FIPS 140-2 Security Policy

BlackBerry Cryptographic Library

Version 2.0.0.7

BlackBerry Security Group, Research in Motion

Document Version 2.2

Document and Contact Information

Version	Date	Description
1.0	3 April 2009	Document creation
1.1	7 July 2009	Minor revisions to policy including certificate numbers
1.2	8 July 2009	Added Approved Mode of Operation section
1.3	22 July 2009	Updated policy with minor revisions from lab
1.4	29 July 2009	Updated policy with minor revisions
2.0	11 Sept 2009	Updated policy with comments from CMVP
2.1	7 October 2009	Updated Table 7 & Table 5 referring to RNG
2.2	20 November 2009	Updated 7.2 with comments 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 Figures

List of Tables

1 Introduction

1.1 Overview

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

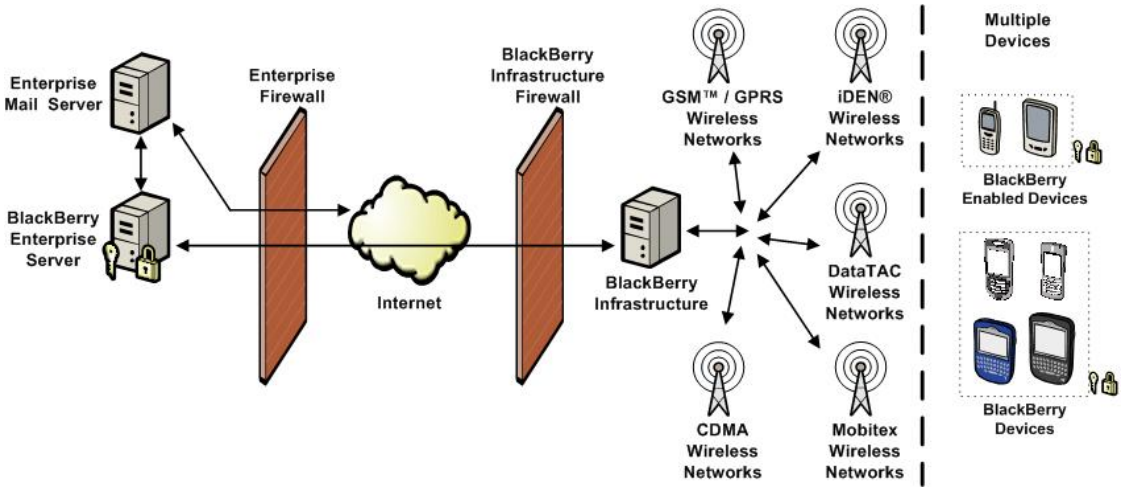

Figure 1. BlackBerry Solution Architecture

BlackBerry® Enterprise Server software tightly integrates with Microsoft® Exchange, IBM® Lotus® Domino®, and Novell® GroupWise® while working with other existing enterprise systems to enable push-based access of wireless email and data. It allows users to securely send and receive email and information from enterprise data stores and applications.

BlackBerry® Desktop Software runs on your computer, allowing you to keep your computer and smartphone data organized. It synchronizes the email and organizer information between your BlackBerry smartphone and your computer.

For more information on the BlackBerry solution, visit http://www.blackberry.com/.

The BlackBerry Cryptographic Library, hereafter referred to as cryptographic module or module, is a software module that provides the following cryptographic services to many BlackBerry desktop products such as the BlackBerry Enterprise Server, BlackBerry Desktop Software, and many others.

- Data encryption and decryption
- Message digest and authentication code generation
- Random data generation
- Elliptic curve key pair generation
- Elliptic curve digital signature generation and verification
- Elliptic curve key agreement

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

Table 1. Summary of achieved Security Level 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	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	3
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	1

2 Cryptographic Module Specification

2.1 Security Functions

The cryptographic module is a software module in the form of a DLL file that implements the following FIPS approved security functions[1]:

Table 2. Approved Security Functions

Algorithm	Description	Certificate Number
AES-128, **AES-192 &** **AES-256**	(encrypt and decrypt), as specified in FIPS 197. The implementation supports the ECB and CBC modes of operation	1122
Triple DES	(encrypt and decrypt), as specified in FIPS 46-3. The implementation supports the ECB and CBC modes of operation	819
SHA-1, **SHA-224,** **SHA-384 &** **SHA-512**	as specified in FIPS 180-2.	1045
HMAC SHA-1, **HMAC SHA-224,** **HMAC SHA-256,** **HMAC SHA-384, &** **HMAC SHA-512**	as specified in FIPS 198.	633
FIPS 186-2 RNG	as specified in FIPS 186-2	625
ECDSA	as specified in FIPS 186-2	131

The module implements the following non approved but allowed security functions:

- 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.

The module implements the following non approved security functions:

- Rijndael. The implementation supports the ECB and CBC modes of operation; key lengths of 128, 160, 192, 224, and 256 bits; and block lengths of 1281, 160, 192, 224, and 256 bits.

2.2 Cryptographic Boundary

The module's physical boundary is the physical boundary of the GPC that executes the module and is shown in the following figure.

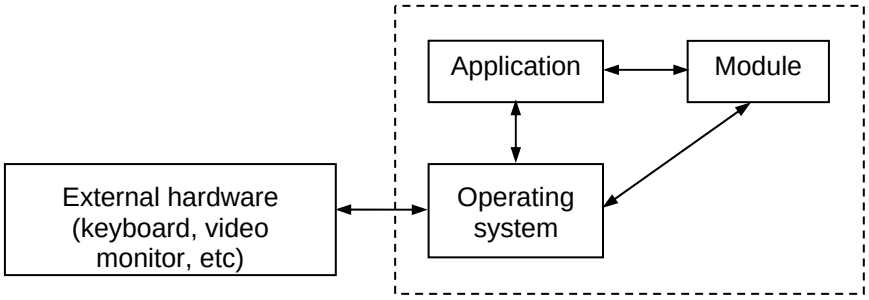

Figure 2. Physical Boundary

2.3 Determining the Module Version

The operator can determine the module version by viewing the Properties screen for the DLL file:

1. Navigate to and right-click the module file name, for example, CE.dll.
2. Select **Properties** from the resulting context menu.
3. Select the **Version** tab.
4. The versioning information screen appears and displays the module version, for example, 2.0.0.7.

3 Cryptographic Module Ports and Interfaces

The module's physical ports correspond to the ports of the GPC that execute the module, and the logical interface of the module is its API. The module implements the FIPS 140-2 interfaces as described in the following table.

Table 3. Implementation of FIPS 140-2 Interfaces

FIPS 140-2 interface	Module ports	Module interfaces
Data input	GPC input ports, for example, the keyboard and mouse	Input parameters of API function calls
Data output	GPC output ports, for example, the video display	Output parameters of API function calls
Control input	GPC control input ports, for example, the keyboard and power switch)	API function calls
Status output	GPC status output ports, for example, the video display and LED	Function calls that return status information and return code provided by each API function call
Power input	GPC power input ports, for example, the power supply	Not supported
Maintenance	GPC maintenance port, for example, the access panel	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 or concurrent operators.

4.2 Services

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

Table 4. Module Services

Service	Description
Show Status	Displays the status of the module
Perform Self-Tests	If invoked through the SelfTest function call, executes the cryptographic algorithm known-answer tests. If invoked by turning on the module, executes the power-up self-tests.
Encrypt Data	Encrypts data using AES , Triple DES, or Rijndael[1], as specified by the operator
Decrypt Data	Decrypts data using AES, Triple DES, or Rijndael[1], as specified by the operator
Create Message Digest	Calculates a message digest using SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512, as specified by the operator
Create MAC	Calculates a message authentication code using HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, or HMAC SHA-512, as specified by the operator
Generate Random Data	Generates random data using the FIPS 186-2 RNG
Generate Key Pair	Generates an elliptic curve key pair, consisting of a public and private key
Generate Signature	Generates a digital signature using ECDSA
Verify Signature	Verifies an ECDSA digital signature
Perform Key Agreement	Cooperatively calculates a symmetric key with another party through elliptic curve Diffie-Hellman or elliptic curve MQV key agreement
Zeroize	Zeroizes all keys and CSPs used during cryptographic service

- [1] Rijndael cannot be used for the Encrypt/Decrypt service in FIPS mode of operation

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	Role implicitly selected	Affected keys and CSPs	Access to keys and CSPs
Show Status	User	N/A	N/A
Perform Self-Tests	Crypto officer	Software Integrity key	Execute
Encrypt Data	User	AES key Triple DES key Rijndael key[2]	Execute
Decrypt Data	User	AES key Triple DES key Rijndael key[2]	Execute
Create Message Digest	User	N/A	N/A
Create MAC	User	HMAC key	Execute
Generate Random Data	User	RNG Seed RNG Seed Key	Execute
Generate Key Pair	User	ECC key pair	Write
Generate Signature	User	ECC private key	Execute
Verify Signature	User	ECC public key	Execute
Perform Key Agreement	User	ECC key pair	Execute
		AES key Triple DES key Rijndael key	Write
Zeroize	Crypto Officer	All software keys	Write

- [2] Rijndael cannot be used for the Encrypt/Decrypt service in FIPS mode of operation

5 Physical Security

The module is implemented entirely in software, thus the FIPS 140-2 physical security requirements are not applicable.

6 Operational Environment

The module is designed to execute on a GPC running an applicable BlackBerry application. The minimum requirements for the operational environment for all BlackBerry applications are listed in the following table:

Table 6. BlackBerry Cryptographic Library Environments

Operating system	Version
Microsoft Windows XP (All Editions)	32 Bit
Microsoft Windows Vista (All Editions)	32 Bit 64 Bit
Microsoft Windows Server 2003 SP2	32 Bit 64 Bit
Microsoft Windows Server 2003 R2	32 Bit 64 Bit
Microsoft Windows Small Business Server 2003	32 Bit

The operating system is restricted to a single-user mode of operation per FIPS 140-2 Implementation Guidance 6.1.

For the purposes of FIPS 140-2 conformance testing, the module was tested on Windows XP Professional SP3, 32 Bit edition. However, the module can be executed on any of the supported operating systems and remain vendor affirmed FIPS-compliant.

7 Cryptographic Keys and Critical Security Parameters

7.1 Cryptographic Keys and CSPs

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

Table 7. Cryptographic Keys and CSPs

Key/CSP	Description
AES key	A symmetric key used to encrypt and decrypt data using the AES algorithm. The module supports AES key lengths of 128, 192, and 256 bits.
Triple DES key	A symmetric key used to encrypt and decrypt data using the Triple DES algorithm. Per the specification of Triple DES, all Triple DES keys are 192 bits in length.
HMAC key	A key used to calculate a message authentication code using the HMAC algorithm. The length of the HMAC key is dependent on the underlying hash algorithm.
Software Integrity key	A 128-bit HMAC SHA-1 key used to verify the integrity of the module
ECC key pair	A key pair used to generate and verify digital signatures or to perform key agreement over elliptic curves.
Rijndael key	A symmetric key used to encrypt and decrypt data using the Rijndael algorithm. The module supports Rijndael key lengths of 160 and 224 bits.
RNG Seed	Seed used for initializing the RNG
RNG Seed Key	Seed key used for initializing the RNG

7.2 Key Input/Output

The module does not allow for manually entry of cryptographic keys. All keys are passed to the module via the API when called upon for a cryptographic service.

All intermediate keys that are created for the use of a service are not output. Immediately after a cryptographic service has been completed all keys and CSPs are zeroized.

7.3 Key Storage

The module does not store any keys or CSPs, any keys that are used by the module are passed in via the API and are zeroized after use.

7.4 Key Zeroization

As the module is called for a cryptographic service, keys are passed to the module via the API, once the service is executed all associated CSPs and keys are zeroized immediately.

8 Self-Tests

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

Table 8. Module Self-Tests

Test	Description
Software Integrity Test	The Software Integrity Test verifies the integrity of the module software using HMAC SHA-1.
FIPS 186-2 RNG Known Answer Test	The FIPS 186-2 RNG Known Answer Test (KAT) verifies that the RNG is operating correctly.
AES Known Answer Test	The AES KAT verifies that the AES encryption and decryption functions are operating correctly.
Triple DES Known Answer Test	The Triple DES KAT verifies that the Triple DES encryption and decryption functions are operating correctly.
SHA-1 Known Answer Test	The SHA-1 KAT verifies that the SHA-1 hashing function is operating correctly.
SHA-224 Known Answer Test	The SHA-224 KAT verifies that the SHA-224 hashing function is operating correctly.
SHA-256 Known Answer Test	The SHA-256 KAT verifies that the SHA-256 hashing function is operating correctly.
SHA-384 Known Answer Test	The SHA-384 KAT verifies that the SHA-384 hashing function is operating correctly.
SHA-512 Known Answer Test	The SHA-512 KAT verifies that the SHA-512 hashing function is operating correctly.
HMAC SHA-1 Known Answer Test	The HMAC SHA-1 KAT verifies that the HMAC SHA-1 function is operating correctly.
HMAC SHA-224 Known Answer Test	The HMAC SHA-224 KAT verifies that the HMAC SHA-224 function is operating correctly.
HMAC SHA-256 Known Answer Test	The HMAC SHA-256 KAT verifies that the HMAC SHA-256 function is operating correctly.
HMAC SHA-384 Known Answer Test	The HMAC SHA-384 KAT verifies that the HMAC SHA-384 function is operating correctly.
HMAC SHA-512 Known Answer Test	The HMAC SHA-512 KAT verifies that the HMAC SHA-512 function is operating correctly.
Continuous RNG Test	The module implements a continuous RNG test, as specified in FIPS 140-2, for the implemented FIPS 186-2 RNG.

Test	Description
ECDH Pair-Wise Consistency Test	The ECDH Pair-Wise Consistency test verifies that the ECDH key agreement functions over elliptic curve are operating correctly during power-up.
ECMQV Pair-Wise Consistency Test	The ECMQV Pair-Wise Consistency test verifies that the ECMQV key agreement functions over elliptic curves are operating correctly during power-up.
ECDSA Pair-Wise Consistency Test	The ECDSA Pair-Wise Consistency test verifies that the ECDSA signature creation and verification functions are operating correctly during power-up and conditionally.

All self-tests including all KATs and Pair-Wise Consistency tests are executed during power-up without requiring operator input or action. The Software Integrity Test is the first self-test executed during power-up.

When an operator attempts to load the module into GPC memory, the power-up self-tests are executed. The power-up self-tests are comprised of all the previously identified tests with the exception of the Continuous RNG Test. The Software Integrity Test is the first self-test executed, and if it fails, the attempt to load the module fails. If a cryptographic algorithm KAT fails, the operator may not access the corresponding algorithm until the KAT is executed successfully.

The operator may invoke the power-up self-tests by unloading and reloading the module into GPC memory. The operator may also invoke all of the power-up self-tests, except the Software Integrity Test, by invoking the Perform Self-Tests service.

9 Mitigation of Other Attacks

The module is not designed to mitigate any specialized attacks, thus the FIPS 140-2 requirements for mitigation of other attacks are not applicable.

10 Approved Mode of Operation

10.1 Installation and Start up

The following steps must be performed to install and initialize the cryptographic module for operating in a FIPS 140-2 compliant manner:

- The BlackBerry Cryptographic Library must be installed as part of a BlackBerry Enterprise Software or BlackBerry desktop products.
- Each instance of the BlackBerry Cryptographic Library must be associated with only one application program.

10.2 Rules for Approved Mode of Operation

The following policy must always be followed in order to ensure a FIPS 140-2 mode of operation:

- The operating system must be restricted to a single user at a time. Multiple concurrent operators are not allowed.
- All keys entered into the cryptographic module must be verified as being legitimate and belonging to the correct entity by the host BlackBerry desktop product.
- Only FIPS Approved cryptographic functions may be used when performing cryptographic operations.

The above conditions must be upheld at all times in order to ensure continued system security after initial setup of the validated configuration. Failure to follow these rules will mean the module is not operating in an approved mode of operation.

Glossary

Acronym	Full term
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	application programming interface
CBC	Cipher block chaining
CSP	Critical security parameter
DES	Data Encryption Standard
DLL	dynamic linked library
EC	Elliptic curve
ECB	Electronic code book
ECC	Elliptic curve cryptography
ECDSA	Elliptic curve Digital Signature Algorithm
ECMQV	Elliptic curve Menezes, Qu, Vanstone
FIPS	Federal Information Processing Standard
GPC	general purpose computer
HMAC	Keyed-hashed message authentication code
IEEE	Institute of Electrical and Electronics Engineers
KAT	Known answer test
MAC	message authentication code
PUB	Publication
RIM	Research In Motion
RNG	random number generator
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SMS	Short Messaging Service