BlackBerry® Enterprise Server Cryptographic Kernel version 1.0.0.2

FIPS 140-2 Non-Proprietary Security Policy
Document Version 1.10

BlackBerry® Security Team

Research In Motion

Document and Contact Information

Version	Date	Author	Description
1.0	24 July 2003	Dave MacFarlane	Document creation.
1.1	31 July 2003	Dave MacFarlane	Included feedback from peer review.
1.2	8 August 2003	Dave MacFarlane	Corrected Microsoft Base Cryptographic Provider information.
1.3	23 September 2003	Dave MacFarlane	Included feedback from CMT lab review.
1.4	29 October 2003	Dave MacFarlane	Incorporated feedback given during CMT testing of module.
1.5	30 October 2003	Dave MacFarlane	Further feedback from CMT testing.
1.6	12 November 2003	Dave MacFarlane	Added algorithm certificate numbers and updated module version number.
1.7	31 March 2004	Dave MacFarlane	Revisions due to CMVP comments.
1.8	31 March 2004	Dave MacFarlane	Corrected Rijndael information.
1.9	11 May 2004	Dave MacFarlane	Updated RNG information.
1.10	28 May 2004	Dave MacFarlane	Updated RNG information.

Contact	Corporate Office
BlackBerry® Security Team BlackBerrySecurity@rim.com (519) 888-7465 ext. 2921	Research In Motion Limited 175 Columbia Street West Waterloo ON Canada N2L 5Z5

Contents

Introduction 3

Cryptographic Module Specification 3

Cryptographic Module Ports and Interfaces 3

Roles, Services, and Authentication 3

Physical Security 3

Operational Environment 3

Cryptographic Key Management 3

- General 3
- Random Number Generators 3
- Key Generation 3
- Key Entry and Output 3
- Key Storage 3
- Key Zeroization 3

Self-Tests 3

Mitigation of Other Attacks 3

Installation and Start-Up 3

FIPS 140-2 Mode of Operation 3

Glossary 3

List of Tables

Table 1. Security Levels Achieved by FIPS 140-2 Section 3
Table 2. Required Module Interfaces 3
Table 3. Module Roles and Approved Services....3
Table 4. Cryptographic Keys and CSPs....3
Table 5. FIPS-Validated Microsoft® Base Cryptographic Providers....3
Table 6. Module Self-Tests....3

Introduction

The BlackBerry® Enterprise Server centralises e-mail redirection for BlackBerry Wireless Handheld™ users in an organisation and performs the following functions for each user:

- Monitors the user's Inbox for new mail;
- Applies filters to new messages to determine if and how to redirect them to a user's BlackBerry® handheld;
- Compresses and encrypts new messages and delivers them to the BlackBerry® handheld over the Internet; and
- Receives, decompresses, and decrypts new messages composed on the BlackBerry® handheld and places them in the user's Outbox for delivery by the corporate mail server.

The BlackBerry Enterprise Server operates in both Microsoft® Exchange and Lotus® Domino™ messaging environments.

The BlackBerry® Enterprise Server Cryptographic Kernel, hereafter referred to as *cryptographic module* or *module*, is a software cryptographic module that provides data encryption and decryption and other cryptographic services to the BlackBerry Enterprise Server. The module has been validated to FIPS 140-2 Security Level 1, and the Security Level achieved for each of the eleven sections of FIPS 140-2 is identified in the following table. Security Levels identified with an asterisk, "*", are chosen commensurately with the overall Security Level.

Table 1. Security Levels Achieved by FIPS 140-2 Section

FIPS 140-2 Section	Security Level Achieved
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 Specification

The BlackBerry® Enterprise Server Cryptographic Kernel is a Microsoft® Windows®-compatible dynamically linked library (DLL) that performs data encryption and decryption and calculates message digests and authentication codes.

The module implements the following FIPS-Approved[1] security functions:

- **AES-128**, **AES-192**, and **AES-256**, as specified in FIPS PUB 197. The ECB and CBC modes of operation are supported. The implementation has been awarded AES validation certificate # 104 on the AES Validation List, http://csrc.nist.gov/cryptval/aes/aesval.html.
- **Triple DES**, as specified in FIPS PUB 46-3. The ECB and CBC modes of operation are supported. The implementation has been awarded Triple DES validation certificate # 216 on the Triple DES Validation List, http://csrc.nist.gov/cryptval/des/tripledesval.html.
- **SHA-1**, as specified in FIPS PUB 180-2. The implementation has been awarded SHS validation certificate # 195 on the SHS Validation List, http://csrc.nist.gov/cryptval/shs/shaval.htm.
- **HMAC SHA-1**, as specified in FIPS PUB 198. In conjunction with SHS validation certificate # 195, the implementation is affirmed to be correct.

The module implements the following non-Approved security functions:

- **Rijndael**. The ECB and CBC modes of operation are supported, as are key lengths of 128, 160, 192, 224 and 256 bits and block lengths of 160, 192, 224 and 256 bits.

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

Cryptographic Module Ports and Interfaces

The logical interface of the module is its Application Programming Interface (API). The module implements the required FIPS 140-2 interfaces as shown in the following table:

Table 2. Required Module Interfaces

FIPS 140-2 Interface	Module Implementation
Data Input	The module implements the Data Input Interface via the input parameters of each API function call.
Data Output	The module implements the Data Output Interface via the output parameters of each API function call.
Control Input	The module implements the Control Input Interface via the API function calls.
Status Output	The module implements the Status Output Interface via specific API function calls that return status information and the return code provided by each API function call after execution.

Roles, Services, and Authentication

The module supports a User role and a Crypto Officer role. The module does not support a Maintenance role. Role selection is performed implicitly and is dependent on the service performed by the operator. The following services are available to the operator:

- **Show Status** – Displays the status of the module.
- **Perform Self-Tests** – Invokes the cryptographic algorithm known answer tests (KATs), a subset of the power-up self-tests.
- **Encrypt Data** – Encrypts data using AES, Triple DES or Rijndael, as specified by the operator.
- **Decrypt Data** – Decrypts data using AES, Triple DES or Rijndael, as specified by the operator.
- **Create Message Digest** – Calculates a message digest using SHA-1.
- **Create Message Authentication Code** – Calculates a message authentication code (MAC) using HMAC SHA-1.
- **Request Random Data** – Requests random data from the FIPS PUB 186 random number generator (RNG) implemented in the Microsoft® Base Cryptographic Provider.

The following table summarises implicit role selection based on service and the associated access to critical security parameters (CSPs).

Table 3. Module Roles and Services

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	Read/Execute
Encrypt Data	User	AES Key Triple DES Key Rijndael Key	Read/Execute
Decrypt Data	User	AES Key Triple DES Key Rijndael Key	Read/Execute
Create Message Digest	User	N/A	N/A
Create Message Authentication Code	User	HMAC Key	Read/Execute
Request Random Data	User	N/A	N/A

Physical Security

The module is implemented purely in software, thus it provides no physical security mechanisms and the FIPS 140-2 physical security requirements are not applicable.

Operational Environment

The module is designed to execute on a general purpose computer (GPC) in conjunction with the BlackBerry Enterprise Server application. The BlackBerry Enterprise Server application supports the following operating systems:

- Microsoft® Windows NT® Server 4.0 Service Pack (SP) 5 or later (for a Microsoft® Exchange environment);
- Microsoft® Windows NT® Server 4.0 SP 6a or later (for a Lotus® Domino™ environment); or
- Microsoft® Windows® 2000 Server SP 1 or later.

The operating system is restricted to a single user mode of operation as per FIPS 140-2 Implementation Guidance 6.1, i.e., the BlackBerry Enterprise Server application is the single user of the module, even when the server application is serving multiple clients.

For the purposes of FIPS 140-2 conformance testing, the module was tested on Windows NT® Server 4.0 SP 6a. This, however, does not invalidate the FIPS 140-2 validation of the module when it is executed on any of the operating systems identified above.

Cryptographic Key Management

General

The following table identifies the keys, key components, and CSPs utilised by the module:

Table 4. 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 calculate and verify the integrity of the module as specified in Self-Tests.
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.

Random Number Generators

The module provides a **Request Random Data** service, yet the module does not implement an RNG. When invoked, the **Request Random Data** service requests random data from the FIPS PUB 186 RNG implemented in the Microsoft® Base Cryptographic Provider, a FIPS-validated cryptographic module developed by Microsoft® and included with Windows® operating systems. Table 5 identifies the FIPS-validated version and the FIPS 140-1 or FIPS 140-2certificate number of the Microsoft® Base Cryptographic Provider for each of the Windows® operating systems supported by the BlackBerry® Enterprise Server Cryptographic Kernel module, as identified in Operational Environment on page 3.

Table 5. FIPS-Validated Microsoft® Base Cryptographic Providers

Windows® Operating System	Filename	Version	FIPS 140-1 / FIPS 140-2 Certificate No.
Windows NT® Server 4.0 SP 5 or later	rsabase.dll	5.0.2150.1	76
Windows® 2000 Server SP 1	rsabase.dll	5.0.2150.1391	103
Windows® 2000 Server SP 2	rsabase.dll	5.0.2150.2228	103
Windows® 2000 Server SP 3	rsabase.dll	5.0.2150.3839	103

Key Generation

The module does not support key generation.

Key Entry and Output

Keys are entered into the module in plaintext via the module API. The module does not support key output.

Key Storage

The module does not support general-purpose persistent key storage. Operational keys are stored in GPC memory only as long as they are required for processing by the module. However, the Software Integrity Key that is used during the Software Integrity Test is permanently stored in the module.

Key Zeroization

The module zeroizes operational keys once they are no longer needed for processing.

Self-Tests

The following table describes the self-tests implemented by the module:

Table 6. Module Self-Tests

Test	Description
Software Integrity Test	The Software Integrity Test verifies the integrity of the module software using HMAC SHA-1.
Triple DES Known Answer Test	The Triple DES KAT verifies that the Triple DES encryption and decryption functions are operating correctly.
AES Known Answer Test	The AES KAT verifies that the AES 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.
HMAC Known Answer Test	The HMAC KAT verifies that the HMAC function is operating correctly.

When an operator attempts to load the module into GPC memory, the power-up self-tests are executed. The power-up self-tests comprise of all the tests identified in Table 6. The Software Integrity Test is the first self-test executed, and if it fails then the attempt to load the module fails. If a cryptographic algorithm KAT fails then 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 accessing the **Perform Self-Tests** service.

Mitigation of Other Attacks

The module is not designed to mitigate any specialised attacks.

Installation and Start-Up

The module is installed as part of the BlackBerry Enterprise Server application, thus there are no specific installation instructions for the module. The installation instructions for the BlackBerry Enterprise Server application should be followed and are given in the following documents[2]:

- *BlackBerry® Enterprise Server for Microsoft® Exchange 5.5 Installation and Getting Started Guide*;
- *BlackBerry® Enterprise Server for Microsoft® Exchange 2000 Installation and Getting Started Guide*; and
- *BlackBerry® Enterprise Server for Lotus® Domino™ Installation and Getting Started Guide*.

[2] The listed installation and getting started guides are available on the BlackBerry® website at http://www.blackberry.com/.

FIPS 140-2 Mode of Operation

In order to operate the module in a FIPS-Approved manner, the following conditions must be met:

- When the **Request Random Data** service is used to obtain random data for use with the module in a FIPS-Approved mode of operation, the GPC on which the module executes must have a FIPS-validated version of the Microsoft® Base Cryptographic Provider installed (refer to Random Number Generators on page 3).
- Either the AES or Triple DES algorithm is used when performing data encryption and decryption. More specifically, the Rijndael algorithm is not used for data encryption or decryption.

Glossary

AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher Block Chaining
CSP	Critical security parameter
DES	Data Encryption Standard
DLL	Dynamically linked library
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
GPC	General purpose computer
HMAC	Keyed-hashed message authentication code
IG	Implementation Guidance
KAT	Known answer test
MAC	Message authentication code
RNG	Random number generator
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SP	Service Pack