# Hewlett-Packard Enterprise Development, L.P.

## Cloud Service Automation v4.10

# Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.6

Prepared for:

**Hewlett-Packard Enterprise Development, L.P.**
3000 Hanover Street
Palo Alto, CA 94304
United States of America

Phone: +1 305 267 4220
Email: info@hpe.com
http://www.hpe.com

Prepared by:

**Corsec Security, Inc.**
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com

# Table of Contents

# Table of Figures

# List of Tables

# 1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the HP Cloud Service Automation v4.10, and will hereafter be referred to as the TOE throughout this document. The TOE is a software application designed to help cloud service providers by automating their ability to broker cloud services to their consumers. The TOE orchestrates the deployment of compute and infrastructure resources and complex multi-tier application architectures. It integrates and leverages the strengths of several HPE datacenter management and automation products, adding resource management, service offering design, and a customer portal to create a comprehensive service automation solution.

## 1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Security Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

## 1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

**Table 1 ST and TOE References**

| | |
|---|---|
| **ST Title** | Hewlett-Packard Enterprise Development, L.P. Cloud Service Automation v4.10 Security Target |
| **ST Version** | Version 1.6 |
| **ST Author** | Corsec Security, Inc. |
| **ST Publication Date** | 8/13/2015 |
| **TOE Reference** | HP Cloud Service Automation v4.10 with hotfix QCCR1D187886 |

| | |
|---|---|
| **FIPS[1] 140-2 Status** | Level 1, RSA[2] BSAFE Crypto-J JSAFE and Java Cryptography Extension (JCE) Software Module, Software Version 6.1, Certificate No. [2057]<br>Level 1, OpenSSL FIPS Object Module, Software Version v2.0.7, Certificate No. [1747] |

## 1.3 Product Overview

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 several HPE datacenter management and automation products, adding resource management, service offering design, and a customer portal to create a comprehensive service automation solution.

The HP CSA Subscription, Service Design, and resource utilization capabilities address three key challenges:

- The HP CSA Market Place Portal provides a customer interface for requesting new cloud services and for monitoring and managing existing services, with Subscription Pricing to meet your business requirements.
- The HP CSA graphical Service Design and content portability tools simplify developing, leveraging, and sharing an array of Service Offerings that can be tailored to the customers' needs.
- The HP CSA lifecycle framework and resource utilization features ease the complexity of mapping your cloud fulfillment infrastructure into reusable, automated Resource Offerings for on-time and on-budget delivery.

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.

Access and usage of CSA is mainly divided between two portals: the Cloud Service Management Console (SMC) and the Market Place Portal (MPP). Also, the product's users are divided into two groups: consumers and administrators. SMC is a web-based user interface that provides access to the provider side of the product. SMC is used by the product administrators to manage various features and functionalities of CSA and its offerings. Based on an administrator's role, it allows them to manage cloud resources, services, Organizations, and Subscriptions. MPP is also a web-based user interface that provides access to the consumer side of the product. The consumers consist of subscribers and approvers. A subscriber is a consumer that has selected a Service Offering from the catalog, received approval for the requested Service Offering, and is actively receiving the service based on the Service Offering ordered. An approver is a consumer with the right to allow or deny other consumers' requests for resources as defined in the approval process. Consumers use the MPP to browse catalogs, subscribe to services, view Subscriptions, and approve/deny subscription requests. Both sides of the product are illustrated in Figure 1 below.

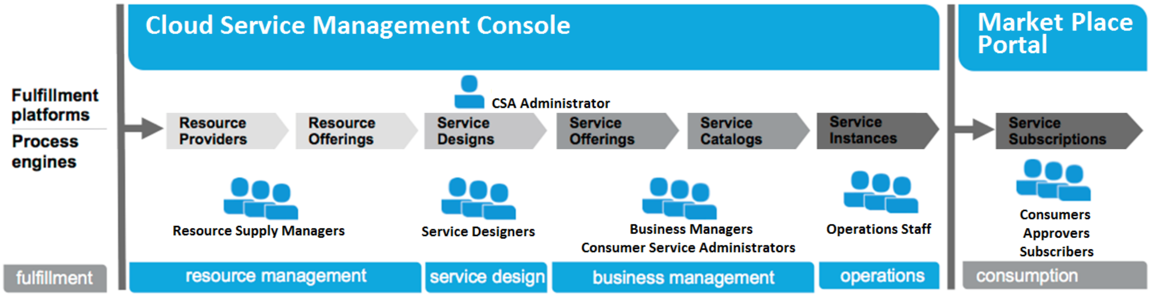

**Figure 1 CSA Workflow**

[1] FIPS – Federal Information Processing Standard
[2] RSA – Rivest, Shamir, Adleman

SMC provides administrators with access to the following features of CSA: resource management, service design, business management, and operations. These features are explained below:

- Resource Management – Administrators with resource management privileges create and manage cloud resources, such as Resource Providers and Resource Offerings. A Resource Provider is an Artifact[3] that encapsulates all of the information HP CSA needs to interact with each public and private cloud provider. Once the Resource Providers have been specified, the Resource Offerings specify the actions required to manage a resource throughout the entire service lifecycle.
- Service Design – Administrators with service designer privileges collaborate to create Service Designs that call upon the Resource Providers and Resource Offerings. Service Designs represent the initial configuration for a Service Instance. Service Designs provide a structure for options or profiles that consumers can select when ordering a service. A service component represents one Service Design element required to realize a Subscription. The service components consist of Component Palettes, Component Types, and Component Templates. The Component Palettes are the grouping structure for component types. A Component Type is a hierarchical classification of service components containing rules that constrain how Service Designs are constructed. A Component Template is a specialized version of a Component Type and is used to simplify Service Design creation.
- Business Management – Once a Service Design is available, a Service Offering is created by an administrator with Service Business Manager privileges. Service Offerings encapsulate all the information that consumers need to select the most appropriate services that fit their needs. Each Service Offering references a Service Design for definition of its service options and components. In the Service Catalogs, the Service Offerings are associated with specific groups of consumers along with the approval processes. The Service Catalogs are used by the consumers to view Service Offerings available to their Organization. An Organization determines a member's entry point into the cloud system and associates its members with services and resources. An Organization may be a company, business unit, department, or group.
- Operations – Once a consumer subscribes to a Service Offering, a Service Instance is constructed as part of the service deployment. Service Instances encapsulate all the details of the deployed service and its components, for example, provisioned Internet Protocol (IP) details for a network segment component. Administrators with Service Operation Manager privileges have access to monitor and manage service Subscriptions and Service Instances for the consumer Organizations.
- Consumption – Before the Service Instance is made, a consumer must create a Subscription to a Service Offering. Subscriptions are used by consumers to request new cloud services and track existing cloud services. If the approval process is applied to a Service Offering, a second consumer would be responsible for approving or denying the Subscription to allow the allocation of network resources.

CSA also supports a Representational State Transfer (REST) Application Programming Interface (API) that can be used by the consumers and administrators to interact programmatically with the product to perform various functions from both portals. Consumer and administrator accounts are verified before they are allowed access to CSA when using REST API calls. There are separate REST API calls that consumers and administrators execute based on their roles and privileges.

The product has the flexibility to balance services across all resources at its disposal and determine which resources best match the consumers' needs based on factors such as: Geographic location, other resources used by that consumer, and utilize new resources without requiring service designers to redesign their service templates.

CSA integrates process engines such as HP Operations Orchestration (OO) and HP Continuous Delivery Automation for runbook automation in order to support dozens of fulfillment platforms such as HP Matrix, HP Server Automation (SA), and VMware vCenter.

[3] Artifact – An HP CSA model object that contains the necessary information to create and manage top-level model elements and their relationships.

# 1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the TOE, describing the TOE environment, describing the TOE minimum requirements, and providing a deployment configuration.

The TOE is a distributed software application running from two separate environments: the Java Runtime Environment (JRE), used for SMC, and NodeJS[4], used for MPP. The portals are designed to allow separate servers to run each portal, while allowing them to communicate securely. In the CC-evaluated configuration, both portals run on the same server. Consumers and administrators, also known as TOE users, access MPP and SMC respectively over HTTPS[5] using a supported web browser from their workstation. The TOE also includes the functionality and features described in section 1.5 below, except for the features and functionality listed below in section 1.5.3. A graphic depicting a typical deployment configuration of the TOE is provided in Figure 2 below. The following previously undefined acronyms are used in Figure 2:

- IdM – Identity Management
- LDAP – Lightweight Directory Access Protocol
- SQL – Structured Query Language
- WAR – Web Application Archive

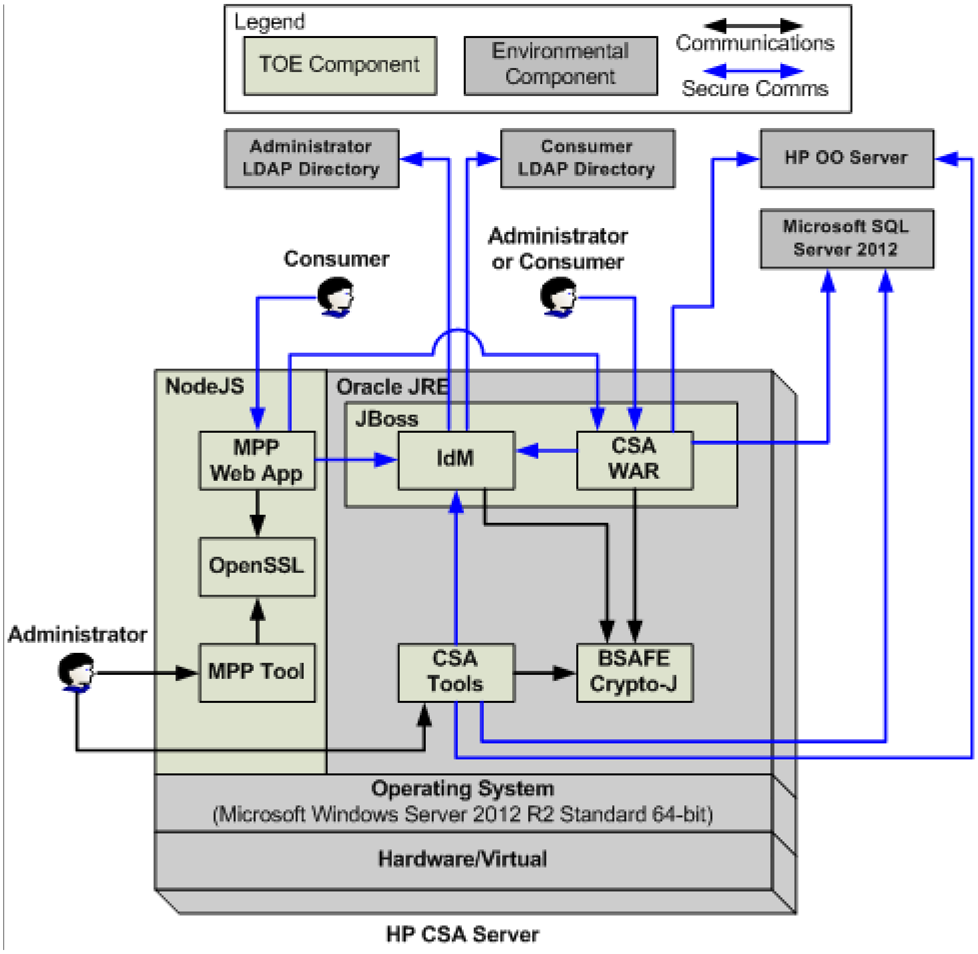

**Figure 2 A Typical Deployment Configuration of the TOE**

[4] NodeJS – Node JavaScript
[5] HTTPS – Hypertext Transport Protocol Secure

## 1.4.1 TOE Components

The TOE is comprised of the components described in the sections below. All TOE components are depicted in Figure 3 below.

### 1.4.1.1 MPP Web App

The MPP Web App component houses the portal used by Service Consumers to request and manage the service to which they subscribe. The portal can be used to request cloud services for themselves or on behalf of others. When requests are made, approvers use the portal to approve or deny the requests for services.

### 1.4.1.2 OpenSSL

The OpenSSL component is the OpenSSL FIPS Object Module v2.0. This module is used to provide FIPS-Approved cryptographic services for secure communications between Service Consumers and MPP.

### 1.4.1.3 MPP Tool

The MPP Tool is the Password Util Tool for MPP, a JavaScript-based CLI[6] tool. It is used to encrypt an integrated MPP account password and output the encrypted text.

### 1.4.1.4 IdM

IdM works within the HP CSA JRE and communicates with the MPP Web App and the CSA WAR through HTTPS to provide authentication services.

### 1.4.1.5 CSA Tools

The CSA Tools are comprised of several different Java-based CLI tools that are used to manage various parts of the TOE. Below is the list of all the tools:

- **Content Archive Tool** – Used for exporting and importing Artifacts to and from CSA archive files. The following Artifacts are supported in CSA Artifact archives: Component Palettes, Resource Offerings, Service Designs, Service Offerings, Resource Environments, and Service Catalogs. The Content Archive Tool communicates securely with the Database (DB) server.
- **DB Purge Tool** – Used to permanently purge Subscriptions that are no longer in use, and all their related data, as to free up additional DB space. Also used to delete audit event records from the DB. Requires authentication, and only users with CSA Administrator role are permitted to use it. The DB Purge Tool communicates securely with the DB server.
- **Process Definition Tool (PDT)** – Used for importing HP OO flow signature-related information into the CSA DB so that this information is stored locally. The PDT communicates securely with HP OO and the DB server.
- **Provider Configuration Tool** – A command line tool used for the management of service providers. It can read or view a list of providers, create new providers, update existing providers, and delete providers. The Provider Configuration Tool communicates securely with the DB server.
- **Password Util Tool for CSA** – Used to encrypt an integrated CSA account password and output the encrypted text.

### 1.4.1.6 CSA WAR

The CSA WAR component houses the SMC, used for the management of CSA. It is used by CSA administrators to perform the following tasks based on their role:

- Assign role to group membership or organizational unit (OU)
- Configure and manage consumer and provider Organizations
- Create and manage cloud resources, such as providers and Resource Offerings
- Create and manage the Service Offerings and Service Catalogs

[6] CLI – Command Line Interface

- Design, implement, and maintain Service Designs, Component Palettes, Component Types, and Component Templates
- View and manage Subscriptions and Service Instances

### 1.4.1.7 BSAFE Crypto-J

The BSAFE Crypto-J component provides FIPS-Approved cryptography for the JRE with the RSA BSAFE Crypto-J Cryptographic Module v6.1. This module provides secure communications between the TOE and the administrators, between various parts of the TOE, and TOE communications with the TOE environmental components.

## 1.4.2 TOE Environment

Cloud Service Automation v4.10 is executed in two parts: as a WAR file in a JBoss[7] application server container running in a JRE and as a web application inside a NodeJS environment. The evaluated configuration of the TOE is evaluated on a server with the Microsoft Windows Server 2012 R2 Standard 64-bit Operating System (OS).

A CSA deployment relies on a Relational Database Management System (RDBMS) in the IT[8] environment to house the CSA DB used to store audit logs and Subscription data. CSA dictates how the data is divided into database tables. A separate DB server needs to be installed in the TOE environment for communication with the TOE. The evaluated configuration of the TOE is evaluated with the Microsoft SQL Server 2012 DB server.

In this configuration, a supported version of JRE and JBoss are installed on the CSA server. The evaluated configuration of the TOE is evaluated with Oracle JRE 7 and JBoss Application Server 7.1.1 Community.

One LDAP server, with two separate LDAP directories, is configured in the TOE environment for user authentication using LDAPv3. A separate server configured with HP OO v10.10 (or higher) is setup in the TOE environment for orchestration where workflows are implemented as instructed by CSA. The HP OO server must be configured to integrate with HP CSA as per the HP CSA 4.10 – Installation Guide. The Microsoft SQL Server software will be installed on a separate server in the TOE environment. The DB, LDAP, and HP OO servers must be able to communicate with the TOE over TLS[9] 1.0. Another requirement of the TOE environment is a reliable time stamp. The server's OS, on which the TOE is -installed, provides reliable system time for the TOE.

Table 2 below specifies the minimum system requirements for proper operation of the TOE.

**Table 2 TOE Evaluated Configuration**

| Name | Description |
|---|---|
| **Hardware Requirements for the TOE Server** | |
| CPU[10] | 4 CPUs at 3.0 GHz[11] |
| RAM[12] | 8 GB[13] |
| Hard Drive | 20 GB |
| **Software Requirements for the TOE Server** | |
| OS Version | Microsoft Windows Server 2012 R2 Standard 64-bit |
| Middleware | JBoss Application Server 7.1.1 Community |

[7] JBoss – JavaBeans Open Source Software
[8] IT – Information Technology
[9] TLS – Transport Layer Security
[10] CPU – Central Processing Unit
[11] GHz – Gigahertz
[12] RAM – Random Access Memory
[13] GB – Gigabyte

| Name | Description |
|---|---|
| | Microsoft Visual C++ 2010 Redistributable Package (x86) |
| | Oracle JRE 7 |
| | JCE Unlimited Strength Jurisdiction Policy Files 7 |
| **TOE Environment Requirements** | |
| DB Server | Microsoft SQL Server 2012 |
| LDAP Server | LDAPv3 |
| HP OO Server | HP Operations Orchestration v10.10 or higher |
| **Requirements for Client Workstations** | |
| Browsers | Microsoft Internet Explorer 9 or higher<br>Google Chrome 28 or higher<br>Mozilla Firefox 24 or higher |
| Flash | Used with SMC only: Adobe Flash Player 12 or higher |
| | Adobe Flash Player plug-in required for Internet Explorer |

# 1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

## 1.5.1 Physical Scope

Figure 3 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE used in this evaluation.

The TOE is a software-only solution designed to help cloud service providers by automating their ability to broker cloud services to their consumers. The deployment configuration runs the minimum hardware and software listed in Table 2. The DB server will be setup with a version of Microsoft SQL listed in Table 2 and installed on a separate machine in the TOE environment. Two LDAP directories are setup on one LDAP server in the TOE environment to keep administrator and consumer accounts separate. In addition, the TOE environment will contain a separate server running HP OO. The TOE must have network access to the LDAP server, DB server, and HP OO server. The administrators and consumers that interface with the server must have a system that can run the minimum browser, listed in Table 2, and a network connection that is allowed to communicate with CSA.

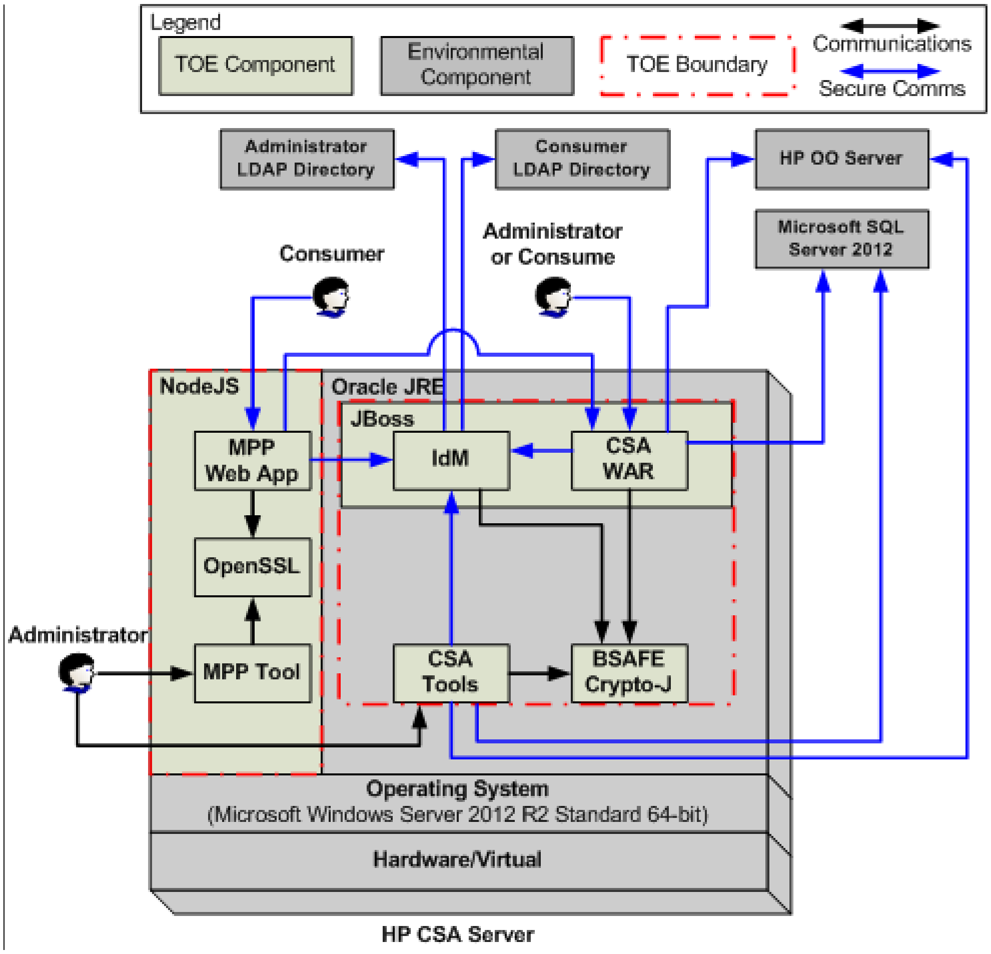

**Figure 3 Physical TOE Boundary**

### 1.5.1.1 TOE Software

The TOE is a software-only solution, for orchestrating the deployment of compute and infrastructure resources and of complex multi-tier application architectures, consisting of the components illustrated in Figure 3. All together, this software is Cloud Service Automation v4.10.

### 1.5.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- HP CSA 4.10 – API Quick Start
- HP CSA 4.10 – API Reference
- HP CSA 4.10 – Content Archive Tool
- HP CSA 4.10 – Concepts Guide
- HP CSA 4.10 – Configuration Guide (Windows)
- HP CSA 4.10 – FIPS 140-2 Compliance Statement
- HP CSA 4.10 – Installation Guide
- HP CSA 4.10 – Integration Pack
- HP CSA 4.10 – Marketplace Portal Help
- HP CSA 4.10 – Open Source and Third-Party Software License Agreements
- HP CSA 4.10 – Provider Configuration Tool
- 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
- HP CSA 4.10 – Upgrade Guide
- HP CSA 4.10 – What's New in Cloud Service Automation 4.10

## 1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF[14]
- TOE Access
- Trusted Path/Channels

### 1.5.2.1 Security Audit

The TOE generates audit records for event types such as Authentication, Create/Update/Delete, and Server Management. The operation type is also captured for each record before being written to the audit log. For the Authentication event type, the Login operation type is captured. For the Create/Update/Delete event type, the Create, Update, and Delete operation types are captured for all Artifacts and Service Offering price. For the Server Management event type, the Start and Stop operation types of the CSA server are captured. When a user generates an audit event, their user ID[15] is associated with the record before being written to the log. The audit log is stored on the DB server.

### 1.5.2.2 Cryptographic Support

The TOE utilizes two FIPS-Approved cryptographic modules for securing communications between its users, components, and the TOE environment. NodeJS contains OpenSSL FIPS Object Module, Version 2.0.7. The JRE uses RSA BSAFE Crypto-J JSAFE and JCE Software Module, Version 6.1. Both modules use FIPS-Approved cryptographic algorithms to perform all cryptographic operations. The TOE generates cryptographic keys to be used with encryption, decryption, keyed hash, and signature operations. Specifics of the cryptographic operations are listed in Table 11 below, including their key sizes and CAVP[16] certificate numbers.

The TOE uses both cryptographic modules to destroy all ephemeral keying material generated. This is accomplished by using FIPS-Approved zeroization methods specified in the security policy document of the cryptographic modules.

### 1.5.2.3 User Data Protection

The TOE provides user data protection by enforcing the CSA access control SFP[17] on the following objects: Resource Offerings, Component Palettes, Component Types, Component Templates, Service Designs, Service Offerings, Service Catalogs, and Subscriptions. The CSA access control SFP limits each user's access based on their LDAP group membership or OU, which is associated to a role within the TOE. A user can have multiple roles by adding that user to multiple corresponding LDAP groups. The

[14] TSF – TOE Security Functionality
[15] ID – Identification
[16] CAVP – Cryptographic Algorithm Validation Program
[17] SFP – Security Functional Policy

operations that can be performed on various objects in the TOE are listed in Table 12. Table 12 also specifies all operations that can be performed by a specified subject on the respective object.

Based on an administrator's role, they have the ability to import or export Resource Offerings, Component Palettes, Service Designs, Service Offerings, and Service Catalogs to and from the TOE. The data will be exported from the TOE without any security attributes associated to it and will ignore any security attributes when importing data from outside the TOE. Any data that is imported into the TOE is required to be contained within a .zip file.

#### 1.5.2.4 Identification and Authentication

The TOE uses an LDAP server with two LDAP directories for user authentication after the initial setup. The TOE maintains the list of security attributes for a user and relies on the LDAP server to maintain the values of the security attributes. The list of security attributes are the associations to LDAP attributes, i.e. the fields for username and group membership. Within each Organization in CSA, the fields of user email, group membership, manager identifier, manager identifier value, and user avatar are specified to be an LDAP attribute.

The TOE will allow the use of the following CLI tools without identification or authentication of a valid user account: Content Archive Tool, Process Definition Tool, Provider Configuration Tool, Password Util Tool for CSA, and Password Util Tool for MPP. These tools are stored locally on the server and require server access before allowing them to be used locally without identification or authentication. The TOE will require all other TSF-mediated actions to be identified and authenticated with a valid LDAP user account.

When a user authenticates to the SMC UI[18] or MPP UI, the TOE will obscure the password feedback with a bullet (•) in place of each character. When a user authenticates through the DB Purge Tool, the TOE will not display any characters while the password is typed.

#### 1.5.2.5 Security Management

The TOE is capable of providing security management functions for the access control associations, LDAP server connection settings, and LDAP user attribute associations. The TOE will restrict access to these security functions to the Consumer Service Administrator, and CSA Administrator roles. These security functions associate a security attribute field in CSA to an LDAP attribute. The individual values are managed by the LDAP server.

After the initial setup of the TOE, the CSA access control SFP will be enforced to provide restrictive default values for the security attributes of new Organizations. The default value for these fields are blank, causing them to be disabled, and will not allow access until they are set.

The TOE will restrict a user's ability to manage TSF data on the following objects: Access control values, LDAP server connections values, LDAP user attribute values, Organizations, Resource Providers, and the CSA DB. Access to manage these objects is based on the administrator's role. All of these objects can be managed by the CSA Administrator. The TOE allows the consumers to approve or deny Subscription requests to Service Offerings when that consumer is part of the Service Offering's approval process. It also allows the administrators to manage the following:

- Access control associations between the TOE and LDAP
- LDAP server connection settings
- TOE to LDAP user attribute associations
- Organizations' settings
- Resource Provider details
- Purging of the CSA DB's old Subscriptions and audit logs

[18] UI – User Interface

There are two sets of roles within the TOE. There are six administrative roles that can access the TOE functionality via SMC: CSA Administrators, Consumer Service Administrator, Resource Supply Manager, Service Business Manager, Service Designer, and Service Operations Manager. There is only one role that can access the TOE functionality via MPP, Service Consumer. These roles are maintained by the TOE and cannot be modified, created, or deleted. All users of the TOE will be associated to at least one of these roles. The role to user association is based on their LDAP group membership or OU, and it is maintained by the TOE.

#### 1.5.2.6 Protection of the TSF

With the use of the two cryptographic modules, one in NodeJS and the other in the JRE, the TOE will protect all TSF data that is transmitted from the MPP Web App component to the IdM component, the MPP Web App component to the CSA WAR component, the CSA Tools to the IdM component, and the CSA WAR to the IdM component. The secure communications are made during a TLS 1.0 session. Therefore, the TOE protects data transmitted between the different parts of the TOE. In Figure 3 above displays the various secure connections used by the TOE to protect its data in-transit.

#### 1.5.2.7 TOE Access

The TOE allows administrators that have management access to Organizations, to configure an access banner for consumer Organizations accessed through the MPP. This feature is not available to the provider Organization. This banner can be configured with a security classification and a disclaimer of use. Also, each consumer Organization may be configured with their own banner. Consumers must click on the "Proceed" button before being granted access to the login fields.

#### 1.5.2.8 Trusted Path/Channels

The TOE provides a trusted channel between itself and the LDAP server, DB server, and HP OO server by making secure connections over TLS 1.0. Only the TOE is allowed to initiate these secure channel communications. The TOE will use an LDAPS[19] connection over TLS 1.0 for communications with the LDAP server during user authentication. An HTTPS connection will be used when the TOE makes DB transactions, purges the DB, uses HP OO for orchestration, and when a system administrator uses the PDT, Content Archive Tool, or Provider Configuration Tool.

A consumer or administrator can initiate a secure connection to the TOE over an HTTPS connection for using the REST API, MPP, and SMC. The HTTPS connection uses TLS 1.0 to protect data communications from modification or disclosure, and ensures end point identification. An HTTPS connection is required for use of all TSF management functions.

### 1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

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

- HP Single Sign-On
- High Availability configuration
- User authentication using Common Access Cards or Personal Identification Verification cards

[19] LDAPS – Lightweight Directory Access Protocol Secure

# 2 Conformance Claims

This section and Table 3 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

**Table 3 CC and PP Conformance**

| | |
|---|---|
| **CC Identification and Conformance** | Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4, September 2012; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM[20] as of 2014/10/06 were reviewed, and no interpretations apply to the claims made in this ST. |
| **PP Identification** | None |
| **Evaluation Assurance Level** | EAL2+ augmented with Flaw Remediation (ALC_FLR.2) |

[20] CEM – Common Evaluation Methodology

# 3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

## 3.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 4 below lists the applicable threats.

**Table 4 Threats**

| Name | Description |
|---|---|
| T.ADMIN_ERROR | An administrator may incorrectly configure the TOE resulting in ineffective security mechanisms. |
| T.MASQUERADE | A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources. |
| T.NACCESS | A non-TOE user may be able to view or modify data that is transmitted between parts of the TOE or between the TOE and a remote authorized external entity. |
| T.TAMPERING | A non-TOE user may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment. |
| T.UNAUTH | An unauthorized person may gain access to the TOE and compromise its security functions by changing its configuration. |

## 3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs for this ST.

## 3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 5 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

**Table 5 Assumptions**

| Name | Description |
|---|---|
| A.ATTRIBUTES | The TOE environment will be able to maintain user security attributes when the TOE is configured to use external authentication. |
| A.INSTALL | The TOE is installed on the appropriate, dedicated hardware, OS, and runtime environment. |
| A.LOCATE | The TOE is located within a controlled access facility. |
| A.MANAGE | There are one or more competent individuals assigned to manage the TOE and the security of the information it contains. |
| A.NETCON | The TOE environment provides the network connectivity required to allow the TOE to provide secure routing and switching functions. |
| A.NOEVIL | The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance. |
| A.PROTECT | The TOE software will be protected from unauthorized modification. |
| A.TIMESTAMP | The TOE environment provides the TOE with the necessary reliable timestamps. |

# 4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

## 4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 6 below.

**Table 6 Security Objectives for the TOE**

| Name | Description |
|---|---|
| O.ADMIN | The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control. |
| O.AUDIT | The TOE will provide the capability to detect security relevant events and record them to the audit trail. |
| O.AUTHENTICATE | The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data. |
| O.BANNER | The TOE client will display an advisory warning regarding use of the TOE. |
| O.CRYPTO | The TOE will provide FIPS-Approved cryptographic algorithms and procedures to TOE users during operation of the TOE. |
| O.PROTECT | The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data. |
| O.PROTECT_COMM | The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities. |
| O.ROLE | The TOE must be able to associate users and Administrators with an appropriate role after the user or Administrator authenticates. |

## 4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

### 4.2.1 IT Security Objectives

Table 7 below lists the IT security objectives that are to be satisfied by the environment.

**Table 7 IT Security Objectives**

| Name | Description |
|---|---|
| OE.ATTRIBUTES | The IT environment must be able to maintain user security attributes when the TOE is configured to use external authentication. |
| OE.PLATFORM | The TOE hardware and OS must support all required TOE functions. |

| Name | Description |
|---|---|
| OE.SECURE_COMM | The TOE Environment must provide a mechanism to provide a secure and authorized user access to the TOE environment for protecting the TOE and TOE data from modification. |
| OE.TIME | The underlying OS must provide reliable timestamps to the TOE. |
| OE.TRAFFIC | The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function. |

### 4.2.2 Non-IT Security Objectives

Table 8 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

**Table 8 Non-IT Security Objectives**

| Name | Description |
|---|---|
| NOE.MANAGE | Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. |
| NOE.PHYSICAL | The physical environment must be suitable for supporting a computing device in a secure setting. |

# 5 Extended Components

There are no extended SFRs and extended SARs for this TOE.

# 6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

## 6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

## 6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

**Table 9 TOE Security Functional Requirements**

| Name | Description | S | A | R | I |
|---|---|---|---|---|---|
| FAU_GEN.1 | Audit Data Generation | ✓ | ✓ | | |
| FAU_GEN.2 | User Identity Association | | | | |
| FCS_CKM.1 | Cryptographic key generation | | ✓ | | |
| FCS_CKM.4 | Cryptographic key destruction | | ✓ | | |
| FCS_COP.1 | Cryptographic operation | | ✓ | | |
| FDP_ACC.1 | Subset access control | | ✓ | | |
| FDP_ACF.1 | Security attribute based access control | | ✓ | | |
| FDP_ETC.1 | Export of user data without security attributes | | ✓ | | |
| FDP_ITC.1 | Import of user data without security attributes | | ✓ | | |
| FIA_ATD.1 | User attribute definition | | ✓ | | |
| FIA_UAU.1 | Timing of authentication | | ✓ | | |
| FIA_UAU.7 | Protected authentication feedback | | ✓ | | |
| FIA_UID.1 | Timing of identification | | ✓ | | |

| Name | Description | S | A | R | I |
|---|---|---|---|---|---|
| FMT_MOF.1 | Management of security functions behavior | ✓ | ✓ | | |
| FMT_MSA.1 | Management of security attributes | ✓ | ✓ | | |
| FMT_MSA.3 | Static Attribute Initialization | ✓ | ✓ | | |
| FMT_MTD.1 | Management of TSF data | ✓ | ✓ | | |
| FMT_SMF.1 | Specification of management functions | | ✓ | | |
| FMT_SMR.1 | Security roles | | ✓ | | |
| FPT_ITT.1 | Basic internal TSF data transfer protection | ✓ | | | |
| FTA_TAB.1 | Default TOE access banners | | | | |
| FTP_ITC.1 | Inter-TSF trusted channel | ✓ | ✓ | | |
| FTP_TRP.1 | Trusted path | ✓ | ✓ | | |

*Note: S=Selection; A=Assignment; R=Refinement; I=Iteration*

## 6.2.1 Class FAU: Security Audit

**FAU_GEN.1 Audit Data Generation**
**Hierarchical to: No other components.**
**Dependencies: FPT_STM.1 Reliable time stamps**

***FAU_GEN.1.1***

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events, for the [not specified] level of audit; and
c) [*other specifically defined auditable events listed in Table 10*]

***FAU_GEN.1.2***

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*the Operation Type listed in Table 10*].

**Table 10 Auditable Events**

| Event Type | Operation Type | Other Information |
|---|---|---|
| Authentication | Login | For successful or unsuccessful user authentication into the TOE. |
| Create/Update/Delete | Create<br>Update<br>Delete | Every time an Artifact is created, updated or deleted.<br>Any change in a Service Offering price. |
| Server Management | Start<br>Stop | The start and stop of the CSA server. |

**FAU_GEN.2 User identity association**
**Hierarchical to: No other components.**
**Dependencies: FAU_GEN.1 Audit data generation**
**FIA_UID.1 Timing of identification**

***FAU_GEN.2.1***

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

### 6.2.2 Class FCS: Cryptographic Support

**FCS_CKM.1 Cryptographic key generation**
**Hierarchical to: No other components.**
**Dependencies: FCS_COP.1 Cryptographic operation**
**FCS_CKM.4 Cryptographic key destruction**

***FCS_CKM.1.1***

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*listed in Table 11*] and specified cryptographic key sizes [*listed in Table 11*] that meet the following: [*list of standards in Table 11*].

**FCS_CKM.4 Cryptographic key destruction**
**Hierarchical to: No other components.**
**Dependencies: FCS_CKM.1 Cryptographic key generation**

***FCS_CKM.4.1***

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 zeroization requirements*].

**FCS_COP.1 Cryptographic operation**
**Hierarchical to: No other components.**
**Dependencies: FCS_CKM.1 Cryptographic key generation**
**FCS_CKM.4 Cryptographic key destruction**

***FCS_COP.1.1***

The TSF shall perform [*the list of cryptographic operations in Table 11*] in accordance with a specified cryptographic algorithm [*listed in Table 11*] and cryptographic key sizes [*listed in Table 11*] that meet the following: [*list of standards in Table 11*].

**Table 11 Cryptographic Operations**

| Cryptographic Operations | Cryptographic Algorithm | Key Size (bits) | Standards (Certificate #) |
|---|---|---|---|
| **For RSA BSAFE Crypto-J JSAFE and JCE Software Module, Software Version 6.1** | | | |
| Symmetric Encryption and Decryption | AES[21] in ECB[22], CBC[23], CFB[24], OFB[25], CTR[26], CCM[27], GCM[28], XTS[29] | 128, 192, 256 | FIPS 197 (Certificate #2249) |
| Message Digest | SHA[30] -256 | N/A[31] | FIPS 180-3 (Certificate # 1938) |
| Message Authentication | HMAC[32]-SHA-256 | 256 | FIPS 198 (Certificate #1378) |

[21] AES – Advanced Encryption Standard
[22] ECB – Electronic Codebook
[23] CBC – Cipher Block Chaining
[24] CFB – Cipher Feedback
[25] OFB – Output Feedback
[26] CTR – Counter Mode
[27] CCM – Counter with CBC-MAC
[28] GCM – Galois Counter Mode
[29] XTS – XEX-based Tweaked-codebook mode with cipher text Stealing
[30] SHA – Secure Hash Algorithm
[31] N/A – Not Applicable
[32] HMAC – Hash-based Message Authentication Code

| Cryptographic Operations | Cryptographic Algorithm | Key Size (bits) | Standards (Certificate #) |
|---|---|---|---|
| Key Generation | RSA GenKey9.31 | 2048, 3072 | FIPS 186-2 (Certificate #1154) |
| Signature Generation | SigGen9.31, SigGenPKCS[33]1.5, SigGenPSS[34] | 2048, 3072 | FIPS 186-2 (Certificate #1154) |
| Signature Verification | SigVer9.31, SigVerPKCS1.5, SigVerPSS | 2048, 3072 | FIPS 186-2 (Certificate #1154) |
| Random Number Generation | HMAC DRBG[35] | N/A | SP[36] 800-90A (Certificate #273) |
| **For OpenSSL FIPS Object Module, Software Version v2.0.7** | | | |
| Symmetric Encryption and Decryption | AES in ECB, CBC, CFB, CTR, OFB, XTS, CMAC[37], CCM, GCM | 256 | FIPS 197 (Certificate #2824) |
| Message Digest | SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 | N/A | FIPS 180-3 (Certificate #2368) |
| Message Authentication | HMAC-SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 | 160, 224, 256, 384, 512 | FIPS 198 (Certificate #1768) |
| Key Generation | RSA GenKey9.31 | 2048, 3072, 4096 | FIPS 186-2 (Certificate #1477) |
| Signature Generation | SigGen9.31, SigGenPKCS1.5, SigGenPSS | 2048, 3072, 4096 | FIPS 186-2 (Certificate #1477) |
| Signature Verification | SigVer9.31, SigVerPKCS1.5, SigVerPSS | 2048, 3072, 4096 | FIPS 186-2 (Certificate #1477) |
| Random Number Generation | HMAC DRBG | N/A | SP800-90A (Certificate #485) |

[33] PKCS – Public-Key Cryptography Standards

[34] PSS – Probabilistic Signature Scheme

[35] DRBG – Deterministic Random Bit Generator

[36] SP – Special Publication

[37] CMAC – Cipher-based MAC

## 6.2.3 Class FDP: User Data Protection

**FDP_ACC.1 Subset access control**
**Hierarchical to: No other components.**
**Dependencies: FDP_ACF.1 Security attribute based access control**

***FDP_ACC.1.1***

The TSF shall enforce the [*CSA access control SFP*] on [

- ***Subjects**: CSA Administrators, Resource Supply Manager, Service Business Manager, Service Designer, Service Operations Manager, Service Consumer*
- ***Objects**: Listed in Table 12*
- ***Operations among subjects and objects covered by the SFP**: Listed in Table 12*].

**Table 12 CSA Objects and Operations**

| Object | All Operations | Subjects |
|---|---|---|
| Resource Offerings | Manage, view, create, import, export, or delete | Resource Supply Manager, CSA Administrator |
| Component Palettes | View, create, edit, import, export, or delete | Service Designer, CSA Administrator |
| Component Types | View, create, edit, or delete | Service Designer, CSA Administrator |
| Component Templates | View, create, edit, or delete | Service Designer, CSA Administrator |
| Service Designs | View, create, copy, import, export, or delete | Service Designer, CSA Administrator |
| Service Offerings | View, create, edit, import, export, or delete | Service Business Manager, CSA Administrator |
| Service Catalogs | View, create, edit, import, export, or delete | Service Business Manager, CSA Administrator |
| Subscriptions | Manage, or view | Service Operations Manager, CSA Administrator |
| Subscriptions | Manage, view, create, or edit | Service Consumer |

**FDP_ACF.1 Security attribute based access control**
**Hierarchical to: No other components.**
**Dependencies: FDP_ACC.1 Subset access control**
**FMT_MSA.3 Static attribute initialization**

***FDP_ACF.1.1***

The TSF shall enforce the [*CSA access control SFP*] to objects based on the following: [

- ***Subjects**: CSA Administrators, Resource Supply Manager, Service Business Manager, Service Designer, Service Operations Manager, Service Consumer*
- ***Objects**: Resource Offerings, Component Palettes, Component Types, Component Templates, Service Designs, Service Offerings, Service Catalogs, and Subscriptions*
- ***Security Attributes**: LDAP group membership or OU*].

***FDP_ACF.1.2***

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*A subject is granted access to perform an operation on an object based on the associated LDAP group or OU with a role within the TOE*].

***FDP_ACF.1.3***

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*none*].

***FDP_ACF.1.4***

The TSF shall explicitly deny access of subjects to objects based on the [*none*].

### FDP_ETC.1 Export of user data without security attributes

**Hierarchical to: No other components.**

**Dependencies: FDP_ACC.1 Subset access control**

***FDP_ETC.1.1***

The TSF shall enforce the [*CSA access control SFP*] when exporting user data, controlled under the SFP(s), outside of the TOE.

***FDP_ETC.1.2***

The TSF shall export the user data without the user data's associated security attributes.

*Application note: The purpose of claiming FDP_ETC.1 and FDP_ITC.1 is for the CSA administrators to provide stable and tested Artifacts to be used in a production environment. This is accomplished when an Artifact is developed in a development environment and tested for use before being deployed in a secure and trusted production environment.*

### FDP_ITC.1 Import of user data without security attributes

**Hierarchical to: No other components.**

**Dependencies: FDP_ACC.1 Subset access control**
**FMT_MSA.3 Static attribute initialization**

***FDP_ITC.1.1***

The TSF shall enforce the [*CSA access control SFP*] when importing user data, controlled under the SFP, from outside of the TOE.

***FDP_ITC.1.2***

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

***FDP_ITC.1.3***

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*The data must be contained within a .zip file before it is imported into the TOE.*].

*Application note: The purpose of claiming FDP_ETC.1 and FDP_ITC.1 is for the CSA administrators to provide stable and tested Artifacts to be used in a production environment. This is accomplished when an Artifact is developed in a development environment and tested for use before being deployed in a secure and trusted production environment.*

### 6.2.4 Class FIA: Identification and Authentication

**FIA_ATD.1 User attribute definition**
**Hierarchical to: No other components.**
**Dependencies: No dependencies**
***FIA_ATD.1.1***

The TSF shall maintain the following list of security attributes belonging to individual users: [

- *User ID*
- *User email*
- *Manager identifier*
- *Manager identifier value*
- *Group membership*
- *User avatar*].

*Application note: The TOE uses LDAP for user authentication after the initial setup, and relies on LDAP to provide and maintain the values for this list of security attributes. The TOE will maintain the list and the associations between CSA fields and LDAP attributes, which will be used to fill in the TOE user's attributes.*

**FIA_UAU.1 Timing of authentication**
**Hierarchical to: No other components.**
**Dependencies: FIA_UID.1 Timing of identification**
***FIA_UAU.1.1***

The TSF shall allow [*the use of the following CLI tools:*

- *Content Archive Tool*
- *Process Definition Tool*
- *Provider Configuration Tool*
- *Password Util Tool for CSA*
- *Password Util Tool for MPP*]

on behalf of the user to be performed before the user is authenticated.

***FIA_UAU.1.2***

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

**FIA_UAU.7 Protected authentication feedback**
**Hierarchical to: No other components.**
**Dependencies: FIA_UAU.1 Timing of authentication**
***FIA_UAU.7.1***

The TSF shall provide only [*an obscured password with a bullet (•) in place of each character when accessing the MPPUI or SMC UI; no visual text when typing a password in the DB Purge Tool*] to the user while the authentication is in progress.

**FIA_UID.1 Timing of identification**
**Hierarchical to: No other components.**
**Dependencies: No dependencies**
***FIA_UID.1.1***

The TSF shall allow [*the use of the following CLI tools:*

- *Content Archive Tool*
- *Process Definition Tool*
- *Provider Configuration Tool*
- *Password Util Tool for CSA*
- *Password Util Tool for MPP*]

on behalf of the user to be performed before the user is identified.

***FIA_UID.1.2***

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

## 6.2.5 Class FMT: Security Management

### FMT_MOF.1 Management of security functions behavior

**Hierarchical to:** **No other components.**
**Dependencies:** **FMT_SMF.1 Specification of management functions**
**FMT_SMR.1 Security roles**

***FMT_MOF.1.1***

The TSF shall restrict the ability to [enable, disable, modify the behavior of] the functions [*listed in Table 13*] to [*the roles listed in Table 13*].

*Application note: The TOE uses LDAP for user authentication and by default all fields are empty, disabling the function. They are enabled by adding a valid entry, and behavior is modified by changing to a different valid entry. The functions can be disabled again by removing the entries.*

**Table 13 Management of Security Functions**

| Security Function | Role |
|---|---|
| Access Control | Consumer Service Administrator, CSA Administrator |
| LDAP Server Connection | |
| LDAP User Attribute | |

### FMT_MSA.1 Management of security attributes

**Hierarchical to:** **No other components.**
**Dependencies:** **FDP_ACC.1 Subset access control**
**FMT_SMF.1 Specification of management functions**
**FMT_SMR.1 Security roles**

***FMT_MSA.1.1***

The TSF shall enforce the [*CSA access control SFP*] to restrict the ability to [modify, delete, [*view*]] the security attributes [

- *Access Control: Group Name, Group or OU DN*[38]
- *LDAP Server Connection: Hostname, Port, Connection Security, Base DN*
- *LDAP User Attributes: User ID, User Email, Group Membership, Manager Identifier, Manager Identifier Value, User Avatar*]

to [*Consumer Service Administrator and CSA Administrator*].

*Application note: For security attributes, the TOE provides the ability to modify, delete, or view the security attributes' association from the attribute field in CSA to the LDAP attribute. The individual values for these attributes are managed by the LDAP server.*

### FMT_MSA.3 Static attribute initialization

**Hierarchical to:** **No other components.**
**Dependencies:** **FMT_MSA.1 Management of security attributes**
**FMT_SMR.1 Security roles**

***FMT_MSA.3.1***

The TSF shall enforce the [*CSA access control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

***FMT_MSA.3.2***

The TSF shall allow the [*Consumer Service Administrator, CSA Administrator*] to specify alternative initial values to override the default values when an object or information is created.

[38] DN – Distinguished Name

### FMT_MTD.1 Management of TSF data

**Hierarchical to: No other components.**
**Dependencies: FMT_SMF.1 Specification of management functions**
**FMT_SMR.1 Security roles**

***FMT_MTD.1.1***

The TSF shall restrict the ability to [*<u>the operations listed in Table 14</u>*] the [*objects listed in Table 14*] to [*the subjects listed in Table 14*].

**Table 14 CSA Objects and Operations Management**

| Object | All Operations | Subjects |
|---|---|---|
| Access Control Values | View, edit, or clear | Consumer Service Administrator, CSA Administrator |
| LDAP Server Connections Values | View, edit, or clear | Consumer Service Administrator, CSA Administrator |
| LDAP User Attribute Values | View, edit, or clear | Consumer Service Administrator, CSA Administrator |
| Organizations | Manage, view, create, or edit | Consumer Service Administrator, CSA Administrator |
| Resource Provider | Manage, view, create, or edit | Resource Supply Manager, CSA Administrator |
| CSA DB | Purge Subscriptions and audit logs | CSA Administrator |

### FMT_SMF.1 Specification of Management Functions

**Hierarchical to: No other components.**
**Dependencies: No Dependencies**

***FMT_SMF.1.1***

The TSF shall be capable of performing the following management functions: [

- *Manage the access control associations between the TOE and LDAP*
- *Manage the LDAP server connection settings*
- *Manage the TOE to LDAP user attribute associations*
- *Manage the Organizations' settings in the SMC*
- *Manage the Resource Provider details in the SMC*
- *Purge the CSA DB of old Subscriptions and audit logs*
- *Approve or deny Subscription requests*].

### FMT_SMR.1 Security roles

**Hierarchical to: No other components.**
**Dependencies: FIA_UID.1 Timing of identification**

***FMT_SMR.1.1***

The TSF shall maintain the roles [*CSA Administrators, Consumer Service Administrator, Resource Supply Manager, Service Business Manager, Service Designer, Service Operations Manager, and Service Consumer*].

***FMT_SMR.1.2***

The TSF shall be able to associate users with roles.

### 6.2.6 Class FPT: Protection of the TSF

**FPT_ITT.1 Basic internal TSF data transfer protection**
**Hierarchical to: No other components.**
**Dependencies: No dependencies**
***FPT_ITT.1.1***

The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

### 6.2.7 Class FTA: TOE Access

**FTA_TAB.1 Default TOE access banners**
**Hierarchical to: No other components.**
**Dependencies: No dependencies**

***FTA_TAB.1.1***

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

### 6.2.8 Class FTP: Trusted Path/Channels

**FTP_ITC.1 Inter-TSF trusted channel**
**Hierarchical to: No other components.**
**Dependencies: No dependencies**

***FTP_ITC.1.1***

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

***FTP_ITC.1.2***

The TSF shall permit [the TSF] to initiate communication via the trusted channel.

***FTP_ITC.1.3***

The TSF shall initiate communication via the trusted channel for [*DB transactions, purging the DB, authentication, use of the PDT, use of the Content Archive Tool, use of the Provider Configuration Tool, and orchestration*].

*Application note: Orchestration is the deployment of compute and infrastructure resources. It is initiated when a Subscription from the TOE is approved. The TOE will then send the workflow instructions to HP OO to coordinate the fulfillment of the Subscription.*

**FTP_TRP.1 Trusted path**
**Hierarchical to: No other components.**
**Dependencies: No dependencies**

***FTP_TRP.1.1***

The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure, [and *no other types of integrity or confidentiality violation*]].

***FTP_TRP.1.2***

The TSF shall permit [remote users] to initiate communication via the trusted path.

***FTP_TRP.1.3***

The TSF shall require the use of the trusted path for [initial user authentication, [*importing/exporting user data, and all TSF management functions performed via the MPP UI and SMC UI*]].

## 6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 15 summarizes the requirements.

**Table 15 Assurance Requirements**

| Assurance Requirements | |
|---|---|
| Class ASE: Security Target Evaluation | ASE_CCL.1 Conformance Claims |
| | ASE_ECD.1 Extended Components Definition |
| | ASE_INT.1 ST Introduction |
| | ASE_OBJ.2 Security Objectives |
| | ASE_REQ.2 Derived Security Requirements |
| | ASE_SPD.1 Security Problem Definition |
| | ASE_TSS.1 TOE Summary Specification |
| Class ALC : Life Cycle Support | ALC_CMC.2 Use of a CM System |
| | ALC_CMS.2 Parts of the TOE CM Coverage |
| | ALC_DEL.1 Delivery Procedures |
| | ALC_FLR.2 Flaw Reporting Procedures |
| Class ADV: Development | ADV_ARC.1 Security Architecture Description |
| | ADV_FSP.2 Security-Enforcing Functional Specification |
| | ADV_TDS.1 Basic Design |
| Class AGD: Guidance Documents | AGD_OPE.1 Operational User Guidance |
| | AGD_PRE.1 Preparative Procedures |
| Class ATE: Tests | ATE_COV.1Evidence of Coverage |
| | ATE_FUN.1 Functional Testing |
| | ATE_IND.2 Independent Testing – Sample |
| Class AVA: Vulnerability Assessment | AVA_VAN.2 Vulnerability Analysis |

# 7 TOE Security Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

## 7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 16 lists the security functionality and their associated SFRs.

**Table 16 Mapping of TOE Security Functionality to Security Functional Requirements**

| TOE Security Functionality | SFR ID | Description |
|---|---|---|
| Security Audit | FAU_GEN.1 | Audit Data Generation |
| | FAU_GEN.2 | User Identity Association |
| Cryptographic Support | FCS_CKM.1 | Cryptographic key generation |
| | FCS_CKM.4 | Cryptographic key destruction |
| | FCS_COP.1 | Cryptographic operation |
| User Data Protection | FDP_ACC.1 | Subset access control |
| | FDP_ACF.1 | Security attribute based access control |
| | FDP_ETC.1 | Export of user data without security attributes |
| | FDP_ITC.1 | Import of user data without security attributes |
| Identification and Authentication | FIA_ATD.1 | User attribute definition |
| | FIA_UAU.1 | Timing of authentication |
| | FIA_UAU.7 | Protected authentication feedback |
| | FIA_UID.1 | Timing of identification |
| Security Management | FMT_MOF.1 | Management of security functions behavior |
| | FMT_MSA.1 | Management of security attributes |
| | FMT_MSA.3 | Static Attribute Initialization |
| | FMT_MTD.1 | Management of TSF data |
| | FMT_SMF.1 | Specification of management functions |
| | FMT_SMR.1 | Security roles |
| Protection of TOE Security Functions | FPT_ITT.1 | Basic internal TSF data transfer protection |
| TOE Access | FTA_TAB.1 | Default TOE access banners |
| Trusted Path/Channels | FTP_ITC.1 | Inter-TSF trusted channel |
| | FTP_TRP.1 | Trusted path |

## 7.1.1 Security Audit

The TOE generates security events that are captured in an audit log. This audit log is stored on the DB server. The TOE captures information on the event types such as Authentication, Create/Update/Delete, and Server Management. The operation type is included with each record that is generated. For the Authentication event type, the Login operation type is captured. In the case of the Authentication event type with the operation type as Login, the TOE captures all successful and unsuccessful user authentications to the TOE. Users accessing the TOE using the DB Purge tool are authenticated users and an audit log is generated with Login as operation type. For Create/Update/Delete event type, the Create, Update, and Delete operation types are captured for Artifacts and Service Offering price. For the Server Management event type, the Start and Stop operation type of the CSA server is captured. When an event is generated by a TOE user, the TOE will associate that record to their user ID before writing it to the audit log. The TOE audit records contain the following information:

**Table 17 Audit Record Contents**

| Field | Content |
|---|---|
| UUID[39] | Universally unique identifier for each record |
| CREATED_ON | Date and time (yyyy-mm-dd hh:mm:ss.fff) when the event occurred. |
| MODIFIED_BY_USERNAME | User's logon name associated to the record |
| MODIFIED_BY_USER_ID | A unique ID associated to each user |
| USER_ORGANIZATION_ID | A unique ID associated to each Organization |
| USER_ORGANIZATION_NAME | The display name of an Organization |
| ARTIFACT_ID | A unique ID associated to each Artifact |
| ARTIFACT_NAME | A name associated to each Artifact |
| ARTIFACT_TYPE | The type of each Artifact, i.e. Group or Organization |
| AUDIT_CLASSIFICATION | The classification of the audit record, i.e. Authentication or Server Management |
| AUDIT_OPERATION | The operation that took place on the Artifact |
| ORIGINATING_SERVER | The name of the server where from user logged in |
| SERVER_TYPE | The type of server that the operation originated from, i.e. CSA or IdM |
| DESCRIPTION | Information on the operation and its success or failure |

**TOE Security Functional Requirements Satisfied:** FAU_GEN.1, FAU_GEN.2

## 7.1.2 Cryptographic Support

The TOE utilizes two FIPS-Approved cryptographic modules, RSA BSAFE Crypto-J JSAFE and JCE Software Module, Software Version 6.1 in the JRE, and OpenSSL FIPS Object Module, Software Version v2.0 in NodeJS. Both of these modules use FIPS-Approved cryptographic algorithms to perform all cryptographic operations. The TOE generates cryptographic keys to be used with encryption, decryption, keyed hash, and signature operations. The TOE uses the cryptographic algorithms when using TLS 1.0 to establish secure communications over HTTPS connection between the following:

[39] UUID – Universally Unique Identifier

- The consumers accessing the TOE via REST APIs and MPP
- The administrators accessing the TOE via REST APIs and SMC
- The MPP Web App communicating with the IdM
- The CSA WAR communicating with the IdM
- The CSA Tools communicating with the IdM
- The MPP Web App communicating with the CSA WAR
- The TOE communicating with the DB server
- The TOE communicating with the HP OO server

TLS 1.0 is also used for securing communications to the LDAP server over LDAPS.

The TOE is responsible for destroying all ephemeral keying material generated within the TOE boundary. The TOE uses the FIPS-Approved zeroization methods from both modules in order to destroy all keys and other critical parameters generated by the TOE at the appropriate time.

Each of the cryptographic algorithms supported by the TOE have been tested and validated by the CAVP[40]. The certificate number for each algorithm is listed in Table 11, under the “Standards (Certificate #)” column. Also in Table 11, each algorithm is listed with their cryptographic operation and key sizes.

**TOE Security Functional Requirements Satisfied:** FCS_CKM.1, FCS_CKM.4, FCS_COP.1

### 7.1.3 User Data Protection

The TOE provides user data protection by enforcing the CSA access control SFP on the following objects: Resource Offerings, Component Palettes, Component Types, Component Templates, Service Designs, Service Offerings, Service Catalogs, and Subscriptions. The CSA access control SFP limits each user’s access based on their LDAP group membership or OU. The LDAP group membership or OU is associated to a role within the TOE. The roles that have access to these objects are limited to the CSA Administrators, Resource Supply Manager, Service Business Manager, Service Designer, Service Operations Manager, and Service Consumer. Each role has different level of access to the CSA objects, as shown in Table 12. The operations that can be performed on each object are also listed in Table 12. Roles cannot be modified, deleted, or created. A user can have multiple roles by adding the user to multiple LDAP groups that are associated to the roles in CSA.

Based on an administrator’s role, they have the ability to import or export different sets of data to and from the TOE. The following Artifacts may be imported and exported: Resource Offerings, Resource Environments, Component Palettes, Service Designs, Service Offerings, and Service Catalogs. The data is exported from the TOE without any security attributes associated to it and will ignore any security attributes when the data is imported from outside the TOE. Any data that is imported into the TOE must be contained within a .zip file. The purpose of importing and exporting Artifacts is that the CSA administrators can provide stable and tested Artifacts to be used in a production environment. The following are user objects that can be exported or imported:

- Resource Offerings – By the Resource Supply Manager and CSA Administrator
- Component Palettes – By the Service Designer and CSA Administrator
- Service Designs – By the Service Designer and CSA Administrator
- Service Offerings – By the Service Business Manager and CSA Administrator
- Service Catalogs – By the Service Business Manager and CSA Administrator

**TOE Security Functional Requirements Satisfied:** FDP_ACC.1, FDP_ACF.1, FDP_ETC.1, FDP_ITC.1

[40] CAVP – Cryptographic Algorithm Validation Program

## 7.1.4 Identification and Authentication

The TOE uses LDAP for user authentication after initial setup. The TOE maintains the list of security attributes for a user and relies on LDAP to provide and maintain the values for following list of security attributes:

- User ID
- User email
- Manager identifier
- Manager identifier value
- Group membership
- User avatar

Within each Organization in CSA, the TOE will maintain the associations between CSA fields and LDAP attributes, which will be used to fill in the TOE user's attributes.

The TOE will allow the use of the following CLI tools without identification or authentication of a valid user account:

- Content Archive Tool
- Process Definition Tool
- Provider Configuration Tool
- Password Util Tool for CSA
- Password Util Tool for MPP

A description of what these tools do is provided in section 1.4.1.5 above. These tools are stored locally on the server and require server access before allowing them to be used locally without identification or authentication. The TOE will require all other TSF-mediated actions to be identified and authenticated with a valid LDAP user account.

When a user authenticates to MPP UI and SMC UI, the TOE will obscure the password with a bullet (•) in place of each character. When a user authenticates through the DB Purge Tool, the TOE will not display any characters while the password is typed. This protects the password feedback from threats while authentication takes place.

**TOE Security Functional Requirements Satisfied:** FIA_ATD.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1

## 7.1.5 Security Management

The TOE is capable of providing security management functions for the access control associations, LDAP server connection settings, and LDAP user attribute associations. The TOE will restrict the ability to enable, disable, or modify the behavior of these security functions to the Consumer Service Administrator, and CSA Administrator roles. All of these fields are empty by default and need to be filled in during the initial setup to enable them, otherwise these functions remain disabled. These values can be modified later by changing to a different valid entry value. The functions can be disabled again by removing the entry value.

The attribute associations that may be modified, deleted, or viewed by the Consumer Service Administrator and CSA Administrator are controlled by the CSA access control SFP. These associations are made from CSA fields to LDAP attributes and the LDAP server manages the individual values. For the access control, the Consumer Service Administrator and CSA Administrator will have access to the Group Name, and Group or OU DN. For the LDAP server connection, the Consumer Service Administrator and CSA Administrator will have access to the Hostname, Port, Connection Security, and Base DN fields. For the LDAP user attributes, the Consumer Service Administrator and CSA Administrator will have access to the User ID, User Email, Group Membership, Manager Identifier, Manager Identifier Value, and User Avatar fields.

After the initial setup of the TOE, the CSA access control SFP will be enforced to provide restrictive default values for the security attributes of new Organizations. The default value for the fields listed in the paragraph above are blank, causing them to be disabled, and will not allow access until they are set. Only the Consumer Service Administrator and CSA Administrator will have access to set these values.

The TOE will restrict the ability to manage TSF data on the following objects: Access control values, LDAP server connections values, LDAP user attribute values, Organizations, Resource Providers, and the CSA DB. All of these objects can be managed by the CSA Administrator. The Consumer Service Administrator can manage all except the Resource Providers and the CSA DB. Those are managed by the Resource Supply Manager and CSA Administrator respectively.

The TOE allows the consumers to approve or deny Subscription requests to Service Offerings when that consumer is part of the Service Offering's approval process. It also allows the administrators to manage the following:

- Access control associations between the TOE and LDAP
- LDAP server connection settings
- TOE to LDAP user attribute associations
- Organizations' settings in the SMC
- Resource Provider details in the SMC
- Purging of the CSA DB's old Subscriptions and audit logs

There are two sets of roles within the TOE. The SMC has six roles: CSA Administrators, Consumer Service Administrator, Resource Supply Manager, Service Business Manager, Service Designer, and Service Operations Manager. The MPP has one role, Service Consumer. These roles are maintained by the TOE and cannot be modified, created, or deleted. All users of the TOE will be associated to one of these roles. The role to user association is based on their LDAP group membership or OU. These roles are described below:

- **CSA Administrator** – This role has access to all features and functionalities available via the SMC interface. A CSA Administrator initially configures authentication and assigns members to roles granting authorization to use the SMC.
- **Consumer Service Administrator** – The Consumer Service Administrator configures and manages consumer and provider Organizations.
- **Resource Supply Manager** – The Resource Supply Manager creates and manages cloud resources, such as providers and Resource Offerings.
- **Service Business Manager** – The Service Business Manager creates and manages the Service Offerings and Service Catalogs.
- **Service Designer** – The Service Designer designs, implements, and maintains Service Designs (also referred to as blueprints), Component Palettes, Component Types, and Component Templates.
- **Service Operations Manager** – The Service Operations Manager views and manages Subscriptions and Service Instances.
- **Service Consumer** – The Service Consumer requests and manages Subscriptions offered to their Organization through the MPP UI.

**TOE Security Functional Requirements Satisfied:** FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

### 7.1.6 Protection of the TSF

With the use of the two cryptographic modules, one in NodeJS and the other in the JRE, the TOE will protect all TSF data that is transmitted from the MPP Web App component to the IdM component, the MPP Web App component to the CSA WAR component, the CSA Tools to the IdM component, and the CSA WAR to the IdM component. The TOE will use the TLS 1.0 connection to protect passwords and the data related to the objects listed in Table 14 from disclosure or modification. Therefore, the TOE protects data transmitted between the different parts of the TOE.

**TOE Security Functional Requirements Satisfied:** FPT_ITT.1

### 7.1.7 TOE Access

The TOE allows administrators, which have management access to Organizations, to configure an access banner for only consumer Organizations accessed through the MPP. This banner can be configured with a security classification and a disclaimer of use. The security classification can be set to the following values:

- Unclassified
- Unclassified FOUO[41]
- Unclassified NOFORN[42]
- Confidential
- Confidential FOUO
- Confidential NOFORN
- Secret
- Top Secret

The security classification cannot be renamed or deleted, and new classifications cannot be added. Each consumer Organization may be configured with their own banner. Consumers must click on the "Proceed" button before being granted access to the login fields.

**TOE Security Functional Requirements Satisfied:** FTA_TAB.1

### 7.1.8 Trusted Path/Channels

The TOE provides a trusted channel between itself and the LDAP server, DB server, and HP OO server. The TOE makes these secure connections over TLS 1.0. Only the TOE is allowed to initiate these secure channel communications. The TOE will use an LDAPS connection over TLS 1.0 for communications with the LDAP server during user authentication. An HTTPS connection is used when the TOE makes DB transactions, purges the DB, uses the PDT, uses the Content Archive Tool, uses the Provider Configuration Tool, and uses HP OO for orchestration. Orchestration takes place when a Subscription from the TOE is approved and the TOE then integrates with HP OO to deploy infrastructure resources. The TOE will use a REST API in HP OO to send the workflow on a secure channel.

Using a supported browser and Flash version, both listed in Table 2 above, a remote user initiates a secure connection to the TOE. The secure path is established using HTTPS for the REST API, MPP, and SMC. The HTTPS connection uses TLS 1.0 to protect data communications from modification or disclosure, and ensures end point identification. An HTTPS connection is required for authentication, importing/exporting user data, and all TSF management functions performed via the MPP UI and SMC UI.

**TOE Security Functional Requirements Satisfied:** FTP_ITC.1, FTP_TRP.1

[41] FOUO – For Official Use Only

[42] NOFORN – No Foreign Nationals

# 8 Rationale

## 8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Release 4.

## 8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

### 8.2.1 Security Objectives Rationale Relating to Threats

Table 18 below provides a mapping of the objects to the threats they counter.

**Table 18 Threats: Objectives Mapping**

| Threats | Objectives | Rationale |
|---|---|---|
| T.ADMIN_ERROR<br>An administrator may incorrectly configure the TOE resulting in ineffective security mechanisms. | NOE.MANAGE<br>Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. | NOE.MANAGE mitigates this threat by ensuring that all administrators are properly trained and follow TOE guidance. |
| | O.ADMIN<br>The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control. | O.ADMIN mitigates this threat by ensuring the TOE provides management functions and restricts these functions to TOE users with appropriate privileges. |
| T.MASQUERADE<br>A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources. | O.AUTHENTICATE<br>The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data. | By ensuring that The TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data, O.AUTHENTICATE counters this threat. |
| | O.BANNER<br>The TOE client will display an advisory warning regarding use of the TOE. | O.BANNER satisfies this threat by presenting a warning banner to users about unauthorized use of the TOE prior to logging in. |

| Threats | Objectives | Rationale |
|---|---|---|
| | O.ROLE<br>The TOE must be able to associate users and Administrators with an appropriate role after the user or Administrator authenticates. | O.ROLE counters this threat by ensuring that the TOE is able to associate users with roles according to their LDAP group membership or OU. |
| T.NACCESS<br>A non-TOE user may be able to view or modify data that is transmitted between parts of the TOE or between the TOE and a remote authorized external entity. | O.CRYPTO<br>The TOE will provide FIPS-Approved cryptographic algorithms and procedures to TOE users during operation of the TOE. | The objective O.CRYPTO ensures that TSF data transmitted over the network is encrypted and protected from modification and disclosure. |
| | O.PROTECT_COMM<br>The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities. | The objective O.PROTECT_COMM ensures that TSF data transmitted over the network is kept secure from modification and disclosure. |
| T.TAMPERING<br>A non-TOE user may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment. | O.ADMIN<br>The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control. | O.ADMIN supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms. |
| | NOE.PHYSICAL<br>The physical environment must be suitable for supporting a computing device in a secure setting. | NOE.PHYSICAL ensures that the TOE and TOE environment are protected from external interference or tampering. |
| | O.AUDIT<br>The TOE will provide the capability to detect security relevant events and record them to the audit trail. | The objective O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE are recorded. |
| | O.PROTECT<br>The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data. | O.PROTECT mitigates this threat by providing mechanisms to protect the TOE data from unauthorized modification. |

| Threats | Objectives | Rationale |
|---|---|---|
| T.UNAUTH<br>An unauthorized person may gain access to the TOE and compromise its security functions by changing its configuration. | O.ADMIN<br>The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control. | The objective O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE. |
| | O.AUDIT<br>The TOE will provide the capability to detect security relevant events and record them to the audit trail. | The objective O.AUDIT ensures that unauthorized attempts to access the TOE are recorded. |
| | O.AUTHENTICATE<br>The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data. | The objective O.AUTHENTICATE ensures that users are identified and authenticated prior to gaining access to TOE security data. |

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

### 8.2.2 Security Objectives Rationale Relating to Policies

There are no OSPs for this ST.

### 8.2.3 Security Objectives Rationale Relating to Assumptions

Table 19 below gives a mapping of assumptions and the environmental objectives that uphold them.

**Table 19 Assumptions: Objectives Mapping**

| Assumptions | Objectives | Rationale |
|---|---|---|
| A.ATTRIBUTES<br>The TOE environment will be able to maintain user security attributes when the TOE is configured to use external authentication. | OE.ATTRIBUTES<br>The IT environment must be able to maintain user security attributes when the TOE is configured to use external authentication. | OE.ATTRIBUTES upholds this assumption by ensuring that the TOE user security attributes are securely maintained by the external IT environment when the TOE is configured to use external authentication. |
| A.INSTALL<br>The TOE is installed on the appropriate, dedicated hardware, OS, and runtime environment. | NOE.MANAGE<br>Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. | NOE.MANAGE satisfies this assumption by ensuring TOE Administrators follow and apply all configuration guidance. |

| Assumptions | Objectives | Rationale |
|---|---|---|
| | OE.PLATFORM<br>The TOE hardware and OS must support all required TOE functions. | OE.PLATFORM upholds this assumption by ensuring that the TOE hardware meets minimum requirements and the OS supports all the TOE functions. |
| A.LOCATE<br>The TOE is located within a controlled access facility. | NOE.PHYSICAL<br>The physical environment must be suitable for supporting a computing device in a secure setting. | NOE.PHYSICAL upholds this assumption by ensuring that the TOE environment provides protection against physical attacks. |
| A.MANAGE<br>There are one or more competent individuals assigned to manage the TOE and the security of the information it contains. | NOE.MANAGE<br>Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. | NOE.MANAGE upholds this assumption by ensuring that those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use. |
| A.NETCON<br>The TOE environment provides the network connectivity required to allow the TOE to provide secure routing and switching functions. | OE.TRAFFIC<br>The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function. | OE.TRAFFIC upholds this assumption by ensuring that the TOE environment provides the appropriate network connectivity required for performance with a proper implementation of the TOE. |
| A.NOEVIL<br>The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance. | NOE.MANAGE<br>Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. | NOE.MANAGE upholds this assumption by ensuring that all administrators assigned to manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all administrator guidance. |
| A.PROTECT<br>The TOE software will be protected from unauthorized modification. | OE.SECURE_COMM<br>The TOE Environment must provide a mechanism to provide a secure and authorized user access to the TOE environment for protecting the TOE and TOE data from modification. | OE.SECURE_COMM upholds this assumption by ensuring that the TOE environment provides a secure and authorized access to its users for protect the data from external interference or tampering. |
| A.TIMESTAMP<br>The TOE environment provides the TOE with the necessary reliable timestamps. | OE.TIME<br>The underlying OS must provide reliable timestamps to the TOE. | OE.TIME upholds this assumption by ensuring that the operating system where the TOE is installed will provide reliable time stamps for the TOE. |

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

## 8.3 Rationale for Extended Security Functional Requirements

There are no extended functional requirements defined for this TOE.

## 8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended functional requirements defined for this TOE.

## 8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

### 8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 20 below shows a mapping of the objectives and the SFRs that support them.

**Table 20 Objectives: SFRs Mapping**

| Objective | Requirements Addressing the Objective | Rationale |
|---|---|---|
| O.ADMIN<br>The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control. | FMT_MOF.1<br>Management of security functions behavior | The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges. |
| | FMT_MSA.1<br>Management of security attributes | The requirement meets the objective by restricting the ability to perform actions on security attributes to specific users. |
| | FMT_MSA.3<br>Static Attribute Initialization | The requirement meets the objective by providing authorized users the ability to change default security attribute values. |
| | FMT_MTD.1<br>Management of TSF data | The requirement meets the objective by ensuring that the TOE restricts access to TSF data based on the user's role. |
| | FMT_SMF.1<br>Specification of management functions | The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF. |
| | FMT_SMR.1<br>Security roles | The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data. |
| O.AUDIT<br>The TOE will provide the capability to detect security relevant events and record | FAU_GEN.1<br>Audit Data Generation | The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event. |

| Objective | Requirements Addressing the Objective | Rationale |
|---|---|---|
| them to the audit trail. | FAU_GEN.2<br>User Identity Association | The requirement meets this objective by ensuring that the TOE associates a user to each auditable event, with which the user caused. |
| O.AUTHENTICATE<br>The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data. | FIA_UAU.1<br>Timing of authentication | The requirement meets the objective by ensuring that users are authenticated before access to TOE administrative functions is allowed. |
| | FIA_UID.1<br>Timing of identification | The requirement meets the objective by ensuring that users are identified before access to TOE administrative functions is allowed. |
| O.BANNER<br>The TOE client will display an advisory warning regarding use of the TOE. | FTA_TAB.1<br>Default TOE access banners | The requirement meets the objective by ensuring that a banner is displayed to users prior to identification and authentication. |
| O.CRYPTO<br>The TOE will provide FIPS-Approved cryptographic algorithms and procedures to TOE users during operation of the TOE. | FCS_CKM.1<br>Cryptographic key generation | The requirement meets the objective by ensuring that the TOE can generate FIPS-Approved cryptographic keys for use during cryptographic operations. |
| | FCS_CKM.4<br>Cryptographic key destruction | The requirement meets the objective by ensuring that the TOE destroys cryptographic keys when no longer in use using FIPS-Approved methods. |
| | FCS_COP.1<br>Cryptographic operation | The requirement meets the objective by ensuring that the TOE provides FIPS-Approved confidentiality and integrity services for the TOE. |
| O.PROTECT<br>The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data. | FDP_ACC.1<br>Subset access control | The requirement meets the objective by requiring the TOE to enforce access control based on the CSA access control SFP on users connecting to the TOE. |
| | FDP_ACF.1<br>Security attribute based access control | The requirement meets the objective by ensuring that the TOE enforces access control based on the CSA access control SFP. |
| | FDP_ETC.1<br>Export of user data without security attributes | The requirement meets the objective by requiring the TOE to enforce access control based on the CSA access control SFP on users connecting to the TOE. |
| | FDP_ITC.1<br>Import of user data without security attributes | The requirement meets the objective by requiring the TOE to enforce access control based on the CSA access control SFP on users connecting to the TOE. |

| Objective | Requirements Addressing the Objective | Rationale |
|---|---|---|
| | FIA_UAU.1<br>Timing of authentication | The requirement meets the objective by ensuring that only authenticated users are allowed access to TOE functions. |
| | FIA_UAU.7<br>Protected authentication feedback | The requirement meets the objective by preventing password material from being obtained from an unauthorized person by obscuring the password. |
| | FIA_UID.1<br>Timing of identification | The requirement meets the objective by ensuring that only identified users are allowed access to TOE functions. |
| | FMT_MOF.1<br>Management of security functions behavior | The requirement meets the objective by ensuring that only privileged users may manage the security behavior of the TOE. |
| | FMT_MSA.1<br>Management of security attributes | The requirement meets the objective by ensuring that only privileged users have access to security attributes. |
| | FMT_MSA.3<br>Static Attribute Initialization | The requirement meets the objective by enforcing restrictive default values for security attributes that are only accessible by privileged users. |
| | FMT_MTD.1<br>Management of TSF data | The requirement meets the objective by ensuring that only privileged users have access to manage TSF data. |
| | FTA_TAB.1<br>Default TOE access banners | The requirement meets the objective by presenting an advisory access banner to users prior to authentication. |
| O.PROTECT_COMM<br>The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities. | FCS_CKM.1<br>Cryptographic key generation | This requirement supports the objective by providing secure keys for use in the network protocols used to protect transmitted TSF data. |
| | FCS_COP.1<br>Cryptographic operation | This requirement meets the objective by providing algorithms for cryptographic operations used to encrypt and decrypt TSF data when sent over the network. |
| | FPT_ITT.1<br>Basic internal TSF data transfer protection | The requirement meets the objective by protecting data being transferred between TOE components from disclosure and modification. |
| | FTP_ITC.1<br>Inter-TSF trusted channel | The requirement meets the objective by providing a secure and trusted communications channel between all trusted IT products and the TOE. |
| | FTP_TRP.1<br>Trusted path | This requirement meets the objective by ensuring that TOE users have a trusted path for communications with the TOE. |

| Objective | Requirements Addressing the Objective | Rationale |
|---|---|---|
| O.ROLE<br>The TOE must be able to associate users and Administrators with an appropriate role after the user or Administrator authenticates. | FIA_ATD.1<br>User attribute definition | The requirement meets the objective by requiring the TOE to maintain a list of roles and their associated LDAP group memberships or OU's. |
| | FMT_SMR.1<br>Security roles | The requirement meets the objective by requiring the TOE to be able to associate user roles with their respective users. |

## 8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment. The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

## 8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 21 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

**Table 21 Functional Requirements Dependencies**

| SFR ID | Dependencies | Dependency Met | Rationale |
|---|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | ✓ | A.TIMESTAMP upholds this dependency by assuming that the OS, where the TOE is installed, will provide reliable time stamps for the TOE. |
| FAU_GEN.2 | FAU_GEN.1 | ✓ | |
| | FIA_UID.1 | ✓ | |
| FCS_CKM.1 | FCS_COP.1 | ✓ | |
| | FCS_CKM.4 | ✓ | |
| FCS_CKM.4 | FCS_CKM.1 | ✓ | |
| FCS_COP.1 | FCS_CKM.1 | ✓ | |
| | FCS_CKM.4 | ✓ | |
| FDP_ACC.1 | FDP_ACF.1 | ✓ | |
| FDP_ACF.1 | FMT_MSA.3 | ✓ | |
| | FDP_ACC.1 | ✓ | |
| FDP_ETC.1 | FDP_ACC.1 | ✓ | |

| SFR ID | Dependencies | Dependency Met | Rationale |
|---|---|---|---|
| FDP_ITC.1 | FMT_MSA.3 | ✓ | |
| | FDP_ACC.1 | ✓ | |
| FIA_ATD.1 | No dependencies | ✓ | |
| FIA_UAU.1 | FIA_UID.1 | ✓ | |
| FIA_UAU.7 | FIA_UAU.1 | ✓ | |
| FIA_UID.1 | No dependencies | ✓ | |
| FMT_MOF.1 | FMT_SMF.1 | ✓ | |
| | FMT_SMR.1 | ✓ | |
| FMT_MSA.1 | FMT_SMR.1 | ✓ | |
| | FMT_SMF.1 | ✓ | |
| | FDP_ACC.1 | ✓ | |
| FMT_MSA.3 | FMT_MSA.1 | ✓ | |
| | FMT_SMR.1 | ✓ | |
| FMT_MTD.1 | FMT_SMR.1 | ✓ | |
| | FMT_SMF.1 | ✓ | |
| FMT_SMF.1 | No dependencies | ✓ | |
| FMT_SMR.1 | FIA_UID.1 | ✓ | |
| FPT_ITT.1 | No dependencies | ✓ | |
| FTA_TAB.1 | No dependencies | ✓ | |
| FTP_ITC.1 | No dependencies | ✓ | |
| FTP_TRP.1 | No dependencies | ✓ | |

# 9 Acronyms

This section and Table 22 define the acronyms and terms used throughout this document.

## 9.1 Acronyms and Terms

**Table 22 Acronyms and Terms**

| Acronym | Definition |
|---|---|
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |
| CAVP | Cryptographic Algorithm Validation Program |
| CBC | Cipher Block Chaining |
| CC | Common Criteria |
| CCEF | Common Criteria Evaluation Facility |
| CCM | Counter with CBC-MAC |
| CEM | Common Evaluation Methodology |
| CFB | Cipher Feedback |
| CLI | Command Line Interface |
| CMAC | Cipher-based MAC |
| CPU | Central Processing Unit |
| CSA | Cloud Service Automation |
| CTR | Counter Mode |
| DB | Database |
| DN | Distinguished Name |
| DRBG | Deterministic Random Bit Generator |
| EAL | Evaluation Assurance Level |
| ECB | Electronic Codebook |
| FIPS | Federal Information Processing Standard |
| FOUO | For Official Use Only |
| GB | Gigabyte |
| GCM | Galois Counter Mode |
| GHz | Gigahertz |
| HMAC | Hash-based Message Authentication Code |
| HTML | HyperText Markup Language |
| HTTPS | Hypertext Transport Protocol Secure |
| ID | Identification |

| Acronym | Definition |
|---|---|
| IdM | Identity Management |
| IP | Internet Protocol |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| IT | Information Technology |
| JBoss | JavaBeans Open Source Software |
| JCE | Java Cryptography Extension |
| JRE | Java Runtime Environment |
| LDAP | Lightweight Directory Access Protocol |
| LDAPS | Lightweight Directory Access Protocol Secure |
| MPP | Marketplace Portal |
| NodeJS | Node JavaScript |
| NOFORN | No Foreign Nationals |
| OFB | Output Feedback |
| OO | Operations Orchestration |
| OS | Operating System |
| OSP | Organizational Security Policy |
| OU | Organizational Unit |
| PDT | Process Definition Tool |
| PKCS | Public-Key Cryptography Standards |
| PP | Protection Profile |
| PSS | Probabilistic Signature Scheme |
| RAM | Random Access Memory |
| RDBMS | Relational DB Management System |
| RSA | Rivest, Shamir, Adleman |
| REST | Representational State Transfer |
| SA | Server Automation |
| SAR | Security Assurance Requirement |
| SFP | Security Functional Policy |
| SFR | Security Functional Requirement |
| SMC | CSA Management Console |
| SP | Service Pack |
| SP | Special Publication |

| Acronym | Definition |
|---|---|
| SQL | Structured Query Language |
| SSA | Signature Scheme with Appendix |
| ST | Security Target |
| TLS | Transport Layer Security |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |
| UI | User Interface |
| UUID | Universally Unique Identifier |
| WAR | Web Application Archive |
| XTS | XEX-based Tweaked-codebook mode with cipher text Stealing |

Prepared by:
**Corsec Security, Inc.**

13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com