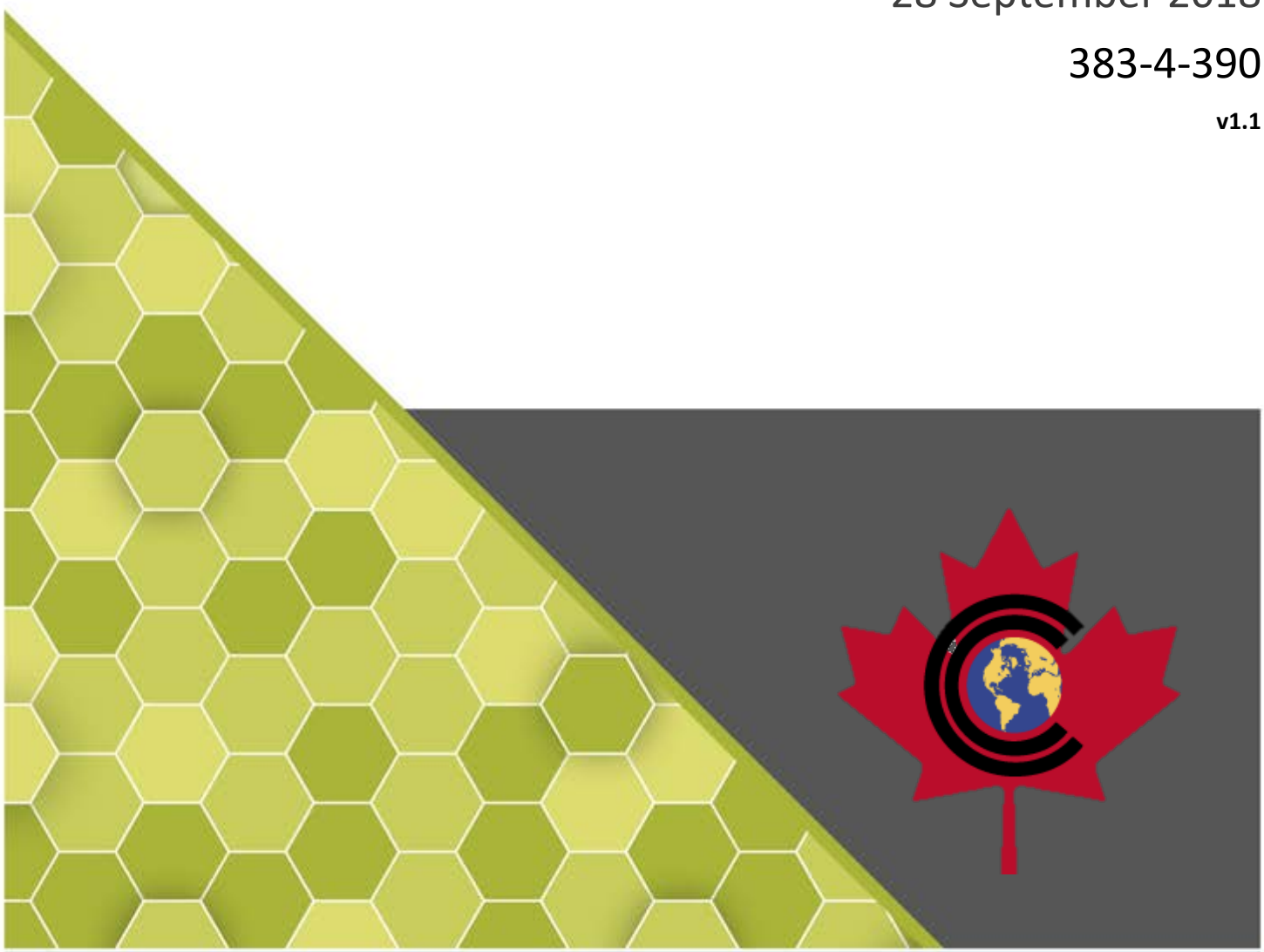
COMMON CRITERIA CERTIFICATION REPORT

BlackBerry Enterprise Service Version 12.5
28 September 2018

383-4-390

v1.1



Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

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 Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. 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 Canadian CC Scheme, 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, 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, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

OVERVIEW

The Canadian Common Criteria Scheme 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 Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the 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.

By awarding a Common Criteria certificate, the 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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

The certification report, certificate of product evaluation and security target are posted to the Certified Products list (CPL) for the Canadian CC Scheme and to the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

BlackBerry Enterprise Service Version 12.5 (hereafter referred to as the Target of Evaluation, or TOE), from BlackBerry, was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed 28 September 2018 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for TOE, and the security functional/assurance 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.

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

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1 TOE Identification

TOE Name and Version	BlackBerry Enterprise Service Version 12.5
Developer	BlackBerry
Conformance Claim	Protection Profile for Mobile Device Management Version 2.0, December 31, 2014

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.

1.2 TOE DESCRIPTION

The TOE is an Enterprise Mobility Management solution from BlackBerry. It provides organizations with the ability to:

- Manage mobile devices for the organization to protect business information
- Maintain a connection to required information for mobile workers
- Provide administrators with efficient business tools to manage policy enforcement

BlackBerry 10 mobile devices, used with the TOE, allow mobile workers secure access to mail, application and content servers in the organization's network, in accordance with the organization’s policies.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

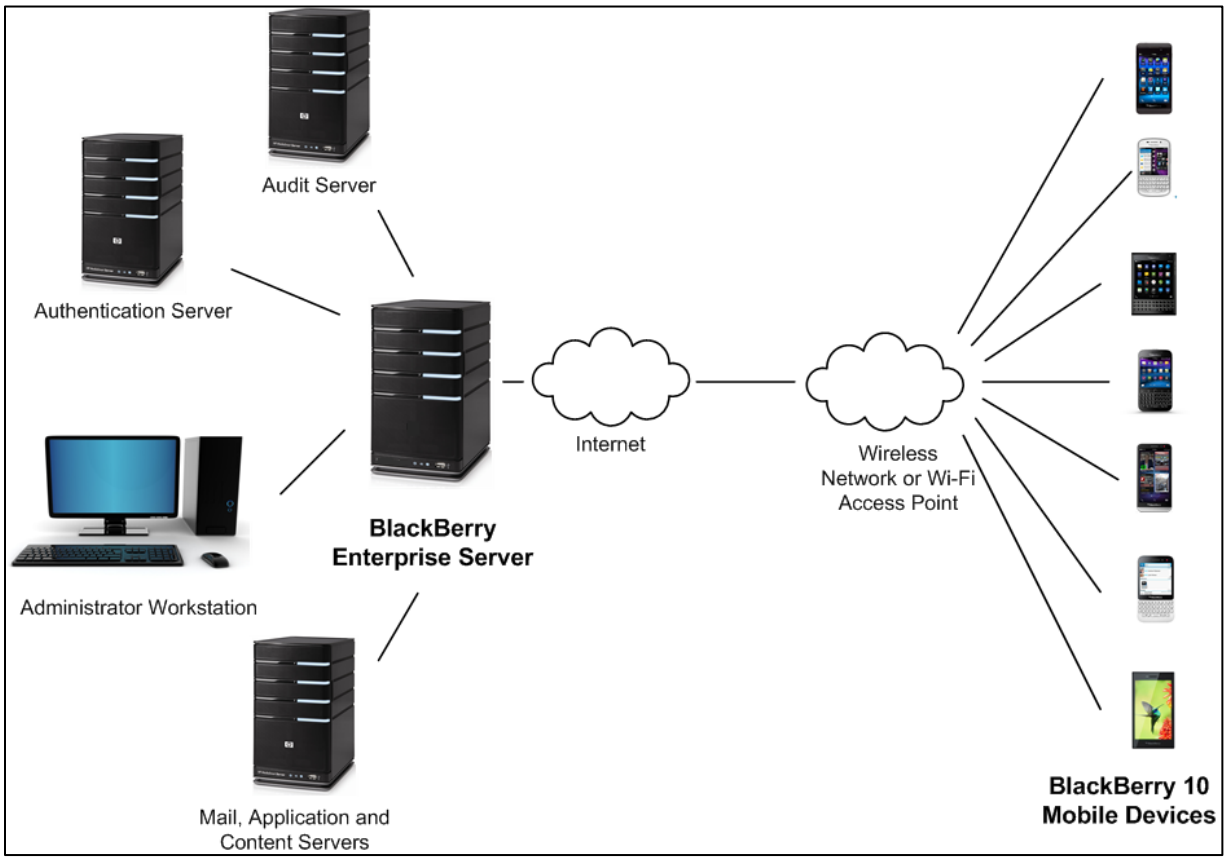


Figure 1 TOE Architecture

2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TOE Security Funcitonality (TSF)
- TOE Access
- Trusted Path/Channel

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following Government of Canada approved cryptographic algorithms were evaluated by the CAVP and used by the TOE:

Table 2 Cryptographic Algorithm(s)

Cryptographic Algorithm	Standard	Certificate Number
Advanced Encryption Standard (AES)	FIPS 197	5342
Rivest Shamir Adleman (RSA)	FIPS 186-4	2858
Secure Hash Algorithm (SHS)	FIPS 180-3	4293
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	3539
Digital Signature Algorithm (DSA)	FIPS 186-4	1378
Deterministic Random Bit Generation (DRBG)	SP 800-90A	2062
Key Agreement Scheme	SP 800-56A	174
Elliptic Curve Digital Signature Algorithm (ECDSA)	FIPS 186-4	1403

3 ASSUMPTIONS AND CLARIFICATIONS OF SCOPE

Consumers of the TOE 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.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The TOE relies on network connectivity to carry out its management activities. The TOE will robustly handle instances when connectivity is unavailable or unreliable.
- The MDM Server relies upon a trustworthy platform and local network from which it provides administrative capabilities.The MDM server relies on the this platform to provide a range of security related services including reliable timestamps, user and group account management, logon and logout services via a local or network directory service, remote access control, and audit log management services to include offloading of audit logs to other servers. The platform is expected to be configured specifically to provide MDM services, employing features such as a host-based firewall, which limits its network role to providing MDM functionality.
- One or more competent, trusted personnel who are not careless, willfully negligent, or hostile, are assigned and authorized as the TOE Administrators, and do so using and abiding by guidance documentation.
- Mobile device users are not willfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy.

3.2 CLARIFICATION OF SCOPE

The TOE incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

Although the TOE supports iOS and Android agents, due to CVE-2016-3128 and CVE-2016-3130, only the agent included with the Blackberry 10 (10.3.3.1668) OS is to be used in the evaluated configuration.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises the BES 12.5.2 build 3.27.61. This includes the BlackBerry Resource Kit for BES 12 (Version 12.5.0 Bundle0008), the BES12 Configuration Tool (BES12ConfigTool.exe Version 1.25.7) and Validate Package (ValidatePackage.exe, Version 3.32.63). These files are not part of the primary installation package. The following components are required in the operational environment:

- Windows Server 2012 R2 platform on general purpose computing hardware for the BES 12.5.2;
- BlackBerry 10 software (10.3.3.1668) on BlackBerry 10 moblie devices (Passport, Classic, Leap, Z30, Z10, Q10, Q5 and P'9983). Evaluation of the BlackBerry 10 mobile device against the Protection Profile for Mobile Device Fundamentals and Extended Package for Mobile Device Management Agents has been performed in parallel with this evaluation;
- Audit Server running Windows Server 2012 R2;
- Active Directory Server running Windows Server 2012 R2; and
- Administrator workstation running Windows 10.

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a. Installation and Upgrade Guide BES12, Version 12.5 published 2016-06-30

b. Configuration Guide BES12, Version 12.5, published 2017-01-27

c. Administration Guide BES12, Version 12.5, published 2016-08-24

d. Policy Reference Spreadsheet, BES12, Version 12.5, 2016-06-30

e. BlackBerry Enterprise Service 12.5 Common Criteria Guidance Supplement, Version 1.0

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TSF interfaces and how the TSF implements the security functional requirements (SFRs). The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes 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 are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

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

6 TESTING ACTIVITIES

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

6.1 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. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT FUNCTIONAL TESTING

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP; and

b. Cryptographic module/library verification: The evaluator verified the cryptographic certificates claimed are valid and present in the TOE.

6.3.1 FUNCTIONAL TEST RESULTS

The developer's tests and the independent functional tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 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:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST.

6.4.1 PENETRATION TEST RESULTS

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

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
BES12	BlackBerry Enterprise Service 12
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
MDM	Mobile Device Management
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
BlackBerry Enterprise Service 12.5 Security Target, v1.11, 7 August 2018
BlackBerry Enterprise Service Evaluation Technical Report, v1.5, 21 August 2018
Assurance Activity Report for BlackBerry Enterprise Service 12.5, v1.10, 21 August 2018