Certification Report

EAL 4+ Evaluation of BlackBerry® Enterprise Server version 5.0.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-101-CR
Version:	1.0
Date:	27 April 2009
Pagination:	i to iii, 1 to 11

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is EWA-Canada located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 27 April 2009, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at: http://www.cse-cst.gc.ca/its-sti/services/cc/cp-pc-eng.html and http://www.commoncriteriaportal.org/

This certification report makes reference to the following trademarked names:

- RIM, Research In Motion, BlackBerry, are either trademarks or registered symbols of Research In Motion Limited;
- Microsoft is a registered trademark of Microsoft Corporation; and
- IBM, Lotus, Domino are registered trademarks of IBM Corporation.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

BlackBerry® Enterprise Server version 5.0.0 (hereafter referred to as Blackberry Enterprise Server), from Research In Motion Limited, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

BlackBerry Enterprise Server is a software application that provides centralized management and control of BlackBerry devices or BlackBerry enabled devices by means of the BlackBerry Infrastructure.

EWA-Canada is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 23 April 2009 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for the Blackberry Enterprise Server, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 4 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. The following augmentation is claimed: ALC_FLR.1 - Basic flaw remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the BlackBerry Enterprise Server evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is the BlackBerry® Enterprise Server (hereafter referred to as Blackberry Enterprise Server), from Research In Motion Limited (RIM).

2 TOE Description

BlackBerry Enterprise Server is a software application that resides on a general purpose computer within an enterprise. BlackBerry Enterprise Server provides a secure wireless extension of the enterprise messaging environment as well as centralized management and control of enterprise BlackBerry devices and BlackBerry enabled devices. BlackBerry Enterprise Server core functionality includes:

- Communication with the enterprise mail server;
- Secure communication with BlackBerry devices;
- Remote management of BlackBerry devices;
- Wireless email messaging; and
- Personal Information Management (PIM) data synchronisation.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Blackberry Enterprise Server is identified in Section 5 of the Security Target (ST).

BlackBerry Enterprise Server incorporates the BlackBerry Enterprise Server Cryptographic Kernel Version 1.0.2.10 which has been awarded FIPS 140-2 certificate #591.

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Blackberry Enterprise Server.

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	554
Advanced Encryption Standard (AES)	FIPS 197	561
Secure Hash Algorithm (SHA-1)	FIPS 180-3	626
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	296
Elliptic Curve Digital Signature Algorithm (ECDSA)	FIPS 186-2	59

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Security Target, BlackBerry® Enterprise Server Version 5.0.0
Version: 1.5

Date: 27 March 2009

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*.

The Blackberry Enterprise Server is:

a. Common Criteria Part 2 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirement defined in the ST: FCS_VAL_EXP.1 - Cryptographic module validation;

b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and

c. Common Criteria EAL 4 augmented, with all the security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.1 - Basic flaw remediation.

6 Security Policies

BlackBerry Enterprise Server enforces flow control security policies that control information flow to and from the BlackBerry Enterprise Server. The policies are:

Service Routing Protocol (SRP) Policy. The SRP Policy controls the flow of communication between the BlackBerry Enterprise Server and a BlackBerry device;

Server Policy. The Server Policy controls the flow of communication between the BlackBerry Enterprise Server and the enterprise mail server; and

IT Command Policy. The IT Command Policy controls the sending of wireless IT commands to a BlackBerry device.

In addition, BlackBerry Enterprise Server implements policies pertaining to cryptography, user data protection, protection of the TOE security functionality, identification and authentication, and security management. Further details on these security policies may be found in Section 5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the Blackberry Enterprise Server should consider assumptions about usage and environmental settings as requirements for the product’s installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage assumptions are listed in the ST:

- The TOE is directly connected to the enterprise network, behind the enterprise firewall, and has sufficient privileges to communicate with the enterprise mail server and the BlackBerry Infrastructure.
- One or more competent, trusted personnel are assigned and authorized to administer the TOE, and do so using the TOE guidance documentation.

7.2 Environmental Assumptions

The following Environmental assumptions are listed in the ST:

- The TOE and enterprise mail server are located in a controlled access facility that prevents unauthorised physical access.
- The environment in which the TOE and the enterprise mail server interact protects their communication from unauthorised modification and disclosure.

7.3 Clarification of Scope

The BlackBerry Enterprise Server offers protection against inadvertent or casual attempts to breach system security, by unsophisticated attackers possessing an enhanced-basic attack potential. It is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Architectural Information

BlackBerry Enterprise Server is a software application that resides on a general purpose computer located within an enterprise. The BlackBerry solution provides a secure wireless extension of the enterprise messaging environment. Refer to Figure 3 - TOE Physical Boundary in the ST. BlackBerry Enterprise Server comprises following main components.:

The **BlackBerry Configuration Database** is a relational database that contains configuration information that is used by the BlackBerry components that do not connect to the enterprise mail server directly. The configuration database includes the following information:

- details about the connection from the BlackBerry Enterprise Server to the wireless network;
- user list;

- PIN-to-email address mapping for connection service push functionality; and
- read-only copy of each user security key.

The **BlackBerry Controller** is designed to monitor the BlackBerry components and restart them if they stop responding.

The **BlackBerry Dispatcher** is designed to compress and encrypt all BlackBerry data. It routes the data through the BlackBerry Router to and from the wireless network.

The **BlackBerry Administration Service** is designed to manage the BlackBerry Domain, which includes BlackBerry Enterprise Server components, user accounts, and features for BlackBerry device administration.

The **BlackBerry Messaging Agent** is designed to connect to the messaging and collaboration server to provide message, calendar, address lookup, attachment, and wireless encryption key generation services. The messaging agent also acts as a gateway for the synchronisation service to access PIM data on the messaging server. It synchronises configuration data between the configuration database and user mailboxes.

The **BlackBerry Policy Service** is designed to perform administration services wirelessly such as sending IT policies and IT commands, and provisioning service books.

The **BlackBerry Router** is designed to connect to the wireless network to route data to and from the BlackBerry device. It is also designed to route data within the corporate network to BlackBerry devices that are connected to the user’s computer using the BlackBerry Device Manager.

The **BlackBerry Synchronisation Service** is designed to synchronise PIM application data between the BlackBerry device and the messaging server wirelessly.

9 Evaluated Configuration

The evaluated configuration comprises:

- BlackBerry Enterprise Server for IBM Lotus Domino Version 5.0.0 (5.0.0 bundle 223) executing on Microsoft Windows Server 2003 Service Pack 2; and
- BlackBerry Enterprise Server for Microsoft Exchange Version 5.0.0 (5.0.0 bundle 223) executing on Microsoft Windows Server 2003 Service Pack 2.

The BlackBerry Enterprise Server version and bundle number is displayed by navigating to the “Add or Remove Programs” interface in Microsoft Windows Server 2003 and clicking the “Click here for support information” link for the BlackBerry Enterprise Server software.

10 Documentation

The RIM documents provided to the consumer are:

a. Guidance documents for BlackBerry Enterprise Server for IBM Lotus Domino Version 5.0.0 are available at the BlackBerry Technical Solution Center: http://na.blackberry.com/eng/support/docs/subcategories/?userType=2&category=BlackBerry+Enterprise+Server+for+IBM+Lotus+Domino.

b. Guidance documents for BlackBerry Enterprise Server for Microsoft Exchange Version 5.0.0 are available at the BlackBerry Technical Solution Center: http://na.blackberry.com/eng/support/docs/subcategories/?userType=2&category=BlackBerry+Enterprise+Server+for+Microsoft+Exchange

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Blackberry Enterprise Server, including the following areas:

Development: The evaluators analysed the Blackberry Enterprise Server functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Blackberry Enterprise Server security architectural description and determined that the initialization process was secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the Blackberry Enterprise Server preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Blackberry Enterprise Server configuration management system and associated documentation was performed. The evaluators found that the Blackberry Enterprise Server configuration items were clearly and uniquely marked, and could be modified and controlled by automated tools. The developer’s configuration management system was observed during a site visit, and it was found to be mature and well developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the Blackberry Enterprise Server during distribution to the consumer.

The evaluators examined the development security procedures during a site visit and determined that they detailed all the security measures for the development environment to protect the confidentiality and integrity of Blackberry Enterprise Server design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by RIM for the Blackberry Enterprise Server. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of Blackberry Enterprise Server. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a focussed search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to Blackberry Enterprise Server in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

RIM employs a rigorous testing process that tests the changes and fixes in each release of the Blackberry Enterprise Server. Comprehensive regression testing is conducted for all releases.

The evaluators analyzed the developer’s test coverage and depth analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification, TOE design, and security architecture description was complete.

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach was the following list of EWA-Canada test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Operation of the BlackBerry Enterprise Server with the BlackBerry Smartphone: The objective of this test goal is to ensure that the operation of the BlackBerry Enterprise Server with the BlackBerry Smartphone is correct; and

c. Management: The objective of this test goal is to confirm that the BlackBerry Smartphone management functions are restricted to the administrator.

12.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and a focussed review of all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Generic vulnerabilities;
b. Bypass/Tampering;
c. Direct attacks;
d. Monitoring; and
e. Misuse.

The BlackBerry Enterprise Server evaluated configuration IT Policy subset comprises features configurations for user BlackBerry devices. The evaluator attempted to apply values and settings outside the IT Policy subset. The values and settings were not allowed.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

12.4 Conduct of Testing

The Blackberry Enterprise Server was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Testing (ITSET) Facility at EWA-Canada.

The CCS Certification Body witnessed a portion of the independent testing. Detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the Blackberry Enterprise Server behaves as specified in its ST, functional specification, TOE design and security architecture description.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The BlackBerry® Enterprise Server version 5.0.0 includes comprehensive Guidance documents.

The BlackBerry® Enterprise Server version 5.0.0 is straightforward to configure, use and integrate into a corporate network.

RIM uses a comprehensive change management process to control any changes to the TOE/product. RIM's Configuration Management (CM) and Quality Assurance (QA) provide all the requisite controls for managing all CM/QA activities.

RIM has a well defined, mature product development process, implementing a complete Product Development Plan (PDP) for each project.

The evaluators noted a high-level of security and confidentiality awareness and measures implemented by RIM. Substantial development and other security measures are in place.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
PDP	Product Development Plan
PIM	Personal Information Management
PIN	Personal Identification Number
QA	Quality Assurance
RIM	Research In Motion Limited
ST	Security Target
SRP	Service Routing Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality

16 References

This section lists all documentation used as source material for this report:

a. CCS-Guide-004 Version 1.1, Technical Oversight for TOE Evaluation, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1R2, September 2007.

c. Common Methodology for Information Technology Security Evaluation, Version 3.1R2, September 2007.

d. Security Target BlackBerry® Enterprise Server Version 5.0.0, Document Version 2.0, 14 April 2009.

e. Evaluation Technical Report (ETR) BlackBerry® Enterprise Server, EAL 4+ Evaluation, Common Criteria Evaluation Number: 383-4-101, Document No. 1604-000-D002, Version 0.5, 23 April 2009.