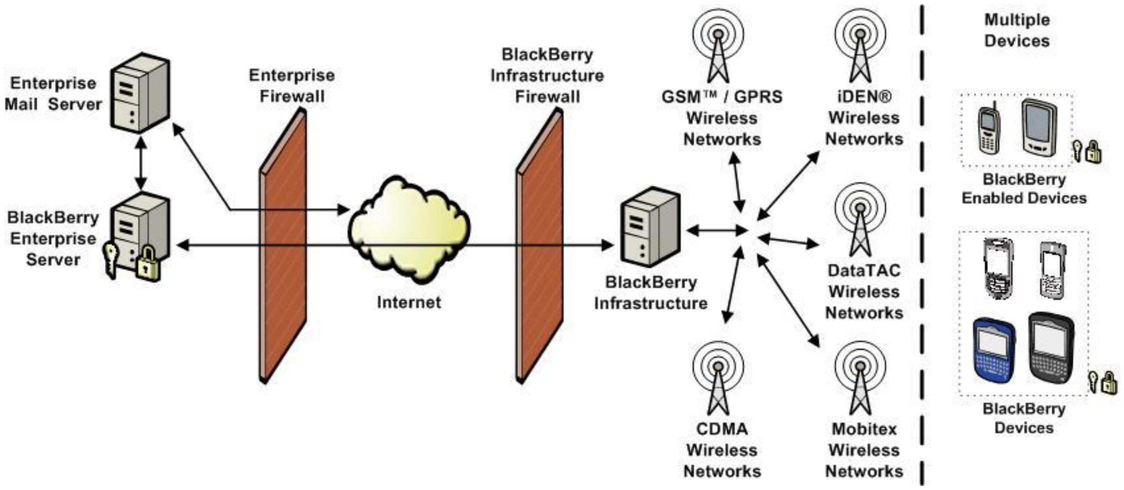
Enterprise Mail Server
BlackBerry Enterprise Server
Enterprise Firewall
Internet
BlackBerry Infrastructure Firewall
BlackBerry Infrastructure
GSM™ / GPRS Wireless Networks
iDEN® Wireless Networks
DataTAC Wireless Networks
CDMA Wireless Networks
Mobitex Wireless Networks
Multiple Devices
BlackBerry Enabled Devices
BlackBerry Devices

Figure 1. BlackBerry Solution Architecture

BlackBerry devices are built on industry-leading wireless technology, allowing users to receive email and information automatically with no need to request delivery. Additionally, users are notified when new information arrives, making it easier to stay informed.

BlackBerry devices also provide an intuitive user experience. Users simply click on an email address, telephone number, or URL inside a message to automatically begin composing the new email, make the call, or link to the web page. BlackBerry device users can also easily navigate through icons, menus, and options with the roll-and-click trackwheel or trackball, and quickly compose messages or enter data using the device keyboard.

Each BlackBerry device[1] contains the BlackBerry Cryptographic Kernel, a firmware module that provides the cryptographic functionality required for basic operation of the device. The BlackBerry Cryptographic Kernel meets the requirements of the FIPS 140-2 Security Level 1.

The BlackBerry Cryptographic Kernel, 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
- digital signature verification
- elliptic curve key agreement

More information on the BlackBerry solution is available from http://www.blackberry.com/.

[1] Excludes RIM 850™, RIM 950™, RIM 857™, and RIM 957™ wireless handheld devices.

The BlackBerry Cryptographic Kernel meets the overall requirements applicable to Level 1 security for FIPS 140-2 as shown in Table 1.

Table 1. Summary of achieved Security Levels per FIPS 140-2 Section

Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	1
Cryptographic Module Security Policy	1

2 Cryptographic Module Specification

2.1 Security Functions

The cryptographic module is a firmware module that implements the following FIPS-approved security functions[2]:

Table 2. Approved Security Functions

Algorithm	Description	Certificate number
AES-256 ASM Code	Encrypts and decrypts, as specified in FIPS 197. The implementation supports the CBC and CTR modes of operation.	#1403
AES-256 Native Code	Encrypts and decrypts, as specified in FIPS 197. The implementation supports the CBC and CTR modes of operation.	#1402
Triple DES	Encrypts and decrypts, as specified in FIPS 46-3. The implementation supports the CBC mode of operation.	#956
SHA-1, SHA-256, and SHA-512	as specified in FIPS 180-3	#1273
HMAC-SHA-1, HMAC-SHA-256 & HMAC-SHA-512	as specified in FIPS 180-3	#824
FIPS 186-2 RNG	As specified in FIPS 186-2. The implementation uses SHA-1 as the function G.	#769
ECDSA	Signature verification, as specified in FIPS 186-2 and ANSI X9.62. The implementation supports elliptic curve K-571.	#177
RSA PKCS#1	Signature verification, as specified in PKCS #1, version 2.1	#682

[2] 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*.

The module implements the following non approved security functions that, per *FIPS 140-2 Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2,* may presently be used in a FIPS-approved mode of operation:

- **EC Diffie-Hellman** (key agreement, key establishment methodology provides 256 bits of encryption strength), Per FIPS 140-2 Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2, the implementation may presently be used in a FIPS-approved mode of operation. The implementation supports elliptic curves P-521 and K-571.
- **ECMQV** (key agreement, key establishment methodology provides 256 bits of encryption strength), Per FIPS 140-2 Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2, the implementation may presently be used in a FIPS-approved mode of operation. The implementation supports elliptic curves P-521 and K-571.

2.2 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.

2.3 Conformance Testing and FIPS-Compliance

For the purposes of FIPS 140-2 conformance testing, the module was executed on the BlackBerry 9800 per FIPS 140-2 Implementation Guidance G.5.The module remains vendor affirmed FIPS-compliant when executed on other BlackBerry devices.

Conformance testing was performed using BlackBerry OS Version 6.0. In order for the module to remain validated on a specific handheld device, both the unchanged module and the tested operating platform shall be ported to any device.

2.4 Cryptographic Boundary

The physical boundary of the module is the physical boundary of the BlackBerry device that executes the module as shown in the following figure. Consequently, the embodiment of the module is a multiple-chip standalone.

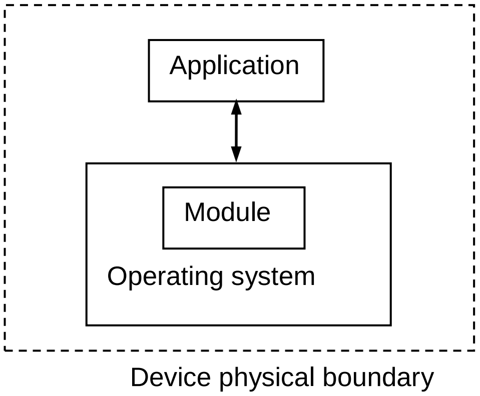

Figure 2. Physical Boundary

2.5 Determining the Module Version

The operator can determine the version of the module on a BlackBerry device by performing the following operations:

1. On the BlackBerry device Home screen, click the **Options** icon.

2. Click **Device → About Device Versions**
3. The About screen displays the module version, for example, Cryptographic Kernel v3.8.6.5

3 Cryptographic Module Ports and Interfaces

The module ports correspond to the physical ports of the BlackBerry device executing the module, and the module interfaces correspond to the logical interfaces to the module. The following table describes the module ports and interfaces.

Table 3. Implementation of FIPS 140-2 Interfaces

FIPS 140-2 interface	Module ports	Module interfaces
Data Input	keyboard, touch screen, microphone, USB port, headset jack, wireless modem, and Bluetooth® wireless radio	input parameters of module function calls
Data Output	speaker, USB port, headset jack, wireless modem, and Bluetooth wireless radio	output parameters of module function calls
Control Input	keyboard, touch screen, USB port, trackball, BlackBerry button, escape button, backlight button, and phone button	module function calls
Status Output	USB port, primary LCD screen, and LED	return codes of module function calls
Power Input	USB port	not supported
Maintenance	not supported	not supported

4 Roles, Services, and Authentication

4.1 Roles

The module supports user and crypto officer roles. 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.

4.2 Services

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

Table 4. Module Services

Service	Description
Reset	Resets the module. The module can be reset by power cycling the module.
View Status	displays the status of the module
Inject Master Key	Replaces the existing Master Key with a new Master Key. The new Master Key is created outside the cryptographic boundary for this service.
Perform Key Agreement	Establishes a secure channel to the module utilizing ECDH and ECMQV key agreement algorithms in transport of the new Master Key that is created outside the cryptographic boundary.
Inject PIN Master Key	Replaces the existing PIN master key with a new PIN master key. The new PIN master key is created outside the cryptographic boundary and is encrypted for input into the module for this service.
Generate Session Key	Generates a session key or a PIN session key. This service is performed automatically on behalf of the operator during the Encrypt Data service.
Encrypt Data	Encrypts data that is to be sent from the device. A session key is automatically generated through the Generate Session Key service and used to encrypt the data. The session key is encrypted with the master key and then the encrypted data and encrypted session key are ready for transmission.
Decrypt Data	Decrypts data that has been received by the device. The encrypted session key is decrypted with the master key and is then used to decrypt the data. This service is performed automatically on behalf of the operator.
Generate HMAC	generates a message authentication code
Perform Self-Tests	executes the module self-tests
Verify Signature	Verifies the digital signature of an IT policy received by the device. This service is performed automatically on behalf of the operator.

Service	Description
Wipe Handheld	zeroizes all software device keys and user data present on device

4.3 Authentication

The module does not support operator authentication. Roles are implicitly selected based on the service performed by the operator. Implicit role selection is summarized in the following table, as are the keys and critical security parameters (CSPs) that are affected by each service.

Table 5. Role Selection by Module Service

Service	Implicitly selected role	Affected keys and CSPs	Access to keys and CSPs
Reset	user	n/a	n/a
View Status	user	n/a	n/a
Inject Master Key	crypto officer	master key	write
Perform Key Agreement	crypto officer	ECC key pair	execute
		master key	write
Inject PIN Master Key	crypto officer	PIN master key	write
Generate Session Key	user	session key or PIN session key	write
Encrypt Data	user	master key or PIN master key	execute
		session key or PIN session key	execute
Decrypt Data	user	master key or PIN master key	execute
		session key or PIN session key	execute
Generate HMAC	user	HMAC key	execute
Perform Self-Tests	user	firmware integrity key	execute
Verify Signature	user	ECC public key	execute
Wipe Handheld	crypto officer	all software keys	write

5 Physical Security

The BlackBerry device that executes the module is manufactured using industry standard integrated circuits and meets the FIPS 140-2 Level 1 physical security requirements.

6 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 or CSP	Description
Master Key	A Triple DES or AES-256 key used to encrypt and decrypt Session Keys. The Master Key is always generated outside the cryptographic boundary. The Key may be input into the module: • in plaintext as parameters to an API call when connected directly to the USB port of a workstation operating BlackBerry Desktop Manager, or • encrypted by the current Master Key if utilizing key agreement with the BlackBerry Enterprise Server.
Session Key	A Triple DES or AES-256 key used to encrypt and decrypt data. The module generates session keys using the implemented FIPS 186-2 RNG.
PIN Master Key	A master key that is specifically a Triple DES key used to encrypt and decrypt PIN session keys. The PIN master key is generated outside the cryptographic boundary The key can be used as input into the module in the following ways: • in plaintext, as parameters to an API call when connected directly to the USB port of a workstation operating BlackBerry Desktop Manager • encrypted by the current master key if utilizing key agreement with the BlackBerry Enterprise Server.
PIN Session Key	A session key that is specifically a Triple DES key used to encrypt and decrypt data for PIN messaging. The module generates PIN session keys using the implemented FIPS 186-2 RNG.
ECC Key Pair	a key pair used to perform key agreement over elliptic curves
ECC Session Key	An ECC session key, that is specifically a short lived ephemeral key, is used during key agreement during Master Key transport and is zeroized after use.
ECC Public Key	a public key used to verify digital signatures over elliptic curves and part of the Key Agreement process
HMAC Key	a key used to calculate a message authentication code using the HMAC algorithm
RSA Public Key	a public key used to verify digital signatures in the Firmware Integrity Test

6.1 Key Zeroization

The BlackBerry security solution provides multiple protective features to ensure algorithmic keys and key components are protected. Similarly, data, and specifically key removal through zeroization, is an integral part of the BlackBerry security solution. A user can also request a zeroization at any time by navigating to **Options** and selecting **Wipe Handheld** using the **Options → Security → Security Wipe**. The BlackBerry Enterprise Server administrator may also zeroize the device remotely to wipe all device data and keys.

Furthermore, session keys that are created per datagram are destroyed after each data fragment is sent.

7 Self-Tests

The module implements the self-tests that are described in the following table:

Table 7. Module Self-Tests

Test	Description
Firmware Integrity Test	The module implements an integrity test for the module software 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 CAT	The module implements a compare answer test (CAT) for the AES-256 variants. Each AES implementation takes the same test data and same test key to perform an encryption operation. The result of each encryption operation is then compared to each other to verify that they were able to calculate the same result. If the results are the same, the test passes. If the results are different, the encrypt test fails. The module then performs a compared test for decryption using known encrypted test data and test key where each implementation is given the same key and data and performs a decryption operation. The results of each decryption operation from the C++ and assembler implementations are then compared against the calculated results. If both implementations are able to calculate the same result, the test passes. If they do not calculate the same result, then the test fails.
Triple DES CBC KAT	The module implements a KAT for Triple DES in the CBC mode of operation. The test 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.

Test	Description
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.
ECDSA Verify KAT	The module implements a KAT for ECDSA 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.
EC Diffie-Hellman KAT	The module implements a KAT for EC Diffie-Hellman. The KAT passes if and only if the calculated output equals the expected output.
ECMQV KAT	The module implements a KAT for ECMQV. The KAT passes if and only if the calculated output equals the expected output.

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.

7.1 Invoking the Self-Tests

The operator can invoke the power-up self-tests by resetting the module using the Reset service.

The operator can also invoke all of the self-tests with the exception of the Firmware Integrity Test and Continuous RNG test by performing the following operations:

1. Navigate to the **Options → Security → Security Status Information**.
2. Click the BlackBerry button to open the options menu.
3. In the menu, click **Verify Security Software**.

When the self-tests are executed in this manner, the module displays the list of self-tests that are being executed and a pass or fail status upon completion.

8 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 maneuvers designed to aid in the protection of cryptographic keys and plaintext 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 Electromagnetic 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

Acronym	Full term
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	application programming interface
CAT	compare answer test
CBC	cipher block chaining
CSP	critical security parameter
DEMA	differential electromagnetic analysis
DES	Data Encryption Standard
DPA	differential power analysis
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-hash message authentication code
IEEE	Institute of Electrical and Electronics Engineers
KAT	known answer test
LCD	liquid crystal display
LED	light-emitting diode
OS	operating system
PIN	personal identification number
PKCS	Public Key Cryptography Standard
PUB	Publication
RIM	Research In Motion

RNG	Random number generator
RSA	Rivest, Shamir, Adleman
SEMA	simple electromagnetic analysis
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SMS	Short Message Service
SPA	simple power analysis
URL	Uniform Resource Locator
USB	Universal Serial Bus