Communications Security Establishment   Centre de la sécurité des télécommunications

COMMON CRITERIA CERTIFICATION REPORT

BlackBerry Smartphones with OS 10.3.3 VPN Client

383-4-415

24 January 2017

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. 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.

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 Smartphones with OS 10.3.3 VPN Client (hereafter referred to as the Target of Evaluation, or TOE), from BlackBerry, was the subject of this Common Criteria evaluation. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

The TOE Client allows remote users to use client resources to establish an encrypted Internet Protocol Security (IPsec) tunnel across an unprotected public network to a private network. The TOE platform is a BlackBerry smartphone device running Operating System (OS) 10.3.3. The TOE is the VPN Client software that loads the VPN Profile which provides protection between itself and another VPN endpoint, such as a VPN Gateway. The TOE VPN Client, together with the TOE platform, protects the data between the device and a VPN Gateway, providing confidentiality, integrity, and protection of data in transit, even though it traverses a public network.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 24 January 2017 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 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 Smartphones with OS 10.3.3 VPN Client
Developer	BlackBerry
Conformance Claim	Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013

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 Client allows remote users to use client resources to establish an encrypted Internet Protocol Security (IPsec) tunnel across an unprotected public network to a private network. The TOE platform is a BlackBerry smartphone device running Operating System (OS) 10.3.3. The TOE is the VPN Client software that loads the VPN Profile which provides protection between itself and another VPN endpoint, such as a VPN Gateway. The TOE VPN Client, together with the TOE platform, protects the data between the device and a VPN Gateway, providing confidentiality, integrity, and protection of data in transit, even though it traverses a public network.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:
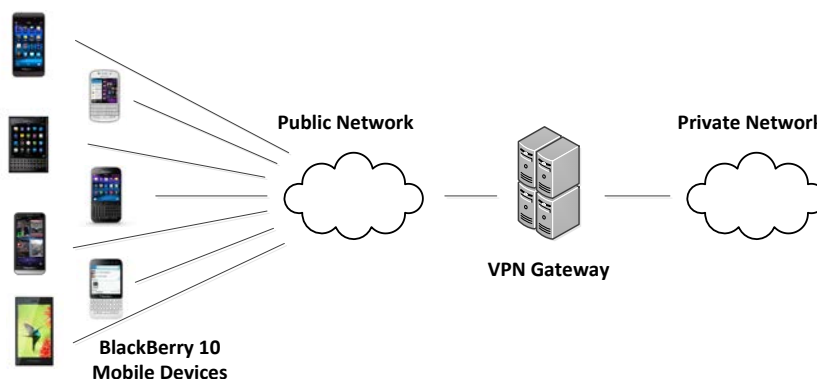
Figure 1   TOE Architecture

2   SECURITY POLICY

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

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- 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 cryptographic module was evaluated by the CMVP and used by the TOE:

Table 2   Cryptographic Module(s)

Cryptographic Module	Certificate Number
BlackBerry OS Cryptographic Library (Software Versions: 5.6, 5.6.1 or 5.6.2)	#1578

The TOE platforms have Wi-Fi CERTIFIED™ Interoperability Certificates:

Table 3   Wi-Fi CERTIFIED™ Interoperability Certificates

Platform	Certificate Number
Passport	WFA57214, WFA55078, WFA60544
Classic	WFA56510, WFA59939, WFA59937, WFA56572, WFA59936, WFA57100
Leap	WFA59167, WFA59168, WFA60172, WFA60171
Z30	WFA59945, WFA59943, WFA59942, WFA59941
Z10	WFA69196, WFA69198, WFA69197
Q10	WFA60143, WFA60161, WFA60162, WFA60163, WFA60164
P'9982 (Porsche Design)	WFA69199, WFA69200
P'9983 (Porsche Design)	WFA60165, WFA60166

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:

- Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.

- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

- Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

3.2   CLARIFICATION OF SCOPE

The TOE is built into the BlackBerry OS 10.3.3.1668; it is not provided as a separate product. It relies extensively on the underlying platform.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

The BlackBerry 10.3.3.1668 OS running on the following platforms;

- Passport (SQW100-1, SQW100-3, SQW100-4)
- Classic (SQC100-1, SQC100-2, SQC100-3, SQC100-4, SQC100-5)
- Leap (STR100-1, STR100-2)
- Z30 (STA100-2, STA100-3, STA100-5, STA100-6)
- Z10 (STL100-2, STL100-3, STL100-4)
- Q10 (SQN100-1, SQN100-2, SQN100-3, SQN100-4, SQN100-5)
- P'9982 (STK100-1, STK100-2)
- P'9983 (SQK100-1, SQK100-2)

With support from the following environmental components;

- BlackBerry Enterprise Service 12.5 with Policy Pack Version 1.9.3.97.

4.1 DOCUMENTATION

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

a. Administration Guide BES12 Version 12.4, SWD-20160323144946763, 23 March 2016

b. Policy Reference Spreadsheet BES12.4, [AGD_POL] 24 March 2016

c. BlackBerry Smartphones with OS 10.3.3 VPN Client Common Criteria Guidance Supplement, Version 1.1, 25 August 2016

d. BlackBerry Classic Smartphone Version: 10.3.3 User Guide, SWD-20160426135955284, 26 April 2016

e. BlackBerry Leap Smartphone Version: 10.3.3 User Guide, SWD-20160427113258316, 27 April 2016

f. BlackBerry P'9982 Smartphone Version: 10.3.3 User Guide, SWD-20160427133504750, 27 April 2016

g. BlackBerry P'9983 Smartphone Version: 10.3.3 User Guide, SWD-20160427132628821, 27 April 2016

h. BlackBerry Passport Smartphone Version: 10.3.3 User Guide, SWD-20160427115319481, 27 April 2016

i. BlackBerry Q10 Smartphone Version: 10.3.3 User Guide, SWD-20160427135115364,27 April 2016

j. BlackBerry Z10 Smartphone Version: 10.3.3 User Guide, SWD-20160427140021771,27 April 2016

k. BlackBerry Z30 Smartphone Version: 10.3.3 User Guide, SWD-20160427134318308,27 April 2016

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 TOE functional specification and design documentation; 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 TOE security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

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 describes 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 evaluators analyzed the developer's test coverage 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 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 activity was performed:

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

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 the 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
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
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories – Canada
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 Smartphones with OS 10.3.3 VPN Client Security Target, Version 1.5, 24 January 2017
Evaluation Technical Report for BlackBerry Smartphones with OS 10.3.3 VPN Client v1.3, 21 December 2016
Assurance Activity Report for BlackBerry BlackBerry Smartphones with OS 10.3.3 VPN Client Version 10.3.3 on BlackBerry 10 Smartphones v2.3, 24 January 2017