Communications Security Establishment
Centre de la sécurité des télécommunications

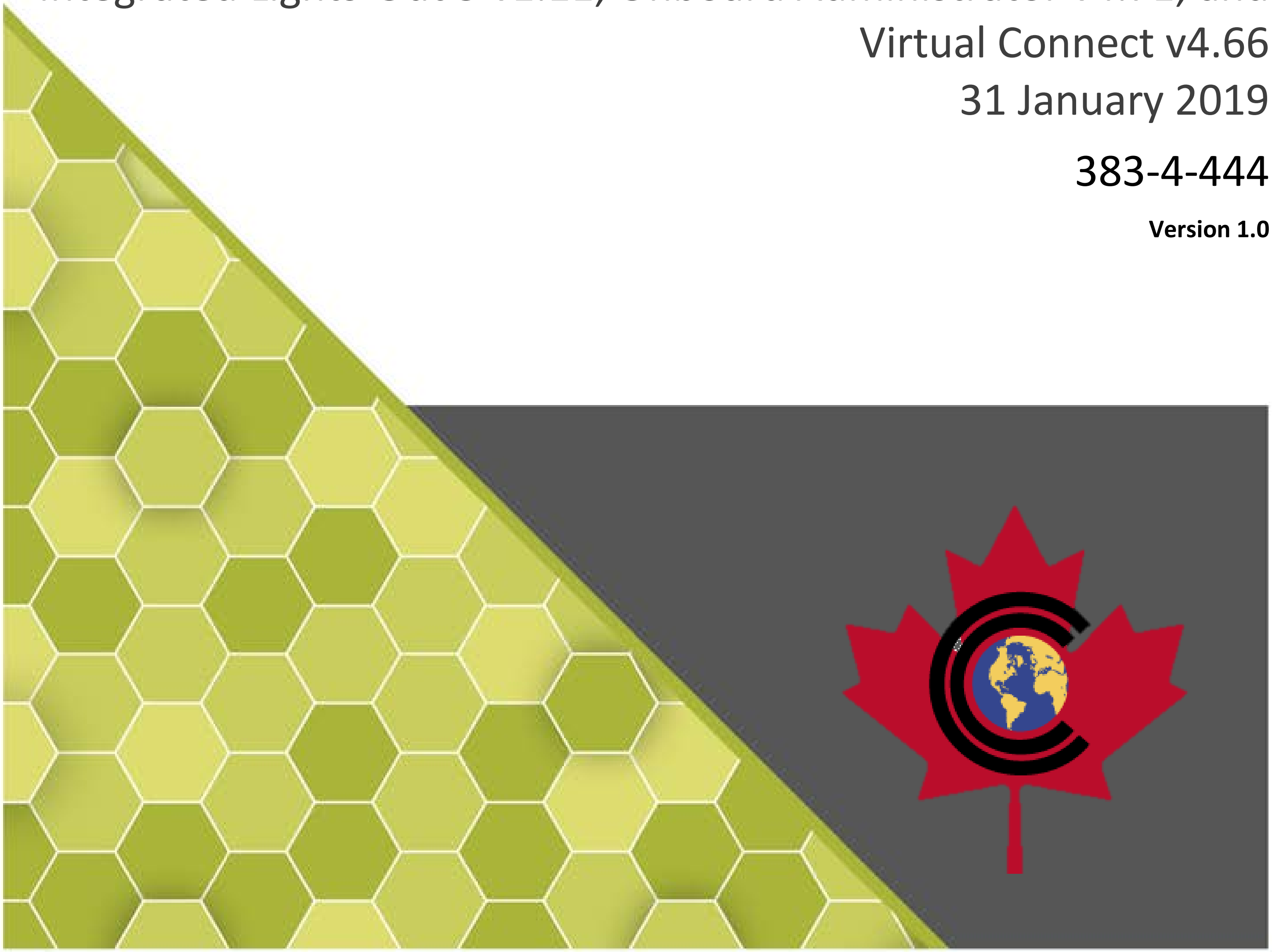
COMMON CRITERIA CERTIFICATION REPORT

Hewlett Packard Enterprise Development LP BladeSystem c7000, Integrated Lights-Out 5 v1.11, Onboard Administrator v4.71, and Virtual Connect v4.66

31 January 2019

383-4-444

Version 1.0



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 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. 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, 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 listed on 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

Executive Summary......1

1 Identification of Target of Evaluation......2

1.1 Common Criteria Conformance......2

1.2 TOE Description......2

1.3 TOE Architecture......3

2 Security Policy......4

2.1 Cryptographic Functionality......4

3 Assumptions and Clarifications of Scope......5

3.1 Usage and Environmental Assumptions......5

3.2 Clarification of Scope......5

4 Evaluated Configuration......6

4.1 Documentation......6

5 Evaluation Analysis Activities......8

5.1 Development......8

5.2 Guidance Documents......8

5.3 Life-cycle Support......8

6 Testing Activities......9

6.1 Assessment of Developer Tests......9

6.2 Conduct of Testing......9

6.3 Independent Functional Testing......9

6.4 Independent Penetration Testing......11

7 Results of the Evaluation......12

7.1 Recommendations/Comments......12

8 Supporting Content......13

8.1 List of Abbreviations......13

8.2 References......14

LIST OF FIGURES

Figure 1 TOE Architecture 3

LIST OF TABLES

Table 1 TOE Identification 2

Table 2 Cryptographic Module(s) 4

Table 3 Cryptographic Algorithm(s) 4

EXECUTIVE SUMMARY

Hewlett Packard Enterprise Development LP BladeSystem c7000, Integrated Lights-Out 5 v1.11, Onboard Administrator v4.71, and Virtual Connect v4.66 (hereafter referred to as the Target of Evaluation, or TOE), from Hewlett Packard Enterprise Development LP, 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.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed 31 January 2019 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	Hewlett Packard Enterprise Development LP BladeSystem c7000, Integrated Lights-Out 5 v1.11, Onboard Administrator v4.71, and Virtual Connect v4.66
Developer	Hewlett Packard Enterprise Development LP
Conformance Claim	EAL 2+ (ALC_FLR.2)

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

1.2 TOE DESCRIPTION

The hardware/firmware TOE is comprised of a BladeSystem c7000 rack-mountable enclosure, one or more Onboard Administrator modules, one or more Virtual Connect modules, one or more blade servers that include Integrated Lights-Out functionality, one or more power supplies, and one or more fan units.

The Onboard Administrator controls the power supplies and fans throughout the enclosure that are necessary to support the installed BladeSystem components. It also provides management and monitoring of the installed interconnect modules, blade servers, fans, and power supplies.

Virtual Connect is an interconnect component which contains management firmware that provides centralized enclosure network and storage management functionality.

Integrated Lights-Out provides out-of-band management of the blade server power including access to virtual server consoles, virtual power, and virtual media.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

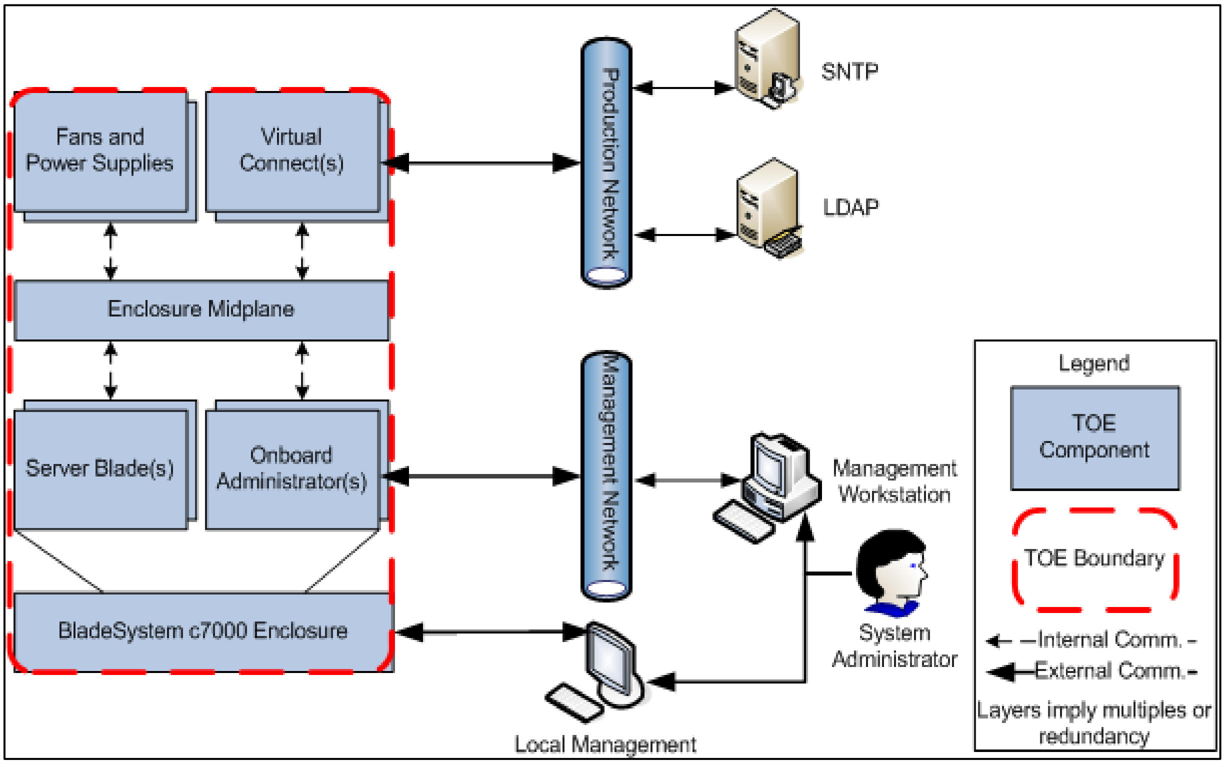


Figure 1 TOE Architecture

2 SECURITY POLICY

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

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Resource Utilization
- TOE Access

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 modules were evaluated by the CMVP and are used by the TOE:

Table 2 Cryptographic Module(s)

Cryptographic Module	Certificate Number
iLO 5 Cryptographic Module	3122
HPE BladeSystem c-Class Onboard Administrator Firmware	3174

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

Table 3 Cryptographic Algorithm(s)

Cryptographic Algorithm	Standard	Certificate Number
Triple-DES (3DES)	FIPS 46-3	2539
Advanced Encryption Standard (AES)	FIPS 197	4777
Rivest Shamir Adleman (RSA)	FIPS 186-4	2618
Secure Hash Algorithm (SHS)	FIPS 180-3	3923
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	3187
Deterministic Random Bit Generation (DRBG)	SP 800-90A	1655

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 is located within a controlled access facility.
- There are one or more competent individuals assigned to manage the TOE, its operating environment, and the security of the information it contains. The individuals are non-hostile, appropriately trained, and follow all guidance.
- The TOE will be protected from unauthorized modification.

3.2 CLARIFICATION OF SCOPE

Integrated Lights-Out and Onboard Administrator both implement CMVP validated modules. The Virtual Connect implements CAVP-validated algorithms for purposes of protecting TSF data.

Features and/or functionality that are not part of the evaluated configuration of the TOE are:

- Use of any SNMP functionality
- XML Reply
- Integrated Lights-Out and Virtual Connect System Maintenance Switches
- ProLiant Blade Server operating systems
- Utility Ready Blades
- Insight Display and KVM (locked in FIPS mode)
- HPE Online Configuration Utility
- HPE Insight Online connecting to an IRS device
- Integrated Lights-Out iOS application
- Integrated Lights-Out Android application
- Using the Integrated Lights-Out service port for mass storage
- Onboard Administrator running with IPv6 enabled

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

- BladeSystem c7000 enclosure and support hardware such as fans and power supplies
- HPE BLc7000 Onboard Administrator with KVM option running firmware version 4.71
- HPE Virtual Connect FlexFabric-20/40 F8 for c-Class BladeSystem with TAA module running firmware version 4.66
- HPE Integrated Lights Out 5 GXP ASIC30 model number 815393-001-B1 with an Advanced Premium Security Edition license running firmware version 1.11 on a HPE ProLiant Gen10 BL460c blade server

4.1 DOCUMENTATION

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

a. Architecture and Technologies in the HPE BladeSystem c7000 Enclosure; HPE Part Number: 4AA4-8125ENW; Published: July 2017, Rev. 3

b. HPE BladeSystem c7000 Enclosure Quick Setup Instructions; HPE Part Number: 411762-404; Published: February 2015; Edition: 13

c. HPE BladeSystem c7000 Enclosure Setup and Installation Guide; HPE Part Number: 411272-401R; Published: November 2015; Edition: 11

d. HPE BladeSystem c-Class Solution Overview; HPE Part Number: 413339-006; Published: March 2012; Edition: 6

e. Error Message Guide for HPE ProLiant Gen10 servers and HPE Synergy; Part Number: 873901-002; Published: July 2017; Edition: 1

f. HPE ProLiant BL460c Gen10 Server Blade User Guide; Part Number: 876833-001; Published: July 2017; Edition: 1

g. HPE iLO 5 Scripting and Command Line Guide; Part Number 882043-001; Published: July 2017; Edition: 1

h. HPE iLO 5 User Guide; Part Number: 880740-001; Published: July 2017; Edition: 1

i. HPE iLO Federation User Guide for iLO 5; Part Number 880724-001; Published: July 2017; Edition: 1

j. UEFI System Utilities User Guide for HPE ProLiant Gen10 Servers and HPE Synergy; Part Number 881334-001; Published: July 2017; Edition: 1

k. HPE BladeSystem Onboard Administrator Command Line Interface User Guide; HPE Part Number: 695523-401; Published: July 2017; Edition: 29

l. HPE BladeSystem Onboard Administrator User Guide; HPE Part Number: 695522-402; Published: June 2017; Edition: 28

m. HPE BladeSystem c-Class Virtual Connect Support Utility Version 1.13.5 User Guide; HPE Part Number: 859819-004; Published: September 2018; Edition: 1

n. HPE Virtual Connect for c-Class BladeSystem Setup and Installation Guide Version 4.65/4.66; Part Number: P01610-002; Published: September 2018; Edition: 1

o. HPE Virtual Connect for c-Class BladeSystem User Guide Version 4.65/4.66; Part Number: P01611-002; Published: September 2018; Edition: 1

p. HPE Virtual Connect Manager Command Line Interface for c-Class BladeSystem User Guide Version 4.65/4.66; HPE Part Number: P01609-002; Published: September 2018; Edition: 1

q. HPE ProLiant Gen9 Troubleshooting Guide Volume II: Error Messages; Part Number: 795673-004; Published: July 2016; Edition: 5

r. Hewlett Packard Enterprise Development LP; BladeSystem c-Class Enclosure Architecture; Including Integrated Lights-Out (iLO) 5 v1.11, Onboard Administrator (OA) v4.71, and Virtual Connect (VC) v4.66; Guidance Documentation Supplement; Evaluation Assurance Level (EAL): EAL2+; Document Version: v0.4

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 TOE security functionality (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. Repeat of Developer's Tests: The evaluator repeated a subset of the developers tests;

b. Failed Login Delay in Onboard Administrator: The objective of this test case is to ensure that the Onboard Administrator enforces a delay between failed login attempts;

c. Session time-out in Virtual Connect. The objective of this test case is to ensure that the VC terminates a user's session due to inactivity;

d. Onboard Administrator LDAP authentication and authorization. The objective of this test case is to ensure that the communication channel between the Onboard Administrator and the LDAP server is secure and to verify that proper access to the TSF is enforced based on the privileges assigned;

e. Integrated Lights-Out LDAP authentication and authorization: The objective of this test case is to ensure that the communication channel between the Integrated Lights-Out and the LDAP server is secure and to verify proper access to the TSF is enforced based on the privileges assigned;

f. Virtual Connect LDAP authentication and authorization. The objective of this test case is to ensure that the communication channel between the Virtual Connect and the LDAP server is secure and to verify proper access to the TSF is enforced based on the privileges assigned; and

g. Cryptographic Module Verification: The objective of this test case is to confirm that the claimed cryptographic modules are implemented 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; and

b. Uniform Resource Identifier (URI) String Sanitize Check: The objective of this test case is to determine whether the TOE is susceptible to a URI string attack.

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 5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 5. 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
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TAA	Trade Agreement Act
TOE	Target of Evaluation
TSF	TOE Security Function
URI	Uniform Resource Identifier

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Hewlett Packard Enterprise Development LP BladeSystem c-Class Enclosure Architecture including BladeSystem c7000 Enclosure, Integrated Lights-Out (iLO) 5 v1.11, Onboard Administrator (OA) v4.71, and Virtual Connect (VC) v4.66 Security Target, Version 0.6, August 31, 2018.
Hewlett Packard Enterprise Development LP, HPE BladeSystem c7000 Enclosure Architecture including Integrated Lights-Out (iLO) 5 v1.11, Onboard Administrator (OA) v4.71, and Virtual Connect (VC) v4.66 Common Criteria EAL 2+ Evaluation Technical Report, Version 1.1, January 31, 2019.