



HP Cloud Service Automation Version 4.0 FIPS 140-2 Compliance Statement

January 2014

TABLE OF CONTENTS

SUMMARY 1

OVERVIEW 1

 ABOUT HP CLOUD SERVICE AUTOMATION 1

 CLOUD SERVICE MANAGEMENT CONSOLE WEB APPLICATION..... 1

 MARKETPLACE PORTAL WEB APPLICATION 1

 HP CSA PASSWORD UTILITY TOOL..... 2

 MARKETPLACE PORTAL PASSWORD UTILITY TOOL..... 2

 CONTENT ARCHIVE TOOL..... 2

 IDENTITY MANAGEMENT SERVICE 2

 ABOUT FIPS 140-2..... 2

 FIPS 140-2 COMPLIANT MODULE AND TECHNOLOGIES..... 3

 FIPS REQUIREMENTS..... 4

HP CLOUD SERVICE AUTOMATION AND FIPS 140-2..... 6

 FIPS 140-2 ARCHITECTURE 6

 DESIGN ASSURANCE 7

 SECURITY GOVERNANCE AND POLICY 10

ACRONYMS 12

REFERENCES..... 12

Summary

The following HP Cloud Service Automation (HP CSA) components comply with Level 1 Federal Information Processing Standard 140-2 (FIPS 140-2), which defines the technical requirements to be used by federal agencies when these organizations specify cryptographic-based security systems for protection of sensitive or valuable data:

- Cloud Service Management Console
- Marketplace Portal
- Password Utility Tool
- Marketplace Portal Password Utility Tool
- Content Archive Tool
- Identity Management Service

The compliance of these CSA components with FIPS 140-2 is ensured by integrating FIPS 140-2 compliant, third party cryptographic module(s), using the module(s) as the only provider(s) of cryptographic services, and using FIPS-approved cryptographic functions, as applicable for HP CSA design, implementation, and operation.

Overview

This section describes the different elements that make up the HP CSA solution.

About HP Cloud Service Automation

HP CSA is a unique platform that orchestrates the deployment of compute and infrastructure resources and of complex multi-tier application architectures. HP CSA integrates and leverages the strengths of a hybrid cloud environment, which provides the ability to design and deploy enterprise-ready cloud services tailored to the business needs of your organization.

For details about how HP CSA implements FIPS 140-2 requirements, see the *HP Cloud Service Automation Configuration Guide*.

Cloud Service Management Console Web Application

The Cloud Service Management Console provides for the overall administration and configuration of the HP CSA system. The primary administration tasks are organized around the creation and configuration of organizations within the system.

Marketplace Portal Web Application

The Marketplace Portal delivers cloud-service catalogs to customers through an innovative, *enterprise-ready* design. In this design, users in each organization order services tailored specifically to their needs, and unless they have proper authorization, cannot access the service catalogs belonging to any other organization.

HP CSA Password Utility Tool

HP CSA's Password Utility tool is a standalone application used to encrypt sensitive data stored by HP CSA. This information includes:

- Seeded (HP CSA internal user) user credentials.
- Passwords as configured through the Cloud Service Management Console.

For details about the Password Utility tool, see the *HP Cloud Service Automation Configuration Guide*.

Marketplace Portal Password Utility Tool

The Marketplace Portal Password Utility Tool is a standalone application used to encrypt passwords stored by the Marketplace Portal. For details about the Marketplace Portal Password Utility tool, see the *HP Cloud Service Automation Configuration Guide*.

Content Archive Tool

HP CSA's Content Archive Tool is used to move various pieces of artifact information from one HP CSA installation to another.

For details about the Content Archive Tool, see the *HP Cloud Service Automation Content Archive Tool Guide*.

Identity Management Service

The Identity Management service (IdM) provides authentication for HP CSA. HP CSA and the Marketplace Portal rely on the centralized IdM component to obtain authentication information. IdM works within the HP CSA Java Runtime Environment (JRE) with all FIPS compliance components. IdM communicates with the Cloud Service Management Console and the Marketplace Portal through the HTTPS protocol to provide authentication and authorization services.

For details about how the identity management service implements FIPS 140-2 requirements, see the *HP Cloud Service Automation Configuration Guide*.



In this document, JRE or JVM refer to Oracle JRE or Oracle JVM respectively.

About FIPS 140-2

The Federal Information Processing Standards Publication (FIPS) 140-2, "Security Requirements for Cryptographic Modules," was issued by the National Institute of Standards and Technology (NIST) in May, 2001. The FIPS 140-2 standard specifies the security requirements for cryptographic modules used within a security system that protects sensitive or valuable data. The requirements can be found in the following documents:

- SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES
<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- Annex A: Approved Security Functions for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*
<http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf>



In this document, the abbreviation “FIPS” means “FIPS 140-2.”

FIPS 140-2 Compliant Module and Technologies

The benefits of using FIPS 140-2 compliant crypto modules is that the FIPS-approved crypto algorithms are deemed appropriate and that they perform the encrypt, decrypt, and hash functions correctly and in a FIPS-compliant manner.

Modes of Operation

HP CSA and its components can be configured and operated in the following two modes:

- FIPS-compliant mode: This mode supports FIPS 140-2 compliant cryptographic functions.
- Standard mode: This is a non-FIPS 140-2 compliant mode that uses existing or available cryptography without 3rd party FIPS-compliant 140-2 crypto modules.

FIPS 140-2 Compliant Third Party Modules

The Marketplace Portal component and the Marketplace Password Utility component are integrated with the 3rd party FIPS 140-2 compliant cryptographic module *OpenSSL FIPS Object Module v2.0*. When the Marketplace Portal is configured to operate in FIPS-compliant mode, its functions and procedures (such as SSL/TLS connections and encryption of stored sensitive data, which require cryptography such as secure hash, encryption, digital signature, and so on) use the cryptography services provided by the OpenSSL FIPS Object Module configured to run in FIPS mode.

All other HP CSA components are integrated with the 3rd party FIPS 140-2 compliant cryptographic module *RSA BSAFE Crypto-J version 6.1*. When HP CSA is configured to operate in FIPS-compliant mode, its functions and procedures (such as SSL/TLS connections and encryption of stored sensitive data, which require cryptography such as secure hash, encryption, digital signature, and so on) use the cryptography services provided by RSA BSAFE Crypto-J configured to run in FIPS mode.

Details about how to configure HP CSA and its components to conform to FIPS 140-2 appear in the following installation and configuration guides:

- *HP Cloud Service Automation Installation Guide*
- *HP Cloud Service Automation Configuration Guide*

FIPS Requirements

HP CSA can be run in FIPS mode in a standalone configuration.

HP CSA-Sensitive Data

HP CSA-sensitive data that requires FIPS-compliant encryption using RSA BSAFE Crypto-J is listed below.

- HP CSA seeded user credentials. There are internal users that are part of the CSA installation. The passwords of these seeded users are considered HP CSA-sensitive data.
- HP CSA transport user credentials and IdM transport user credentials. The Cloud Service Management Console has a REST web service interface. REST requests are authenticated using HP CSA's transport user credentials. In a typical HP CSA installation, the REST API is used by HP CSA to communicate with the Cloud Service Management Console. These passwords are stored in the following files: `csa.properties`, `csa-consumer-users.properties`, `idm-security.properties`, and `integrationusers.properties`. Transport user passwords are considered HP CSA-sensitive data.
- Access Point credentials. Every organization listed in the Cloud Service Management Console can be associated with an LDAP, SMTP, or one or more CSA Resource Provider access points. The access point passwords are stored in the HP CSA database and are considered HP CSA-sensitive data.
- The HP CSA SSL truststore contains 3rd party certificates that are implicitly trusted by HP CSA during SSL communication. The HP CSA truststore password is considered HP CSA-sensitive data. When run in FIPS mode, HP CSA does not use the default Java truststore.

Note: Data that does not compromise HP CSA-sensitive data as described above is not considered HP CSA-sensitive data.

Marketplace Portal-Sensitive Data

Marketplace Portal-sensitive data that requires FIPS-compliant encryption using the OpenSSL FIPS Object Module is listed below.

- IdM transport user credentials. The Marketplace Portal has a REST web service interface. REST requests are authenticated using IdM transport user credentials. In a typical HP CSA installation, the REST API is used by the Marketplace Portal to communicate with the Cloud Service Management Console. These passwords are stored in the `mpp.json` file. Transport user passwords are considered Marketplace Portal-sensitive data.
- Cookie password. This is the key used to encrypt the cookie that stores the user's organization name and the session ID to make the login persistent.
- SSL keystore password.
- List of 3rd party CA certificates (in PEM format or DER format) that the Marketplace Portal reads in that are implicitly trusted by the Marketplace Portal during SSL communication.

Note: Data that does not compromise Marketplace Portal-sensitive data as described above is not considered Marketplace Portal-sensitive data.

FIPS Supported Configuration for Data at Rest

When run in FIPS mode, HP CSA uses the following RSA BSAFE Crypto module FIPS certified algorithms for encryption and storage of HP CSA sensitive data:

1. Supported Encryption Keystore format: PKCS 12
2. Supported asymmetric algorithm for HP CSA Encryption Keystore: RSA (recommended size 2048)
3. Supported symmetric key algorithm used by HP CSA: AES (128-bit (default), 192-bit, and 256-bit key sizes)
4. Supported Random Number Generation algorithm used by HP CSA for encryption is HMAC DRBG (128-bit)



The Marketplace Portal contains no data at rest.

Data In Transit

When run in FIPS mode, HP CSA uses the FIPS-certified Cipher Suites provided by the RSA BSAFE Crypto module. The supported SSL Keystore and truststore format is PKCS 12.

When run in FIPS mode, the Marketplace Portal uses the OpenSSL FIPS Object Module for SSL. The supported SSL Keystore and truststore format is PKCS 12.

TLS1.x (HP CSA)

All HP CSA component communications are secured with FIPS-compliant Transport Layer Security TLS1.0. It is relying on FIPS 140-2 approved hash algorithms and symmetric and asymmetric ciphers provided by the RSA BSAFE Crypto module.

- TLS handshake, key negotiation and authentication provide data integrity and make use of secure hash, asymmetric key cryptography and digital signature.
- TLS encryption of data in transit provides confidentiality and makes use of symmetric cryptography.

TLS1.x (Marketplace Portal)

All Marketplace Portal component communications can be secured with FIPS-compliant Transport Layer Security TLS1.0. It is relying on FIPS 140-2 approved hash algorithms and symmetric ciphers provided by the OpenSSL FIPS Object Module.

- TLS handshake, key negotiation and authentication provide data integrity and make use of secure hash, and digital signature.
- TLS encryption of data in transit provides confidentiality and makes use of symmetric cryptography.

To enable TLS1.0, you must:

- Compile OpenSSL with the OpenSSL FIPS Object Module while specifying TLS1.0.

- Add the proper settings to enable TLS1.0 in the Marketplace Portal mpp.json configuration file. For more information, see the “Configure the Marketplace Portal for FIPS 140-2 Compliance” section in the *HP Cloud Service Automation Configuration Guide*.

Secure Hash

HP CSA supports the secure hash algorithms supported by RSA BSAFE Crypto-J when run in FIPS-compliant mode. For details, refer to the FIPS compliance documentation provided by the RSA BSAFE Crypto-J module provider.

The Marketplace Portal supports the secure hash algorithms supported by the OpenSSL FIPS Object Module when run in FIPS-compliant mode. For details, refer to the FIPS compliance documentation regarding the OpenSSL FIPS Object Module at <http://www.openssl.org/docs/fips/>.

Message Digest

HP CSA supports the secure Message Digest algorithms supported by RSA BSAFE Crypto-J when run in FIPS-compliant mode. For details, refer to the FIPS compliance documentation provided by the RSA BSAFE Crypto-J provider.

The Marketplace Portal supports the secure Message Digest algorithms supported by the OpenSSL FIPS Object Module when run in FIPS-compliant mode. For details, refer to the FIPS compliance documentation regarding the OpenSSL FIPS Object Module at <http://www.openssl.org/docs/fips/>.

Digital Signature

HP CSA supports the secure digital signature algorithms supported by RSA BSAFE Crypto-J when run in FIPS-compliant mode. For details, refer to the FIPS compliance documentation provided by the RSA BSAFE Crypto-J provider.

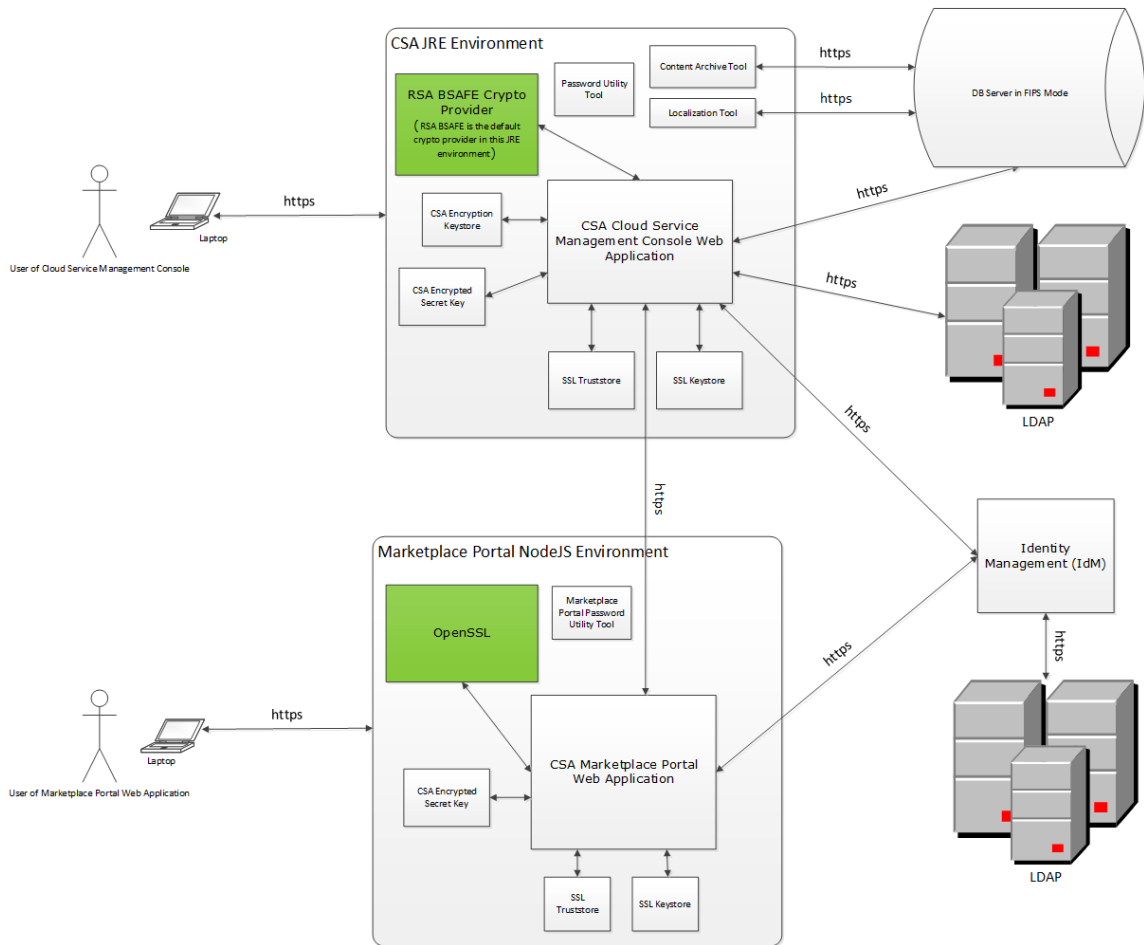
The Marketplace Portal supports the secure digital signature algorithms supported by the OpenSSL FIPS Object Module when run in FIPS-compliant mode. For details, refer to the FIPS compliance documentation regarding the OpenSSL FIPS Object Module at <http://www.openssl.org/docs/fips/>.

HP Cloud Service Automation and FIPS 140-2

HP CSA is expected to operate on general-purpose systems with no additional physical security controls. The RSA BSAFE Crypto-J module and the OpenSSL FIPS Object Module installed on such platforms provide compliance to Level 1 FIPS 140-2 compliant crypto services. For RSA BSAFE Crypto-J, you install the Crypto-J module. For the OpenSSL FIPS Object Module, you download the source code from the OpenSSL website and recompile it. For more information, see the *HP Cloud Service Automation Configuration Guide*.

FIPS 140-2 Architecture

All HP CSA instances in a HP CSA deployment must be run in FIPS-compliant mode. HP CSA does not support a deployment architecture that contains a mix of HP CSA instances that run in FIPS and non-FIPS mode.



Standalone Configuration

The CSA JRE environment corresponds to the JRE being used by HP CSA components. This JRE must be configured using the RSA BSAFE JSafeJCE crypto library (as described in "Configure HP CSA for FIPS 140-2 Compliance" in the *HP Cloud Service Automation Configuration Guide*). For the Marketplace Portal, NodeJS must be compiled with the OpenSSL FIPS Object Module.

You can deploy multiple Marketplace Portal instances in standalone mode.

Supported Platforms

Refer to the *HP Cloud Service Automation Solution and Software Support Matrix* for more information.

Design Assurance

The following sections illustrate the design, operation, and use of the FIPS-compliant crypto components by HP CSA and by the Marketplace Portal when run in FIPS-compliant mode.

Key Management

All aspects of key management, such as random number and key generation, are provided by functions of the RSA BSAFE Crypto-J crypto module (for HP CSA) or

the OpenSSL FIPS Object Module (for the Marketplace Portal) and thus meet FIPS 140-2 compliance requirements. The application-specific key management functions are identified below.

FIPS Compliance of HP CSA for Sensitive Data at Rest (Storage)


The following sections detail configuration and key management design used by the FIPS-compliant components of HP CSA.

Configuration of HP CSA

To configure FIPS-compliant components of HP CSA:

1. Create the HP CSA Encryption Keystore.
2. Create a file with a secret key in an encrypted form using the Password Utility tool or the Marketplace Portal Password Utility Tool as appropriate.

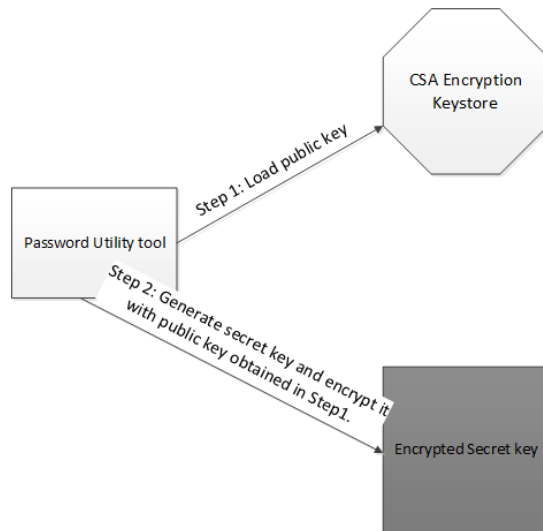
For additional details refer to the “Configure HP CSA for FIPS 140-2 Compliance” section in the *HP Cloud Service Automation Configuration Guide*.

 The Marketplace Portal contains no data at rest.

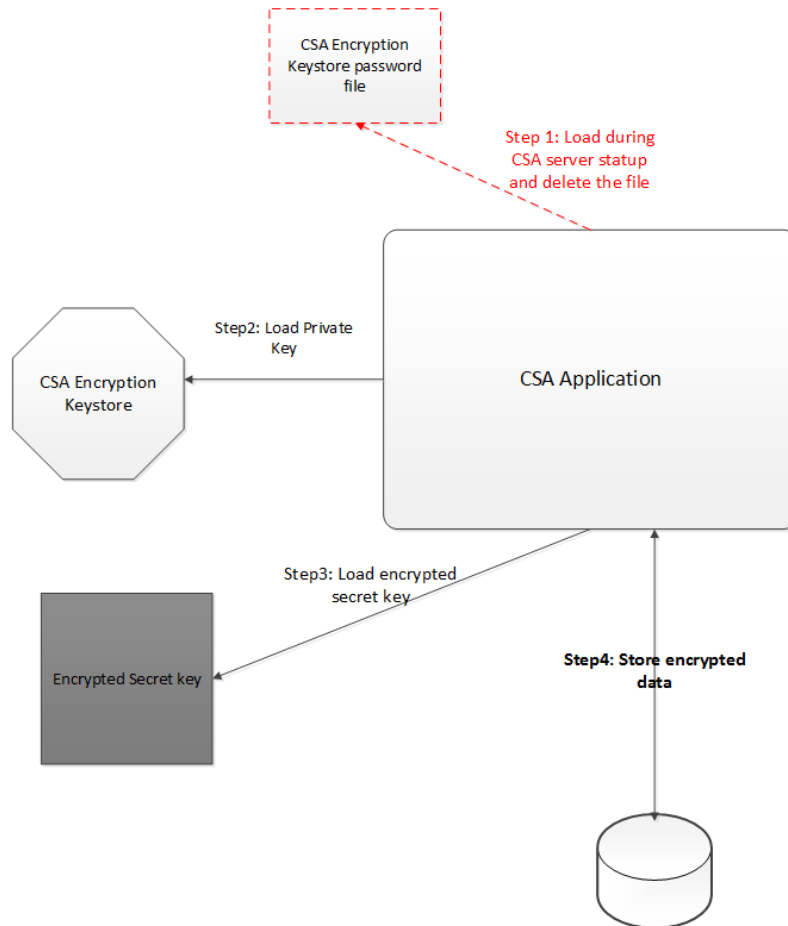
Key Management Design Used by HP CSA FIPS-Compliant Components

To perform key management using HP CSA FIPS-compliant components:

1. HP CSA Key Generation
 - The secret key is generated and stored in encrypted form by the Password Utility Tool. This tool uses the HP CSA Encryption keystore to encrypt the key. The crypto algorithms used are provided by the FIPS-certified RSA BSAFE provider.



2. HP CSA Encryption/Decryption Operation



- The secret key used by HP CSA is stored in a FIPS-compliant encrypted form. This key is loaded in encrypted form for encryption/decryption of HP CSA sensitive data. The location of the secret key has to be configured in the `csa.properties` file and the `idm-security.properties` file. See the *HP Cloud Service Automation Configuration Guide* for details.
- The plain text password for the HP CSA Encryption keystore is loaded from a file during startup, and the file is deleted to ensure that the password for the encryption keystore is present only in the JVM memory of the HP CSA server.

The administrator must recreate this file with the HP CSA encryption keystore password if the HP CSA server has to be restarted. The HP CSA server will fail to start up in FIPS mode if this file does not exist.

Usage

HP CSA uses the encrypted secret key to encrypt HP CSA sensitive data.

FIPS Compliance of HP CSA for Data in Transit

HP CSA supports only TLSv1.0 in FIPS compliance mode. As part of HP CSA configuration for FIPS, HP CSA requires the JRE to be configured to use the RSA BSAFE security provider in FIPS-certified mode for SSL (as mentioned in “Configure HP CSA for FIPS 140-2 Compliance” in the *HP Cloud Service Automation Configuration Guide*).

HP CSA Configuration

1. Create the SSL keystore in PKCS 12 format.

2. Configure JBoss to support TLS v1.0.
3. Create and configure the HP CSA SSL Truststore. In FIPS mode, HP CSA will not use the default Java CAcert truststore.

HP CSA SSL Operation and Usage

With the JRE configured to use the RSA BSAFE crypto provider in FIPS certified mode, the SSL cipher suites used by HP CSA will be the FIPS certified cipher suites of the RSA BSAFE provider. Refer to “FIPS 140-2 Architecture” for details on the SSL components of HP CSA.

The 3rd party software components that HP CSA integrates with are expected to be set in FIPS-compliant mode in order to interact with HP CSA in a FIPS-compliant manner using SSL. The 3rd party components are:

- LDAP server of each organization configured in the Cloud Service Management Console
- Database instance used by HP CSA
- SMTP server

FIPS Compliance of the Marketplace Portal for Data in Transit

The Marketplace Portal supports only TLSv1.0 in FIPS compliance mode. As part of the Marketplace Portal configuration for FIPS, it requires the OpenSSL FIPS Object Module in FIPS certified mode for SSL (as mentioned in “Configure the Marketplace Portal for FIPS 140-2 Compliance” in the *HP Cloud Service Automation Configuration Guide*).

Marketplace Portal Configuration

1. Create the SSL keystore in PKCS 12 format.
2. Configure NodeJS to support TLS v1.0.

Marketplace Portal SSL Operation and Usage

With NodeJS configured to use the OpenSSL FIPS Object Module in FIPS certified mode, the SSL cipher suites used by the Marketplace Portal will be the FIPS certified cipher suites of the OpenSSL FIPS Object Module. Refer to “FIPS 140-2 Architecture” for details on the SSL components of the Marketplace Portal.

Security Governance and Policy

Physical security

The production servers on which HP CSA is installed must allow only users with valid credentials access to the system.

Configuration data security

HP CSA installation and configuration requires additional information such as credentials to access the database and the SSL keystore password. These credentials, though confidential, are not considered HP CSA sensitive data, because:

- This data does not compromise the encrypted FIPS-compliant sensitive data stored by HP CSA that are configured by end users of HP CSA.
- This data is not exposed to the end users of HP CSA.

- This data cannot be read, updated, or modified remotely by 3rd party systems integrated with HP CSA.

The security policies mentioned below are required to be followed for these credentials to provide sufficient risk mitigation for these data points.

Datasource password for HP CSA

The datasource password is used by JBoss to connect to the HP CSA database server on behalf of HP CSA. When HP CSA is run in FIPS compliant mode, this value must be encrypted using the JBoss 7.1.1 vault functionality. Refer to "Create a New Keystore and Truststore for SSL Communication" in the *HP Cloud Service Automation Configuration Guide* for more information.

SSL keystore password for HP CSA

The SSL keystore password is used by JBoss to access the SSL keystore when initiating an SSL connection. When HP CSA is run in FIPS compliant mode, this value must be encrypted using the JBoss 7.1.1 vault functionality. Refer to "Create a New Keystore and Truststore for SSL Communication" in the *HP Cloud Service Automation Configuration Guide* for more information.

Acronyms

AES

Advanced Encryption Standard.

CSA

HP Cloud Service Automation.

HMAC DRBG

Keyed-hash message authentication code deterministic random bit generator, which is a random number generation algorithm.

FIPS

Federal Information Processing Standard.

IdM

Identity Management component of HP CSA.

JBoss

JavaBeans Open Source Software Application Server, which is an application server that implements the Java Platform, Enterprise Edition.

JVM

Java Virtual Machine. HP CSA uses the JVM included in the Oracle Java Runtime Environment (JRE).

MPP

Marketplace Portal.

PKCS 12

Personal Information Exchange Syntax Standard #12.

REST

Representational State Transfer.

RSA

An algorithm for public-key cryptography. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman.

SMC

Service Management Console.

SSL

Secure Sockets Layer, which is the standard security technology for establishing an encrypted link between a web server and a browser.

TLS

Transport Security Layer.

References

HP Cloud Service Automation Installation Guide

HP Cloud Service Automation Configuration Guide

HP Cloud Service Automation Solution and Software Support Matrix