Certification Report

HP Cloud Service Automation v4.10

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-322-CR
Version: 1.0
Date: September 15, 2015
Pagination: i to iii, 1 to 9

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 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 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, 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.

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.

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, 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 CGI IT Security Evaluation & Test Facility.

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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated September 15, 2015, 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).

TABLE OF CONTENTS

Executive Summary

HP Cloud Service Automation v4.10 (hereafter referred to as HP CSA), from Hewlett Packard Enterprise Development L.P., is the Target of Evaluation. The results of this evaluation demonstrate that HP CSA meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

HP CSA is a software-only solution designed to help cloud service providers by automating their ability to broker cloud services to their customers. HP CSA integrates and leverages the strengths of several HP datacenter management and automation products, adding resource management, service offering design, and a customer portal to create a comprehensive service automation solution.

The product provides an environment that can be used by cloud service provider personnel to design templates for demanded services, and by their consumers to automatically broker the provisioning of these services among available resources.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on September 15, 2015 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 HP CSA, 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 CCS Certification Body, declares that the HP CSA 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

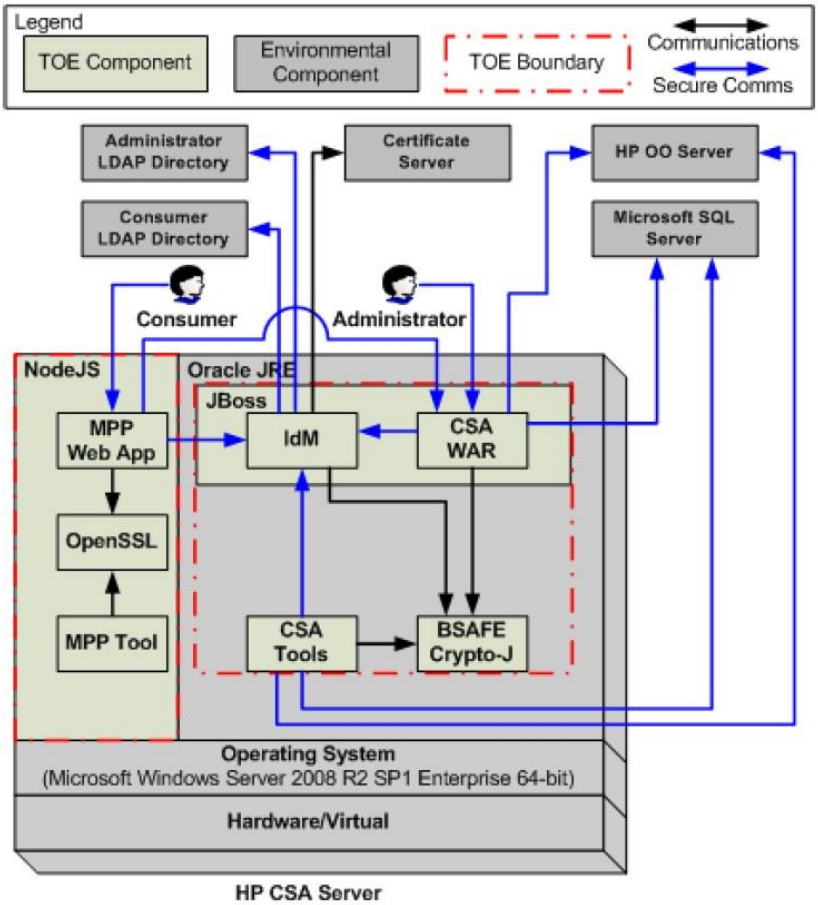
The Target of Evaluation (TOE) for this EAL 2+ evaluation is HP Cloud Service Automation v4.10 (hereafter referred to as HP CSA), from Hewlett Packard Enterprise Development L.P.

2 TOE Description

HP CSA is a software-only solution designed to help cloud service providers by automating their ability to broker cloud services to their customers. HP CSA integrates and leverages the strengths of several HP datacenter management and automation products, adding resource management, service offering design, and a customer portal to create a comprehensive service automation solution.

The product provides an environment that can be used by cloud service provider personnel to design templates for demanded services, and by their consumers to automatically broker the provisioning of these services among available resources.

A diagram of the HP CSA architecture is as follows:



3 Security Policy

HP CSA implements a role-based access control policy to control administrative access to the system. In addition, HP CSA 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;

TOE Access; and

Trusted Path/Channels.

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate**
RSA B-SAFE Crypto-J JSAFE and JCE Cryptographic Library version 6.1	*2057*
OpenSSL FIPS Object Module, Software Version v2.0.7	*1747*

4 Security Target

The ST associated with this Certification Report is identified below:

Hewlett Packard Enterprise Development L.P., Cloud Service Automation v4.10 Security Target, August 13, 2015, version 1.6

5 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.*

HP CSA is:

a. *EAL 2 augmented, containing all security assurance requirements listed, as well as the following:*

   ALC_FLR.2 – Flaw Reporting Procedures.

b. *Common Criteria Part 2 conformant; with security functional requirements based only upon functional components in Part 2;*

c. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of HP CSA 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- *There are one or more competent individuals assigned to manage the TOE and the security of the information it contains;*
- *The Users who manage the TOE are non-hostile, appropriately trained, and follow all guidance; and*
- *The TOE software will be protected from unauthorized modification.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The TOE environment will be able to maintain user security attributes when the TOE is configured to use external authentication;*
- *The TOE is installed on the appropriate, dedicated hardware, OS, and runtime environment;*
- *The TOE is located within a controlled access facility;*
- *The TOE environment provides the network connectivity required to allow the TOE to provide secure routing and switching functions; and*
- *The TOE environment provides the TOE with the necessary reliable timestamps.*

7 Evaluated Configuration

The evaluated configuration for HP Cloud Service Automation v4.10 comprises the following components:

- *MPP (Market Place Portal) Web Application;*
- *OpenSSL;*
- *MPP Tool;*
- *IdM (Identity Management);*
- *CSA (Cloud Service Automation) Tools;*
- *CSA WAR (Web Application Archive); and*
- *BSAFE Crypto-J.*

The following environmental components are required for the proper operation of the TOE in the evaluated configuration:

- A GPC running Microsoft Windows Server 2012 R2 Standard 64-bit;
- A DB Server;
- An LDAP Server;
- A Certificate Server; and
- An HP OO Server.

The publications entitled:

- HP Cloud Service Automation v4.10 - Installation Guide
- HP Cloud Service Automation v4.10 - Windows Configuration Guide, August 2014
- HP Cloud Service Automation v4.10 - Process Definition Tool
- HP Cloud Service Automation v4.10 - API Reference, July 2014
- HP Cloud Service Automation v4.10 - Marketplace Portal Help, July 2014
- HP Cloud Service Automation v4.10 Guidance Documentation Supplement v1.3

describe the procedures necessary to install and operate HP CSA in its evaluated configuration.

8 Documentation

The Hewlett Packard Enterprise Development L.P. documents provided to the consumer are as follows:

- HP CSA 4.10 – API Quick Start, July 2014;
- HP CSA 4.10 – API Reference, July 2014;
- HP CSA 4.10 – Content Archive Tool, July 2014;
- HP CSA 4.10 – Concepts Guide bb;
- HP CSA 4.10 – Configuration Guide (Windows) ;
- HP CSA 4.10 – FIPS 140-2 Compliance Statement , August 2014;

- HP CSA 4.10 – Installation Guide;
- HP CSA 4.10 – Integration Pack, July 2014;
- HP CSA 4.10 – Marketplace Portal Help, July 2014;
- HP CSA 4.10 – Open Source and Third-Party Software License Agreements;
- HP CSA 4.10 – Provider Configuration Tool, July 2014;
- HP CSA 4.10 – Process Definition Tool;
- HP CSA 4.10 – Release Notes;
- HP CSA 4.10 – Cloud Service Management Console Help;
- HP CSA 4.10 – System and Software Support Matrix;
- HP CSA 4.10 – Troubleshooting Guide, August 2014;
- HP CSA 4.10 – Upgrade Guide; and
- HP CSA 4.10 – What's New in Cloud Service Automation 4.10.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of HP CSA, including the following areas:

Development: The evaluators analyzed the HP CSA 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 HP CSA 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.

Guidance Documents: The evaluators examined the HP CSA 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.

Life-cycle support: An analysis of the HP CSA configuration management system and associated documentation was performed. The evaluators found that the HP CSA 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 HP CSA during distribution to the consumer.

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

All these evaluation activities resulted in **PASS** verdicts.

10 ITS Product Testing

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

10.1 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[1].

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.

10.2 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. Resulting from this test coverage approach is the following list of test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Administrative Actions: The objective of this test goal is to verify that all administrative actions generate an audit record;

c. Password and Message Obfuscation: The objective of this test goal is to confirm that passwords are not displayed in the clear and that any failure message is ambiguous;

d. Access before Authentication: The objective of this test goal is to confirm the ability of a user to use certain CLI tools prior to authentication to the TOE;

e. User Roles and Access Control: The objective of this test goal is to verify user role`s permissions and what options are available to each role when logged in;

f. Secure Communication: The objective of this test goal is to confirm the REST API communicates over a secure channel; and

g. Subscription Request Denial: The objective of this test goal is to demonstrate the ability of an administrator to deny a subscription request via the REST API.

[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.

10.3 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:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities; and

b. Disclosure of Ports: The objective of this test goal is to scan for open ports and then determine if the open ports should be open.

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

10.4 Conduct of Testing

HP CSA 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.

10.5 Testing Results

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

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
CSA	Cloud Service Automation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
GPC	General Purpose Computer
HP OO Server	HP Operations Orchestration Server
IDM	Identity Management
IT	Information Technology
ITSET	Information Technology Security

Acronym/Abbreviation/ Initialization	Description
	Evaluation and Testing
LDAP	Lightweight Directory Access Protocol
MPP	Market Place Portal
PALCAN	Program for the Accreditation of Laboratories - Canada
REST API	Representational State Transfer Application Programming Interface
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
WAR	Web Application Archive

13 References

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

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Hewlett Packard Enterprise Development L.P., Cloud Service Automation v4.10 Security Target, August 13, 2015, version 1.6

e. Hewlett Packard Enterprise Development L.P., Cloud Service Automation v4.10 Evaluation Technical Report, September 15, 2015, v1.0.