# Certification Report

## EAL 4+ Evaluation of BlackBerry® Device Software 5.0.0

Issued by:

**Communications Security Establishment Canada**

**Certification Body**

**Canadian Common Criteria Evaluation and Certification Scheme**

| | |
|---|---|
| **Evaluation number**: | 383-4-100-CR |
| **Version**: | 1.1 |
| **Date**: | 12 March 2010 |
| **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 3*, for conformance to the *Common Criteria for Information Technology  Security Evaluation, Version 3.1 Revision 3*. 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, 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 12 March 2010, 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 (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

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;
- JAVA is a trademark of Sun Microsystems Incorporated; and
- Wi-Fi is a trademark of the Wi-Fi Alliance.

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

# TABLE OF CONTENTS

# Executive Summary

The BlackBerry® Device Software 5.0.0 (hereafter referred to as BlackBerry Device Software), from Research In Motion Limited, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

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

BlackBerry Device Software integrates with the BlackBerry Enterprise Server which provides centralized management and control of the BlackBerry Device Software using IT policies and software configuration rules.

BlackBerry Device Software provides advanced security features to meet user confidentiality and security requirements. Data remains encrypted at all points between the BlackBerry Device Software and the BlackBerry Enterprise Server using FIPS 140-2 validated cryptography.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 25 February 2010 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 Device Software, 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 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 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.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the BlackBerry Device Software 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) 4 augmented evaluation is BlackBerry® Device Software 5.0.0 (hereafter referred to as BlackBerry Device Software), from Research In Motion Limited.

# 2 TOE Description

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

BlackBerry Device Software integrates with the BlackBerry Enterprise Server which provides centralized management and control of the BlackBerry Device Software using IT policies and software configuration rules.

BlackBerry Device Software provides advanced security features to meet user confidentiality and security requirements. Data remains encrypted at all points between the BlackBerry Device Software 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 Device Software is identified in Section 6 of the Security Target (ST).

BlackBerry Device Software implements the BlackBerry Cryptographic Kernel version 3.8.5.85 that provides cryptographic functionality. This Cryptographic Module was validated to FIPS 140-2 and was awarded certificate number 1252.

# 4 Security Target

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

Title: Security Target BlackBerry® Device Software 5.0.0
Version: 5.0
Date: 4 March 2010

# 5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*.

BlackBerry Device Software is:

- Common Criteria Part 2 extended, with functional requirements based on 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.
- Common Criteria Part 3 conformant, with security assurance requirements based on assurance components in Part 3; and
- Common Criteria EAL 4 augmented, with all the security assurance requirements in the EAL 4, as well as the following: ALC_FLR.1 - Basic Flaw Remediation.

# 6 Security Policy

BlackBerry Device Software 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 TOE determines the configuration was sent by an authorised BlackBerry Enterprise Server.

**Local Administration Policy**. The local administration policy controls the ability of the TOE 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 wireless IT commands 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. Users are restricted to downloading only applications that are authorized by the BlackBerry Enterprise Server administrator.

**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 and Short Messaging Service (SMS) and Multimedia Messaging Service (MMS) messaging.

**Radio Policy**. The Radio policy controls the ability to send and receive Bluetooth, Wi-Fi and Global Positioning System (GPS) communications.

**Software Configuration Policy**. The software configuration policy allows or prevents the installation of third-party applications on the TOE, and limits the permissions of the applications, including the resources that an application can access and the types of connections that can be established. Users are restricted to loading  applications that are authorized by the BlackBerry Enterprise Server administrator.

**Multimedia**. The multimedia policy controls the ability to take pictures, record video and voice notes, and store multimedia user data on the BlackBerry Device Software external memory device.

**Secure/Multipurpose Internet Mail Extensions (S/MIME) Policy**. The S/MIME policy controls the ability to send and receive S/MIME messages.

# 7 Assumptions and Clarification of Scope

Consumers of the BlackBerry Device Software product 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 wireless network required by the TOE is available, and the TOE has permission to use the network.

## 7.2 Environmental Assumptions

The TOE is compliant with the Organisational Security Policies (OSP) provided in Section 3.2 of the ST.  These OSPs require that the TOE be provisioned by the BlackBerry Enterprise Server in accordance with the Baseline Configuration defined in Section 8 of the ST and that the BlackBerry Enterprise Server administrator authorize all third party applications.

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 Device Software offers protection against attempts to breach system security by attackers possessing enhanced-basic attack potential. It is not intended for situations which involve determined attempts by hostile or well-funded attackers possessing moderate or higher attack potential.

## 8 Architectural Information

BlackBerry Device Software includes a suite of applications, and provides an application programming interface (API) to allow for third-party development of additional applications. BlackBerry Device Software core component functionality includes:

- Secure communication with the BlackBerry Enterprise Server;
- Secure communication with other BlackBerry devices;
- Remote management of the TOE;
- Content protection on the TOE;
- File encryption on an external memory device;
- Third-party application control;
- Wireless communication, including Secure/Multipurpose Internet Mail Extensions (S/MIME) email messaging;
- Wireless personal information management (PIM) items synchronisation; and
- Management of multimedia applications.

The API consists of a Java Platform, Micro Edition (Java ME) runtime environment, based on the Connected Limited Device Configuration (CLDC) 1.1 and Mobile Information Device Profile (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.

For further detail refer to ST Figure 3 – TOE Physical Boundary.

## 9 Evaluated Configuration

The evaluated configuration for the BlackBerry Device Software comprises the following:

- BlackBerry Handheld Software Version 5.0.0 (5.0.0.321 bundle 499) executing on the BlackBerry 9700 Series;
- BlackBerry Handheld Software Version 5.0.0 (5.0.0.344 bundle 541) executing on the BlackBerry 9700 Series;

- BlackBerry Handheld Software Version 5.0.0 (5.0.0.351 bundle 554) executing on the BlackBerry 9700 Series; and
- BlackBerry Handheld Software Version 5.0.0 (5.0.0.320 bundle 497) executing on the BlackBerry 9500 Series.

BlackBerry Device Software must be provisioned on a BlackBerry Enterprise Server according to the Baseline Configuration defined in Section 8 of the ST.

BlackBerry Device Software version numbers are displayed on a BlackBerry device by navigating to the Options list and selecting the 'About' item.

# 10 Documentation

Guidance documents for the BlackBerry 9500 and BlackBerry 9700 series Handheld devices can be found on the BlackBerry website.

# 11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the BlackBerry Device Software, including the following areas:

**Development**: The evaluators analyzed the BlackBerry Device Software functional specification, design documentation, and a subset of the implementation representation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the BlackBerry Device Software 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 Device Software 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 Device Software configuration management (CM) system and associated documentation was performed. The evaluators found that the BlackBerry Device Software configuration items were clearly 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 BlackBerry Device Software during distribution to the consumer.

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the BlackBerry Device Software 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 BlackBerry Device Software. 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 Device Software.  Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables.  The evaluators identified potential vulnerabilities for testing applicable to the BlackBerry Device Software 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].

The evaluators analyzed the developer’s test coverage and depth analysis and found them to be complete and accurate.  The correspondence between the tests identified in the developer’s test documentation and the functional specification and TOE design 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:

- Initialization: The objective of this test goal is to confirm that the BlackBerry Device Software can be installed and configured into the evaluated configuration, as identified in the TOE Description of the ST, by following all instructions in the developer's Installation and Administrative guidance;
- Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests on the evaluator's TOE installation;
- Operation of BlackBerry Device Software with a CC-Configured BlackBerry Enterprise Server (BES): The objective of this test goal is to ensure that correct operation of the TOE with the BES;
- User Data Protection: The objective of this test goal is to confirm that user data is protected when transferred between the BES and the BlackBerry Device Software; and
- Security Management: The objective of this test goal is to confirm that the Security Functional Policies are enforced.

## 12.3 Independent Penetration Testing

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

- Search for Generic Vulnerabilities: Vulnerability sites were searched for BlackBerry Device Software vulnerabilities. No vulnerabilities were found;
- IT Policy: The evaluated configuration IT Policy was downloaded from the BlackBerry Enterprise Server to the BlackBerry Device Software. The evaluator attempted to apply values and settings outside the IT Policy. These values and settings were not allowed;
- Passwords: Testing was performed using different password complexity rules to ensure that the rules were enforced and the BlackBerry Device Software would not reveal the length of the password or complexity requirements to a user attempting to authenticate; and

- Date and Time: It was confirmed that the behaviour of the BlackBerry Device Software was as expected when the time and/or time zone of the BlackBerry Device Software was changed.

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

### 12.4 Conduct of Testing

BlackBerry Device Software 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. 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 Device Software 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 documentation for the BlackBerry Device Software includes comprehensive user guidance and the BlackBerry Device Software is straightforward to configure, use and integrate into a corporate network.

Research In Motion Limited has a well-defined product development process and configuration management (CM) and quality assurance (QA) provide the requisite controls for managing all CM/QA activities.

## 15 Acronyms, Abbreviations and Initializations

| Acronym/Abbreviation/ Initialization | Description |
|---|---|
| API | Application Programming Interface |
| BES | BlackBerry Enterprise Server |
| CCEF | Common Criteria Evaluation Facility |

| Acronym/Abbreviation/ Initialization | Description |
|---|---|
| CM | Configuration Management |
| CPL | Certified Products list |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| GME | Gateway Message Envelope |
| GPS | Global Positioning System |
| IT | Information Technology |
| ITSET | Information Technology Security Evaluation and Testing |
| MMS | Multimedia Messaging Service |
| PALCAN | Program for the Accreditation of Laboratories-Canada |
| PIM | Personal Information Management |
| PIN | Personal Identification Number |
| QA | Quality Assurance |
| SFR | Security Functional Requirement |
| S/MIME | Secure/Multipurpose Internet Mail Extensions |
| SMS | Short Messaging Service |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |
| TSFI | TSF Interface |
| Wi-Fi | Used as a synonym for IEEE 802.11 technology |

## 16 References

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

- CCS Publication #4, Technical Oversight, Version 1.1, August 2005.
- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.
- Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.
- Security Target BlackBerry® Device Software 5.0.0, Document Version 5.0, 4 March 2010.
- Evaluation Technical Report for EAL 4+ Common Criteria Evaluation of Research In Motion Limited BlackBerry® Device Software 5.0.0, Document No. 1603-000-D002, Version 0.6, 25 February 2010, Common Criteria Evaluation Number: 383-4-100.