BlackBerry SecuSUITE Server Version 6.0 Security Target

Version 0.7
1/23/26

Prepared for:
BlackBerry Ltd.

Prepared By:

www.gossamersec.com

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is SecuSUITE Server provided by BlackBerry Ltd. The TOE is being evaluated as an Enterprise Session Controller.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In this ST, iteration may be indicated by a parenthetical number placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement. Alternately, a usually descriptive textual extension may be added after a slash (/) character to identify a specific iteration. For example, iterations of a requirement such as FCS_COP.1 might be identified as FCS_COP.1/HASH and FCS_COP.1/CRYPT.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – BlackBerry SecuSUITE Server Version 6.0 Security Target

ST Version – Version 0.7

ST Date – 1/23/26

1.2 TOE Reference

TOE Identification – BlackBerry SecuSUITE Server Version 6.0

TOE Developer – BlackBerry Ltd

Evaluation Sponsor – BlackBerry Ltd

1.3 TOE Overview

The Target of Evaluation (TOE) is SecuSUITE Server Version 6.0. The SecuSUITE Server Version 6.0 enables use of the Session Initiation Protocol (SIP) to establish secure connections between mobile devices. The SecuSUITE Server runs on RHEL 8 OS within an ESXi version 8 virtualized environment using one of the following physical platforms:

- Dell PowerEdge R660 system with an Intel Xeon Silver 4510 processor (Sapphire Rapids microarchitecture) running ESXi 8
- PacStar 451 system with an Intel Xeon D-1539 (Broadwell microarchitecture) running ESXi 8.

The Dell PowerEdge R660 system can support either Broadcom Ethernet or Intel Ethernet network interfaces, while the PacStar 451 system supports only Intel Ethernet network interfaces.

The SecuSUITE Server is the centerpiece in the SecuSUITE Security Solution. The SecuSUITE Security Solution includes the SecuSUITE SIP Server and client software[1] for mobile device platforms. Together these form a system that provides end-to-end secure mobile voice communication and instant messaging, using IP-based mobile data connections such as EDGE, UMTS/HSPA, LTE, and Wi-Fi.

This Security Target (ST) pertains to only the SecuSUITE Server v6.0 component.

The TOE is considered a virtual Network Device (vND) as described by Use Case 2 in the NDcPP30e.

1.4 TOE Description

The TOE is the SecuSUITE Server version 6.0. The SecuSUITE Server enables use of the Session Initiation Protocol (SIP) to establish secure connections between mobile devices.

The SecuSUITE Server is an infrastructure component of the SecuSUITE Security Solution shown in Figure 1-1 below. The SecuSUITE Server does not work in isolation but relies on other infrastructure components to enable secure VoIP communications.

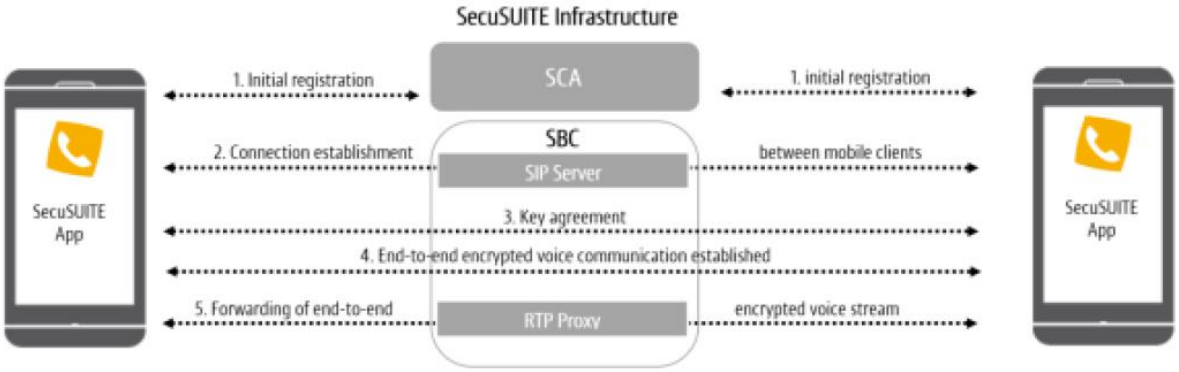

Figure 1-1 SecuSUITE Security Solution

As shown in Figure 1, the SecuSUITE VoIP process flow is as follows[2]:

a) Step 1 Initial Registration. Every participating client has to register first to the Secure Client Authentication (SCA) server. The TOE acts as a SCA server to authenticate users. The SCA server authenticates users and credentials to access services. Only clients that have been enrolled via the SCA service are able to connect to the SIP server and are allowed to establish end-to-end encrypted communication to other SecuSUITE clients. Note: Clients must also register to the SIP server using a SIP password. This is in addition to initial client registration with the SCA server.

[1] The client software is the target for another evaluation.
[2] SBC is session border controller – a short name for the SecuSUITE Server.

b) Step 2 Connection establishment. The Session Initiation Protocol (SIP) together with TLS is used to establish a secure connection between mobile devices and the SIP server (aka SIP Calling). The use of a TLS connection, providing encryption and mutual authentication, ensures that the devices connect with authorized SIP servers and the dialed call numbers are transmitted encrypted.

c) Step 3 Key agreement. When a call is placed and accepted, SecuSUITE clients exchange SIP messages that include digital certificates used to confirm caller identity and perform key agreement for SRTP encryption.

d) Step 4 End-to-end encrypted voice communication established. Clients utilize the SRTP protocol to exchange encrypted voice communications. The voice stream remains encrypted while traversing the SecuSUITE infrastructure and only the clients have access to the session keys.

e) Step 5 Forwarding of end-to-end encrypted voice stream. During connection signaling, the SIP server sets up the RTP/RTCP packet bridging in the Real-Time Transport Protocol (RTP) Proxy for this connection. The RTP Proxy relays / bridges the encrypted data stream between clients. The main purpose of the RTP Proxy is to make the communication between SIP user agents behind NAT/NAPT possible.

1.4.1 TOE Architecture

The SecuSUITE SIP Server v6.0 is a network appliance providing SIP Server, RTP Proxy, and SCA functionality as well as interfaces for management. The SecuSUITE SIP Server TOE is composed of hardware, an internal supporting Red Hat Enterprise Linux OS (the TOE does not offer general purpose computer capabilities), and custom software. The custom software provides SIP Server, RTP Proxy, and SCA functionality. It runs on a Red Hat Enterprise Linux (RHEL 8) and utilizes the OpenSSL FIPS object module along with other supporting software.

Specifically, the TOE utilizes the Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module, which provides cryptographic functionality used by the TOE. The TOE's software executes on the RHEL 8 operating system on ESXi on a physical platform as specified in section 1.3 above.

1.4.1.1 Physical Boundaries

The TOE boundary is illustrated in Figure 1-2.

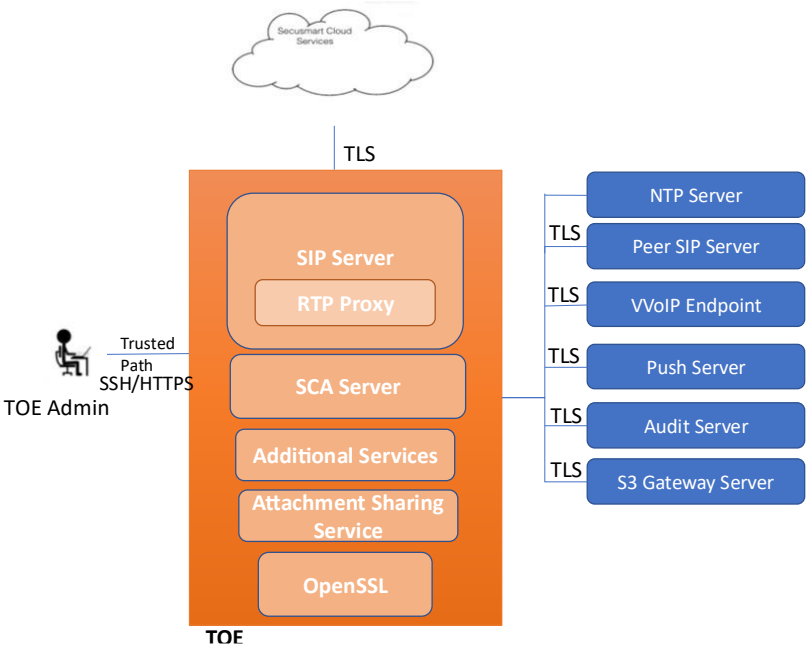

Figure 1-2 TOE Boundary

The TOE operates in a network environment mediating connections between VVoIP endpoints while utilizing services from other network entities.

SIP Server Functionality

The SIP Server interacts with the SecuSUITE VoIP client and provides registrar and proxy capabilities required for call-session management (e.g. establishing, processing, and terminating VoIP calls). As a SIP registrar, the SIP Server accepts REGISTER requests and places the information received into the location service on the SIP Server. As a SIP proxy server, the SIP Server is a stateful server that manages transactions to route SIP requests and responses. The SIP Server also provides a secure connection between mobile devices running the SecuSUITE app using TLS, providing encryption and mutual authentication.

RTP Proxy Functionality

The Real-Time Transport Protocol (RTP) Proxy bridges media packets sent between clients. The TOE creates and deletes RTP and Real-Time Transport Control Protocol (RTCP) bridging sessions in the RTP Proxy.

Secure Client Authentication Functionality (SCA0)

The SCA functionality authenticates users, facilitates VoIP client enrollment, and pushes client SIP configuration to the client. Only clients which have been enrolled via the SCA service are able to connect to the SIP Server. During SCA enrollment the SCA authorizes authenticated clients (via activation code) to use SIP Service and Additional Services and provisions them with the credentials and a TLS client certificate for the required trusted channels.

Additional Services functionality (SCA1)

SecuSUITE VoIP clients may interact with the TOE's Additional Services using a dedicated mutually authenticated TLS trusted channel which is common for all Additional Services. Additional Services include e.g. Secure Contacts Push, Group Calling and Secure Text Messaging services.

- **Secure Contact Push**: The contact push service is used to push available contact information to the SecuSUITE clients.
- **The Group Calling** service distributes group call related status information and metadata and ensures that all group call participants have an up-to-date list of all current members of the group call.
- **Secure Text Messaging** service allows encrypted instant message transfer between client applications.

Attachment sharing

SecuSUITE clients may interact with the TOE to share larger content e.g. media files by using the TOE's internal content sharing service. Connections between SecuSUITE clients and the TOE's attachment sharing service are mutually authenticated TLS trusted channels.

NON-TOE Components

The TOE is part of a broader system (SecuSUITE security solution) and requires the following components to be present in the environment:

- Audit Server. The TOE is able to send audit logs to a remote syslog server.
- NTP Server. The TOE is able to obtain time from an NTP server using SHA256 as the message digest algorithm for authentication.
- Peer SIP Server. The TOE can communicate with another SIP server (such as Asterisk SIP or similar) over TLS.
- Push Server. The TOE can communicate with a push notification server that allows the VVoIP endpoint OS to execute deep sleep cycles and wake-up client applications for incoming events.
- VVoIP Endpoints. The TOE mediates connections initiated by a VVoIP client enrolled through the SCA Server to another VVoIP endpoint.

- S3 Gateway Server: The TOE may provide SeuSUITE clients the possibility to store their shared content to an external S3 Server.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by SecuSUITE SIP Server:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

1.4.1.2.1 Security audit

The TOE generates audit events for numerous activities including policy enforcement, system management, authentication, and system status (i.e., system log records). The TOE also generates call detail records providing information about connections that are mediated by the TOE. A syslog server in the environment is relied on to store audit and system log records generated by the TOE. The TOE generates a complete audit record including the IP address of the TOE, the event details, and the time the event occurred. The time stamp is provided by the TOE appliance hardware.

1.4.1.2.2 Cryptographic support

The TOE contains CAVP-tested cryptographic implementations that provide key management, random bit generation, encryption/decryption, digital signature, and secure hashing and key-hashing features in support of higher-level cryptographic protocols, including HTTPS, NTP, SSH, and TLS.

1.4.1.2.3 User data protection

The TOE mediates connections between VVoIP endpoints, allowing enrolled endpoints to establish “calls” with other enrolled endpoints.

1.4.1.2.4 Identification and authentication

The TOE authenticates administrative users. In order for an administrative user to access the TOE, a user account including a username and password must be created for the user, and an administrative role must be assigned. The TOE performs the validation of the login credentials. The TOE also performs extensive X.509v3 certificate validation checks on certificates it receives as identification and authentication material.

1.4.1.2.5 Security management

The TOE also provides a Web UI (protected by HTTPS) and Command Line Interface (protected by SSH) to configure the TOE. Security management commands are limited to authorized users (i.e., administrators) and available only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of privileges associated with roles that can be assigned to TOE users. Among the available privileges, only the Authorized Administrator role can actually manage the security policies provided by the TOE and the TOE offers a complete set of functions to facilitate effective management.

1.4.1.2.6 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability) and must obtain time from external time sources using NTP.

The TOE performs self-tests and integrity checks on TOE executables during system start-up as well as periodically during normal operation. The TOE also includes mechanisms (i.e., verification of the digital signature of each new update package) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

1.4.1.2.7 TOE access

The TOE can be configured to display a warning banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

1.4.1.2.8 Trusted path/channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access, ensuring both integrity and disclosure protection. The TOE also provides a Web UI API interface for security management that is protected with HTTPS/TLS. If the negotiation of an encrypted session (either SSH or TLS) fails or if the user does not have authorization for remote administration, an attempted connection is not established.

The TOE protects communication with network peers, such as an audit server, VVoIP endpoints, ESC devices for trunking, S3 gateway server, and push notification server using TLS connections to prevent unintended disclosure or modification of data.

1.4.2 TOE Documentation

BlackBerry Ltd offers documentation that describes the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features of the TOE. The following list of documents were examined as part of the evaluation.

BlackBerry SecuSUITE Server Common Criteria Configuration Guide SecuSUITE for Government 6.0 Version 1.2

2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
  - Part 3 Conformant
- Package Claims:
  - PP-Configuration for Network Device and Enterprise Session Controller (ESC), Version 2.0, 2024-04-25 (CFG_NDcPP-ESC_V2.0)
    - Base PP: collaborative Protection Profile for Network Devices, Version 3.0e (CPP_ND_V3.0E)
    - PP Module: PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0)
  - Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021 (PKG_SSH_V1.0)

with the following technical decisions:

Package	Technical Decision	Applied	Notes
CPP_ND_V3.0E	TD0836 - NIT Technical Decision: Redundant Requirements in FPT_TST_EXT.1	Yes	
CPP_ND_V3.0E	TD0868 - NIT Technical Decision: Clarification of time frames in FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8	No	IPsec is not claimed
CPP_ND_V3.0E	TD0879 - NIT Decision: Correction of Chapter Headings in CPP_ND_V3.0E	Yes	
CPP_ND_V3.0E	TD0880 - NIT Decision: Removal of Duplicate Selection in FMT_SMF.1.1	Yes	
CPP_ND_V3.0E	TD0886 - Clarification to FAU_STG_EXT.1 Test 6	Yes	
CPP_ND_V3.0E	TD0899 - NIT Technical Decision: Correction of Renegotiation Test for TLS 1.2	Yes	
CPP_ND_V3.0E	TD0900 - NIT Technical Decision: Clarification to Local Administrator Access in FIA_UIA_EXT.1.3	Yes	
CPP_ND_V3.0E	TD0921 - NIT Technical Decision: Addition of FIPS PUB 186-5 and Correction of Assignment	Yes	
CPP_ND_V3.0E	TD0923 - NIT Technical Decision: Auditable event for FAU_STG_EXT.1 in FAU_GEN.1.2	Yes	
MOD_ESC_V1.0	TD0665 - Corrections to MOD_ESC_v1.0 SFRs	Yes	
MOD_ESC_V1.0	TD0835 - Aligning MOD_ESC 1.0 with NDcPP 3.0E	Yes	
PKG_SSH_V1.0	TD0682 - Addressing Ambiguity in FCS_SSHS_EXT.1 Tests	Yes	
PKG_SSH_V1.0	TD0695 - Choice of 128 or 256 bit size in AES-CTR in SSH Functional Package.	Yes	
PKG_SSH_V1.0	TD0732 - FCS_SSHS_EXT.1.3 Test 2 Update	Yes	
PKG_SSH_V1.0	TD0777 - Clarification to Selections for Auditable Events for FCS_SSH_EXT.1	Yes	
PKG_SSH_V1.0	TD0909 - Updates to FCS_SSH_EXT.1.1 App Note in SSH FP 1.0	Yes	

For ease of reference, the following acronyms will be used:

- CPP_ND_V3.0E – NDcPP30e
- MOD_ESC_V1.0 – ESC10
- PKG_SSH_V1.0 – SSH10

2.1 Conformance Rationale

The ST conforms to the NDcPP30e/ESC10/SSH10. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

3. Security Objectives

The Security Problem Definition may be found in the NDcPP30e/ESC10/SSH10 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDcPP30e/ESC10/SSH10 offers additional information about the identified security objectives, but that has not been reproduced here and the NDcPP30e/ESC10/SSH10 should be consulted if there is interest in that material.

In general, the NDcPP30e/ESC10/SSH10 has defined Security Objectives appropriate for a dedicated network appliance providing / enterprise session controller capabilities and as such are applicable to the SecuSUITE SIP Server TOE.

3.1 Security Objectives for the Operational Environment

OE.ADMIN_CREDENTIALS_SECURE The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

OE.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.

OE.NO_THRU_TRAFFIC_PROTECTION The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

OE.RESIDUAL_INFORMATION The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

OE.SECURED_PLATFORM The operating system of the network device does not provide an interface or other capability that can be used to adversely affect the TOE or its own functionality.

OE.TRUSTED_ADMIN Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.

OE.UPDATES The TOE frmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

OE.VM_CONFIGURATION (applies to vNDs only)
For vNDs, the Security Administrator ensures that the VS and VMs are configured to

- reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and
- correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting).

The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration.

If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDcPP30e/ESC10/SSH10. The NDcPP30e/ESC10/SSH10 defines the following extended requirements and since they are not redefined in this ST, the NDcPP30e/ESC10/SSH10 should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- NDcPP30e:FAU_STG_EXT.1: Protected Audit Event Storage
- ESC10:FAU_VVR_EXT.1: Recording Voice and Video Call Data
- NDcPP30e:FCS_HTTPS_EXT.1: HTTPS Protocol
- ESC10:FCS_NTP_EXT.1: NTP Protocol
- NDcPP30e/ESC10:FCS_NTP_EXT.1: NTP Protocol
- NDcPP30e:FCS_RBG_EXT.1: Random Bit Generation
- SSH10:FCS_SSH_EXT.1: SSH Protocol - per TD0732 & TD0777
- SSH10:FCS_SSHS_EXT.1: SSH Protocol – Server – per TD0682
- NDcPP30e/ESC10:FCS_TLSC_EXT.1: TLS Client Protocol – per TD0835
- NDcPP30e/ESC10:FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication
- NDcPP30e/ESC10:FCS_TLSS_EXT.1: TLS Server Protocol – per TD0835
- NDcPP30e/ESC10:FCS_TLSS_EXT.2: TLS Server Support for Mutual Authentication
- NDcPP30e:FIA_PMG_EXT.1: Password Management
- NDcPP30e:FIA_UIA_EXT.1: User Identification and Authentication
- NDcPP30e/ESC10:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
- NDcPP30e/ESC10:FIA_X509_EXT.2: X.509 Certificate Authentication
- NDcPP30e/ESC10:FIA_X509_EXT.3: X.509 Certificate Requests
- ESC10:FMT_CFG_EXT.1: Secure by Default Configuration
- NDcPP30e:FPT_APW_EXT.1: Protection of Administrator Passwords
- NDcPP30e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all symmetric keys)
- NDcPP30e/ESC10:FPT_STM_EXT.1: Reliable Time Stamps
- NDcPP30e:FPT_TST_EXT.1: TSF testing - per TD0836
- NDcPP30e:FPT_TUD_EXT.1: Trusted update
- NDcPP30e:FTA_SSL_EXT.1: TSF-initiated Session Locking

5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the NDcPP30e/ESC10/SSH10. The refinements and operations already performed in the NDcPP30e/ESC10/SSH10 are not identified (e.g., highlighted) here, rather the requirements have been copied from the NDcPP30e/ESC10/SSH10 and any residual operations have been completed herein. Of particular note, the NDcPP30e/ESC10/SSH10 made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the NDcPP30e/ESC10/SSH10. The NDcPP30e/ESC10/SSH10 should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by SecuSUITE SIP Server TOE.

Requirement Class	Requirement Component
FAU: Security audit	NDcPP30e/ESC10:FAU_GEN.1: Audit Data Generation
	ESC10:FAU_GEN.1/CDR: Audit Data Generation - CDR (Call Detail Record)
	ESC10:FAU_GEN.1/Log: Audit Data Generation - Log (System Log)
	NDcPP30e:FAU_GEN.2: User identity association
	ESC10:FAU_SAR.1/Log: Audit Review - Log (System Log)
	NDcPP30e/ESC10:FAU_STG.1 Protected Audit Trail Storage
	ESC10:FAU_STG.1/CDR: Protected Audit Trail Storage (Call Detail Record)
	NDcPP30e:FAU_STG_EXT.1: Protected Audit Event Storage
	ESC10:FAU_VVR_EXT.1: Recording Voice and Video Call Data
FCS: Cryptographic support	NDcPP30e:FCS_CKM.1: Cryptographic Key Generation
	NDcPP30e:FCS_CKM.2: Cryptographic Key Establishment
	NDcPP30e:FCS_CKM.4: Cryptographic Key Destruction
	NDcPP30e:FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)
	NDcPP30e:FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)
	NDcPP30e:FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)
	NDcPP30e:FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)
	NDcPP30e:FCS_HTTPS_EXT.1: HTTPS Protocol
	NDcPP30e/ESC10:FCS_NTP_EXT.1: NTP Protocol
	NDcPP30e:FCS_RBG_EXT.1: Random Bit Generation
	SSH10:FCS_SSH_EXT.1: SSH Protocol - per TD0732 & TD0777
	SSH10:FCS_SSHS_EXT.1: SSH Protocol – Server - per TD0682
	NDcPP30e/ESC10:FCS_TLSC_EXT.1: TLS Client Protocol
	NDcPP30e/ESC10:FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication
	NDcPP30e/ESC10:FCS_TLSS_EXT.1: TLS Server Protocol
	NDcPP30e/ESC10:FCS_TLSS_EXT.2: TLS Server Support for Mutual Authentication
FDP: User data protection	ESC10:FDP_IFC.1: Subset Information Flow Control
	ESC10:FDP_IFF.1: Simple Security Attributes
	ESC10:FDP_RIP.1: Subset Residual Information Protection
FIA: Identification and authentication	NDcPP30e:FIA_AFL.1: Authentication Failure Management
	NDcPP30e:FIA_PMG_EXT.1: Password Management

	ESC10:FIA_UAU.2/TC: User Authentication before Any Action - TC (Telecommunications Devices)
	ESC10:FIA_UAU.2/VVoIP: User Authentication before Any Action - VVoIP (VVoIP Endpoints)
	NDcPP30e:FIA_UAU.7: Protected Authentication Feedback
	NDcPP30e:FIA_UIA_EXT.1: User Identification and Authentication
	NDcPP30e/ESC10:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
	NDcPP30e/ESC10:FIA_X509_EXT.2: X.509 Certificate Authentication
	NDcPP30e/ESC10:FIA_X509_EXT.3: X.509 Certificate Requests
FMT: Security management	ESC10:FMT_CFG_EXT.1: Secure by Default Configuration
	NDcPP30e:FMT_MOF.1/ManualUpdate: Management of security functions behaviour
	NDcPP30e:FMT_MTD.1/CoreData: Management of TSF Data
	NDcPP30e:FMT_MTD.1/CryptoKeys: Management of TSF Data
	NDcPP30e:FMT_SMF.1: Specification of Management Functions - per TD0880
	ESC10:FMT_SMF.1/ESC: Specification of Management Functions
	NDcPP30e:FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	NDcPP30e:FPT_APW_EXT.1: Protection of Administrator Passwords
	ESC10:FPT_FLS.1: Failure with Preservation of a Secure State
	NDcPP30e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all symmetric keys)
	NDcPP30e/ESC10:FPT_STM_EXT.1: Reliable Time Stamps
	NDcPP30e:FPT_TST_EXT.1: TSF testing - per TD0836
	NDcPP30e:FPT_TUD_EXT.1: Trusted update
FTA: TOE access	NDcPP30e:FTA_SSL.3: TSF-initiated Termination
	NDcPP30e:FTA_SSL.4: User-initiated Termination
	NDcPP30e:FTA_SSL_EXT.1: TSF-initiated Session Locking
	NDcPP30e:FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	NDcPP30e:FTP_ITC.1: Inter-TSF trusted channel
	ESC10:FTP_ITC.1/ESC: Inter-TSF Trusted Channel (ESC Communications)
	NDcPP30e:FTP_TRP.1/Admin: Trusted Path

Table 5-1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit Data Generation (NDcPP30e/ESC10:FAU_GEN.1)

NDcPP30e/ESC10:FAU_GEN.1.1

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

a) Start-up and shut-down of the audit functions;

b) All auditable events for the not specified level of audit; and

c) All administrative actions comprising:

- Administrative login and logout (name of Administrator account shall be logged if individual accounts are required for Administrators).
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
- [***no other actions***];

d) Specifically defined auditable events listed in Table 5-2.

Requirement	Audit Event	Additional Contents
ESC10:FAU_GEN.1	None	None

NDcPP30e:FAU_GEN.1	None	None
ESC10:FAU_GEN.1/CDR	None	None
ESC10:FAU_GEN.1/Log	None	None
NDcPP30e:FAU_GEN.2	None	None
ESC10:FAU_SAR.1/Log	None	None
NDcPP30e/ESC10:FAU_STG.1	None	None
ESC10:FAU_STG.1/CDR	None	None
NDcPP30e:FAU_STG_EXT.1	Configuration of local audit settings.	Identity of account making changes to the audit configuration.
ESC10:FAU_VVR_EXT.1	None	None
NDcPP30e:FCS_CKM.1	None	None
NDcPP30e:FCS_CKM.2	None	None
NDcPP30e:FCS_CKM.4	None	None
NDcPP30e:FCS_COP.1/DataEncryption	None	None
NDcPP30e:FCS_COP.1/Hash	None	None
NDcPP30e:FCS_COP.1/KeyedHash	None	None
NDcPP30e:FCS_COP.1/SigGen	None	None
NDcPP30e:FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.
NDcPP30e/ESC10:FCS_NTP_EXT.1	Configuration of a new time server. Removal of configured time server.	Identity if new/removed time server.
NDcPP30e:FCS_RBG_EXT.1	None	None
SSH10:FCS_SSHS_EXT.1	Failure to establish an SSH connection.	Reason for failure.
NDcPP30e/ESC10:FCS_TLSC_EXT.1	Failure to establish a TLS Session.	Reason for failure.
NDcPP30e/ESC10:FCS_TLSC_EXT.2	Failure to establish a TLS Session.	Reason for failure.
NDcPP30e/ESC10:FCS_TLSS_EXT.1	Failure to establish a TLS Session.	Reason for failure.
NDcPP30e/ESC10:FCS_TLSS_EXT.2	Failure to authenticate the client.	Reason for failure.
ESC10:FCS_TLSS_EXT.2	None	None
ESC10:FDP_IFC.1	None	None
ESC10:FDP_IFF.1	None	None
ESC10:FDP_RIP.1	None	None
NDcPP30e:FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
NDcPP30e:FIA_PMG_EXT.1	None	None
ESC10:FIA_UAU.2/TC	Successful or failed authentication of trunk connected network component	ID of Administrator that attempts to connect trunk to external device (if available); IP address of device where trunk request was initiated (if available); IP address of external device where trunk is to be connected (if available).
ESC10:FIA_UAU.2/VVoIP	Authentication of external VVoIP endpoint/device	NOTE: Same as above for: FIA_UAU.2/VVoIP. Authentication of external VVoIP endpoints must occur before registration. In short, no successful registration of VVoIP endpoint can happen until after the successful

		authentication of the VVoIP endpoint.
NDcPP30e:FIA_UAU.7	None	None
NDcPP30e:FIA_UIA_EXT.1	All use of identification and authentication mechanisms.	Origin of the attempt (e.g., IP address).
NDcPP30e/ESC10: FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation. Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
NDcPP30e/ESC10:FIA_X509_EXT.2	None	None
NDcPP30e/ESC10:FIA_X509_EXT.3	None	None
ESCEP10:FMT_CFG_EXT.1	None	None
NDcPP30e: FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None
NDcPP30e:FMT_MTD.1/CoreData	None	None
NDcPP30e:FMT_MTD.1/CryptoKeys	None	None
ESC10:FMT_SMF.1 /ESC	Modification of TOE Call Details Records (CDR) Enabling/disabling VVoIP endpoint device features	ID of Administrator attempting to modify the CDR; IP-address of device where modification was initiated; the modification that was performed. ID of Administrator attempting to enable/disable service or feature on ESC or on external registered device; IP-address of device where enabling/disabling of services or features was initiated; the feature or service that was enabled/disabled.
NDcPP30e:FMT_SMF.1	All management activities of TSF data.	None
NDcPP30e:FMT_SMR.2	None	None
NDcPP30e:FPT_APW_EXT.1	None	None
ESC10:FPT_FLS.1	None	None
NDcPP30e:FPT_SKP_EXT.1	None	None
ESC10:FPT_STM_EXT.1	None	None
NDcPP30e:FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
NDcPP30e:FPT_TST_EXT.1	None	None
NDcPP30e:FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	None
NDcPP30e:FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None
NDcPP30e:FTA_SSL.4	The termination of an interactive session.	None

NDcPP30e:FTA_SSL_EXT.1	The termination of a local session by the session lock.	None
NDcPP30e:FTA_TAB.1	None	None
NDcPP30e:FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	None. None. Reason for failure.
ESC10:FTP_ITC.1/ESC	None	None
NDcPP30e:FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None. None. Reason for failure.

Table 5-2 Audit Events

NDcPP30e: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, 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 cPP/ST, information specified in column three of Table 5-2.

5.1.1.2 Audit Data Generation - CDR (Call Detail Record) (ESC10:FAU_GEN.1/CDR)

ESC10:FAU_GEN.1.1/CDR

The TSF shall be able to generate a call detail record (CDR) for communications between VVoIP endpoints that are established by the TOE.

ESC10:FAU_GEN.1.2/CDR

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

- calling party number (i.e. call originator)
- called party number (i.e. call receiver or terminating number)
- unique transaction sequence number
- call disposition (e.g. call connected, call terminated, call transferred)
- call type (e.g. voice only, voice and video, text)
- call start time
- call end time
- call duration
- unique identifier of the TOE
- call routing into TOE
- call routing out of TOE
- time zone
- call release cause, if applicable (i.e. reason for termination of call)
- fault condition(s), if applicable

5.1.1.3 Audit Data Generation - Log (System Log) (ESC10:FAU_GEN.1/Log)

ESC10:FAU_GEN.1.1/Log

The TSF shall be able to generate a system log record for current IP connections, NTP status, CPU usage, memory usage, disk and file storage capacity, audit storage capacity, [***no other activities***].

ESC10:FAU_GEN.1.2/Log

The TSF shall record within each system log 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, [event details described in Table 5-3].

c)

Event	Additional System Log Record Contents

Current IP connections	Network interface card (NIC); Status (up or down).
CPU usage	Utilization percentage of TOE CPU(s)
Memory usage	Percentage and/or amount of free memory available for use
Disk and file storage capacity	Percentage and/or amount of available space remaining for each disk or disk partition on the TOE

Table 5-3 System Log Contents

5.1.1.4 User identity association (NDcPP30e:FAU_GEN.2)

NDcPP30e: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.

5.1.1.5 Audit Review - Log (System Log) (ESC10:FAU_SAR.1/Log)

ESC10:FAU_SAR.1.1/Log
The TSF shall provide System Administrators with the capability to read [**all records**] from the system log records.
ESC10:FAU_SAR.1.2/Log
The TSF shall provide the system log records in a real-time first-in first-out scrolling method.

5.1.1.6 Protected Audit Trail Storage (NDcPP30e/ESC10:FAU_STG.1)

NDcPP30e/ESC10:FAU_STG.1.1
The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
NDcPP30e/ESC10:FAU_STG.1.2
The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

Application Note: The PP-Module ESC version 1.0 indicates that this SFR is optional in the NDcPP but is mandated by this PP-Module because the ESC is expected to maintain audit data internal to the TOE which must be protected from unauthorized access.

Application Note: ESC10:FAU_STG.1 is intended to require inclusion of NDcPP30e:FAU_STG.1.

5.1.1.7 Protected Audit Trail Storage (Call Detail Record) (ESC10:FAU_STG.1/CDR)

ESC10:FAU_STG.1.1/CDR
The TSF shall protect the stored call detail records from unauthorized disclosure and deletion.
ESC10:FAU_STG.1.2/CDR
The TSF shall be able to prevent unauthorized modifications to the stored call detail records.

5.1.1.8 Protected Audit Event Storage (NDcPP30e:FAU_STG_EXT.1)

NDcPP30e:FAU_STG_EXT.1.1
The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.
NDcPP30e:FAU_STG_EXT.1.2
The TSF shall be able to store generated audit data on the TOE itself. In addition [***The TOE shall consist of a single standalone component that stores audit data locally***].
NDcPP30e:FAU_STG_EXT.1.3
The TSF shall maintain a [***log rotation with 5 log files***] of audit records in the event that an interruption of communication with the remote audit server occurs.
NDcPP30e:FAU_STG_EXT.1.4
The TSF shall be able to store [***persistent***] audit records locally with a minimum storage size of [**25 Mbytes**].

NDcPP30e:FAU_STG_EXT.1.5

The TSF shall [***overwrite previous audit records according to the following rule: [delete the oldest audit log file]***] when the local storage space for audit data is full.

NDcPP30e:FAU_STG_EXT.1.6

The TSF shall provide the following mechanisms for administrative access to locally stored audit records [***ability to view locally***].

5.1.1.9 Recording Voice and Video Call Data (ESC10:FAU_VVR_EXT.1)

ESC10:FAU_VVR_EXT.1.1

The TSF shall [***not have***] the capability to record voice and video call data.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation (NDcPP30e:FCS_CKM.1)

NDcPP30e:FCS_CKM.1.1

The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- ***RSA schemes using cryptographic key sizes of [*3072-bit*] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.3 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", A.1;***
- ***ECC schemes using 'NIST curves' [P-256, P-384] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix A.2, or ISO/IEC 14888-3, "IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms", Section 6.6;***].

5.1.2.2 Cryptographic Key Establishment (NDcPP30e:FCS_CKM.2)

NDcPP30e:FCS_CKM.2.1

The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- ***Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography'***].

5.1.2.3 Cryptographic Key Destruction (NDcPP30e:FCS_CKM.4)

NDcPP30e:FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- For plaintext keys in volatile storage, the destruction shall be executed by a [***single overwrite consisting of [zeroes]***];
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [***logically addresses the storage location of the key and performs a [[*single*]-pass] overwrite consisting of [zeroes]***]

that meets the following: No Standard.

5.1.2.4 Cryptographic Operation (AES Data Encryption/Decryption) (NDcPP30e:FCS_COP.1/DataEncryption)

NDcPP30e:FCS_COP.1.1/DataEncryption

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [***CTR, GCM***] mode and cryptographic key sizes [***128 bits, 256 bits***] that

meet the following: AES as specified in ISO 18033-3, [***CTR as specified in ISO 10116, GCM as specified in ISO 19772***].

5.1.2.5 Cryptographic Operation (Hash Algorithm) (NDcPP30e:FCS_COP.1/Hash)

NDcPP30e:FCS_COP.1.1/Hash

The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-256, SHA-384, SHA-512***] and message digest sizes [***256, 384, 512***] bits that meet the following: ISO/IEC 10118-3:2004.

5.1.2.6 Cryptographic Operation (Keyed Hash Algorithm) (NDcPP30e:FCS_COP.1/KeyedHash)

NDcPP30e:FCS_COP.1.1/KeyedHash

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [***HMAC-SHA-256, HMAC-SHA-384***] and cryptographic key sizes [**256, 384**] and message digest sizes [***256, 384***] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 'MAC Algorithm 2'.

5.1.2.7 Cryptographic Operation (Signature Generation and Verification) (NDcPP30e:FCS_COP.1/SigGen)

NDcPP30e:FCS_COP.1.1/SigGen

The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [

- ***RSA Digital Signature Algorithm,***
- ***Elliptic Curve Digital Signature Algorithm***]

and cryptographic key sizes [

- ***For RSA: [modulus 2048 bits or 3072 bits],***
- ***For ECDSA: [256 bits, 384 bits***]

that meet the following: [

- ***For RSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5.5, using PKCS #1 v2.1 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5.4 using PKCS #1 v2.2 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,***
- ***For ECDSA schemes implementing [P-256, P-384] curves that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 6 and Appendix D, Implementing 'NIST Recommended' curves; or FIPS PUB 186-5, 'Digital Signature Standard (DSS)', Section 6 and NIST SP 800-186 Section 3.2.1, Implementing Weierstrass curves; or ISO/IEC 14888-3, 'IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms', Section 6.6***].

5.1.2.8 HTTPS Protocol (NDcPP30e:FCS_HTTPS_EXT.1)

NDcPP30e:FCS_HTTPS_EXT.1.1

The TSF shall implement the HTTPS protocol that complies with RFC 2818.

NDcPP30e:FCS_HTTPS_EXT.1.2

The TSF shall implement HTTPS using TLS.

5.1.2.9 NTP Protocol (NDcPP30e/ESC10:FCS_NTP_EXT.1)

NDcPP30e/ESC10:FCS_NTP_EXT.1.1

The TSF shall use only the following NTP version: [***NTP v4 (RFC 5905)***].

NDcPP30e/ESC10:FCS_NTP_EXT.1.2

The TSF shall update its system time using [***Authentication using [SHA256] as the message digest algorithm(s)***].

NDcPP30e/ESC10:FCS_NTP_EXT.1.3

The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

NDcPP30e/ESC10:FCS_NTP_EXT.1.4

The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

5.1.2.10 Random Bit Generation (NDcPP30e:FCS_RBG_EXT.1)

NDcPP30e:FCS_RBG_EXT.1.1

The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [***CTR_DRBG (AES)***].

NDcPP30e:FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [***[1] platform-based noise source***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011Table C.1 'Security Strength Table for Hash Functions', of the keys and hashes that it will generate.

5.1.2.11 SSH Protocol - per TD0732 & TD0777 (SSH10:FCS_SSH_EXT.1)

SSH10:FCS_SSH_EXT.1.1

The TOE shall implement SSH acting as a [***server***] in accordance with that complies with RFCs 4251, 4252, 4253, 4254, [***5647, 5656, 6668***] and no other standard.

SSH10:FCS_SSH_EXT.1.2

The TSF shall ensure that the SSH protocol implementation supports the following authentication methods: [

- ***'password' (RFC 4252),***
- ***'publickey' (RFC 4252): [ecdsa-sha2-nistp256 (RFC 5656), ecdsa-sha2-nistp384 (RFC 5656)]***

] and no other methods.

SSH10:FCS_SSH_EXT.1.3

The TSF shall ensure that, as described in RFC 4253, packets greater than ***[262126 bytes]*** in an SSH transport connection are dropped.

SSH10:FCS_SSH_EXT.1.4

The TSF shall protect data in transit from unauthorized disclosure using the following mechanisms: [

- ***aes128-ctr (RFC 4344)***
- ***aes256-ctr (RFC 4344)***
- ***aes128-gcm@openssh.com (RFC 5647)***
- ***aes256-gcm@openssh.com (RFC 5647)***

] and no other mechanisms.

SSH10:FCS_SSH_EXT.1.5

The TSF shall protect data in transit from modification, deletion, and insertion using: [

- ***hmac-sha2-256 (RFC 6668),***
- ***implicit***

] and no other mechanisms.

SSH10:FCS_SSH_EXT.1.6

The TSF shall establish a shared secret with its peer using: [

- ***ecdh-sha2-nistp256 (RFC 5656),***
- ***ecdh-sha2-nistp384 (RFC 5656)***

] and no other mechanisms.

SSH10:FCS_SSH_EXT.1.7

The TSF shall use SSH KDF as defined in [***RFC 5656 (Section 4)***] to derive the following cryptographic keys from a shared secret: session keys.

SSH10:FCS_SSH_EXT.1.8

The TSF shall ensure that [***a rekey of the session keys***] occurs when any of the following thresholds are met:

- one hour connection time
- no more than one gigabyte of transmitted data, or

- no more than one gigabyte of received data.

5.1.2.12 SSH Protocol - Server - per TD0682 (SSH10:FCS_SSHS_EXT.1)

SSH10:FCS_SSHS_EXT.1.1

The TSF shall authenticate itself to its peer (SSH Client) using: [

- ***ecdsa-sha2-nistp256 (RFC 5656),***
- ***ecdsa-sha2-nistp384 (RFC 5656)***].

5.1.2.13 TLS Client Protocol – per TD0835 (NDcPP30e/ESC10:FCS_TLSC_EXT.1)

NDcPP30e/ESC10:FCS_TLSC_EXT.1.1

The TSF shall implement TLS 1.2 (RFC 5246) and [***no other TLS versions***] supporting the following ciphersuites:[

- ***TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,***
- ***TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289]***

] and no other ciphersuites.

NDcPP30e/ESC10:FCS_TLSC_EXT.1.2

The TSF shall verify that the presented identifier matches [***the reference identifier per RFC 6125 Section 6, IPv4 address in the CN or in the SAN***].

NDcPP30e/ESC10:FCS_TLSC_EXT.1.3

The TSF shall not establish a trusted channel if the server certificate is invalid: [***without any administrator override mechanism.***].

NDcPP30e/ESC10:FCS_TLSC_EXT.1.4

The TSF shall [***present the Supported Groups Extension with the following curves/groups: [secp384r1] and no other curves/groups***] in the Client Hello.

NDcPP30eESC10:FCS_TLSC_EXT.1.5

The TSF shall [

- ***present the signature_algorithms extension with support for the following algorithms: [***
  - ***ecdsa_secp384r1 with sha384(0x0503)***
  - rsa_pkcs1_sha384

  ] and no other algorithms,

  ].

NDcPP30e/ESC10:FCS_TLSC_EXT.1.6

The TSF [***provides***] the ability to configure the list of supported ciphersuites as defined in NDcPP30e:FCS_TLSC_EXT.1.1. connections

NDcPP30e/ESC10:FCS_TLSC_EXT.1.7

The TSF shall prohibit the use of the following extensions:

- Early data extension
- Post-handshake client authentication according to RFC 8446, Section 4.2.6.

NDcPP30e/ESC10:FCS_TLSC_EXT.1.8

The TSF shall [***not use PSKs***].

NDcPP30e/ESC10:FCS_TLSC_EXT.1.9

The TSF shall [***support TLS 1.2 secure renegotiation through use of the 'renegotiation_info' TLS extension in accordance with RFC 5746, reject [TLS 1.2] renegotiation attempts***].

Application Note: This SFR is selection-based in the NDcPP but is mandated by the ESC PP-Module because Transport Layer Security (TLS) is used to secure SIP and H.323 communications. Additionally, the PP-Module mandates the use of TLS 1.2.

Application Note: There are several TLS client channels. Some of these channels allow for configuration of the list of supported ciphersuites, while some channels do not allow the list of ciphersuites to be configured. As a result, both “provides” and “does not provide” have been selected for FCS_TLSC_EXT.1.6. The TSS expands on which channels have configurable ciphersuite lists.

Application Note: TLS connections are implemented using two different software stacks (SIP TLS stack for SIP related connections and TLS tunnel for the rest). For TLS client connections, the SIP TLS stack rejects TLS 1.2 renegotiation attempts and the TLS tunnel stack supports renegotiation attempts. Thus both selections have been made in FCS_TLSC_EXT.1.9. The TSS expands on which channels leverage each stack.

5.1.2.14 TLS Client Support for Mutual Authentication (NDcPP30e/ESC10:FCS_TLSC_EXT.2)

NDcPP30e/ESC10:FCS_TLSC_EXT.2.1
The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

5.1.2.15 TLS Server Protocol – per TD0835 (NDcPP30e/ESC10:FCS_TLSS_EXT.1)

NDcPP30e/ESC10:FCS_TLSS_EXT.1.1
The TSF shall implement TLS 1.2 (RFC 5246) and [***no other TLS versions***] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- ***[***
- ***TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,***
- ***TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289]***

] and no other ciphersuites.

NDcPP30e/ESC10:FCS_TLSS_EXT.1.2
The TSF shall authenticate itself using X.509 certificate(s) using [***RSA with key size [2048, 3072] bits; ECDSA over NIST curves [secp384r1] and no other curves***].

NDcPP30e/ESC10:FCS_TLSS_EXT.1.3
The TSF shall perform key exchange using: [***EC Diffie-Hellman key agreement over NIST curves [secp384r1] and no other curves***].

NDcPP30e/ESC10:FCS_TLSS_EXT.1.4
The TSF shall support [***no session resumption***].

NDcPP30e/ESC10:FCS_TLSS_EXT.1.5
The TSF [***provides, does not provide***] the ability to configure the list of supported ciphersuites as defined in NDcPP30e:FCS_TLSS_EXT.1.1.

NDcPP30e/ESC10:FCS_TLSS_EXT.1.6
The TSF shall prohibit the use of the following extensions:

- Early data extension

NDcPP30e/ESC10:FCS_TLSS_EXT.1.7
The TSF shall [***not use PSKs***].

NDcPP30e/ESC10:FCS_TLSS_EXT.1.8
The TSF shall [***reject [TLS 1.2] renegotiation attempts***].

Application Note: This SFR is selection-based in the NDcPP but is mandated by the ESC PP-Module because TLS is used to secure SIP and H.323 communications. Additionally, the PP-Module mandates the use of TLS 1.2.

Application Note: There are several TLS server channels. Some of these channels allow for configuration of the list of supported ciphersuites, while some channels do not allow the list of ciphersuites to be configured. As a result, both "provides" and "does not provide" have been selected for FCS_TLSS_EXT.1.5. The TSS expands on which channels have configurable ciphersuite lists.

5.1.2.16 TLS Server Support for Mutual Authentication (NDcPP30e/ESC10:FCS_TLSS_EXT.2)

NDcPP30e/ESC10:FCS_TLSS_EXT.2.1
The TSF shall support TLS communication with mutual authentication of TLS clients using X.509v3 certificates and shall [***reject the connection if the client either does not provide a client certificate at all or the client certificate cannot be successfully validated by the TOE (except for override mechanisms that might be defined in NDcPP30e:FCS_TLSS_EXT.2.2) ('hard fail')***].

NDcPP30e/ESC10:FCS_TLSS_EXT.2.2
When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the

client certificate is invalid. The TSF shall also [***not implement any administrator override mechanism***].

NDcPP30e/ESC10:FCS_TLSS_EXT.2.3

The TSF shall not establish a trusted channel if the identifier contained in a certificate does not match an expected identifier for the client. If the identifier is a Fully Qualified Domain Name (FQDN), then the TSF shall match the identifiers according to RFC 6125, otherwise the TSF shall parse the identifier from the certificate and match the identifier against the expected identifier of the client as described in the TSS.

NDcPP30e/ESC10:FCS_TLSS_EXT.2.4

The TSF shall present a [***TLS 1.2***] Certificate Request message containing the following algorithms: [

- ***ecdsa_secp384r1 with sha384(0x0503)***
- ***rsa_pkcs1 with sha384(0x0501)***

] and no other algorithms.

Application Note: The TOE TLS Web Server does not support mutual authentication.

5.1.3 User data protection (FDP)

5.1.3.1 Subset Information Flow Control (ESC10:FDP_IFC.1)

ESC10:FDP_IFC.1.1

The TSF shall enforce the enterprise session controller SFP on caller-callee pairs attempting to communicate through the TOE.

5.1.3.2 Simple Security Attributes (ESC10:FDP_IFF.1)

ESC10:FDP_IFF.1.1

The TSF shall enforce the enterprise session controller SFP based on the following types of subject and information security attributes: [**SIP username and password**] using the following call control protocols: [***SIP***] and [***no other call control protocols***].

ESC10:FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: when valid communication through the TOE is attempted, the TSF will establish a connection between itself and the caller; the TSF will establish a second connection between itself and the callee; and the TSF will redirect all communications that it receives between the two endpoints out through the proper connection.

ESC10:FDP_IFF.1.3

The TSF shall enforce the additional information flow control SFP rules: no additional rules.

ESC10:FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules: [**no additional rules**].

ESC10:FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [**no additional rules**].

5.1.3.3 Subset Residual Information Protection (ESC10:FDP_RIP.1)

ESC10:FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***deallocation of the resource from***] the following objects: [**TOE private keys**].

5.1.4 Identification and authentication (FIA)

5.1.4.1 Authentication Failure Management (NDcPP30e:FIA_AFL.1)

NDcPP30e:FIA_AFL.1.1

The TSF shall detect when an Administrator configurable positive integer within [**3 to 7**] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a password.

NDcPP30e:FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [***prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until [an authorized administrator unlocks the locked user account] is taken by an Administrator; prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed***].

5.1.4.2 Password Management (NDcPP30e:FIA_PMG_EXT.1)

NDcPP30e:FIA_PMG_EXT.1.1

The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [***'!', '@', '#', '$', '%', '^', '&', '*', '(', ')'***];

b) Minimum password length shall be configurable to between [**8**] and [**32**] characters.

5.1.4.3 User Authentication before Any Action - TC (Telecommunications Devices) (ESC10:FIA_UAU.2/TC)

ESC10:FIA_UAU.2.1/TC

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

5.1.4.4 User Authentication before Any Action - VVoIP (VVoIP Endpoints) (ESC10:FIA_UAU.2/VVoIP)

ESC10:FIA_UAU.2.1/VVoIP

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

5.1.4.5 Protected Authentication Feedback (NDcPP30e:FIA_UAU.7)

NDcPP30e:FIA_UAU.7.1

The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

5.1.4.6 User Identification and Authentication (NDcPP30e:FIA_UIA_EXT.1)

NDcPP30e:FIA_UIA_EXT.1.1

The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [***no other actions***].

NDcPP30e:FIA_UIA_EXT.1.2

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

NDcPP30e:FIA_UIA_EXT.1.3

The TSF shall provide the following remote authentication mechanisms [***Web GUI password,***

SSH password, SSH public key] and [***no other mechanism***]. The TSF shall provide the following local authentication mechanisms [***password-based***]. (TD0900 applied)

NDcPP30e:FIA_UIA_EXT.1.4

The TSF shall authenticate any administrative user's claimed identity according to each authentication mechanism specified in NDcPP30e:FIA_UIA_EXT.1.3.

5.1.4.7 X.509 Certificate Validation (NDcPP30e/ESC10:FIA_X509_EXT.1/Rev)

NDcPP30e/ESC10:FIA_X509_EXT.1.1/Rev

The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [***Certificate Revocation List (CRL) as specified in RFC 5759 Section 5, Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3***]].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

5.1.4.8 X.509 Certificate Authentication (NDcPP30e/ESC10:FIA_X509_EXT.2)

NDcPP30e/ESC10:FIA_X509_EXT.2.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for TLS [***no other protocols***], VVoIP endpoint registration, and [***no additional uses***].

NDcPP30e/ESC10:FIA_X509_EXT.2.2

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [***allow the Administrator to choose whether to accept the certificate in these cases***].

5.1.4.9 X.509 Certificate Requests (NDcPP30e/ESC10:FIA_X509_EXT.3)

NDcPP30e/ESC10:FIA_X509_EXT.3.1

The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [***Common Name, Organization, Organizational Unit, Country***].

NDcPP30e/ESC10:FIA_X509_EXT.3.2

The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.1.5 Security management (FMT)

5.1.5.1 Secure by Default Configuration (ESC10:FMT_CFG_EXT.1)

ESC10:FMT_CFG_EXT.1.1

The TSF shall provide only enough functionality to set new Security Administrator credentials when configured with default credentials or no credentials.

ESC10:FMT_CFG_EXT.1.2

The TSF shall be configured by default with permissions which protect it and its data from unauthorized access.

5.1.5.2 Management of security functions behaviour (NDcPP30e:FMT_MOF.1/ManualUpdate)

NDcPP30e:FMT_MOF.1.1/ManualUpdate

The TSF shall restrict the ability to enable the functions to perform manual updates to Security Administrators.

5.1.5.3 Management of TSF Data (NDcPP30e:FMT_MTD.1/CoreData)

NDcPP30e:FMT_MTD.1.1/CoreData

The TSF shall restrict the ability to manage the TSF data to Security Administrators.

5.1.5.4 Management of TSF Data (NDcPP30e:FMT_MTD.1/CryptoKeys)

NDcPP30e:FMT_MTD.1.1/CryptoKeys

The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

5.1.5.5 Specification of Management Functions - per TD0880 (NDcPP30e:FMT_SMF.1)

NDcPP30e:FMT_SMF.1.1

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

- Ability to administer the TOE remotely;
- Ability to configure the access banner;
- Ability to configure the remote session inactivity time before session termination;
- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates;
- [
  - ***Ability to manage the cryptographic keys,***
  - ***Ability to configure the cryptographic functionality,***
  - ***Ability to re-enable an Administrator account,***
  - ***Ability to set the time which is used for time-stamps,***
  - ***Ability to configure NTP,***
  - ***Ability to configure the reference identifier for the peer,***
  - ***Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors,***
  - ***Ability to administer the TOE locally,***
  - ***Ability to configure the local session inactivity time before session termination or locking,***
  - ***Ability to configure the authentication failure parameters for FIA_AFL.1***].

(TD0880 applied)

5.1.5.6 Specification of Management Functions (ESC10:FMT_SMF.1/ESC)

ESC10:FMT_SMF.1.1/ESC

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

- Ability to display the real-time connection status of all VVoIP endpoints (hardware and software) and telecommunications devices;
- Ability to clear all TSF data stored on disk;
- [***no other capabilities***]

5.1.5.7 Restrictions on Security Roles (NDcPP30e:FMT_SMR.2)

NDcPP30e:FMT_SMR.2.1

The TSF shall maintain the roles:

- Security Administrator.

NDcPP30e:FMT_SMR.2.2
The TSF shall be able to associate users with roles.

NDcPP30e:FMT_SMR.2.3
The TSF shall ensure that the conditions
- The Security Administrator role shall be able to administer the TOE remotely are satisfied.

5.1.6 Protection of the TSF (FPT)

5.1.6.1 Protection of Administrator Passwords (NDcPP30e:FPT_APW_EXT.1)

NDcPP30e:FPT_APW_EXT.1.1
The TSF shall store administrative passwords in non-plaintext form.

NDcPP30e:FPT_APW_EXT.1.2
The TSF shall prevent the reading of plaintext administrative passwords.

5.1.6.2 Failure with Preservation of a Secure State (ESC10:FPT_FLS.1)

ESC10:FPT_FLS.1.1
The TSF shall preserve a secure state through the following means: [**/generate an audit and disabling TOE network services/**] when the following types of failures occur: failure of self-tests defined in FPT_TST_EXT.1, failure of [**no hardware components**].

5.1.6.3 Protection of TSF Data (for reading of all symmetric keys) (NDcPP30e:FPT_SKP_EXT.1)

NDcPP30e:FPT_SKP_EXT.1.1
The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.1.6.4 Reliable Time Stamps (NDcPP30e/ESC10:FPT_STM_EXT.1)

NDcPP30e/ESC10:FPT_STM_EXT.1.1
The TSF shall be able to provide reliable time stamps for its own use.

NDcPP30e/ESC10:FPT_STM_EXT.1.2
The TSF shall [***synchronize time with an NTP server***].

5.1.6.5 TSF testing - per TD0836 (NDcPP30e:FPT_TST_EXT.1)

NDcPP30e:FPT_TST_EXT.1.1
The TSF shall run a suite of the following self-tests:
- During initial start-up (on power on) to verify the integrity of the TOE firmware and software
- Prior to providing any cryptographic service and [***at no other time***] to verify correct operation of cryptographic implementation necessary to fulfil the TSF
- [***at the conditions*** **/during initial start-up (on power on)/**] self-tests [**Cryptographic Known Answer Test (KAT), TOE software integrity checks and AIDE file and directory integrity checks**]

to demonstrate the correct operation of the TSF. (TD0836 applied)

NDcPP30e:FPT_TST_EXT.1.2
The TSF shall respond to [***all failures***] by [**/generating an audit event and disabling TOE network services/**].

5.1.6.6 Trusted update (NDcPP30e:FPT_TUD_EXT.1)

NDcPP30e:FPT_TUD_EXT.1.1
The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [***no other TOE firmware/software version***].

NDcPP30e:FPT_TUD_EXT.1.2
The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and [***no other update mechanism***].

NDcPP30e:FPT_TUD_EXT.1.3
The TSF shall provide means to authenticate firmware/software updates to the TOE using a [***digital signature***] prior to installing those updates.

5.1.7 TOE access (FTA)

5.1.7.1 TSF-initiated Termination (NDcPP30e:FTA_SSL.3)

NDcPP30e:FTA_SSL.3.1
The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

5.1.7.2 User-initiated Termination (NDcPP30e:FTA_SSL.4)

NDcPP30e:FTA_SSL.4.1
The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.1.7.3 TSF-initiated Session Locking (NDcPP30e:FTA_SSL_EXT.1)

NDcPP30e:FTA_SSL_EXT.1.1
The TSF shall, for local interactive sessions, [***terminate the session***] after a Security Administrator-specified time period of inactivity.

5.1.7.4 Default TOE Access Banners (NDcPP30e:FTA_TAB.1)

NDcPP30e:FTA_TAB.1.1
Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

5.1.8 Trusted path/channels (FTP)

5.1.8.1 Inter-TSF trusted channel (NDcPP30e:FTP_ITC.1)

NDcPP30e:FTP_ITC.1.1
The TSF shall be capable of using [***TLS***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [**/push server, ESC devices, VVoIP endpoint, S3 Gateway server/**] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

NDcPP30e:FTP_ITC.1.2
The TSF shall permit [***the TSF, the authorized IT entities***] to initiate communication via the trusted channel.

NDcPP30e:FTP_ITC.1.3
The TSF shall initiate communication via the trusted channel for [**audit server, push server, ESC device, S3 Gateway Server**].

5.1.8.2 Inter-TSF Trusted Channel (ESC Communications) (ESC10:FTP_ITC.1/ESC)

ESC10:FTP_ITC.1.1/ESC
The TSF shall be capable of using TLS and [***no other protocols***] to provide a communication channel between itself and another trusted IT product supporting the following capabilities: VVoIP endpoints (for protection of signaling protocols), VVoIP endpoints (for protection of

voice/video/media content), other ESC devices (for SIP trunking), [***no other capabilities***] 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.

ESC10:FTP_ITC.1.2/ESC

The TSF shall permit the TSF, another trusted IT product to initiate communication via the trusted channel.

ESC10:FTP_ITC.1.3/ESC

The TSF shall initiate communication via the trusted channel for [**ESC devices**].

5.1.8.3 Trusted Path (NDcPP30e:FTP_TRP.1/Admin)

NDcPP30e:FTP_TRP.1.1/Admin

The TSF shall be capable of using [***SSH, HTTPS***] to provide a communication path between itself and authorized remote Administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and provides detection of modification of the channel data.

NDcPP30e:FTP_TRP.1.2/Admin

The TSF shall permit remote Administrators to initiate communication via the trusted path.

NDcPP30e:FTP_TRP.1.3/Admin

The TSF shall require the use of the trusted path for initial Administrator authentication and all remote administration actions.

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM coverage
ATE: Tests	ATE_IND.1: Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability survey

Table 5-4 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic functional specification (ADV_FSP.1)

ADV_FSP.1.1d

The developer shall provide a functional specification.

ADV_FSP.1.2d

The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4c

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1d

The developer shall provide operational user guidance.

AGD_OPE.1.1c

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6c

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c

The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1d

The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1c

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e
The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d
The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c
The TOE shall be labelled with its unique reference.

ALC_CMC.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 TOE CM coverage (ALC_CMS.1)

ALC_CMS.1.1d
The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c
The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c
The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Independent testing - conformance (ATE_IND.1)

ATE_IND.1.1d
The developer shall provide the TOE for testing.

ATE_IND.1.1c
The TOE shall be suitable for testing.

ATE_IND.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e
The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability survey (AVA_VAN.1)

AVA_VAN.1.1d
The developer shall provide the TOE for testing.

AVA_VAN.1.1c
The TOE shall be suitable for testing.

AVA_VAN.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2e

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Security audit

The TOE is a single standalone device that stores its audit data locally and can send audit data to an external audit server in real time. The TOE uses the Linux Audit System (auditd) to log the events and information identified by the 'Audit Events' table in section 5.1.1. Audits of administrative actions affecting cryptographic keys (i.e., generation, import, modification or deletion) include a keyword indicating the service using the key (e.g., est_tls, syslog_tls, pabx_sip_tls) which corresponds with the naming of the service in the TOE Web UI interface for certificate assignment.

The Linux auditd daemon process receives audit data from applications and the kernel. The daemon runs as a root process and writes audit data to an audit log file on the local machine. Only the root and the SuperAdmin have read and write access to the locally saved audit log. Audit logs are saved in a dedicated disk partition. The default maximum size of the audit logs is 30 MB.

Linux auditd can be configured by the SuperAdmin to write audit logs additionally to the local rsyslogd that can forward the logs to an external syslog server via TLS.

The TOE generates system log records indicating the current IP connections, NTP status, CPU usage, memory usage, disk and file storage capacity, and audit storage capacity of the TOE. This data is periodically written into the TOE system log that can be forwarded to an external syslog. The TOE generates these system log records every 60 seconds. The TOE connects "calls" between VVoIP endpoints in accordance with the policies defined by FDP_IFC.1 and FDP_IFF.1. The TOE also keeps a record of various call details for each connection it processes (not call contents). A call detail records for a communication attempt between two endpoints is known as a Call Detail Record (CDR). A CDR is recorded internally and contains the following meta-data:

- calling party number (i.e. call originator),
- called party number (i.e. call receiver or terminating number),
- unique transaction sequence number,
- call disposition (e.g. call connected, call terminated, call transferred),
- call type (e.g. voice only, voice and video, text),
- call start time,
- call end time,
- call duration,
- unique identifier of the TOE,
- call routing into TOE,
- call routing out of TOE,
- time zone, and
- call release cause, if applicable (i.e. reason for termination of call).

CDRs are stored in the system internal database that does not provide direct access to external administrators or users nor to IT entities. CDRs are only accessible as download via administrative interface functions.

The TOE implements an internal clock provided by the OS to keep reliable time. Linux auditd, rsyslogd and TOE Call detail mechanism make use of the internal clock for timestamps in audit records, system log records and CDR.

The TOE allows administrators to use TOE interfaces to view all records that have been sent to the system log. System log messages are sent to the configured syslog server for longer term storage and review.

The Security audit function satisfies the following security functional requirements:

- NDcPP30e/ESC10:FAU_GEN.1: The TOE uses the Linux Audit System (auditd) to log the events and information identified by the 'Audit Events' table in section 5.1.1. The TOE also audits administrator actions that are performed through TOE interfaces. The TOE includes in each audit record a date/time stamp, an event type, an identifier of the subject responsible for the activity, the outcome of the activity, and other data specific to each event type as defined by the 'Audit Events' table in section 5.1.1. Audit records stored by ‘auditd’ are transferred to a network peer using rsyslogd over a TLS protected connection.
- ESC10:FAU_GEN.1/CDR: The TOE creates a call detail record and saves that CDR into an internal database that is available for review. The contents of a CDR are described above.
- ESC10:FAU_GEN.1/Log: The TOE creates system log records and saves those records into the same rsyslogd system that is used for audit data. The system log mechanism content and frequency are described above.
- NDcPP30e:FAU_GEN.2: The TOE identifies the responsible user for each event based on the specific administrator or network entity (identified by IP address) that caused the event.
- ESC10:FAU_SAR.1/Log: The TOE allows administrators to use TOE interfaces to view all records that are stored in the local system log.
- NDcPP30e/ESC10:FAU_STG.1: The maximum size (30Mb) and protections of the audit logs are described above in the text of this section. Audit records can be deleted only when the entire audit trail is cleared by an administrator.
- ESC10:FAU_STG.1/CDR: The CDRs are protected from disclosure and modification as described above.
- NDcPP30e:FAU_STG_EXT.1: The TOE stores audit data locally and uses rsyslogd to forward log data to an external syslog server via TLS. The TOE uses log rotation with 5 log files where the oldest is deleted when the sixth log file is started. The log rotation is triggered when the current audit log file exceeds 6 Mbyte. Thus, the TOE can store 30 Mbytes of data locally. Additionally, the TOE can store a minimum of 25 Mbytes of data locally. The kind of audit records stored are persistent.
- ESC10:FAU_VVR_EXT.1: The TOE cannot record voice or video data from calls.

6.2 Cryptographic support

The TOE is a network device that runs on a physical platform that is the Dell PowerEdge R660 system with Intel Xeon Silver 4510 processor or the PacStar 451 system with Intel Xeon E-2276ME processor. Both of these processors support the Intel RDRAND feature. The TOE utilizes the Red Hat Enterprise Linux 8 OpenSSL Cryptographic library as the cryptographic provider for all cryptographic operations. These functions have been CAVP tested and received the certificates identified by Table 6-1 Cryptographic Functions.

Requirements	Functions	Standards	Cert
FCS_CKM.1/	ECC key generation schemes using 'NIST curves' P-256, P-384	FIPS Pub 186-4	A7215
	RSA Key Generation with 3072 bits	FIPS Pub 186-4	A7215
FCS_CKM.2	Elliptic curve-based key establishment schemes	NIST SP 800-56A	A7215
FCS_COP.1/ DataEncryption	AES CTR (128 and 256 bits)	FIPS Pub 197	A7215
	AES GCM (128 and 256 bits)	NIST SP 800-38A	A7215
FCS_COP.1 / Hash	SHA-256, SHA-384, SHA-512	FIPS Pub 180-3	A7215
FCS_COP.1/KeyedHash	HMAC-SHA-256, HMAC-SHA-384	FIPS Pub 198-1 FIPS Pub 180-3	A7215
FCS_COP.1/SigGen	RSA Digital Signature Algorithm (rDSA) (modulus 2048 and 3072)	FIPS Pub 186-4	A7215
	Elliptic Curve Digital Signature Algorithm (ECDSA) with an elliptical curve size of 256 or 384 bits	FIPS Pub 186-4	A7215
FCS_RBG_EXT.1	AES-256 CTR_DRBG	FIPS SP 800-90A	A7215

Table 6-1 Cryptographic Functions

The TOE uses hashing for the following functions:

- SHA-256
  - TLS server authentication with ECDHE-RSA
  - TLS pseudorandom function (PRF) with AES128-GCM
  - SSH server and client authentication with ecdsa-sha2
  - SSH key exchange with ecdh-sha2
  - Digest Access Authentication
  - AIDE file integrity
- SHA-384
  - Certificate signature
  - TLS PRF with AES256-GCM
- SHA-512
  - Admin password hashing
  - SSH password hashing

The TOE uses key-hash message authentication with TLS and SSH (HMAC-SHA-256).

HMAC	Key Length	Block Size	Output Length
SHA-256	256 bit	512 bit	256 bit
SHA-384	384 bit	1024 bit	384 bit

Table 6-2 Keyed Hashing

The TOE provides security administrators with flexibility to control cryptographic functions. This includes control over the choice of algorithm (RSA or ECDSA), the key sizes or curves, cipher algorithms (GCM), integrity algorithms (SHA), key establishment methods, signature algorithms, and signature sizes. By using this configurability, an administrator can operate the TOE with only strong ECDSA P-384 certificates, 384-bit hashes, ecdsa-sha2-nistp384 public key authentication and ecdh-sha2-nistp384 key exchange methods. Some TOE interfaces (e.g., Logging PABX transport) are individually configured to accept specific cryptographic parameters, such as ciphersuites, curves, and Signature Algorithms. The SSH protocol is restricted by enabling the "Restricted SSH ciphers" setting. The TLS protocol for non-configurable interfaces is restricted by enabling the "Restricted TLS ciphers" setting.

When the UI setting "Restricted SSH ciphers" is NOT enabled the TOE supports SSH as follows:

> The TOE supports SSHv2 using AES-CTR with 128 and 256 bit ciphers, in conjunction with HMAC-SHA2-256 for message integrity. The TOE also supports using aes128-gcm@openssh.com and aes256-gcm@openssh.com ciphers in conjunction with the matching AES-GCM integrity algorithm. The TOE supports the ecdsa-sha2-nistp256 or ecdsa-sha2-nistp384 public key authentication methods. The TOE offers the ecdh-sha2-nistp256 or ecdh-sha2-nistp384 key exchange methods. No optional aspects of the protocol are supported.

When the UI setting "Restricted SSH ciphers" is enabled the TOE supports SSH as follows:

> The TOE supports SSHv2 using aes256-gcm@openssh.com cipher, in conjunction with the matching GCM integrity algorithm. The TOE supports ecdsa-sha2-nistp384 public key authentication method. The TOE offers the ecdh-sha2-nistp384 key exchange method. No optional aspects of the protocol are supported.

The TOE allows administrative users to perform SSHv2 authentication using password based authentication and allows administrative users to upload a public key for SSHv2 public key authentication. The TOE's SSHv2 implementation limits SSH packets to a size of 262126 bytes.

Whenever the timeout period or authentication retry limit is reached, the TOE closes the applicable TCP connection and releases the SSH session resources. As SSH packets are being received, the TOE uses a buffer to build all packet information. Once complete, the packet is checked to ensure it can be appropriately decrypted. However, if it is not complete when the buffer becomes full (262126 bytes) the packet will be dropped and the connection terminated. There is a TOE initiated rekey before 1 hour or before 1GB whichever comes first. The TOE implements default values of 64MB for the data rekey and 1 hour for the time rekey. The TOE does not offer a method for these default rekey values to be modified by the administrator.

The TOE supports the SSHv2 (compliant with RFCs 4251, 4252, 4253, 4254, 5656, 6668), TLS v1.2 (RFC 5246) secure communication protocols. KDFs based on RFC 5656 are supported.

The TOE provides support for the following TLS ciphersuites using TLSv1.2 (as defined in RFC 5246). These ciphersuites are supported for all services where the TOE is a client or a server (See Table 6-3) and are configurable only as a TLS client and as a TLS SIP server.

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

TLS connections are implemented using two different software stacks (SIP TLS stack for SIP related connections and TLS tunnel stack for the rest).

The TOE services and roles which utilize the TLS stacks are shown in Table 6-3 below.

Service	TOE Role	Manually Configured	Stack Leveraged
Push Server	Client	No	TLS tunnel
S3 Gateway Server	Client	No	TLS tunnel
Embedded Attachment Server	Server	No	TLS tunnel
Syslog	Client	Yes	TLS tunnel
Web UI	Server	No	TLS tunnel
Secure Client Authentication (SCA0)	Server	No	TLS tunnel
Additional Services (SCA1)	Server	Yes	TLS tunnel
VVoIP/SIP Calling	Server	No	SIP TLS
SIP Trunking[3]	Server	Yes	SIP TLS
	Client	Yes	SIP TLS

Table 6-3 TLS Support by Service

Scheme	SFR	Service
ECDH	FCS_SSHS_EXT.1	Remote CLI for remote administration
ECDH	FCS_TLSS_EXT.1	Secure Client Authentication (SCA0), Additional Services(SCA1), Embedded Attachment Server, VVoIP/SIP Calling, WebUI
ECDH	FCS_TLSC_EXT.1 & FCS_TLSC_EXT.2	Syslog, Push Server, S3 Gateway Server
ECDH	FCS_TLSC_EXT.1 & FCS_TLSC_EXT.2 & FCS_TLSS_EXT.1	SIP Trunking

Table 6-4 Key Establishment Schemes

Server and client (TOE) establish a shared TLS premaster secret with the TLS key exchange. All key exchange methods use the same algorithm then to convert the premaster secret into the master secret.

Together with client random (in ClientHello message) and server random (in ServerHello message), client and server generate session encryption and MAC keys from the master secret with the TLS PRF.

[3] Trunking is communication with another ESC or PABX system.

If a TLS server requests client authentication from the TOE with the ClientCertificateRequest message, the TOE answers with ClientCertificate and CertificateVerify messages. The TOE is configured by administrators with an X.509v3 certificate which it presents to a TLS server requesting authentication.

While acting as a TLS client, the TOE allows administrators to specify the peer TLS server (e.g., push server, or syslog server) by IP address or DNS name. The TOE also allows an administrator to explicitly map an IP address to a DNS name. The IP address and DNS names specified by the administrator are considered reference identifiers and are matched against the CN and SAN values in certificates received from the TLS peer. Only the Common Name field within the DN is used and the CN must be an exact match for the entire CN string. The SAN may be matched with a reference identifier that is either an IPv4 address or DNS name. A SAN value match or mismatch takes precedence over any CN value comparison. When IP addresses are used in CN as reference identifiers, the TOE performs the CN match by converting the binary representation of the peer IP address in network byte order to text representation. Canonical format according to RFC 3986 is not enforced.

The TOE supports TLS v1.2 with the ciphersuites listed above when acting as a TLS Server to administrative users and during SIP client enrollment. The VVoIP client enrollment and administrator Web UI interfaces do not require mutual authentication using TLS. Authentication on these interfaces uses other mechanisms. The TOE rejects all connection attempts using SSL and older TLS versions (1.0 and 1.1) on all interfaces where the TOE is a TLS server. The key agreement parameters of the server key exchange message are specified in the RFC 5246 (section 7.4.3) for TLSv1.2.

The TOE uses TLS (OpenSSL) for communication with VVoIP clients and registered SCA devices[4] when it is acting as a TLS server. The TOE TLS server requests client authentication by sending the ClientCertificateRequest message, and the client is expected to answer with ClientCertificate and CertificateVerify messages. This TLS authentication is certificate-based with the TOE presenting its X.509v3 certificate and expecting the client to present a valid X.509v3 certificate. The TOE will match the presented identifiers from certificates received during TLS negotiation against configured reference identifiers. Reference identifiers within a certificate are either a Distinguished Name (DN) or Subject Alternate Name (SAN). Only the Common Name field within the DN is used; and the CN must be an exact match for the entire CN string. The SAN may be matched with a reference identifier that is either an IPv4 address or DNS name.

For all TLS interfaces, the TOE performs all X.509v3 certificate validation checks as described by FIA_X509_EXT.1 and FIA_X509_EXT.2. If the client certificate is determined to not be valid or not from an expected client identity, the TOE does not establish the connection. The TOE TLS Server performs key agreement using NIST curve secp384r1. By default, the TOE acting as a TLS client presents the supported elliptic-curve extension in the Client Hello with NIST curve secp384r1.

The Cryptographic support function satisfies the following security functional requirements:

- NDcPP30e:FCS_CKM.1: The TOE performs key generation in accordance with the RSA (3072-bit) and ECDSA (P-256, P-384) schemes. The RSA keys are used in support of TLS. While the ECDSA keys are used in support of both TLS and SSH. The TOE acts as both sender and receiver (i.e., depending on the channel) schemes in TLS. The RSA scheme is used to support CSR and device authentication. By default, the Web UI will generate keys using ECDSA P-384, administrators must explicitly choose to create RSA or ECDSA P-256 curve key.
- NDcPP30e:FCS_CKM.2: The TOE performs key establishment in accordance with ECC / NIST SP 800-56A in support of TLS and SSH. In accordance with NIST SP 800-56B, the TOE does not reveal specific error details but raises generic errors during TLS handshake. See Table 6-4 for information about the key establishment schemes used for each service offered by the TOE, and Table 6-3 Support by Service to determine if the TOE is an initiator (client) or recipient (server).
- NDcPP30e:FCS_CKM.4: The TOE stores all private keys in plaintext in a secure directory that is not readily accessible to administrators. This directory is the /etc/pki directory which is protected with root or

[4] A registered SCA device may obtain services from the TOE's SCA1 interface by presenting the same certificate presented to the TOE SIP interface (e.g., a contacts list).

service access permissions. These keys are destroyed by a secure wipe operation which performs a single-pass overwrite consisting of zeroes.

- NDcPP30e:FCS_COP.1/DataEncryption: The TOE performs AES encryption and decryption in CTR and GCM mode with key sizes of 128-bits or 256-bits.
- NDcPP30e:FCS_COP.1/Hash: The TOE performs SHA-256, SHA-384, and SHA-512 cryptographic hashing in support of the functions listed above. The TOE performs SHA-256, SHA-384, and SHA-512 cryptographic hashing with message digest sizes of 256-bit, 384-bit, or 512-bit for the corresponding hashing algorithm.
- NDcPP30e:FCS_COP.1/KeyedHash: The TOE performs HMAC-SHA-256 and HMAC-SHA-384 keyed-hash message authentication with key sizes of 256-bit and 384-bit, with message digest sizes of 256-bit and 384-bit.
- NDcPP30e:FCS_COP.1/SigGen: The TOE performs ECDSA cryptographic signature services (generation and verification) for certificates based on curves P-256 and P-384. The TOE can also perform RSA cryptographic signature services (generation and verification) for certificates based on key sizes 2048-bit and 3072-bit.
- NDcPP30e:FCS_HTTPS_EXT.1: The TOE provides a Web User Interface (Web UI) for remote administration, for VVoIP endpoint registration (registration interface), and for accepting VVoIP call requests (referred to as the SCA interface). These interfaces fully support RFC 2818. The TOE acts as an HTTPS server and waits for client connections on TCP port 443, 3978, and 5061. The TOE's HTTPS server supports TLS version 1.2, and will deny connection requests from TLS clients with lower versions. The TOE ignores any certificate provided during the TLS negotiations on the Web UI and Registration interfaces because these interfaces do not authenticate the peer using a certificate, but rather authenticate the peer using a user ID and password. The TOE's SCA interface does authenticate the client using an X.509v3 certificate and does not establish a TLS connection if the certificate provided by the peer is deemed invalid. The TOE sends all HTTP data as encrypted TLS "application data".
- NDcPP30e/ESC10:FCS_NTP_EXT.1: The TOE supports NTPv4 as defined by RFC 5905. The communication channel between the TOE and NTP time source is authenticated using a SHA-256 message digest. The TOE can be configured to obtain time from multiple sources (up to 4) and does not accept time updates from broadcast or multicast addresses.
- NDcPP30e:FCS_RBG_EXT.1: The TOE leverages Intel's RdRand TRNG to provide seed material to /dev/random. OpenSSL CTR_DRBG (AES) uses 384 bits of seed material from /dev/random, ensuring at least 256 bits of entropy.
- SSH10:FCS_SSH_EXT.1 & FCS_SSHS_EXT.1: The TOE supports SSHv2 as described above.
- NDcPP30e/ESC10:FCS_TLSC_EXT.1: Depending upon service, the TOE supports TLS as shown above. When acting as a TLS client, the TOE can authenticate itself using an X.509v3 certificate to a TLS server requesting authentication. The TOE does not support certificate pinning. The TOE does support validation of certificates containing IP addresses and wildcards in DNS names for all TLS client-side connections. If the certificate presented by a TLS server cannot be validated, the TOE does not establish the connection. NIST curve secp384r1 is the only presented elliptic-curve for a TLS client side connection. Therefore, the only signature_algorithms extension presented supports the ecdsa_secp384r1 with sha384 (0x0503) algorithm. Additionally, the Signature Scheme ecdsa_secp384r1 with sha384 (0x0503) is the only signature_algorithms_cert extension presented. The TOE does not provide the ability to configure the list of supported TLS ciphersuites detailed above. In addition to this, early data extension and post-handshake client authentication according to RFC 8446 (section 4.2.6) are prohibited for use. The PJSIP stack rejects TLS 1.2 renegotiation attempts and the TLS tunnel stack supports TLS 1.2 renegotiation attempts. Finally, the TOE does not use PSKs.
- NDcPP30e/ESC10:FCS_TLSC_EXT.2: When acting as a TLS client, the TOE can authenticate itself using an X.509v3 certificate to a TLS server requesting authentication.

- NDcPP30e/ESC10:FCS_TLSS_EXT.1: The TOE supports TLS v1.2 with the ciphersuites listed above when acting as a TLS Server to administrative users and during SIP client enrollment (SCA0). The SIP client enrollment and administrator WebUI interfaces do not require mutual authentication using TLS. Authentication on these interfaces uses other mechanisms. The TOE supports TLS v1.2 with the ciphersuites listed above when acting as a TLS Server with SIP clients (i.e., SCA1 and SIP Calling) and when acting as a TLS Server with trunking peers. The TOE rejects all connection attempts using SSL and older TLS versions (1.0 and 1.1). The key agreement parameters of the server key exchange message sent by the TOE are specified in the RFC 5246 (section 7.4.3) for TLSv1.2. The TOE authenticates itself using X.509 certificates using RSA (with key sizes of 2048 bits and 3072 bits) and ECDSA (over NIST curve secp384r1 only). Key exchanges are performed using EC Diffie-Hellman key agreement over NIST curve secp384r1. The TOE provides the ability to configure the list of supported TLS ciphersuites when acting as a TLS SIP Server. The TOE does not provide the ability to configure the list of supported TLS ciphersuites for the other TLS server interfaces. Additionally, the use of the early extension data extension is prohibited. The TOE rejects all renegotiation attempts. Finally, the TOE does not use PSKs.
- NDcPP30e/ESC10:FCS_TLSS_EXT.2: When acting as a TLS Server, the TOE supports TLS communication with mutual authentication of TLS clients using X.509v3 certificates. When establishing a trusted channel, by default the TSF shall not establish a trusted channel is the client certificate is invalid. The TSF shall also not implement any administrator override mechanism. The TSF shall not establish a trusted channel if the identifier contained in a certificate does not match an expected identifier for the client. If the identifier is a Fully Qualified Domain Name (FQDN), then the TSF shall match the identifiers according to RFC 6125, otherwise the TSF shall parse the identifier from the certificate and match the identifier against the expected identifier of the client as described in the TSS. The TOE supports TLS communication with mutual authentication of TLS clients using X.509v3 certificates. If the client either does not provide a client certificate at all or the client certificate cannot be successfully validated by the TOE, the connection is rejected (‘hard fail’). The TOE presents TLS 1.2 Certificate Request messages with the ecdsa_secp384r1 with sha 384 (0x0503) and rsa_pkcs1 with sha384(0x0501) algorithms. These algorithms are supported by default and may not be configured.

6.3 User data protection

The TOE enforces the enterprise session controller SFP upon enrolled endpoints (i.e., a caller and callee). The TOE uses a SIP username to determine the identity of the parties involved in a call. The TOE ensures that the certificate presented during the TLS negotiations with the caller and callee correspond to the expected SIP users. Otherwise, any valid authenticated SIP user can connect to any other valid SIP user. There are no additional whitelist or blacklist rules, or policy overrides enforced by the TOE. The TOE supports only the SIP protocol, it does not support the H.323, SS7 or MGCP call-setup and teardown protocols. The TOE proxies streaming media data traffic between VoIP endpoints registered with the TOE as well as transmitting media data between a VoIP endpoint registered with the TOE and a remote ESC (trunking peer) if a trunking session is active and a registered VoIP endpoint is a party in a call to an endpoint on the remote ESC.

The TOE performs a secure wipe operation when deleting resources that contain private keys. The secure wipe operation is used to destroy the following files in the file system after use (via TOE interfaces):

- Appropriate private TLS keys:
  - SIP external (to SecuSUITE clients),
  - SIP trunk (to external SIP servers),
  - SCA0 TLS,
  - SCA1 TLS,
  - syslog client,
  - web portal,
  - push client,
  - S3 gateway
- Private embedded CA keys
- Private Voice SMIME keys

- SSH server host key

The secure wipe operation overwrites files to be deleted with three iterations of random data and the fourth iteration with zeros. The TOE uses ext4 file system on which the secure wipe operation is effective. An administrator is able to generate, import, or re-generate (i.e., delete a key and generate a new key for the same purpose) of each of these keys.

The User data protection function satisfies the following security functional requirements:

- ESCEP10:FDP_IFC.1: The TOE enforces the enterprise session controller SFP as described above.
- ESCEP10:FDP_IFF.1: The TOE enforces the enterprise session controller SFP as described above.
- ESCEP10:FDP_RIP.1: The TOE clears resource as described above.

6.4 Identification and authentication

The TOE supports certificate status checking using a Certificate Revocation List (CRL) as specified in RFC 5759 for X509v3 certificate validation. Revocation checking of a certificate is performed the same for all certificate validation operations. Revocation status checking is performed on leaf and intermediate CA certificates received by the TOE for authentication purposes. If the revocation status of a certificate cannot be verified because a current CRL is unavailable, the TOE will alternatively accept or reject the certificate based on the configuration of the TOE.

The following login methods are supported for administrative users:

- HTTPS Web UI. Administrators may login with a correct username and password combination.
- Local console. Administrators may login locally with a correct username and password combination.
- SSH. Administrators may login via SSH with either:
  - Correct username and password combination, or
  - Recognized ECDSA public keys

The Identification and authentication function satisfies the following security functional requirements:

- NDcPP30e:FIA_AFL.1: The TOE implements a locking feature which prevents an account from being able to successfully authenticate after a configured number of failed login attempts. Failed login attempts at the Web UI or via SSH accumulate until the TOE locks the account, and it cannot be used to login. The TOE maintains the locked status of the account for the lockout period configured by the administrator (a value between 1 and 10080 minutes, with 10 minutes being the default). The administrator can configure the lockout threshold between 3 and 7 failed attempts. The TOE also offers commands via its CLI interface which can be used to unlock an account before the configured lockout period.
- NDcPP30e:FIA_PMG_EXT.1: The TOE supports a defined character set for password-based authentication. Minimum password length is configurable by the TOE administrator; however, this minimum value must be between 8 and 32 characters in length (default is 15). Passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters, '!', '@', '#', '$', '%', '^', '&', '*', '(', ')'
- ESC10:FIA_UAU.2/TC: The TOE authenticates all SIP compatible SIP proxy or PBX telecommunication devices as endpoints before any communication is permitted. These endpoints authenticate using TLS exchanged X509v3certificates. Section 6.3 explains the authentication details.
- ESC10:FIA_UAU.2/VVoIP: The TOE communicates with VVoIP endpoints that are running the SecuSUITE client application. The TOE authenticates this VVoIP endpoint via the X.509v3certificate presented during the TLS exchange before any communication is permitted. The TOE does not support update of the software in these endpoints. Section 6.3 explains the authentication details.
- NDcPP30e:FIA_UAU.7: The TOE obscures feedback during password-based authentication.
- NDcPP30e:FIA_UIA_EXT.1: The TOE requires entities to perform identification and authentication before performing any actions other than displaying a warning banner. The TOE provides the SSH password, SSH public key, and HTTPS remote authentication mechanisms. The TOE provides the password-based and SSH public key-based local authentication mechanisms. A successful login has occurred when the administrative user is greeted with a CLI prompt (Local console and SSH) or the Home page of the HTTPS Web UI.

- NDcPP30e/ESC10: FIA_X509_EXT.1/Rev:
  Note that NDcPP30e:FIA_X509_EXT.1/Rev validates certificate status according to RFC 5280, while the ESC functions satisfy RFC 5759. Certificates are validated as part of the authentication process when they are presented to the TOE and when they are loaded into the TOE. Certificate validation is performed by two subsystems on the TOE. The central certificate validation system is responsible for TLS related checks and is used by both the SIP TLS stack and the TLS Tunnel stack. The administrative certificate validation subsystem handles certificate validation tasks related to administrative operations, such as certificate import and export. The following fields are verified as appropriate: SAN checks, CN checks, key usages, basic constraints, chain validation, and expiration status. The common name must contain a FQDN. The SAN, if present, can include IP addresses or DNS names. Wildcards in DNS names are allowed in certificates. The TOE performs validation of a certificate including the following checks as appropriate:
  - Verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field.
  - Verify a server certificate that contains a CN that does not match the reference identifier and does not contain the SAN extension is rejected.
  - Verify a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier is rejected.
  - Verify a server certificate that contains a CN that does not match the reference identifier, but does contain an identifier in the SAN that matches, is accepted.
  - Verify the certificate chain is valid.
  - Verify the expiration status of the certificate.
  - Verify the revocation status of the certificate.
- NDcPP30e/ESC10:FIA_X509_EXT.2: The TOE uses X.509v3 certificates to authenticate peer devices through the TLS protocol. Peers authenticated with X.509v3 certificates are TC, VVoIP endpoints, or various servers (i.e., syslog, push). If the TOE cannot establish a connection to determine the revocation status of a certificate, the TOE will accept or not accept the certificate as being valid depending on the configuration set by the administrator. The administrator configures a certificate for each service and those certificates are used for all further processing. Certificates are checked and if found not valid are not accepted. If a certificate contains a CRL Distribution Point, and a current version of the identified CRL cannot be obtained, then the TOE will accept or reject the certificate based on what behavior has been configured by the administrator. All certificate validity checks must pass in order for the certificate to be treated as valid.
- NDcPP30e/ESC10:FIA_X509_EXT.3: The TOE is able to generate certificate signing requests and validate the CA response. The TOE generates certificate requests with the ability to include values for Common Name, Organization, Organizational Unit, and Country. The TOE validates certificates imported into the TOE configuration during import.

6.5 Security management

The TOE provides administrators with the ability to perform management operation using either a local console or remote administrative connection (i.e., SSH protected CLI and TLS protected Web UI). Using these interfaces, the following management operations are available to an administrator to:

Management Operation	Local Console	SSH CLI	Web UI
Display the real time connection status of all VVoIP endpoints (hardware and software) and telecommunication devices	Yes	Yes	No
Clear all TSF data stored on disk	Yes	Yes	No
Configure the access banner	Yes	Yes	No
Configure the session inactivity time before session termination or locking	Yes	Yes	No
Update the TOE, and to verify the updates using digital signature capability prior to installing those updates	No	No	Yes
Configure the authentication failure parameters for FIA_AFL.1	Yes	Yes	No
Manage the cryptographic keys	Yes	Yes	Yes
Configure the cryptographic functionality	Yes	Yes	Yes

Re-enable an administrator account	Yes	Yes	No
Set the time which is used for time-stamps	Yes	Yes	No
Configure NTP	No	No	Yes
Configure the reference identifier for the peer	No	No	Yes
Manage the TOE's trust store and designate X.509v3 certificates as trust anchors	No	No	Yes
Import X.509v3 certificates to the TOE's trust store	No	No	Yes

Table 6-5 Management Operations Available on Admin Interfaces

The Security management function satisfies the following security functional requirements:

- ESC10:FMT_CFG_EXT.1: The TOE defines the following built-in, predefined accounts: secuadmin (CLI security Admin) and admin (Web Root Admin) during installation with default passwords. There is also a default 'superadmin' role that has root access. The administrator is instructed not to use that role in the evaluated configuration. Its sole purpose is disaster recovery. Prior to login, no operations are available to users attempting to open a management connection at the TOE Web UI or CLI. Upon the first login using these default accounts, the only operation the TOE allows is to specify a new password for the account. The TOE also provides a 'superadmin' account that an installation can use for disaster recovery. This account also requires a password be changed upon first login (and guidance instructs the password and account be locked away until needed).
- NDcPP30e:FMT_MOF.1/ManualUpdate: Only the authorized administrator can update the TOE.
- NDcPP30e:FMT_MTD.1/CoreData: The TOE does not allow any management functions prior to login.
- NDcPP30e:FMT_MTD.1/CryptoKeys: Security management is restricted to administrators using either the CLI or Web UI. The TOE requires system administrators to be logged in before they are allowed to set the time or configure NTP servers (which can modify time). The TOE restricts manipulation of the TOE certificates and trust store to administrators.
- NDcPP30e:FMT_SMF.1: The TOE provides administrative interfaces to perform the functions identified above.
- ESC10:FMT_SMF.1/ESC: The TOE provides administrative interfaces to perform the functions identified above.
- NDcPP30e:FMT_SMR.2: The TOE maintains administrative user roles. The TOE allows users in the system administrator or user role to connect using the HTTPS Web UI, SSH protected CLI, or local console.

6.6 Protection of the TSF

The TOE implements the Advanced Intrusion Detection Environment (AIDE) file and directory integrity checker to confirm the integrity of critical files and directories on start-up. AIDE is configured to perform the following:

- construct a database of TSF critical files
- uses OpenSSL to create a SHA-256 hash of each protected file
- perform an integrity check of protected files at start-up (utilizing OpenSSL to generate hashes for comparison to database)
- if the integrity test fails the TOE will generate an audit event

The TOE incorporates the OpenSSL FIPS Object Module as specified in section 6.2 which runs start-up self-tests to confirm the correct operation of the cryptographic functions of the TOE. OpenSSL performs the following power on self-tests:

- Software integrity
- Cryptographic Known Answer Tests (KAT)
    - AES KAT, encryption and decryption

- RSA KAT, signature generation and verification
- ECDSA PCT sign and verify
- SP 800-90A CTR_DRBG KAT
- HMAC KAT
- SHA KAT

Together, these tests ensure that the TOE is operating correctly. If any of these AIDE or OpenSSL self-tests fail, the TOE produces an audit and shuts down any related cryptographic functionality or network services.

Software updates are made available via an update server hosted within SecuSmart cloud services. The TOE does not support automatic checking for updates. Each update is a tar file signed with a private SecuSmart key dedicated for software package signing (ECDSA P-256) – the update package includes this digital signature. The SIP server has the corresponding public key in its filesystem, and only root can access this key. Using this public key the software update function of the TOE verifies the signature of the new update using the OpenSSL cryptographic library.

When the security administrator starts the software update process, the software update function:

- checks the SecuSmart signature
- unpacks the tar file
- starts the installation script included in the tar file

Installation of the update fails if the digital signature verification fails. In this case an error message is displayed to the administrator, a log event is generated, the update is aborted, and the original software remains unchanged. If an update is successful, a message is displayed to the administrator and the new software begins running. Installation of an update is not delayed and requires a non-optional system reboot to complete.

The Protection of the TSF function satisfies the following security functional requirements:

- NDcPP30e:FPT_APW_EXT.1: The TOE ensures that plaintext user passwords will not be disclosed even to administrators. Admin passwords are stored locally in a hashed form using SHA-512 hash. No interfaces are offered to administrators to view passwords in cleartext form.
- ESC10:FPT_FLS.1: The TOE can preserve a secure state after a cryptographic test failure or a TOE integrity error. Following integrity failures and cryptographic test failures, the TOE will generate an audit record documenting the failure and stop the TOE from SIP and SCA processing. For cryptographic test failures the TOE also ends support for all cryptographic operations thus stopping all remote administration. This allows administrators to abort, resolve failures, or continue operation through use of the TOE local console.
- NDcPP30e:FPT_SKP_EXT.1: The TOE stores all private keys in a secure directory that is not readily accessible to administrators. This directory is the /etc/pki directory which is protected with root or service access permissions. Security administrators cannot view contents of this directory using commands available through the CLI (and the Web UI does not present the file system abstraction to Web users).
- NDcPP30e/ESC10:FPT_STM.1: The TOE implements an internal clock provided by the OS to keep reliable time. The TOE requires the administrator to configure the use of NTPv4 to set the clock and maintain accurate time. This time is used by the TOE for audit timestamps, certificate validation activities, session timeouts, and rekeys.
- NDcPP30e:FPT_TST_EXT.1: The TOE provides self-test functions as described above.
- NDcPP30e:FPT_TUD_EXT.1: The TOE provides functions on the Web UI that will display the current running version of the TOE. The TOE performs software updates upon verification of the update using a digital signature within the update and the known SecuSmart update public key stored within the TOE as described above.

6.7 TOE access

The TOE access function satisfies the following security functional requirements:

- NDcPP30e:FTA_SSL.3: The TOE terminates SSHv2 and Web UI sessions after an administrator configured period of inactivity.
- NDcPP30e:FTA_SSL.4: TOE administrators are able to perform actions to terminate their current interactive session.
- NDcPP30e:FTA_SSL_EXT.1: The TOE terminates console sessions after a configured period of inactivity.
- NDcPP30e:FTA_TAB.1: The TOE displays a configurable advisory notice and consent warning message regarding use of the TOE when connecting via Web UI, local console, or SSHv2.

6.8 Trusted path/channels

The TOE communicates with network peers using TLS protected communication channels for connections with a VVoIP endpoint, an audit server, ESC devices for trunking, an S3 Gateway Server, and a push notification server. The TOE can act as a client to an audit server, S3 Gateway server, push server, or ESC device (i.e., SIP server for trunking). The TOE acts as a server for remote administration and SCA registration with the VVoIP endpoint, as well as when communicating with VVoIP endpoints or other ESC devices for accepting a request for trunking.

The Trusted path/channels function satisfies the following security functional requirements:

- ESC10: FTP_ITC.1 & NDcPP30e:FTP_ITC.1: In the evaluated configuration, the TOE must be configured to use TLS to ensure that all exported communication channels with network peers are sent only to the configured peer so they are not subject to inappropriate disclosure or modification. The TOE validates the peer and against the TOE configuration using the certificates presented during TLS negotiation.
- NDcPP30e:FTP_TRP.1/Admin: TOE administrators can use either the Web UI protected by HTTPS or a command line interface available through an SSHv2 connection for remote administration. Administrators logging in to the TOE Web UI must negotiate a TLS connection and then provide a valid username and password combination. Administrators do not need to present a certificate during the TLS exchange.