Certification Report

EAL 2+ Evaluation of Research In Motion Limited

BlackBerry® Enterprise Server Version 4.1.3

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-55-CR
Version: 1.0
Date: 12 September 2007
Pagination: i to v, 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 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. This certification report, and its associated certificate, applies 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 (CSE), 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 CSE, 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 (CSE).

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 Standard 17025, General requirements for the accreditation of calibration and testing 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 Electronic Warfare Associates-Canada, Ltd. 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 12 September 2007, 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/services/common-criteria/trusted-products-e.html and on the official Common Criteria Program website at: http://www.commoncriteriaportal.org/ .

This certification report makes reference to the following trademarked or registered trademarks:

- RIM, Research In Motion, BlackBerry, are either trademarks or registered symbols of Research In Motion Limited
- Microsoft is a registered trademark of Microsoft Corporation
- IBM, Lotus, Domino are registered trademarks of IBM Corporation
- Novell, Groupwise are registered trademarks of Novell, Inc.
- CVE is a trademark of MITRE Corporation

TABLE OF CONTENTS

Executive Summary

The BlackBerry® Enterprise Server Version 4.1.3 (hereafter referred to as BlackBerry Enterprise Server), from Research In Motion Limited is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

The 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.

Electronic Warfare Associates-Canada, Ltd. is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 4 September 2007 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 2 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*. The following augmentation is claimed: ALC_FLR.1 – Basic Flaw Remediation.

CSE, 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) 2 augmented evaluation is the BlackBerry Enterprise Server Version 4.1.3 (hereafter referred to as BlackBerry Enterprise Server), from Research In Motion Limited.

2 TOE Description

The BlackBerry Enterprise Server is a software application that resides on a general purpose computer within an enterprise. The 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
- Wireless personal information management (PIM) items synchronisation.

3 Evaluated Security Functionality

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

In addition, the BlackBerry Enterprise Server Cryptographic Kernel version 1.0.2.5 is implemented in BlackBerry Enterprise Server, and has been awarded FIPS 140-2 validation certificate #591.

4 Security Target

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

Title: BlackBerry® Enterprise Server Version 4.1.3 Security Target
Version: 1.8
Date: 23 August 2007

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*.

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 2 augmented, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.1 - Basic flaw remediation.

6 Security Policy

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

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

7 Assumptions and Clarification of Scope

Consumers of the BlackBerry Enterprise Server product should consider the following 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 unauthorized physical access.
- The environment in which the TOE and the enterprise mail server interact protects their communication from unauthorized modification and disclosure.

7.3 Clarification of Scope

The BlackBerry Enterprise Server level of protection is appropriate for low robustness environments. It offers protection against inadvertent or casual attempts to breach system security, by unsophisticated attackers possessing a low 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

The BlackBerry Enterprise Server is a software application that resides on a general purpose computer located within an enterprise. The BlackBerry Enterprise Server is comprised of the following main components (refer to Figure 3 - TOE Physical Boundary in the ST):

The **BlackBerry Controller** monitors BlackBerry components and restarts them if they stop responding.

The **BlackBerry Router** connects to the wireless network to route data to and from the BlackBerry devices. It also routes data within the corporate network to BlackBerry devices that are connected to the user's computer using the BlackBerry Device Manager.

The **BlackBerry Dispatcher** compresses and encrypts BlackBerry data. It routes the data through the BlackBerry Router to and from the wireless network.

The **BlackBerry Manager** connects to the configuration database allowing remote administration.

The **BlackBerry Messaging Agent** connects 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 Synchronisation Service** synchronises PIM application data between BlackBerry devices and the messaging server wirelessly.

The **BlackBerry Policy Service** performs administration services wirelessly such as sending IT policies and IT commands.

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 details about the connection between the BlackBerry Enterprise Server and the wireless network, user list, PIN-to-email address mapping, and a read-only copy of each user security key.

9 Evaluated Configuration

The evaluated configuration for the BlackBerry Enterprise Server comprises:

- BlackBerry Enterprise Server for IBM Lotus Domino Version 4.1.3 (4.1.3 bundle 37) executing on Microsoft Windows Server™ 2003 Service Pack 1.
- BlackBerry Enterprise Server for Microsoft Exchange Version 4.1.3 (4.1.3 bundle 37) executing on Microsoft Windows Server™ 2003 Service Pack 1.
- BlackBerry Enterprise Server for Novell GroupWise Version 4.1.3 (4.1.3 bundle 47) executing on Microsoft Windows Server™ 2003 Service Pack 1.

The BlackBerry Enterprise Server version and bundle numbers are 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:

- BlackBerry Enterprise Server for IBM Lotus Domino Version 4.1.3 System Administration Guide, 26-Jan-07;
- BlackBerry Enterprise Server for Novell GroupWise Version 4.1.3 System Administration Guide, 08-Mar-07;
- BlackBerry Enterprise Server for Microsoft Exchange Version 4.1.3 System Administration Guide, 31-Jan-07; and
- BlackBerry Enterprise Server All released versions (4.1.3 and earlier) Policy Reference Guide (Version 12), 22-Mar-07.

11 Evaluation Analysis Activities

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

Configuration management: 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 marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: 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 and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the BlackBerry Enterprise Server functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the BlackBerry Enterprise Server user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: 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 BlackBerry Enterprise Server ST's strength of function claims were validated through independent evaluator analysis. The evaluators also validated the developer's vulnerability analysis and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

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

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent 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].

[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.

The evaluators analyzed the developer's test coverage analysis, and found that the correspondence between tests identified in the developer's test documentation and the functional specification was complete and accurate.

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. These tests focused on:

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 Wireless Handheld: The objective of this test goal is to ensure that the operation of the BlackBerry Enterprise Server with the BlackBerry Wireless Handheld is correct; and

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

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis and the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focussed on:

- Generic vulnerabilities; and
- Security policy conflicts/vulnerabilities.

Vulnerability sites were searched for BlackBerry Enterprise Server vulnerabilities. None were found.

The evaluated configuration IT Policy comprises a subset of many possible settings (e.g. the IT Policy maximum allowable password length is 4 characters, whereas the maximum password length can be up to 14 characters). 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 ITSET Facility at Electronic Warfare Associates-Canada, Ltd. and at the developer's facility. The 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 Version 4.1.3 behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 2+ 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 4.1.3 includes a comprehensive Installation and Users Guide.

The BlackBerry® Enterprise Server Version 4.1.3 is straightforward to configure, use and integrate into a corporate network.

RIM's Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

Although the evaluation of development security was not part of this EAL 2+ site visit, the evaluators noted the high-level of security and confidentiality awareness and measures implemented within the RIM Waterloo campus. Physical (e.g., security card access, sign-in and issue of visitor badges, and visitor escort), procedural, personnel security and other security measures were in place.

15 Acronyms, Abbreviations and Initializations

This section expands any acronyms, abbreviations and initializations used in this report.

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
CSE	Communications Security Establishment
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
PIN	Personal Identification Number
PIM	Personal Information Management
QA	Quality Assurance
RIM	Research in Motion
ST	Security Target
TOE	Target of Evaluation

16 References

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

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) Publication #4, Technical Oversight, Version 1.0.

b. Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005.

c. Common Methodology for Information Technology Security Evaluation, CEM, version 2.3, August 2005.

d. Evaluation Technical Report (ETR) BlackBerry® Enterprise Server Version 4.1.3, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-55, Document No. 1533-000-D002, Version 0.7, 4 September 2007.

e. BlackBerry® Enterprise Server Version 4.1.3 Security Target, Revision No. 1.8, 23 August 2007.

f. Evaluation Work Plan for Common Criteria EAL 2+ BlackBerry® Enterprise Server Version 4.1.3, 1.5, 16 January 2007.

g. CC Evaluation Site Visit Report BlackBerry Wireless Handheld Software Version 4.1.0 and BlackBerry Enterprise Server Version 4.1.2 EAL 2 Augmented Evaluation, 1.1, 16 January 2007.