Communications Security Establishment
Centre de la sécurité des télécommunications

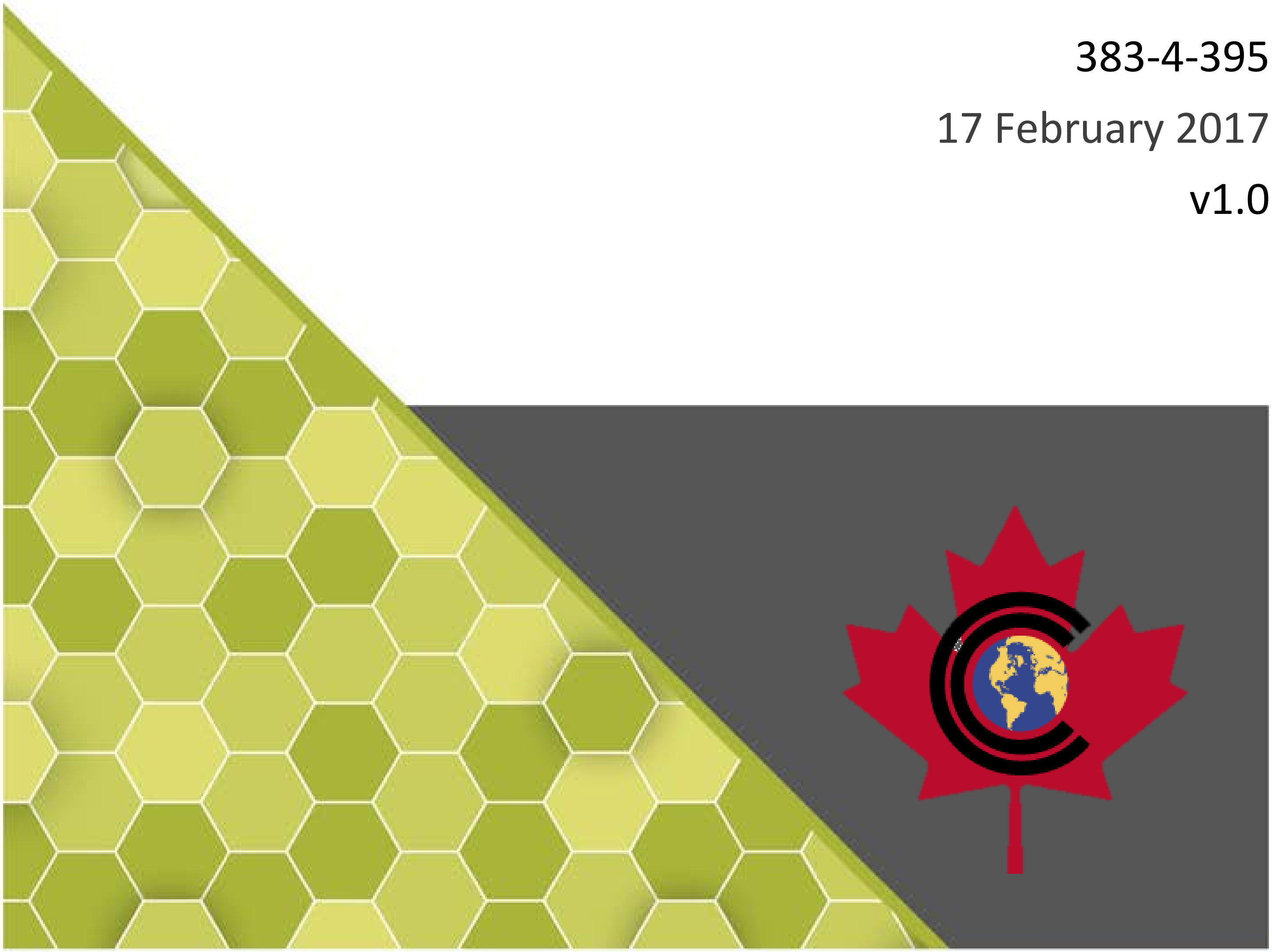
COMMON CRITERIA CERTIFICATION REPORT

HP Service Manager v9.41 Patch 3

383-4-395

17 February 2017

v1.0



© Government of Canada. This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

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 CSC Security Testing/Certification 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

HP Service Manager v9.41 Patch 3(hereafter referred to as the Target of Evaluation, or TOE), from Hewlett Packard Enterprise Development LP, 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 is an Information Technology Service Management (ITSM) software suite that enables service level management for IT organizations. The TOE is built on the Information Technology Infrastructure Library (ITIL) framework, which provides best practices for governing ITSM. The TOE is an “on-premises”, consolidated service desk that connects people, processes, and technology to implement and manage IT services across an enterprise.

CSC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed on 17 February 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	HP Service Manager v9.41 Patch 3
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 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 Information Technology Service Management (ITSM) software suite that enables service level management for IT organizations. The TOE is built on the Information Technology Infrastructure Library (ITIL) framework, which provides best practices for governing ITSM. The TOE is an “on-premises”, consolidated service desk that connects people, processes, and technology to implement and manage IT services across an enterprise.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

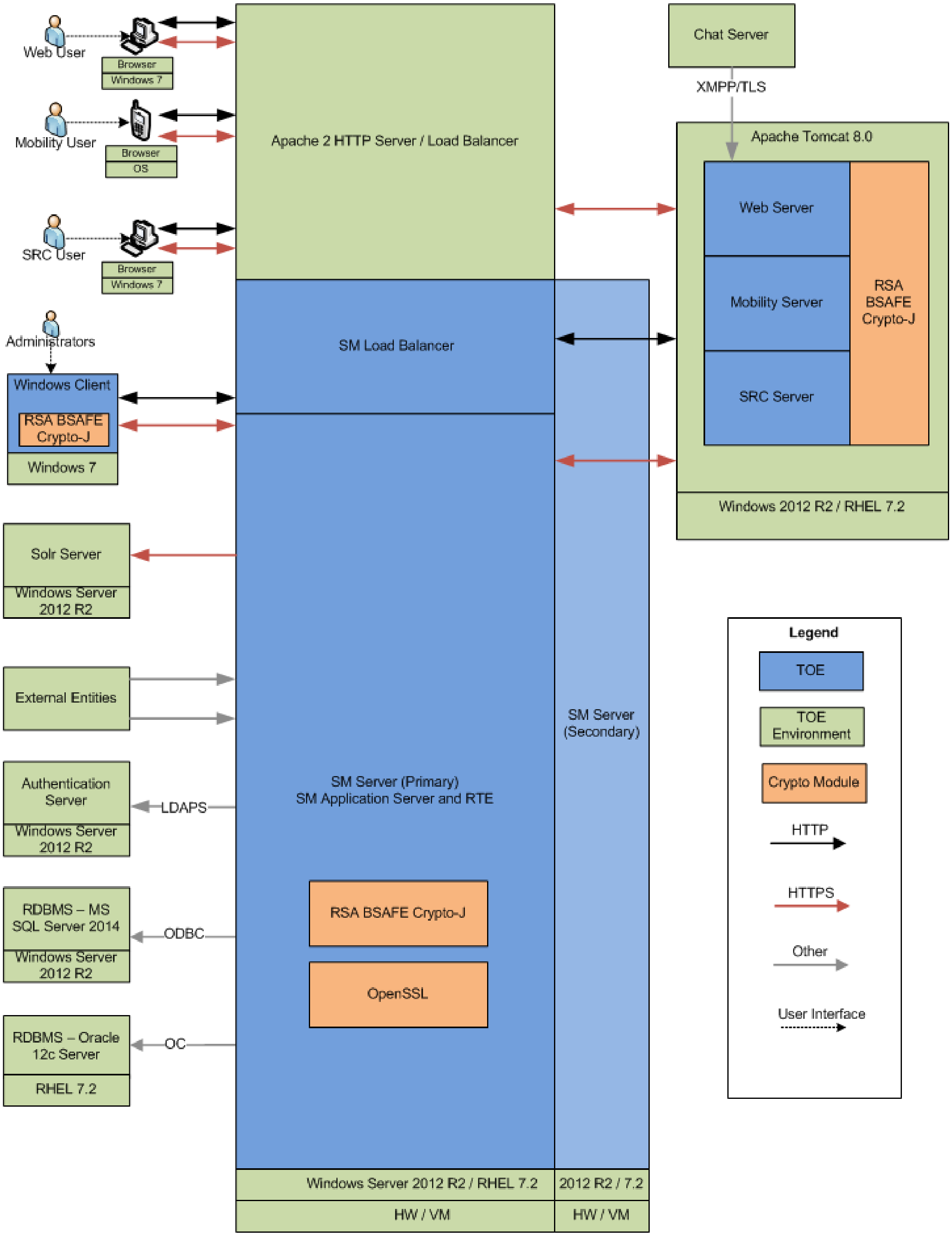


Figure 1 TOE Architecture

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 TOE Security Functions (TSF)
- Resource Utilization
- Trusted Path/Channels
- 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 implemented in the TOE:

Table 2 Cryptographic Module(s)

Cryptographic Module	Certificate Number
OpenSSL FIPS Object Module SE (Software Version: 2.0.11)	# 2398
RSA BSAFE® Crypto-J JSAFE and JCE Software Module (Software Version: 6.2)	# 2468

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 environment will provide an authentication server for the identification and authentication of users and devices attempting to access the TOE. The authentication server will support Windows domain and certificate authentication.
- The TOE, and supporting third party applications, will be installed on the appropriate dedicated operating system.
- The TOE will be located within a controlled access facility and appropriately located within a secure internal network to perform its functions.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. Administrators of the TOE are assumed to be appropriately trained to undertake configuration and management of the TOE in a secure and trusted manner.
- The authorized administrators who manage the TOE and database administrators who manage the TOE environmental components will be non-hostile, appropriately trained, and follow all guidance.
- The TOE software will be protected from unauthorized modification.
- The IT environment will provide the TOE with reliable timestamps.
- Cryptographic functionality will be provided by FIPS 140-2 validated crypto modules. Only FIPS 140-2 approved cryptographic algorithms and services will be used and the TOE will be configured to operate in "FIPS-mode" only.
- All account names, passwords or public key certificates used by external applications to communicate with the TOE via its APIs will be appropriately safeguarded and not shared with any user.

3.2 CLARIFICATION OF SCOPE

The following features and functionality are excluded from the scope of the evaluation:

- Use of the command line interface.
- Use of the TOE in non-FIPS mode
- Human user access to REST and SOAP APIs
- Failover/load balancing for REST and SOAP APIs
- Access to the Mobility Client from mobile devices.
- Mobility Client in the X.509 authentication configuration
- X.509 authentication for the Windows Client, REST and SOAP APIs
- The use of CAC or PIV cards for X.509 authentication
- TOE account lockout under TSO and X.509 configuration
- Session timeout for TSO and X.509 authentication
- TSO authentication for the REST and SOAP APIs
- LW-SSO authentication
- “Classic mode” of operation
- Custom user roles
- All Windows Client views except HP Service Manager
- All Web Client views except ESS and Power User
- All Mobility Client views except Power User

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

SM Server v9.41 Patch 3 Build #3016 (2 instances) with the included SM Load Balancer running on the first instance, and the following HP SM modules:

- Service Desk
- Incident Management
- Problem Management
- Employee Self-Service
- Knowledge Management
- Change Management
- Request Fulfillment
- Service Level Management
- Survey
- Calendar
- Reporting
- Collaboration
- Case Exchange

Windows Client v9.41 Patch 3 Build #3016

Web Server v9.41 Patch 3 Build #3016

Mobility Server v9.41 Patch 3 Build #3016

SRC Server v9.41 Patch 3 Build #3016

The TOE components are installed on General Purpose Computers/Servers running the following Operating Systems;

SM Server and SM Load Balancer

- Windows Server 2012 R2
- Red Hat Enterprise Linux 7.2

Windows Client

- Windows 7 64-bit

Web Server

- Apache Tomcat 8.0
- JRE 8

Mobility Server

- Apache Tomcat 8.0
- JRE 8

SRC Server

- Apache Tomcat 8.0
- JRE 8

The following are required environmental components:

Database Servers

- Oracle Database 12c
- Microsoft SQL Server 2014

Authentication Server

- Microsoft Windows Active Directory Domain Services and Certificate Services

Knowledge Management

- Apache Solr

Collaboration (Chat Server)

- Ignite Realtime Openfire

4.1 DOCUMENTATION

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

a. HP Service Manager; Software Version: 9.41 for the supported Windows® and UNIX® operating systems; Collaboration Guide; Document Release Date: September 2015

b. HP Service Manager; Software Version: 9.41 for the supported Windows® and UNIX® operating systems; Mobile Applications User Guide; Document Release Date: September 2015

c. HP Service Manager; Software Version: 9.41 for the supported Windows® and UNIX® operating systems; Processes and Best Practices Guide (Codeless Mode); Document Release Date: September 2015

d. HP Service Manager; Software Version: 9.41 for the supported Windows® and UNIX® operating systems; Solr Search Engine Guide; Document Release Date: September 2015

e. HP Service Manager; Software Version: 9.41 for the supported Windows® and UNIX® operating systems; Web Services Guide (Codeless Mode); Document Release Date: September 2015

f. HP Service Manager; Software Version: 9.41 for the supported Windows® and UNIX® operating systems; Service Manager 9.41 Patch 3 Release Notes; Document Release Date: April 2016

g. HP Service Manager; Software Version: 9.3x and 9.4x; Security Guide; Document Release Date: April 9, 2015

h. HP Service Manager 9.41 Patch 3; Guidance Supplement; Document Version: 1.2; February 8, 2017

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 0 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.

The evaluators reviewed the flaw remediation procedures used by developer for the TOE. 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 TOE.

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 activities were performed:

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

b. User Creation: This test case tests "user creation" capability of the TOE;

c. Role Based Access Control: This test case verifies that that the TOE's role based access control functions as expected;

d. Security Group based Restrict Query: This test case verifies Security Group definition based (Mandanten Restrict) Query access control capability of the TOE function as expected;

e. Mandant table and field: This test case verifies the TOE's query access control capability based on Operator Security Group and table Mandant Field;

f. Folder Entitlement: This test case verifies folder entitlement based access control capability of the TOE;

g. Knowledge Management Access Control: This test case verifies kmgroup and kmprofile based access control capability of the TOE;

h. Internal and External TLS: This test case verifies the protection of communication capability of the TOE;

i. Database Audit: This test case verifies the database audit security functionality and the security management of the database audit configuration;

j. Service Level Management: This test case verifies the Service Level Management Alert functionality and the security management of the Service Level Management;

k. Application Service TLS: This test case verifies the TLS protection of the SOAP and RESTful API communications;

l. User Session Time out: This test case verifies that an interactive client session is terminated after a defined period of no user activity;

m. Password based I&A: This test case verifies the Identification, (password based) Authentication, account lockout and Auditing features of the TOE;

n. Fail Secure: This test case verifies the automatic failover services of the TOE;

o. X509 Authentication: This test case verifies the X509 authentication services of the TOE; and

p. TSO Authentication: This test case verifies the TSO authentication services of 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, GHOST, and other web application vulnerabilities.

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
REST	Representational state transfer
SFR	Security Functional Requirement
SOAP	Simple Object Access Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSO	Trusted Sign-On

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.
Hewlett Packard Enterprise Development LP HP Service Manager Security Target V1.4, 17 February 2017
Evaluation Technical Report for HP Service Manager v9.41 Patch 3 build #3016 v1.2, 17 February 2017