Certification Report

EAL 2+ Evaluation of Research In Motion Limited

BlackBerry® Wireless Handheld Software Version 4.1.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-54-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® Wireless Handheld Software Version 4.1.0 (hereafter referred to as BlackBerry Wireless Handheld), from Research In Motion Limited is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

The BlackBerry Wireless Handheld allows users to stay connected to a suite of applications including email, phone, enterprise applications, Internet, Short Messaging Service (SMS), and organiser information.

The BlackBerry Wireless Handheld integrates with the BlackBerry Enterprise Server which provides centralized management and control of the BlackBerry Wireless Handheld.

The BlackBerry Wireless Handheld provides advanced security features to meet the confidentiality and security requirements of the public sector. Data remains encrypted at all points between the BlackBerry Wireless Handheld and the BlackBerry Enterprise Server using FIPS 140-2 validated cryptography, allowing users to feel confident about wirelessly sending and receiving sensitive information.

Electronic Warfare Associates-Canada, Ltd. is the CCEF 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 Wireless Handheld, 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.

[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.

CSE, as the CCS Certification Body, declares that the BlackBerry Wireless Handheld 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 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is the BlackBerry Wireless Handheld Software Version 4.1.0 (hereafter referred to as BlackBerry Wireless Handheld), from Research In Motion Limited.

2 TOE Description

The BlackBerry Wireless Handheld allows users to stay connected to a suite of applications including email, phone, enterprise applications, Internet, Short Messaging Service (SMS), and organiser information.

The BlackBerry Wireless Handheld integrates with the BlackBerry Enterprise Server which provides centralized management and control of the BlackBerry Wireless Handheld.

The BlackBerry Wireless Handheld provides advanced security features to meet the confidentiality and security requirements of the public sector. Data remains encrypted at all points between the BlackBerry Wireless Handheld and the BlackBerry Enterprise Server using FIPS 140-2 validated cryptography.

3 Evaluated Security Functionality

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

In addition, the BlackBerry Cryptographic Kernel version 3.8.3.7 is implemented in the BlackBerry Wireless Handheld, and has been awarded FIPS 140-2 validation certificate #593.

4 Security Target

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

Title: BlackBerry® Wireless Handheld Software Version 4.1.0 Security Target
Version: 1.12
Date: 31 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 Wireless Handheld is:

a. Common Criteria Part 2 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
   - FCS_VAL_EXP.1 - Cryptographic module validation;
   - FDP_SDP_EXP.1 - Stored data non-disclosure;
   - FDP_SDP_EXP.2 - Stored data deletion; and
   - FTA_SSL_EXP.4 - Event-initiated session locking.

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 Wireless Handheld enforces access and flow control security policies that control access to TOE functionality and resources. The policies are:

IT Policy. The IT policy controls the application of an IT policy configuration received from a BlackBerry Enterprise Server. The IT policy configuration is only applied if the BlackBerry Wireless Handheld determines the configuration was sent by an authorised BlackBerry Enterprise Server.

Local Administration Policy. The local administration policy controls the ability of the user to manage the TOE through the local administration screens. The user can modify particular configuration items only if permitted by the IT policy configuration. The user is explicitly denied the ability to modify the IT policy configuration of the TOE.

Gateway Message Envelope (GME) Policy. The GME policy controls the information flow between the TOE and a BlackBerry Enterprise Server, and Personal Identification Number (PIN) messaging between the TOE and another BlackBerry device.

IT Command Policy. The IT command policy controls the execution of a wireless IT command received from a BlackBerry Enterprise Server. The IT command is only executed if the TOE determines the command was sent by an authorised BlackBerry Enterprise Server.

Personal Information Management (PIM) Policy. The PIM policy controls the wireless synchronisation of PIM data between the TOE and the corresponding enterprise email account.

Application Download Policy. The application download policy controls the downloading and installation of third-party applications.

Application Flow Policy. The application flow policy controls the communication initiated by a third-party application with an entity external to the TOE.

Cellular Policy. The cellular policy controls the ability to send and receive cellular phone communication.

Short Messaging Service (SMS) Policy. The SMS policy controls the ability to send and receive SMS messages.

Bluetooth Policy. The Bluetooth policy controls the ability to send and receive Bluetooth communication.

7 Assumptions and Clarification of Scope

Consumers of the BlackBerry Wireless Handheld 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 wireless network required by the TOE is available, and the TOE has permission to use the network

7.2 Environmental Assumptions

The TOE user is not malicious, attempts to interact with the TOE in compliance with the enterprise security policy, and exercises precautions to reduce the risk of loss or theft of the TOE.

7.3 Clarification of Scope

The BlackBerry Wireless Handheld 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 Wireless Handheld includes a suite of applications, and provides an application programming interface (API) to allow for third-party development of additional applications. BlackBerry Wireless Handheld core component functionality (refer to Figure 3 – TOE Physical Boundary in the ST) includes:

- Secure communication with the BlackBerry Enterprise Server;
- Secure communication with other BlackBerry devices;
- Remote management of the TOE;
- Content protection;
- Third-party application control;
- Wireless communication; and
- Wireless personal information management (PIM) items synchronisation.

The API consists of a Java Platform Micro Edition runtime environment, based on the CLDC 1.1 and MIDP 2.0 specifications, and BlackBerry API extensions that provide additional capabilities and integration with BlackBerry devices. Supporting the API is the BlackBerry Platform, which comprises the BlackBerry Java Virtual Machine and the BlackBerry operating system.

9 Evaluated Configuration

The evaluated configuration for the BlackBerry Wireless Handheld comprises:

- BlackBerry® Wireless Handheld Software version 4.1.0 (4.1.0.351, Platform 2.0.0.143) executing on the BlackBerry 8700r;

- BlackBerry® Wireless Handheld Software version 4.1.0 (4.1.0.194, Platform 2.0.0.90) executing on the BlackBerry 8700c;

- BlackBerry® Wireless Handheld Software version 4.1.0 (4.1.0.355, Platform 3.1.0.17) executing on the BlackBerry 8707g; and

- BlackBerry® Wireless Handheld Software version 4.1.0 (4.1.0.207, Platform 2.2.0.86) executing on the BlackBerry 7130e.

BlackBerry Wireless Handheld version numbers are displayed on a BlackBerry device by navigating to the Options list and selecting the ‘About’ item.

10 Documentation

The RIM documents provided to the consumer are:

- BlackBerry 7130e Version 4.1 User Guide, 13 February 2006;
- BlackBerry Wireless Handheld Version 4.1 User Guide (8700), 16 January 2006;
- BlackBerry 8707g User Guide, 14 February 2006; and
- BlackBerry Enterprise Server All released versions (4.1.3 and earlier) Policy Reference Guide (Version 12), 22 March 2007.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the BlackBerry Wireless Handheld, including the following areas:

Configuration management: An analysis of the BlackBerry Wireless Handheld configuration management system and associated documentation was performed. The evaluators found that the BlackBerry Wireless Handheld 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 Wireless Handheld 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 Wireless Handheld 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 Wireless Handheld 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 Wireless Handheld. 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 Wireless Handheld ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the

developer's vulnerability analysis for the BlackBerry Wireless Handheld 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].

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.

[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.

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

c. User Data Protection: The objective of this test goal is to confirm that user data is protected when transferred between the BlackBerry Wireless Handheld and the BlackBerry Enterprise Server; and

d. Policy Enforcement: The objective of this test goal is to confirm that the BlackBerry Wireless Handheld security policies are enforced.

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 vulnerabilities.

Vulnerability sites were searched for BlackBerry Wireless Handheld vulnerabilities. No vulnerabilities were found.

The evaluated configuration IT Policy is downloaded from the BlackBerry Enterprise Server to the BlackBerry Wireless Handheld. The evaluator attempted to apply values and settings outside the IT Policy. These 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 Wireless Handheld 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 Test (ITSET) Facility at Electronic Warfare Associates-Canada, Ltd. 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 Wireless Handheld 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 Wireless Handheld documentation includes a comprehensive Installation and Users Guide.

The BlackBerry Wireless Handheld is straightforward to configure, use, and integrate with a BlackBerry Enterprise Server.

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 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
API	Application Programming Interface
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

Acronym/Abbreviation/ Initialization	Description
GME	Gateway Message Envelope
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 Limited
SMS	Short Messaging Service
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® Wireless Handheld Software Version 4.1.0, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-54, Document No. 1532-000-D002, Version 0.8, 4 September 2007.

e. *BlackBerry® Wireless Handheld Software Version 4.1.0 Security Target*, Revision No. 1.12, 31 August 2007.

f. Evaluation Work Plan for Common Criteria EAL 2+ BlackBerry® Wireless Handheld Software Version 4.1.0, 1.4, 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.