Security Target

Cellcrypt Server v5.0

Ref:	ST-FED-SRV-2
Ver:	0.5.1
Date:	Oct 2, 2025

Contents

Figures

Tables

Releases

Issue	Description
0.1.0	Initial release
0.1.1	Removed item under FMT_SMF_1.1 and change to RHEL 9.5
0.1.2	Moved Audited Events table. Removed item from FMT_SMF.1.1
0.2.0	Updated according to CCTL feedback
0.3.0	Removed XMPP and AIDE and made a few cosmetic updates.
0.4.0	Removed CBC algorithms and STunnel refs. Changed FIPS 140-2 to 140-3
0.4.1	Accepted all changes so far
0.5.0	Updated TSS. Added CAVP certs. Updated FMT_SMF.1 and FMT_SMF.1/ESC
0.5.1	Removed RSA key establishment from FCS_CKM.2

1. INTRODUCTION

This Security Target (ST) specifies the requirements for the Cellcrypt Server v5.0 Target of Evaluation (TOE) for evaluation and accreditation under the Common Criteria (CC).

The format and contents of this ST conforms with Common Criteria (CC), Part 1, Annex A, and Part 2.

1.1. ST and TOE Reference

Table 1 ST and TOE Reference Information

Attribute	Description
ST Title	Cellcrypt Server Security Target
ST Version	0.5.1
ST Reference	ST-FED-SRV-2
TOE Title	Cellcrypt Server v5.0
TOE Version	5.0
Date	Oct 2, 2025

1.2. Overview

Cellcrypt Server v5.0 is a secure networking device providing a core set of services for the Cellcrypt communications network. The Cellcrypt network enables end-to-end encrypted multimedia communications between users of mobile and desktop computers. Secure multimedia services include:

- Voice and video (Realtime)
- Text messaging and voice notes (store-and-forward)
- File sharing (store-and-forward)

All network communications are encrypted and interoperability with third-party networks using standards-based Realtime and store-and-forward protocols (SIP/SRTP). Cellcrypt Server v5.0 consists of several services for the management of users, devices and multimedia networks. These services are integrated in a way that takes advantage of common proxying and network security interfaces to better facilitate security analysis.

1.3. Description

1.3.1. Physical Scope of the TOE

The TOE platform consists of Red Hat Enterprise Linux 9 (64 bit) on an Intel Xeon Gold 5218R processor with Processor Algorithm Accelerators (PAA). The TOE hardware is implemented as a rack-mounted server (see Figure 1).

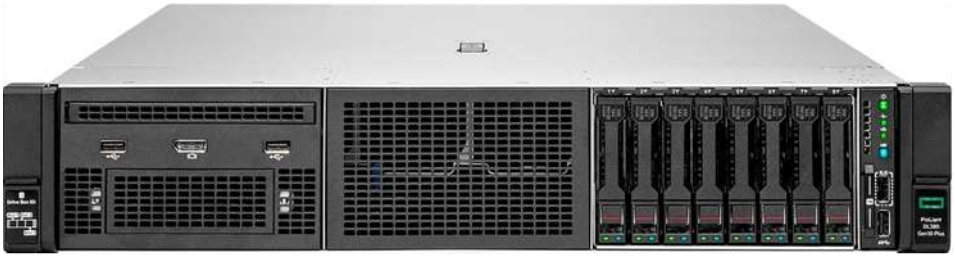

Figure 1 TOE Hardware Platform

The TOE hardware consists of a Hewlett-Packard (HP) rack-mounted server with the following specifications:

Feature	Details
Server Model	HPE ProLiant DX380 Gen10
Processor	2 x Intel Xeon Gold 5218R 2.1GHz 20 Core (Cascade Lake architecture)
Chipset family	2nd Generation Intel Xeon Scalable Processors
Memory	512GB 2667MHz DDR4 RAM DIMMs
Disk storage	2 x 2TB 3.5-inch SATA hot-plug disks Smart Array P440ar 12Gbps 2GB Cache RAID Controller
I/O slots	Embedded 4x1GbE Network Adapter; Serial Port Connector (Optional); 3 x PCIe 3.0 Slots; 2 x USB 3.0 Connectors; VGA Video Connector; Dedicated iLO 4 connectors; FlexibleLOM bay (Optional)
Ports	Front: 2 USB-3; Rear: 4 USB, video (1600 x 1200), network; Internal: 1 USB, 1 SD Card
Power Supplies	2 x 800W PSUs
Form Factor	8 SFF Drive Cage Bay (2U Server)

1.3.2. Logical Scope of the TOE

The TOE consists of several security functions that make up the logical scope of the TOE:

- Security audit
- Cryptographic support
- Data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access

- Trusted path/channels

1.3.2.1. Security Audit

All significant events occurring on the TOE e.g. warnings, errors, and particularly security-related events are logged by the TOE as audit events. The logs also include Call Detail Records (CDR's). All events are uploaded to a remote syslog server protected by a TLS link.

1.3.2.2. Cryptographic Support

All TOE cryptography is performed by the FIPS 140-3 security module with OpenSSL 3.5.1. The TOE cryptographic support includes functions supporting key management, encryption and decryption, random number generation, digital signatures, secure hashing and keyed secure hashing. Cryptographic protocol support includes TLS, SSH, HTTPS.

Table 2 Cryptographic algorithms

Functions	Standards	Certificates
Asymmetric key generation (FCS_CKM.1)		
RSA Schemes (2048, 3072, 4096-bit)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix A.1	A7364 RSA KeyGen (FIPS186-5)
ECC Schemes (P-256, P-384, P-521 curves)	FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix A.2	A7364 ECDSA KeyGen (FIPS186-5)
FFC Schemes using 'safe-prime' groups (MODP Groups 14, 16, 18)	NIST SP 800-56A Revision 3; RFC 3526	CCTL Tested
Key Establishment (FCS_CKM.2)		
ECDSA Elliptic curve-based scheme (P-256, P-384, P-521)	NIST Special Publication 800-56A Revision 3	A7364 KAS-ECC-SSC-Sp800-56Ar3
FFC Schemes using 'safe-prime' groups (MODP Groups 14, 16, 18)	NIST Special Publication 800-56A Revision 3, RFC 3526	CCTL Tested
Encryption/Decryption (FCS_COP.1/DataEncryption)		
AES in GCM mode (128, 256 bits)	AES as specified in ISO 18033-3 GCM as specified in ISO 19772	A7364 AES-GCM
AES in CTR mode (128, 256 bits)	AES as specified in ISO 18033-3 CTR as specified in ISO 10116	A7364 AES-CTR
Cryptographic signature services (Signature Generation and Verification) (FCS_COP.1/SigGen)		
RSA Digital Signature Algorithm (2048, 3072, and 4096-bit modulus)	FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5.4, using PKCS #1 v2.2 Signature Schemes RSASSA-PSS and/or RSASSAPKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	A7364 RSA SigGen (FIPS186-5) RSA SigVer (FIPS186-5)

Functions	Standards	Certificates
ECDSA Elliptic Curve Digital Signature Algorithm (P-256, P-384, P-521 curves)	FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST Recommended" [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4	A7364 ECDSA SigGen (FIPS186-5) ECDSA SigVer (FIPS186-5)
Cryptographic hashing (FCS_COP.1/Hash)		
SHA-256 (digest size 256 bits) SHA-384 (digest size 384 bits) SHA-512 (digest size 512 bits)	ISO/IEC 10118-3:2004	A7364 SHA2-256, SHA2-384, SHA2-512
Keyed-hash message authentication (FCS_COP.1/KeyedHash)		
HMAC-SHA-256 (key/digest sizes 256 bits) HMAC-SHA-384 (key/digest sizes 384 bits) HMAC-SHA-512 (key/digest sizes 512 bits)	ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"	A7364 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512
Random bit generation (FCS_RBG_EXT.1)		
CTR-DRBG (AES) – 256 bits entropy	ISO/IEC 18031:2011	A7364 Counter DRBG

1.3.2.3. Data Protection

The TOE enforces the enterprise session controller SFP on all VVoIP calls and mediates the data flow between enrolled caller and callee pairs.

1.3.2.4. Identification and Authentication

The TOE enforces role-based authorisation for all administrative access. Administrators must have a user account on the TOE with an assigned administrative role and the TOE authenticates administrators by username and password and validates the administrator's login credentials based on possession of an SSH private key. The TOE also validates X.509v3 certificate access on all TLS ports that make use of client certificates.

1.3.2.5. Security Management

In addition to command line access, the TOE also provides administrators with HTTPS web portals allowing authorized access to database functionality for administrating user and device profiles. Access to the web portals is based on username and password.

1.3.2.6. Protection of the TSF

The TOE provides comprehensive protection mechanisms to prevent unauthorised modification of its software. Built-In Self-Tests (BIST) are used to validate the integrity of all files stored on the TOE's persistent storage media and updates to the TOE software are validated using digital signatures. All file modification events are logged locally and remotely based on reliable timestamps due the use of an external NTP time source. Warning banners are used at the start of any interactive session and session inactively timers are used to terminate inactive sessions.

1.3.2.7. TOE Access

Before any Administrator access to the TOE is established the TOE displays a security banner with an advisory notice and consent warning message. All inactive Administrator user sessions are automatically terminated after a preconfigured period. Both Administrators and normal users can manually terminate sessions at any time requiring re-authentication to the TOE before establishing a new session.

1.3.2.8. Trusted Path/Channels

All communication channels on the TOE are cryptographically protected and all administrative interaction is authenticated. ESC SFP is enforced on all user communications based on authorised user subscriptions.

1.3.3. TOE Logical Architecture

The TOE software architecture, indicating the TOE logical boundary, is shown in Figure 2. Note that the TOE boundary encapsulates the entire Cellcrypt Server v5.0 and includes the operating system Red Hat Enterprise Linux 9 (64-bit) OS (RHEL 9.5).

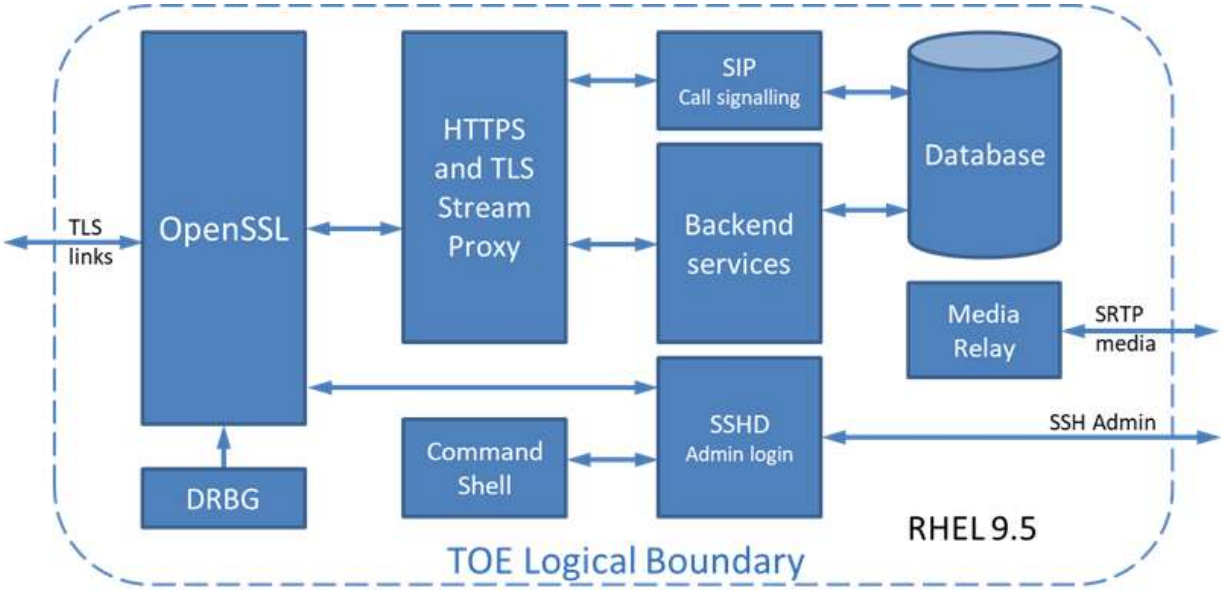

Figure 2 TOE Software Architecture

1.3.4. Network Services

The network services shown in Figure 2 are described in more detail below. The web proxy (nginx) provides TLS services for the HTTPS virtual hosts using the FIPS 140-3 security module. The other TLS hosts use the FIPS 140-3 security module directly for TLS services. Command shell access is protected with SSH also using the FIPS 140-3 security module crypto algorithms. This provides a consistent secure network interface for the TOE. The FIPS 140-3 security module with its own validated DRBG receiving seeding from the Intel RDSEED instruction. ECS and the Secure Gateway provide media conferencing services protected by SRTP. The media relay is simply a TURN service facilitating SRTP media to traverse NAT routers.

1.3.4.1. SIP Server

The SIP server provides the main ESC service facilitating all secure voice/video calls by connecting calls and signalling call progress/status using the SIP protocol in accordance with RFC 3261. In addition to normal SIP calling services, SDES key management is handled via the SIP server. The SDES key exchange occurs in the Session Description Protocol (SDP) in accordance with RFC 4566. Based on OpenSIPS 3.4.8 (TLS supported by nginx proxy).

1.3.4.2. Enterprise Management Portal (EMP)

The Enterprise Management Portal provides a secure web application for Enterprise clients to manage their users. Licenses can be purchased, assigned to users and features can be enabled or disabled for users within the Enterprise group. The Enterprise Management Portal provides advanced control of the Cellcrypt user’s devices, providing features such as remote wipe, and information about the user's device, such as operating system and version.

1.3.4.3. MY Server

The MY server is a user-oriented web service, allowing users to manage things like changing passwords, adding devices to the same account, etc. This service may be limited to administrator-only usage.

1.3.4.4. API Server

The API server is a web service mainly facilitating secure Suite B messaging. All Cellcrypt Suite B messaging clients send and retrieve secure messages via the API server. The API server also provides a general Cellcrypt client API for other housekeeping services.

1.3.4.5. Vault Server

The Vault service provides its own database (MariaDB) for storing message attachments. All file attachments are encrypted by the clients prior to uploading. The encryption key, together with the Vault attachment URI is distributed to recipients of the attachment via the Cellcrypt secure messaging service (see Cryptography section).

1.3.4.6. Enterprise Communications Service

Enterprise Communications Service (ECS) allows administrators to set up scheduled voice conferences and add users into groups. The group feature allows, not only administrators, but also users, to create communication groups. Users within groups can communicate with each other just like a Whatsapp group. Group communication features include messaging, attachments, voice notes, and normal voice conferencing.

1.3.4.7. Auxiliary service

This service provides general purpose information and configuration options for Cellcrypt client devices e.g. The latest version of the Cellcrypt client application software can be queried here.

1.3.4.8. MAP Service

The MAP service provides secure mapping information to facilitate secure navigation and location privacy for field personnel.

1.3.4.9. Secure Gateway

The Secure Gateway (SG) provides a hub for voice mixing in voice conferences. The SG can bridge calls to a standard PBX as well as standalone SIP phones. Conferences can include a mixture of Cellcrypt users, PBX SIP/analog phones as well as standalone SIP phones.

1.3.4.10. Secure Shell Host Daemon

This Secure Shell Host Daemon (SSHD) is the standard Linux OpenSSH server which will be used to provide a command terminal for remote server administration. The SSH protocol is secured using the FIPS 140-3 security module.

1.3.4.11. Audit Daemon

The audit daemon (Auditd) is a standard service on Linux providing a user-space central point for sending auditable notifications. All security and other important activities are logged using this service. Auditd is configured to provide remote audit reporting and connects to a remote audit server. The link to the remote audit server is TLS-secured using the FIPS 140-3 security module.

1.3.4.12. Network Time Protocol Daemon

The Network Time Protocol Daemon (NTPD) is a Linux service for synchronizing the server's local real-time clock with an online server's real-time clock using the standard NTP protocol [Ref 14]. The link to the remote NTP server is TLS-secured using the FIPS 140-33 security module.

1.3.4.13. ISeed Entropy gathering Utility

The ISeed utility gathers entropy using the Intel Processor's RDSEED instruction. The RDSEED instruction provides access to a high-speed NIST SP800-90B & SP 800-90C(draft) compliant entropy source. This will ensure that the FIPS 140-3 security module DRBG always has sufficient entropy even under high network usage conditions.

1.3.5. Network Deployment Diagram

Figure 3 illustrates a typical TOE deployment network layout showing interoperable access of client devices. The TOE boundary is clearly identified as including the entire Cellcrypt Server. Both Cellcrypt and other Third-party devices make use of the standards based Realtime services (SIP- RFC 3261 and SRTP – RFC 3711). Cellcrypt devices use a proprietary protocol for messaging and attachments via the API and Vault services.

Although not strictly necessary, a VPN server can be set up in a Demilitarized Zone (DMZ) to further protect the internal TOE network.

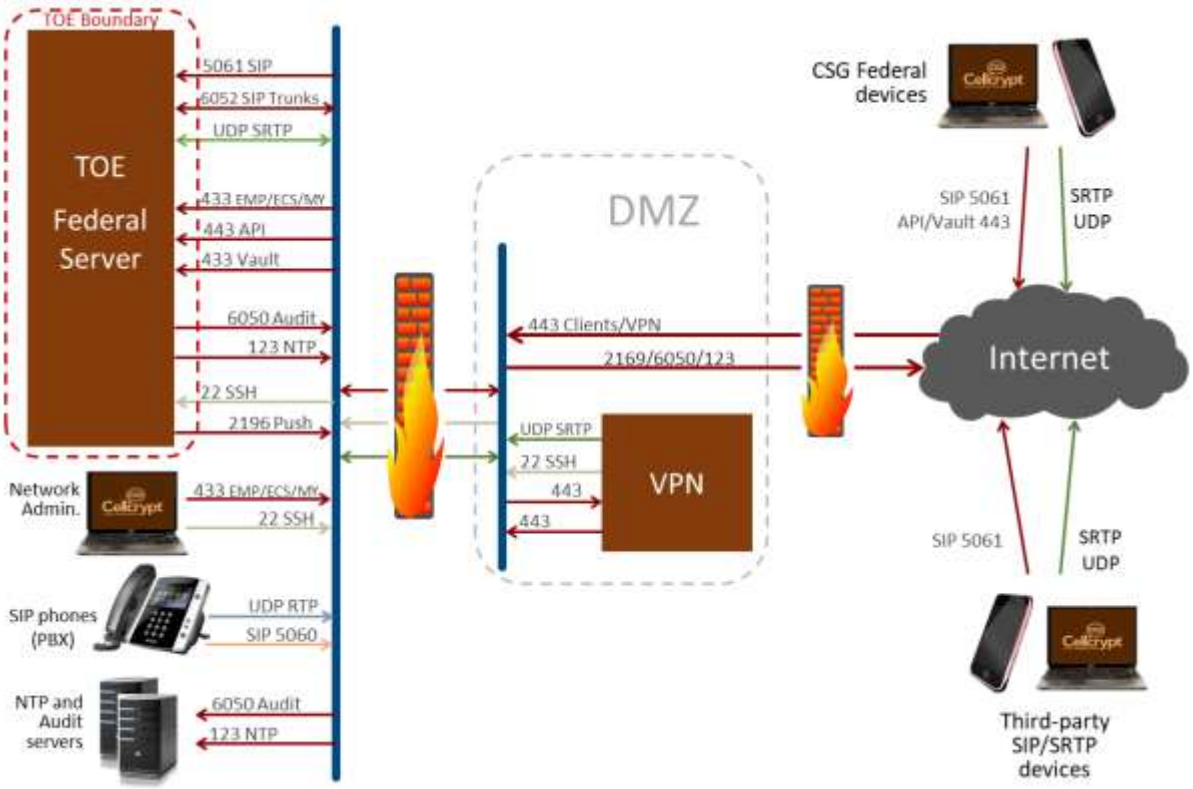

Figure 3 TOE Deployment Network Diagram

1.3.6. List of Secure Communications Ports

The Cellcrypt Server provides several secure communication ports. These are listed in Table 3 below

Table 3 Secure Communication Ports

Description	Direction	Port	Protocol
SIP Server (can route to other SIP servers)	In/Out	5061	TLS
Remote system administration	In	22	SSH
Remote audit server	Out	11514	TLS
Remote NTP Time Stamp server	Out	123	UDP
Enterprise Management Portal (EMP)	In	443	HTTPS/TLS
User Management Portal (MY)	In	443	HTTPS/TLS
Enterprise Communication System (ECS)	In	443	HTTPS/TLS
Application Services API (Text messaging)	In/Out	443	TLS
Vault Server (File attachments)	In/Out	443	TLS
Auxiliary Information	In/Out	443	TLS
TURN server	In	3478	UDP
Conferencing Hub + Media STUN/Turn relay	In	16384 – 32767	SRTP

1.3.7. TOE operational components

The TOE's operational environment consists of several components that fall outside the scope of the TOE. These non-TOE components consist of the following:

- Peer SIP server – The TOE may contact peer SIP servers from other networks over a TLS-secured link for Switch-to-Switch communications.
- Remote Audit server – The TOE can send audit logs to a remote syslog server.
- NTP Server – The TOE can contact a remote NTP time server over a TLS-secured link.
- Push Server. The TOE can send push notifications to mobile client devices by connecting to a Push Service over a TLS-secured link.

1.3.8. TOE Exclusions

No exclusions.

2. CONFORMANCE CLAIMS

This ST conforms to the requirements of Common Criteria v3.1, Release 5, including CC Part 2 extended and CC Part 3 Conformant.

This ST also conforms to the following PP-Configuration:

2.1. PP-Configuration

The TOE claims exact conformance to the following PP-Configuration:

- PP-Configuration for Network Device and Enterprise Session Controller (ESC), Version 2.0, 2024-04-25.
- This PP-Configuration includes the following components:
  - 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)
  - PP-Package: Functional Package for Secure Shell (SSH), Version 1.0 (PKG_SSH_V1.0)

Individual PP-Configuration components and all applicable technical decisions are listed below.

2.1.1. Base-PP: Network Devices

NDcPP

U.S. Government Approved Protection Profile – collaborative Protection Profile for Network Devices Version 3.0e (cpp_nd_v3.0e)

2.1.1.1. Technical Decisions for the Base-PP

Technical Decisions for cpp_nd_v3.0e listed in Table 4 below.

Table 4 CPP_NDv3.0e Technical Decisions (TD's)

TD No.	Applies	Description
0923	Yes	NIT Technical Decision: Auditable event for FAU_STG_EXT.1 in FAU_GEN.1.2
0921	Yes	NIT Technical Decision: Addition of FIPS PUB 186-5 and Correction of Assignment
0900	Yes	NIT Technical Decision: Clarification to Local Administrator Access in FIA_UIA_EXT.1.3
0899	Yes	NIT Technical Decision: Correction of Renegotiation Test for TLS 1.2

TD No.	Applies	Description
0886	Yes	Clarification to FAU_STG_EXT.1 Test 6
0880	No	NIT Decision: Removal of Duplicate Selection in FMT_SMF.1.1
0879	No	NIT Decision: Correction of Chapter Headings in CPP_ND_V3.0E
0868	No	NIT Technical Decision: Clarification of time frames in FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8
0836	Yes	NIT Technical Decision: Redundant Requirements in FPT_TST_EXT.1

2.1.2. PP-Module: Enterprise Session Controller

MOD_ESC

U.S. Government Approved Protection Profile – PP-Module for Enterprise Session Controller (ESC) Version 1.0 (mod_esc_v1.0)

2.1.2.1. Technical Decisions for the PP-Module

Technical Decisions for mod_esc_v1.0 listed in Table 4 below.

Table 5 MOD_ESCv1.0 Technical Decisions (TD's)

TD No.	Applies	Description
0835	Yes	Aligning MOD_ESC 1.0 with NDcPP 3.0E
0665	Yes	Corrections to MOD_ESC_v1.0 SFRs

2.1.3. PP-Package: SSH Protocol

[PKG_SSH]

U.S. Government Approved Protection Profile – Functional Package for SSH Version 1.0 (pkg_ssh_v1.0)

2.1.3.1. Technical Decisions for the PP-Package

Technical Decisions for pkg_ssh_v1.0 listed in Table 4 below.

Table 6 PKG_SSHv1.0 Technical Decisions (TD's)

TD No.	Applies	Description
0909	Yes	Updates to FCS_SSH_EXT.1.1 App Note in SSH FP 1.0
0777	Yes	Clarification to Selections for Auditable Events for FCS_SSH_EXT.1
0732	Yes	FCS_SSHS_EXT.1.3 Test 2 Update

TD No.	Applies	Description
0695	Yes	Choice of 128 or 256 bit size in AES-CTR in SSH Functional Package
0682	Yes	Addressing Ambiguity in FCS_SSHS_EXT.1 Tests

3. SECURITY PROBLEM DEFINITION

3.1. Threats

The following threats against the TOE are identified below. Note that these include the threats listed in the NDcPP and MOD_ESC (only the summaries are included).

3.1.1. NDcPP Threats

3.1.1.1. T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

3.1.1.2. T.WEAK_CRYPTOGRAPHY

Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

3.1.1.3. T.UNTRUSTED_COMMUNICATION_CHANNELS

Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.

3.1.1.4. T.WEAK_AUTHENTICATION_ENDPOINTS

Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.

3.1.1.5. T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

3.1.1.6. T.UNDETECTED_ACTIVITY

Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

3.1.1.7. T.SECURITY_FUNCTIONALITY_COMPROMISE

Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.

3.1.1.8. T.SECURITY_FUNCTIONALITY_FAILURE

An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.1.2. MOD_ESC Threats

3.1.2.1. T.MALICIOUS_TRAFFIC

A malformed packet is a protocol packet containing modified data not recognizable by the receiving device (e.g. TOE), or contains modified protocol packets intended to crash or cause the TOE to act in ways unintended. An attacker may attempt to use a VVoIP endpoint to send these malformed packets or malicious traffic towards the TOE in an attempt to control or crash the call control system and connected network devices. To mitigate VVoIP endpoint devices from being used to successfully launch malicious traffic, the TOE must provide encryption remedies to prevent modification of protocol packets. The TOE must also provide authentication mechanisms to prevent unauthorized VVoIP endpoints from improperly registering to the ESC for the purpose of launching malicious attacks.

3.1.3. T.NETWORK_DISCLOSURE

An attacker may attempt to "map" IP addresses of VVoIP endpoint/devices and other telecommunications equipment for the purpose of determining the organizational structure of the enterprise, providing reconnaissance for future targeted attacks.

3.1.3.1. T.UNAUTHORIZED_CLIENT

An attacker may attempt to register an unauthorized VVoIP endpoint to the TOE for the purpose of impersonating a legitimate end user device in order to gain unauthorized connectivity to other clients or active calls.

3.2. Assumptions

3.2.1.1. A.PHYSICAL_PROTECTION

The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.

3.2.1.2. A.LIMITED_FUNCTIONALITY

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

3.2.1.3. A.NO_THRU_TRAFFIC_PROTECTION

A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

3.2.1.4. A.TRUSTED_ADMINISTRATOR

The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or

intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

3.2.1.5. A.REGULAR_UPDATES

The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

3.2.1.6. A.ADMIN_CREDENTIALS_SECURE

The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.

3.2.1.7. A.RESIDUAL_INFORMATION

The Administrator must ensure 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.

3.3. Organizational Security Policies (OSP)

3.3.1. P.ACCESS_BANNER

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

3.3.2. P.SECURED_PLATFORM

Administrators in the organization ensure that general purpose computers use secure operating systems and are configured in accordance with applicable security standards.

4. SECURITY OBJECTIVES

The security objectives are based on the threats and policies listed in the previous section. Each security objective must match at least one threat or policy. Those listed below include a reproduction of security objectives listed in the NDcPP and MOD_ESC.

4.1. Security Objectives for the TOE

The following security objectives are identified for the TOE itself. The flowing list of security objectives come from the MOD_ESC.

4.1.1. O.AUTHORIZED_ADMINISTRATION

All network devices are expected to provide services that allow the security functionality of the device to be managed. The ESC, as a specific type of network device, has a refined set of management functions to address its specialized behavior.

Addressed by: FAU_STG.1 (refined from Base-PP), FAU_SAR.1/Log, FAU_STG.1/CDR, FMT_CFG_EXT.1, FMT_SMF.1/ESC, FAU_STG.1/VVR (selection-based)

4.1.2. O.MEDIA_RECORDING

The ESC has the ability to capture and store metadata for the communications it facilitates in the form of call detail records. It also may optionally capture and store audio/video recordings of these communications. This data can be used to create a record of potential unauthorized or malicious activity that is occurring on the network in which the ESC is deployed.

Addressed by: FCS_NTP_EXT.1 (refined from Base-PP), FPT_STM_EXT.1 (refined from Base-PP), FAU_GEN.1/CDR, FAU_STG.1/CDR, FAU_VVR_EXT.1, FAU_STG.1/VVR (selection-based), FAU_VVR_EXT.2 (selection-based)

4.1.3. O.SECURE_VVOIP

The ESC has the ability to securely broker VVoIP communications between endpoint devices as well as external telecommunications equipment. This involves authentication and encryption of VVoIP communications as well as the enforcement of policies that route valid traffic to its intended destination while discarding unauthorized traffic flows. The ESC optionally has the ability to function as an update server for VVoIP software/firmware to ensure that endpoint devices are securely configured.

Addressed by: FCS_DTLSS_EXT.1 (refined from Base-PP), FCS_DTLSS_EXT.2 (refined from Base-PP), FCS_NTP_EXT.1 (refined from Base-PP), FCS_TLSC_EXT.1 (refined from Base-PP), FCS_TLSC_EXT.2 (refined from Base-PP), FCS_TLSS_EXT.1 (refined from Base-PP), FCS_TLSS_EXT.2 (refined from Base-PP), FIA_X509_EXT.1 (refined from Base-PP), FIA_X509_EXT.2 (refined from Base-PP), FIA_X509_EXT.3 (refined from Base-PP), FPT_STM_EXT.1 (refined from Base-PP), FDP_IFC.1, FDP_IFF.1, FIA_UAU.2/TC, FIA_UAU.2/VVoIP, FTP_ITC.1/ESC, FPT_TUD_EXT.1/VVoIP (implementation-dependent)

4.1.4. O.SELF_PROTECTION

The ESC has the ability to capture diagnostic data about its own functionality in real-time so that anomalous behavior or failures can be diagnosed. The ESC also has the ability to respond securely if a failure state is detected so that a crash of the TOE cannot be used to facilitate malicious activity. The ESC also enforces purging of residual data so that security-relevant information cannot be obtained from a decommissioned or refurbished device.

Addressed by: FAU_GEN.1/Log , FDP_RIP.1 and FPT_FLS.1

4.1.5. O.SYSTEM_MONITORING

In order to ensure that potentially malicious activity is detected, the NDcPP requires security-relevant events to be audited. The ESC also provides security functions to support system monitoring for the functionality that it adds to the NDcPP. This includes the generation of audit records and system log data, the secure storage and ability to review stored data with authorization, and optionally the ability to suppress the generation of certain audit records to reduce log volume as a means to decrease the likelihood that a critical event is overlooked.

Addressed by: FAU_GEN.1 (refined from Base-PP), FAU_STG.1 (refined from Base-PP), FCS_NTP_EXT.1 (refined from Base-PP), FPT_STM_EXT.1 (refined from Base-PP), FAU_GEN.1/Log, FAU_SAR.1/Log, FAU_SEL.1 (selection-based)

4.2. Security Objectives for the Operational Environment

4.2.1. OE.PHYSICAL

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

4.2.2. 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 its own VM, and does not include other VMs or the VS.

4.2.3. 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.

4.2.4. 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.

4.2.5. OE.UPDATES

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

4.2.6. 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.

4.2.7. 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.

4.2.8. 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.

4.3. Security Objectives Rationale

This section describes how the assumptions, threats, and organizational security policies map to the security objectives. Note that this section only provides mappings for the security objectives defined in the MOD_ESC.

Table 7 Security Objective Rationale

Objective	Threat or OSP	Rationale
O.AUTHORIZED_ADMINISTRATION	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS (from Base-PP)	The TOE further mitigates the threat of unauthorized administrator access defined in the Base-PP by defining additional TSF management functions that are specific to ESC functionality with the expectation that they are authorized in the same manner as Base-PP management functions.
O.MEDIA_RECORDING	T.MALICIOUS_TRAFFIC	The TOE mitigates the threat of malicious traffic by recording VVoIP communications so that potential sources of malicious traffic can be identified.

Objective	Threat or OSP	Rationale
O.SECURE_VVOIP	P.SECURED_PLATFORM	The organizational security policy that expects secure configuration of environmental systems helps satisfy the secure VVoIP objective by reducing the likelihood that a malicious user has compromised a system with a VVoIP endpoint on it.
	T.MALICIOUS_TRAFFIC	The TOE mitigates the threat of malicious traffic by ensuring that all connected VVoIP and telecommunications devices are authenticated and that information will only flow through the TOE if it is validated by the TSF.
	T.NETWORK_DISCLOSURE	The TOE mitigates the threat of network disclosure by ensuring that all connected VVoIP communications are encrypted.
	T.UNAUTHORIZED_CLIENT	The TOE mitigates the threat of unauthorized client connectivity by requiring endpoint devices to be authenticated and by implementing encryption to prevent spoofing.
O.SELF_PROTECTION	T.MALICIOUS_TRAFFIC	The TOE mitigates the threat of malicious traffic by enforcing self-protection mechanisms to ensure that the TOE receiving malicious traffic will not cause it to fail to enforce its security functionality.
	T.UNDETECTED_ACTIVITY (from Base-PP)	The TOE further mitigates the threat of undetected activity defined in the Base-PP by enforcing the monitoring of behavior that is specific to ESC functionality.
O.SYSTEM_MONITORING	T.UNAUTHORIZED_CLIENT	The TOE mitigates the threat of unauthorized client access by monitoring system activity so that an audit trail of all client activity exists for future analysis if malicious activity is discovered.
	T.UNDETECTED_ACTIVITY (from Base-PP)	The TOE further mitigates the threat of undetected activity defined in the Base-PP by enforcing the monitoring of behavior that is specific to ESC functionality.
OE.SECURED_PLATFORM	P.SECURED_PLATFORM	In order to ensure that the ESC is not subject to compromise, it is important for the OS that it is installed on to be

Objective	Threat or OSP	Rationale
		secure in terms of closing unnecessary interfaces and providing appropriate security functionality. However, it is necessary for this PP-Module to make this an organizational policy in the scenario where the TOE uses a commercial third-party OS because the ESC vendor is not responsible for providing the OS and therefore has no control over its inherent functionality or administrative configuration.

5. EXTENDED COMPONENTS DEFINITION

The extended components i.e. those not defined in CC Part 2 or CC Part 3 are listed in Table 8 below. These are from the NDcPP and MOD_ESC.

Table 8 Extended Components

PP	SFR	Description
MOD_ESC	FAU_STG_EXT.1	Recording Voice and Video Call Data
NDcPP	FAU_STG_EXT.1	Protected Audit Event Storage
NDcPP	FCS_HTTPS_EXT.1	HTTPS Protocol
NDcPP	FCS_RBG_EXT.1	Random Bit Generation
PKG_SSH	FCS_SSH_EXT.1	SSH Protocol
PKG_SSH	FCS_SSHS_EXT.1	SSH Protocol - Server
NDcPP	FCS_TLSC_EXT.2	TLS Client Protocol with authentication
NDcPP	FCS_TLSS_EXT.1	TLS Server Protocol
NDcPP	FCS_TLSS_EXT.2	TLS Server Protocol with mutual authentication
NDcPP	FIA_PMG_EXT.1	Password Management
NDcPP	FIA_UIA_EXT.1	User Identification and Authentication
NDcPP	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
MOD_ESC	FIA_X509_EXT.2	X.509 Certificate Authentication
NDcPP	FIA_X509_EXT.2	X.509 Certificate Authentication
NDcPP	FIA_X509_EXT.3	X.509 Certificate Requests
MOD_ESC	FMT_CFG_EXT.1	Secure by Default Configuration
NDcPP	FPT_APW_EXT.1	Protection of Administrator Passwords
NDcPP	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
NDcPP	FPT_STM_EXT.1	Reliable Time Stamps
NDcPP	FPT_TST_EXT.1	TSF testing
NDcPP	FPT_TUD_EXT.1	Trusted update
NDcPP	FTA_SSL_EXT.1	TSF-initiated Session Locking

6. SECURITY FUNCTIONAL REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE and/or Platform.

6.1. Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations performed in the ST:

- Unaltered SFRs are stated in the form used in [CC2] or their extended component definition (ECD);
- Refinement: indicated with **bold text** and ~~strikethroughs~~;
- Assignment: Indicated with *italicized* text;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with ***underlined bold italics*** text.

Note: The font conventions for Assignments and Assignments within a Selection overlap with existing NDcPP, MOD_ESC or formatting.

The ST does not perform any iteration operations.

6.2. Security Functional Requirements

6.2.1. Summary

The Security Functional Requirements (SFR's) are specified in this section. The SFR's are summarized in Table 9 below.

Table 9 SFR Summary

Class Name	Component Identification	Component Name
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.1/CDR (MOD_ESC)	Audit Data Generation - CDR (Call Detail Record)
	FAU_GEN.1/Log (MOD_ESC)	Audit Data Generation - Log (System Log)
	FAU_GEN.2	User identity association
	FAU_SAR.1/Log (MOD_ESC)	Audit Review - Log (System Log)
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.1/CDR (MOD_ESC)	Protected Audit Trail Storage (Call Detail Record)
	FAU_STG_EXT.1	External Audit Event Storage
	FAU_VVR_EXT.1 (MOD_ESC)	Recording voice and video call data
	FAU_SEL.1 (MOD_ESC)	Selective Audit

Class Name	Component Identification	Component Name
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed-hash Algorithm)
	FCS_RBG_EXT.1	Random Bit Generation
	FCS_HTTPS_EXT.1	HTTPS Protocol
	FCS_SSH_EXT.1 (PKG_SSH)	SSH Protocol
	FCS_SSHS_EXT.1 (PKG_SSH)	SSH Protocol - Server
	FCS_TLSC_EXT.1	TLS Client Protocol without mutual authentication
	FCS_TLSC_EXT.2	TLS Client Protocol with mutual authentication
	FCS_TLSS_EXT.1	TLS Server Protocol without mutual authentication
	FCS_TLSS_EXT.2	TLS Server Protocol with mutual authentication
	FCS_NTP_EXT.1	NTP Protocol
FIA: Identification and Authentication	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU.2/TC (MOD_ESC)	User Authentication before Any Action - TC (Telecommunications Devices)
	FIA_UAU.2/VVoIP (MOD_ESC)	User Authentication before Any Action - VVoIP (VVoIP Endpoints)
	FIA_UAU.7	Protected Authentication Feedback
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
	FIA_X509_EXT.2 (NDCPP+MOD_ESC)	X.509 Certificate Authentication
	FIA_X509_EXT.3	X.509 Certificate Requests
	FIA_AFL.1	Authentication Failure Management
	FIA_PMG_EXT.1	Password Management
FMT: Security management	FMT_MOF.1/ManualUpdate	Management of SF behaviour
	FMT_MOF.1/Services	Management of Security Functions behaviour

Class Name	Component Identification	Component Name
	FMT_MOF.1/Functions	Management of Security Functions Behaviour
	FMT_MTD.1 (NDCPP+MOD_ESC)	Management of TSF Data
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_MTD.1/CryptoKeys	Management of TSF Data
	FMT_SMF.1 (NDCPP+MOD_ESC)	Specification of Management Functions
	FMT_SMR.2 (NDCPP+MOD_ESC)	Restrictions on Security Roles
	FMT_CFG_EXT.1 (MOD_ESC)	Secure by Default Configuration
FPT: Protection of the TSF	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	FPT_STM.1 (MOD_ESC)	Reliable Time Stamps
	FPT_STM_EXT.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF testing
	FPT_TUD_EXT.1	Trusted update
	FPT_FLS.1 (MOD_ESC)	Failure with Preservation of a Secure State
	FPT_APW_EXT.1	Protection of Administrator Passwords
FTA: TOE Access	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1 (NDCPP+MOD_ESC)	Inter-TSF trusted channel
	FTP_TRP.1/Admin	Trusted Path
FDP: User data protection	FDP_IFC.1 (MOD_ESC)	Subset Information Flow Control
	FDP_IFF.1 (MOD_ESC)	Information Flow Control Functions
	FDP_RIP.1 (MOD_ESC)	Subset Residual Information Protection

6.2.2. FAU_GEN.1 Audit data generation

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 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).*
- Resetting passwords (name of related Administrator account shall be logged), no other actions.

d) *Specifically defined auditable events listed in Table 13.*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, *information specified in column three of Table 13*.

6.2.3. FAU_GEN.1/CDR Audit Data Generation (Call Detail Record) (MOD_ESC)

FAU_GEN.1.1/CDR[1] – The TSF shall be able to generate a **call detail** record **(CDR)** for **communications between VVoIP endpoints that are established by the TOE**.

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**

]

6.2.4. FAU_GEN.1/Log Audit Data Generation (System Log) (MOD_ESC)

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, power status.**

[1] In accordance with TD 0665

FAU_GEN.1.2/Log[2] – 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 System Log Events Table (Table 10)*].

Table 10 System Event Logs

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.
Power status (conditional)	Status (on or off).

6.2.5. FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.6. FAU_SAR.1/Log Audit Review (System Log) (MOD_ESC)

FAU_SAR.1.1/Log The TSF shall provide [*Security Administrators*] with the capability to read *list of audit information* from the **system log** records.

FAU_SAR.1.2/Log The TSF shall provide the **system log** records in a **real-time first-in first-out scrolling method. (MOD_ESC)**

6.2.7. FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

[2] In accordance with TD 0665

6.2.8. FAU_STG.1/CDR Protected Audit Trail Storage (Call Detail Record) (MOD_ESC)

FAU_STG.1.1/CDR The TSF shall protect the stored **call detail records** from unauthorized **disclosure and** deletion.

FAU_STG.1.2/CDR[3] The TSF shall be able to [*prevent*] unauthorized modifications to the stored **call detail records**.

6.2.9. FAU_STG_EXT.1 Protected Audit Event Storage

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.

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.

FAU_STG_EXT.1.3 The TSF shall maintain log file, database of audit records in the event that an interruption of communication with the remote audit server occurs.

FAU_STG_EXT.1.4 The TSF shall be able to store persistent audit records locally with a minimum storage size of *1 million records*.

FAU_STG_EXT.1.5 The TSF shall overwrite previous audit records according to the following rule: ***overwrite starting from oldest records, alert administrator well in advance*** when the local storage space for audit data is full.

FAU_STG_EXT.1.6 The TSF shall provide the following mechanisms for administrative access to locally stored audit records ability to view locally.

6.2.10. FAU_VVR_EXT.1 Recording Voice and Video Call Data (MOD_ESC)

FAU_VVR_EXT.1.1 The TSF shall not have the capability to record voice and video call data.

6.2.11. FAU_SEL.1 Selective Audit (MOD_ESC)

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) object identity, user identity, subject identity, host identity, event type;

b) *time stamp, user agent*.

6.2.12. FCS_CKM.1 Cryptographic Key Generation (Refinement)

FCS_CKM.1.1 The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

[3] In accordance with TD 0665

- RSA schemes using cryptographic key sizes ***of 2048-bit or greater*** 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, P-521] 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;
- FFC Schemes using ‘safe-prime’ groups that meet the following: “NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526, RFC 7919].

~~] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].~~

6.2.13. FCS_CKM.2 Cryptographic Key Establishment (Refinement)

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”;
- FFC Schemes using ‘safe-prime’ groups that meet the following: “NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526].

~~] that meets the following: [assignment: *list of standards*].~~

6.2.14. FCS_CKM.4 Cryptographic Key Destruction

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 a new value of the key;

]

that meets the following: *No Standard*.

6.2.15. FCS_COP.1/DataEncryption[4] Cryptographic Operation (AES Data Encryption/Decryption)

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 ISO10116, GCM as specified in ISO 19772.

6.2.16. FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)[5,6]

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 greater***,
- For ECDSA: ***256 bits or greater***

]

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, P-521 curves that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST Recommended curves” ~~[selection: P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4,~~; 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.

].

[4] In accordance with TD 0695
[5] In accordance with TD 0695
[6] In accordance with TD 0921

6.2.17. FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)[7]

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 cryptographic key sizes [*assignment: cryptographic key sizes*]~~ and **message digest sizes 256, 384, 512 bits** that meet the following: *ISO/IEC 10118-3:2004*.

6.2.18. FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)[8]

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, HMAC-SHA-512, implicit and cryptographic key sizes *[256, 384 and 512 bits used in HMAC]* **and message digest sizes 256, 384, 512 bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2".*

6.2.19. FCS_RBG_EXT.1 Random Bit Generation

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).

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from ***One*** platform-based noise source with a minimum of 256 bits of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

6.2.20. FCS_HTTPS_EXT.1 HTTPS Protocol (PKG_SSH)

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS ~~protocol~~ using TLS.

6.2.21. FCS_SSH_EXT.1 SSH Protocol

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, 4256, 4344, 5647, 5656, 6668, 8308, 8332, no other RFCs and [*no other standard*].

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): [selection:
    - rsa-sha2-256 (RFC 8332),
    - rsa-sha2-512 (RFC 8332),

[7] In accordance with TD 0695
[8] In accordance with TD 0695

- ecdsa-sha2-nistp256 (RFC 5656),
- ecdsa-sha2-nistp384 (RFC 5656),
- ecdsa-sha2-nistp521 (RFC 5656)

]

] and no other methods.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*256K bytes*] in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 The TSF shall protect data in transit from unauthorised 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.

FCS_SSH_EXT.1.5 The TSF shall protect data in transit from modification, deletion, and insertion using: [

- hmac-sha2-256 (RFC 6668),
- hmac-sha2-512 (RFC 6668),
- implicit

] and no other mechanisms.

FCS_SSH_EXT.1.6 The TSF shall establish a shared secret with its peer using: [

- diffie-hellman-group14-sha256,
- diffie-hellman-group16- sha512,
- diffie-hellman-group18-sha512
- ecdh-sha2-nistp256 (RFC 5656),
- ecdh-sha2-nistp384 (RFC 5656),
- ecdh-sha2-nistp521 (RFC 5656)

] and no other mechanisms.

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*.

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.

6.2.22. FCS_SSHS_EXT.1 SSH Protocol – Server (PKG_SSH)

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

- rsa-sha2-256 (RFC 8332),
- rsa-sha2-512 (RFC 8332),
- ecdsa-sha2-nistp256 (RFC 5656),
- ecdsa-sha2-nistp384 (RFC 5656),
- ecdsa-sha2-nistp521 (RFC 5656)

].

6.2.23. FCS_TLSC_EXT.1.1 TLS Client Protocol with authentication (MOD_ESC)

FCS_TLSC_EXT.1.1[9] The TSF shall implement **TLS 1.2 (RFC 5246) and** TLS 1.3 (RFC8446) supporting the following ciphersuites: (see Table 11 and Table 12) and no other ciphersuites.

Table 11 TLS 1.2 Ciphersuites

Cipher suite	Code	RFC
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xC02C	RFC 5289
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xC030	RFC 5289
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009F	RFC 5288
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xC02B	RFC 5289
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xC02F	RFC 5289
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x009E	RFC 5288

Table 12 TLS 1.3 Ciphersuites

Cipher suite	Code	RFC
TLS_AES_256_GCM_SHA384	0x1302	RFC 8446
TLS_AES_128_GCM_SHA256	0x1301	RFC 8446

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches the reference identifier per RFC 6125 section 6.

FCS_TLSC_EXT.1.3 The TSF shall not establish a trusted channel if the server certificate is invalid without any administrator override mechanism.

[9] In accordance with TD 0835

FCS_TLSC_EXT.1.4 The TSF shall present the Supported Groups Extension with the following curves/groups: secp256r1, secp384r1, secp521r1 and no other curves/groups in the Client Hello.

FCS_TLSC_EXT.1.5 The TSF shall [

- present the signature algorithms extension with support for the following algorithms:
  - rsa_pkcs1 with sha256(0x0401),
  - rsa_pkcs1with sha384(0x0501),
  - rsa_pkcs1 with sha512(0x0601),
  - ecdsa_secp256r1 with sha256(0x0403),
  - ecdsa_secp384r1 with sha384(0x0503),
  - ecdsa_secp521r1 with sha512(0x0603),

] *and no other algorithms;*

FCS_TLSC_EXT.1.6 The TSF provides, the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.

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.

FCS_TLSC_EXT.1.8 The TSF shall only use PSKs in TLS 1.3 session resumption with forward secrecy.

FCS_TLSC_EXT.1.9 The TSF shall reject [TLS 1.2] renegotiation attempts.

6.2.24. FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

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

6.2.25. FCS_TLSS_EXT.1 TLS Server Protocol (MOD_ESC)

FCS_TLSS_EXT.1.1[10] The TSF shall implement **TLS 1.2 (RFC 5246) and** TLS 1.3 (RFC 8446) and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: (see Table 11 and Table 12) and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall authenticate itself using X.509 certificate(s) using RSA with key size [2048, 3072, 4096] bits; ECDSA over NIST curves [secp256r1, secp384r1, secp521r1] and no other curves].

FCS_TLSS_EXT.1.3 The TSF shall perform key exchange using: [

- RSA key establishment with key size [2048 bits, 3072 bits, 4096] bits;
- EC Diffie-Hellman key agreement over NIST curves [secp256r1, secp384r1, secp521r1] and no other curves;

[10] In accordance with TD 0835

- Diffie-Hellman parameters [of size 2048 bits, of size 3072 bits, of size 4096 bits]

].

FCS_TLSS_EXT.1.4 The TSF shall support no session resumption.

FCS_TLSS_EXT.1.5 The TSF provides the ability to configure the list of supported ciphersuites as defined in FCS_TLSS_EXT.1.1.

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

- Early data extension

FCS_TLSS_EXT.1.7 The TSF shall not use PSKs.

FCS_TLSS_EXT.1.8 The TSF shall reject [TLS 1.2. TLS 1.3] renegotiation attempts.

6.2.26. FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication (MOD_ESC)

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 FCS_TLSS_EXT.2.2) ('hard fail')

].

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.

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.

FCS_TLSS_EXT.2.4 The TSF shall present a TLS 1.2, TLS 1.3 Certificate Request message containing the following algorithms: [

- rsa_pkcs1 with sha256(0x0401),
- rsa_pkcs1 with sha384(0x0501),
- rsa_pkcs1 with sha512(0x0601),
- ecdsa_secp256r1 with sha256(0x0403),
- ecdsa_secp384r1 with sha384(0x0503),
- ecdsa_secp521r1 with sha512(0x0603)

];

6.2.27. FCS_NTP_EXT.1 NTP Protocol

FCS_NTP_EXT.1.1 The TSF shall only use only the following NTP version(s) NTP v4 (RFC 5905).

FCS_NTP_EXT.1.2 The TSF shall update its system time using:

- Authentication using SHA1 as the message digest algorithm(s).

FCS_NTP_EXT.1.3 The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

FCS_NTP_EXT.1.4 The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

6.2.28. FIA_UIA_EXT.1 User Identification and Authentication

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.

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.

FIA_UIA_EXT.1.3[11] 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.

FIA_UIA_EXT.1.4 The TSF shall authenticate any administrative user's claimed identity according to each authentication mechanism specified in FIA_UIA_EXT.1.3.

6.2.29. FIA_UAU.2/TC User Authentication before Any Action (Telecommunications Devices) (MOD_ESC)

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**.

6.2.30. FIA_UAU.2/VVoIP User Authentication before Any Action (VVoIP Endpoints) (MOD_ESC)

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**.

6.2.31. FIA_UAU.7 Protected Authentication Feedback (Refinement)

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the **administrative**

[11] In accordance with TD0900

user while the authentication is in progress **at the local console**.

6.2.32. FIA_X509_EXT.1/Rev X.509 Certificate Validation

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 the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5.
- 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 DTLS/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 DTLS/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.*

FIA_X509_EXT.1.2/Rev The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

6.2.33. FIA_X509_EXT.2 X.509 Certificate Authentication (NDCPP+MOD_ESC)

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for **TLS,** HTTPS and code signing for system software updates, ***VVoIP endpoint registration*****,** no additional uses.

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.

6.2.34. FIA_X509_EXT.3 X.509 Certificate Requests

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 device-specific information, Common Name, Organization, Organizational Unit, Country.

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

6.2.35. FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within *6* unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

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 Administrator defined time period has elapsed.

6.2.36. FIA_PMG_EXT.1 Password Management

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 *9* and *20* characters.

6.2.37. FMT_MOF.1 Management of functions in TSF

FMT_MOF.1.1/ManualUpdate The TSF shall restrict the ability to enable the functions *to perform manual updates to Security Administrators*.

6.2.38. FMT_MOF.1/Services Management of Security Functions Behaviour

FMT_MOF.1.1/Services The TSF shall restrict the ability to **start and stop** ~~the functions~~ services to *Security Administrators*.

6.2.39. FMT_MOF.1/Functions Management of Security Functions Behaviour

FMT_MOF.1.1/Functions The TSF shall restrict the ability to modify the behaviour of the functions transmission of audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full to *Security Administrators*.

6.2.40. FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to manage the TSF data to Security Administrators.

6.2.41. FMT_MTD.1/CoreData Management of TSF Data

FMT_MTD.1.1/CoreData The TSF shall restrict the ability to manage the *TSF data to Security Administrators.*

6.2.42. FMT_MTD.1/CryptoKeys Management of TSF Data

FMT_MTD.1.1/CryptoKeys The TSF shall restrict the ability to *manage* the cryptographic keys to *Security Administrators*.

6.2.43. FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1[12] 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 session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using* digital signature *capability prior to installing those updates;*
- [
    - Ability to start and stop services;
    - Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);
    - Ability to modify the behaviour of the transmission of audit data to an external IT entity;
    - Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;
    - Ability to manage the cryptographic keys;
    - Ability to configure the cryptographic functionality;
    - Ability to configure thresholds for SSH rekeying;
    - Ability to re-enable an Administrator account;
    - Ability to set the time which is used for time-stamps;
    - Ability to configure NTP;
    - 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 authentication failure parameters for FIA_AFL.1;
    - Ability to manage the trusted public keys database;
    - Ability to manage the public key or certificate used to validate the digital
    - update;
    - No other capabilities

  ].

[12] In accordance with TF 0665

6.2.44. FMT_SMF.1/ESC Specification of Management Functions (ESC) (MOD_ESC)

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;
- [
    - Ability to configure the password policy;
    - Ability to specify the set of audited events;
    - Ability to configure the behavior of the TOE in response to a self-test failure;
    - No other capabilities
-].

6.2.45. FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator.*

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

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.

6.2.46. FMT_CFG_EXT.1 Secure by Default Configuration (MOD_ESC)

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.

FMT_CFG_EXT.1.2 The **TSF** shall be configured by default with permissions which protect it and its data from unauthorized access.

6.2.47. FPT_SKP_EXT.1 Protection of TSF Data

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

6.2.48. FPT_STM_EXT.1 Reliable Time Stamps

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

FPT_STM_EXT.1.2 The TSF shall synchronise time with an NTP server.

6.2.49. FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1[13] 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;
- ~~During start-up (~~pPrior to providing any cryptographic service~~s)~~ and, on-demand, ***[the following tests can be run:***
  - ***System Power On Self-Test (POST);***
  - ***Cryptography self-test***

  ]

  to verify correct operation of cryptographic implementation necessary to fulfil the TSF;
- No other.

]

To demonstrate the correct operation of the TSF

FPT_TST_EXT.1.2 The TSF shall respond to ***[the following failures:***

- ***System Power On Self-Test (POST);***
- ***Cryptography self-test;***
- ***hardware components that affect the proper functioning of the TOE***

]

by ***[stopping the main service]***.

6.2.50. FPT_TUD_EXT.1 Trusted Update

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 the most recently installed version of the TOE firmware/software.

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.

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.

6.2.51. FPT_FLS.1 Failure with Preservation of a Secure State (MOD_ESC)

FPT_FLS.1.1 The TSF shall preserve a secure state **through the following means: stop the main service** when the following types of failures occur: [*failure of self-tests defined in FPT_TST_EXT.1, failure of* ***hardware components that affect the proper functioning of the TOE***].

6.2.52. FPT_APW_EXT.1 Protection of Administrator Passwords

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

[13] In accordance with TD 0836

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

6.2.53. FTA_SSL.3 TSF-initiated Termination (Refinement)

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

6.2.54. FTA_SSL.4 User-initiated Termination (Refinement)

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

6.2.55. FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, terminate the session

after a Security Administrator-specified time period of inactivity.

6.2.56. FTA_TAB.1 Default TOE Access Banners (Refinement)

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

6.2.57. FTP_ITC.1 Inter-TSF Trusted Channel (Refinement) (NDCPP+MOD_ESC)

FTP_ITC.1.1 The TSF **shall be capable of using HTTPS, TLS to** provide a **trusted** communication channel between itself and ~~another trusted IT product~~ **authorized IT entities supporting the following capabilities: audit server, *VVoIP endpoints (for protection of signalling protocols), other ESC devices (for SIP trunking), TLS Software Applications: HTTPS/TLS Clients on authorized End User Devices (EUDs)*** 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 **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2 The TSF shall permit ~~another trusted IT product,~~ the TSF, **the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for ***remote auditing; communication with other ESC devices.***

6.2.58. FTP_ITC.1/ESC Inter-TSF Trusted Channel (ESC Communications)

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), TLS Software Applications: HTTPS/TLS Clients on authorized End User Devices (EUDs)** that is logically distinct from other communication channels and provides

assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/ESC The TSF shall permit [*the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3/ESC The TSF shall initiate communication via the trusted channel for ***remote auditing; communication with other ESC devices***.

6.2.59. FTP_TRP.1/Admin Trusted Path (Refinement)

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** ~~users~~ 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**.

FTP_TRP.1.2/Admin The TSF shall permit remote **Administrators** ~~users~~ to initiate communication via the trusted path.

FTP_TRP.1.3/Admin The TSF shall require the use of the trusted path for *initial Administrator authentication and all remote administration actions*.

6.2.60. FDP_IFC.1 Subset Information Flow Control (MOD_ESC)

FDP_IFC.1.1 The TSF shall enforce the [*enterprise session controller SFP*] on [*caller-callee pairs attempting to communicate through the TOE*].

6.2.61. FDP_IFF.1 Information Flow Control Functions (MOD_ESC)

FDP_IFF.1.1 The TSF shall enforce the [*enterprise session controller SFP*] based on the following types of subject and information security attributes: *method by which the TSF identifies each endpoint for a call* **using the following call control protocols:** SIP **and** no other call control protocols.

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*].

FDP_IFF.1.3 The TSF shall enforce the [*additional information flow control SFP rules: no additional rules*].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: **[*SIP caller registration*]**.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **[*SIP caller registration*].**

6.2.62. FDP_RIP.1 Subset Residual Information Protection (MOD_ESC)

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: *disk storage location(s) erased by the TSF during factory reset or other wipe operation*.

Table 13 Auditable Events

Requirement	Auditable Events	Additional Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	Configuration of local audit settings.	Identity of account making changes to the audit configuration.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_RBG_EXT.1	None.	None.
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None.
FMT_MTD.1/CoreData	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	None.
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).

Requirement	Auditable Events	Additional Record Contents
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions.	• None. • None. • Reason for failure
FTP_TRP.1/Admin	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions.	• None. • None. • Reason for failure
FCS_TLSC_EXT.2	None	None
FCS_TLSS_EXT.2	Failure to authenticate the client	Reason for failure
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session	Reason for failure
FCS_NTP_EXT.1	• Configuration of a new time server • Removal of configured time server	Identity if new/removed time server
FCS_SSH_EXT.1	Failure to establish an SSH session	Reason for failure and Non-TOE endpoint of attempted connection (IP Address)
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure
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

Requirement	Auditable Events	Additional Record Contents
		removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None	None
FIA_X509_EXT.3	None	None
FMT_MOF.1/Services	None	None
FMT_MTD.1/CryptoKeys	None	None
FMT_MOF.1/Functions	None	None
FPT_APW_EXT.1	None.	None.
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).
FIA_UAU.2/VVoIP	Successful or failed registration of VVoIP endpoint/device	ID of Administrator that attempt to register VVoIP endpoint to TOE (if available); IP-address of device where registration attempt was initiated (if available); IP-address of VVoIP endpoint that attempt to register to ESC (if available).
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.
FMT_SMF.1/ESC	Modification of TOE Call Detail Records (CDR)	ID of Administrator attempting to query or modify database; IP-address of device where database query was initiated;

Requirement	Auditable Events	Additional Record Contents
		the exact SQL command/instruction that was executed.
FMT_SMF.1/ESC	Enabling/disabling VVoIP endpoint/device features	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.

6.3. NDcPP Security Assurance Requirements

The NDcPP Security Assurance Requirements, as reproduced from the NDcPP protection profile, are summarized in Table 14 below.

Table 14 Security Assurance Requirements

Assurance Class	Assurance Components
Security Target (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives for the operational environment (ASE_OBJ.1)
	Stated security requirements (ASE_REQ.1)
	Security Problem Definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Basic functional specification (ADV_FSP.1)
Guidance Documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life Cycle Support (ALC)	Labelling of the TOE (ALC_CMC.1)
	TOE CM coverage (ALC_CMS.1)
Tests (ATE)	Independent testing – conformance (ATE_IND.1)
Vulnerability Assessment (AVA)	Vulnerability survey (AVA_VAN.1)

6.4. TOE ESC Security Functional Requirements Rationale

Table 15 provides justification for each security objective for the TOE, showing that the SFRs are suitable to meet and achieve the security objectives.

Table 15 SFT-Objective Rationale

Objective	Addressed By	Rationale
O.AUTHORIZED_ADMINISTRATION	FAU_STG.1 (refined from Base-PP)	This SFR supports the objective by ensuring that stored audit data is protected from unauthorized access.
	FAU_SAR.1/Log	This SFR supports the objective by requiring the TSF to ensure that only authorized users can view system log data.
	FAU_STG.1/CDR	This SFR supports the objective by requiring the TSF to ensure that only authorized users can view stored call detail records.
	FMT_CFG_EXT.1	This SFR supports the objective by defining a secure default configuration for the TOE so that a user cannot access the TSF or its data using default or blank credentials.
	FMT_SMF.1/ESC	This SFR supports the objective by defining the authorized management functions supported by the TOE.
	FAU_STG.1/VVR (selection-based)	This SFR supports the objective by requiring the TSF to ensure that only authorized users can access stored voice/video recordings, if generated by the TSF.
O.MEDIA_RECORDING	FCS_NTP_EXT.1 (refined from Base-PP)	This SFR supports the objective by requiring the TSF to support NTP communications to obtain reliable time data that is used for accurate recording of call metadata.
	FPT_STM_EXT.1 (refined from Base-PP)	This SFR supports the objective by requiring the TSF to synchronize with an NTP server for reliable time data that is used for accurate recording of call metadata.
	FAU_GEN.1/CDR	This SFR supports the objective by requiring the TSF to generate call detail records of VVoIP communications.
	FAU_STG.1/CDR	This SFR supports the objective by requiring the TSF to securely store call detail records.
	FAU_VVR_EXT.1	This SFR supports the objective by allowing the TOE to claim whether or not it performs voice/video recording of VVoIP communications.

Objective	Addressed By	Rationale
O.SECURE_VVOIP	FCS_DTLSS_EXT.1 (refined from Base-PP)	This SFR supports the objective by requiring the use of DTLS to protect transmitted voice/video media if this is the chosen method for securing it.
	FCS_DTLSS_EXT.2 (refined from Base-PP)	This SFR supports the objective by requiring any implementation of DTLS to use mutual authentication.
	FCS_TLSC_EXT.1 (refined from Base-PP)	This SFR supports the objective by requiring TLS for SIP and H.323 communications.
	FCS_TLSC_EXT.2 (refined from Base-PP)	This SFR supports the objective by requiring TLS for SIP and H.323 communications.
	FCS_TLSS_EXT.1 (refined from Base-PP)	This SFR supports the objective by requiring TLS for SIP and H.323 communications.
	FCS_TLSS_EXT.2 (refined from Base-PP)	This SFR supports the objective by requiring TLS for SIP and H.323 communications.
	FIA_X509_EXT.1/Rev (refined from Base-PP)	This SFR supports the objective by requiring X.509 validation in support of establishing TLS communications.
	FIA_X509_EXT.2 (refined from Base-PP)	This SFR supports the objective by requiring X.509 authentication in support of establishing TLS communications.
	FIA_X509_EXT.3 (refined from Base-PP)	This SFR supports the objective by requiring the TSF to be able to request an X.509 certificate that it can present to external entities when establishing cryptographic communications.
	FPT_STM_EXT.1 (refined from Base-PP)	This SFR supports the objective by requiring the TSF to synchronize with an NTP server for reliable time data that is used for establishment of valid cryptographic channels.
	FDP_IFC.1	This SFR supports the objective by defining an enterprise session controller policy to broker VVoIP endpoint communications.
	FDP_IFF.1	This SFR supports the objective by defining the rules enforced by the enterprise session controller policy.
	FIA_UAU.2/TC	This SFR supports the objective by requiring authentication of telecommunications devices that are connected to the TOE before the TSF will interact with them.
	FIA_UAU.2/VVoIP	This SFR supports the objective by requiring authentication of VVoIP endpoints that are connected to the TOE before the TSF will interact with them.

Objective	Addressed By	Rationale
	FTP_ITC.1/ESC	This SFR supports the objective by defining the trusted channels used for protection of signaling and media data used in VVoIP and SIP trunking communications.
	FPT_TUD_EXT.1/VVoIP (implementation-dependent)	This SFR supports the objective by optionally allowing the TOE to distribute software/firmware updates to connected VVoIP endpoints.
O.SELF_PROTECTION	FAU_GEN.1/Log	This SFR supports the objective by generating real-time diagnostic activity for the TOE's behavior that can be used to determine if it is experiencing conditions that could lead to a failure state.
	FDP_RIP.1	This SFR supports the objective by ensuring the permanent erasure of residual data so that a decommissioned or refurbished device cannot be used to disclose TSF data without authorization.
	FPT_FLS.1	This SFR supports the objective by ensuring that the TSF enters a secure failure state if specific hardware or software failures are detected.
O.SYSTEM_MONITORING	FAU_GEN.1 (refined from Base-PP)	This SFR supports the objective by defining additional required auditable events that are specific to ESC functionality that extend the audit generation requirement defined in the Base-PP.
	FAU_STG.1 (refined from Base-PP)	This SFR supports the objective by requiring all stored audit data to be protected against unauthorized access.
	FCS_NTP_EXT.1 (refined from Base-PP)	This SFR supports the objective by requiring the TSF to support NTP communications to obtain reliable time data that is used for accurate recording of log data.
	FPT_STM_EXT.1 (refined from Base-PP)	This SFR supports the objective by requiring the TSF to synchronize with an NTP server for reliable time data that is used for accurate log data.
	FAU_GEN.1/Log	This SFR supports the objective by requiring the TSF to generate a real-time system log of its own diagnostic details.
	FAU_SAR.1/Log	This SFR supports the objective by defining what users are able to review the real-time system log.
	FAU_SEL.1 (selection-based)	This SFR supports the objective by optionally allowing an administrator to suppress the generation of certain audit records.

7. TOE SUMMARY SPECIFICATIONS

7.1. NDcPP SFR Enforcing Measures

The TOE provides several measures for enforcing the SFR's. These measures are listed and briefly described in Table 16 below:

Table 16 NDcPP SFR Enforcing Measures

Measure	Description
TOE_Secure_Monitoring	The TOE employs the Linux Audit System (auditd) to log events (see Table 13). All critical event notification required by the NDcPP and MOD_ESC, including other useful information from all services running on the TOE, are configured to output to auditd. The auditd daemon gets its configuration from */etc/audit/auditd.conf* and its operational rules from */etc/audit/audit.rules*. The audit events and information from each service are configured to a common format where possible. Secure timestamps (NTP-over-TLS) are used to guarantee the correct time and date of each audit entry. TOE_Secure_Monitoring also provides the ability to detect and report any unauthorised changes to program and data files using special protected scripts.
TOE_Cryptography	All cryptography used by the TOE is implemented in the FIPS 140-3 security module. The algorithms used by the TOE are all NIST-approved and FIPS 140-3 validated.
TOE_Secure_Communications	Only two methods are used to secure communications in the TOE – TLS and SSH. Both are secured using TOE Cryptography. All TLS channels use X.509 certificates and the TOE supports both server authentication and client authentication (mutual authentication). Client mutual authentication is only supported on the SIP server.
TOE_Trusted_Administration	The TOE provides a secure administration facility that can be used remotely via a secure command line shell. The shell is secured using OpenSSH and the link is secured using the TOE cryptography. Additional HTTPS web services (EMP, MY, ECS) allow management of users, devices, and licences.

Measure	Description
TOE_SIP_Server	All users of the TOE are registered and authenticated by the TOE_SIP_Server based on a valid user ID and password. Voice and Video calls can only be set up and terminated by the TOE_SIP_Server.
TOE_Secure_Provisioning	The TOE_Secure_Provisioning facility manages and validates all software updates. Software updates are either digitally signed or based on hash verification.
TOE_Secure_Storage	The TOE uses the Operating System's secure key store for storing private keys, passwords and other sensitive data.

Table 17 lists each applicable SFR in the NDcPP and describes the corresponding measures taken by the TOE to meet the SFRs.

Table 17 NDcPP SFR Measures

SFR	Measures
FAU_GEN.1	The TOE employs the TOE_Secure_Monitoring facility which make use of Linux Audit System (auditd) and rsyslog to log events locally and remotely (see Table 13). The major services in the TOE are configured to use rsyslog so that they can be offloaded to a remote audit server. **Admin login/logout** – Logged by the OS via auditd and rsyslog. **Config changes and what has changed** – Logged using special protected scripts that monitor changes to config files. **Crypto key changes (key name)** – This will be done using special protected scripts to detect changes to the file name. All key file names will reflect the key names. **Admin and user password reset (user name)** – Logged by the OS. **Start/stop of services (App note 2)** – Logged by OS and individual services. **Bad login limit (origin e.g. IP)** – Logged by OS/SSHD. **Local login (on machine)** – Logged by the OS. **Attempt to manual update TOE** – Logged by the OS. **TOE update success/failure** – Logged by the OS.

SFR	Measures
	Management of TSF data – Logged by the OS and the use of special protected scripts to detect file changes. **Changes to time/date (origin e.g. IP for successful and failed attempts, old and new values)** – Logged by OS. **Termination of a local session by the session locking mechanism** – OS can timeout idle logins. Set up in ~./bash_profile (e.g. TMOUT=100). This is logged in the audit log by the OS (USER_LOGOUT). **Termination of an interactive session** – SSHD configured to timeout on idle. This is logged in the audit log by SSHD (pam_unix(sshd:session): session closed for user). **Start/stop/fail of trusted channel/path** – Logged by OpenSIPS, OS and SSHD. All audit log entries are time-stamped using an accurate time-base continuously updated by a remote NTP server. More details of logged events can be found in Table 13.
FAU_GEN.1/CDR	Audit Data Generation (Call Detail Record) – CDR details logged by OpenSIPS.using OpenSIPS xlog script. The CDR's are recorded in the general audit log output and contain the following fields: • TOE unique identifier • Call originator identifier • Call receiver identifier • Unique transaction sequence number • Call status (missed / connected / terminated / failures) • Call type (voice / voice + video) • Call start time • Call end time • Call duration • Call direction (incoming / outgoing) • call routing into TOE • call routing out of TOE • Time zone
FAU_GEN.1/Log	Audit Data Generation (System Log) – Logs all items listed in Table 2 of MOD_ESC. Audit data accumulated from several services plus the OS itself using syslog. The System Log records for: • Current IP connections:

SFR	Measures
	• NTP status • CPU usage • Memory usage • Disk and file storage capacity • Audit storage capacity • Power status The following information can be found in each record: • Date and time of the event • Type of event • Subject identity (if applicable) • Outcome (success or failure of the event) See examples in Table 10.
FAU_GEN.2	Each user-initiated event in the logs can be traced back to the user identity.
FAU_SAR.1/Log	Audit Review (System Log) – Local log viewed by Administrator via secure SSH command shell. System is also configured for remote audit logging using an external audit server containing larger historical log.
FAU_STG.1 FAU_STG.1/CDR	Protected Audit Trail Storage – All audit log files and CDRs (local and remote) are stored in protected directories only accessible by authorized Security Administrators. The remote audit facility protects audit logs and CDRs by moving them off-machine. This preserves the records even if they subsequently get deleting/modified on the TOE.
FAU_STG_EXT.1	The TOE consist of a single standalone component that stores audit data locally and it is capable of securely transmitting the audit logs to a remote audit server. Uses Linux auditd configured for real-time remote auditing (rsyslog) and secured using TLS. Local audit files are automatically archived numerically in compressed form after a configurable term (default is weekly). Each log is archived after reaching a configurable size (default is 800KB). These archives can be periodically deleted by the Network Administrator to save disk space as they would have already been captured by the remote audit server. A remote log entry is issued when the disk is nearly full, alerting the administrator to delete the older logs. All local audit logs are stored in an administrator-protected directory (/var/log/audit).

SFR	Measures
	Although the minimum number of locally stored records is specified as 1 million, the actual number of records can be very much larger depending on the size of the TOE hard disk, thus preventing records from being lost if the TOE loses contact with the remote audit server. The TOE logs rollover with oldest audit logs being overwritten with new logs and the remote audit server is also used to ensure that no logs are lost. The administrator is alerted via the local and remote audit facility when the TOE storage is close to being full.
FAU_ VVR_EXT.1	VVoIP recording is Not implemented. This is for security reasons. All calls are protected end-to-end such that attacks on the TOE can only yield metadata.
FAU_SEL.1	The audited events and logging sequence are specified in configuration files. Only the Network Administrator can select the logged events and their sequence.
FCS_CKM.1	**Key gen –** RSA 2048, 3072 and 4092 bits or greater, ECC curves P-256, P-384 and P-521, FFC schemes using safe-primes of 2048, 3072 and 4096 bits – Uses NIST-validated cryptography (CAVP #A7364) for SSH and TLS cryptography.
FCS_CKM.2	**ECC (SP800-56A-3)** – Uses NIST-validated cryptography (CAVP #A7364) for SSH and TLS. Keys generated according to FCS_CKM.1 **DH (RFC 3526 sect. 3)** – Uses NIST-validated cryptography (CAVP #A7364) for SSH and TLS cryptography. Keys generated according to FCS_CKM.1
FCS_CKM.4	**Key zeroize** – Keys stored in RAM are erased after use by a single-pass overwrite consisting of zeroes. These include TLS session and SSH session keys. Long term keys are stored on disk in an OS-protected permissioned folder. When no longer used they are either destroyed by a single-pass overwrite with a new key or they can be erased using an OS wipe utility such as the Red Hat “scrub” package (see guidance documentation).
FCS_COP.1	**DataEncryption –** AES 128/256 (CTR, GCM) using NIST-validated cryptography (CAVP #A7364) for data confidentiality on TLS and SSH sessions.

SFR	Measures
	SigGen – RSA DSA with key sizes 2048, 3072 and 4096 bits according to FIPS PUB 186-4 Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3, and EC DSA with key sizes of 256 bits or greater according to FIPS PUB 186-4 supporting curves P-256, P-384 and P-521 used for SSH and TLS authentication. **Hash –** SHA-256/384/512 in byte mode using NIST-validated cryptography (CAVP #A7364). Output block length and MAC length is equal to the hash size e.g. 256/384/512 bits according to *ISO/IEC 10118-3:2004*. The hash functions are used for data integrity. **KeyedHash –** Supports HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512 using NIST-validated cryptography (CAVP #A7364) with cryptographic key sizes of 256, 384 and 512 bits. Message digest sizes supported: 256, 384 and 512 bits conforming to ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2” and used for data authentication.
FCS_RBG_EXT.1	Random numbers used with key generation are obtained from the DRBG using the NIST-validated (CAVP #A7364) CTR_DRBG (AES-256) method according to ISO18031:2011,SP800-90A. Additional entropy seeding is provided using the Intel processor RDSEED instruction.
FCS_RBG_EXT.1.2	**Entropy** Provided in accordance with ISO/IEC 18031:2011 using NIST-validated (CAVP #A7364) CTR_DRBG (AES). The entropy source is the NIST-compliance Intel processor that supports RDSEED instruction. Complies with SP 800-90A Rev. 1 and SP 800-90C (Draft). The entropy strength is 256 bits.
FCS_HTTPS_EXT.1	**HTTPS Protocol –** Supported by web portals (EMP, MY, ECS) and using NIST-validated cryptography (CAVP #A7364) for the underlying TLS. The web portals make use of the nginx proxy to provide the HTTPS protocol in accordance with RFC 2818.
FCS_SSHS_EXT.1	**SSH Server Protocol –** Supported by OpenSSH 8.7p1-46.el9.x86_64 using password-based and public-key based authentication. The OpenSSH service is configured to only accept users with the correct SSH private key, and the username and password is authenticated by the Red Hat Enterprise server operating system. Successful login allows the

SFR	Measures
	administrator to perform TOE administration through a remote shell command terminal. Supported public key algorithms: • rsa-sha2-256 (RFC 8332) • rsa-sha2-512 (RFC 8332) • ecdsa-sha2-nistp256 (RFC 5656) • ecdsa-sha2-nistp384 (RFC 5656) • ecdsa-sha2-nistp521 (RFC 5656) Packets larger than 256KB are dropped (RFC 4253). The TOE uses a 256KB buffer to accumulate the packet information and checks that the packet has completed correctly before reaching the end of buffer. If not, the packet is discarded before being decrypted. Only the following encryption algorithms are permitted: • aes128-ctr (RFC 4344) • aes256-ctr (RFC 4344) • aes128-gcm@openssh.com (RFC 5647), • aes256-gcm@openssh.com (RFC 5647) Only the following hash algorithms are permitted: • hmac-sha2-256 (RFC 6668) • hmac-sha2-512 (RFC 6668) • implicit Only the following key exchange algorithms are permitted: • diffie-hellman-group14-sha256 • diffie-hellman-group16- sha512 • diffie-hellman-group18-sha512 • ecdh-sha2-nistp256 (RFC 5656) • ecdh-sha2-nistp384 (RFC 5656) • ecdh-sha2-nistp521 (RFC 5656) Session keys derived from a shared secret use SSH KDF according to RFC 5656 (Section 4) and are valid for no longer than one hour and for no more than one 1GB of data. Rekey after any of these thresholds are reached. Standards compliance: • For ECDSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [selection: P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4.

SFR	Measures
	• For Hash schemes: ISO/IEC 10118-3:2004. • For HMAC schemes: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.
FCS_TLSC_EXT.1	**Client TLS without mutual authentication –** Supported by services with client TLS interfaces. Supported ciphersuites listed in (see Table 11 and Table 12) are configurable during TOE installation/update (see guidance documentation). The TLS client matches the server X.509 Common Name (CN) as per RFC 6125 section 6 with allowed hostnames configured by the administrator in the associated client configuration file. SAN hostnames and wildcards are supported but no IP addresses are allowed. Only the following elliptic curves are supported, and these must be defined in the client configuration file: • secp256r1 • secp384r1 • secp521r1 With TLS 1.2 DHE ciphers are offered (Table 11) and the client will terminate the session if unsupported DH parameters are returned by the server.
FCS_TLSC_EXT.2	**TLS Client Protocol with Authentication –** Some interfaces are configured for TLS client authentication. The client rejects the connection if the server FQDN does not match the server’s X.509 certificate Common Name (CN matching). Supported configurable ciphersuites are listed in Table 11 and Table 12. All cryptography is NIST-validated (CAVP #A7364). Supported Groups: • secp256r1 • secp384r1 • secp521r1 Supported signature algorithms: • rsa_pkcs1 with sha256 • rsa_pkcs1with sha384 • rsa_pkcs1 with sha512 • ecdsa_secp256r1 with sha256 • ecdsa_secp384r1 with sha384

SFR	Measures
	• ecdsa_secp521r1 with sha512 The client interface does not support for Early data extension or Post-handshake client authentication. Session resumption is only supported with TLS 1.3 using PSKs with forward secrecy. Renegotiation is not supported with TLS 1.2
FCS_TLSS_EXT.1	**Server TLS without mutual authentication –** Services with server TLS and HTTPS interfaces include EMP, MY, AUX, ECS. All cryptography is NIST-validated (CAVP #A7364). Supported (configurable) ciphersuites listed in (see Table 11 and Table 12). Ciphersuites offered use the following algorithms: ECC with curves P-256, P-384 and P-521 RSA with key lengths of 2048, 3072 and 4096 bits DH with key lengths of 2048, 3072 and 4096 bits Only the following ECDHE curves are permitted: • secp256r1 • secp384r1 • secp521r1 The web portals do not require a client certificate and instead authenticate users using username and password. The TOE only permits the use of TLS 1.2 and TLS 1.3 with restricted ciphers (rejects all others). The key agreement parameters sent by the TOE in the “Server Hello” message are specified in RFC 5246 (7.4.3) and only the TLS cipher suites in Table 11 and Table 12 are permitted. All cryptography is NIST-validated (CAVP #A7364). No session resumption is supported.
FCS_TLSS_EXT.2	**TLS Server Protocol with Authentication –** The TOE expects to receive an X.509v3 client certificate as part of the TLS exchange. The TOE matches the Common Name (CN) in the client certificate using a pre-configured pattern and rejects the connection if there is a mismatch. There is no fallback to username and password and no administrator override to ignore client certificates. The TOE only permits the use of TLS 1.2 and TLS1.3 with restricted ciphers (rejects all others). The key

SFR	Measures
	agreement parameters sent by the TOE in the “Server Hello” message are specified in RFC 5246 (7.4.3). Only the TLS cipher suites in Table 11 and Table 12 are permitted and only. All cryptography is NIST-validated (CAVP #A7364).
FCS_NTP_EXT.1	**NTP Protocol –** Uses NTP v4 (RFC 5905) supported by the NTP daemon. NTP timestamp authentication uses the SHA-1 keyed hash method. The implemented method consists of a local NTP daemon that communicates with at least 3 authenticated NTP servers to synchronise the local system clock. The SHA-1 keyed hash method is compatible with RFC 3174 and has been tested with NIST’s authenticated NTP servers. The NTP service is used primarily to provide reliable audit timestamps but also provides a reliable clock for general system use.
FIA_UIA_EXT.1	Administrator access is based on password and SSH private key, all managed by the SSHD service. The web services (EMP, MY, ECS) also require a username and password. The TOE will display a warning banner (SSHD) and require user identification (OS) and user authentication (SSHD, OS). A warning banner is provided on the login pages of EMP, MY, and ECS. All administrators need to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.
FIA_UAU.2/VVoIP FIA_UAU.2/TC	**TSF requires VVoIP endpoint authentication –** Each subscriber must first be registered on the EMP database and each connection to the ESC (SIP REGISTER) enforces ESC subscriber authentication using TLS client certificates and requiring the X.509 CN to match the EMP subscriber name. **User Authentication before Any Action** – Only permitted trunks registered on EMP can establish a session with the TOE. Uses client-side TLS enabled on the trunk.
FIA_UAU.7	**No password feedback –** OS/SSHD terminal configured for no password feedback i.e. No echo, no asterisks. The EMP, MY, and ECS web portals also hide password entry (displays dots).
FIA_X509_EXT.1/Rev	**X.509 Certificate Validation -** Enforced by the FIPS 140-3 validated security module and supported by services with HTTPS and TLS interfaces.

SFR	Measures
	RFC 5280 certificate and certification path validation supporting a minimum path length of three certificates. Certification path terminates with a trusted CA certificate and all CA certificates must have basicConstraints extension with CA flag set to TRUE. Certificates validated using OCSP (RFC 6960, RFC 5280 Section 6.3) and CRL (RFC 5759 Section 5). For the certificate extendedKeyUsage field the following rules apply: • Server TLS certificates must contain the Server Authentication purpose or else the TOE will refuse (disconnect) the TLS connection. • Client TLS certificates must contain the Client Authentication purpose or else the TOE will refuse (disconnect) the TLS connection. • OCSP certificates must contain the OCSP Signing purpose or else the TOE will refuse (disconnect) the TLS connection. Only full server certificate chains are allowed i.e. the server certificate plus all intermediate CA certificates.
FIA_X509_EXT.2	**X.509 Certificate Authentication –** Enforced by the FIPS 140-3 security module and supported by services with HTTPS and TLS interfaces, including VVoIP endpoint registrations. Only X.509v3 certificates allowed as defined by RFC 5280. When the TOE cannot establish a connection to determine the validity of a certificate, the TOE allows the Administrator to choose whether to accept the certificate in these cases.
FIA_X509_EXT.3	**X.509 Certificate Requests –** CSR's can be requested by the Administrator using the FIPS 140-3 security module supported by a script ("csr-req") or using OpenSSL commands only within the private key OS-protected permissioned folder. The device-specific fields that can be specified by the customer are included with the csr-req script. The details are specified in the Acceptance Guidance Document (AGD).
FIA_AFL.1	**Password access** – Managed by OS PAM module. Parameters set in /etc/pam.d/system-auth and /etc/pam.d/password-auth files. SSH based access is configured for a maximum number of failed login attempts. The

SFR	Measures
	Audit log records all failed logins. Local terminal access provided in case of Administrator permanently locked out (lost password). The TOE prevents 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.
FIA_PMG_EXT.1	SSH and local shell login passwords are managed by configuring the rules in the operating system file /etc/security/pwquality.conf. The EMP admin portal password rules are managed by the EMP web app itself using the same rules. Passwords are composed of upper- and lower-case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “[“, “]”, “{“, “}”, “:”, “;”]; Password lengths are configurable to between 9 and 20 characters.
FMT_MOF.1	**TOE updates restricted** – OS restricts TOE updates to Administrators only.

FMT_MOF.1/Services
FMT_MOF.1.1/Functions
FMT_MTD.1/CryptoKeys
	Management of Security Functions and TSF data –
	Only authorized Administrators are permitted to update the TOE and the TOE does not permit any management functions to take place prior to login.
	Only authorized Administrators are permitted to:
	• start/stop or configure the following operational services as described in the guidance:
	  ○ OpenSIPS (ESC)
	  ○ ntpd
	  ○ auditd
	  ○ Web portals (EMP, MY, ECS)
	• modify parameters affecting the transmission of audit data to a remote audit server
	• modify the handling of local audit data
	• generate keys
	• import/modify keys and certificates
	• erase keys

FMT_MTD.1	**TOE management restricted** – OS restricts TOE data management restricted to Security Administrators only. “Management” includes (not limited to) create, init, view, change default, modify, delete, clear and append. Includes

SFR	Measures
	resetting of operator passwords. Admin passwords only resettable via local terminal access. All admins need to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.
FMT_SMF.1 FMT_SMF.1/ESC	**Local and remote security administration** – performed by only by a Security Administrator with access enforced by the OS and SSHD. OS user groups can be used to restrict roles. **Access banner** – configured with SSHD access banner. **Session inactivity time** – Configurable period and session inactivity time before session termination. **TOE updates verified** – update packages are verified by a Security Administrator using digital signature verification. **Display real-time connection status of VVoIP endpoints (hardware and software) and telecommunications devices** – Connection status activity can be scrolled in real time using OS tools such as “tail -f” to scroll the audit trails. **Configure Auth failure parameters** – OS ensures that only Administrators can configure these parameters. **Session inactivity time** – Uses OpenSIPS setting in /etc/secure-conf/opensips.cfg. **Clear disk TSF data** – Remote Administration via SSH. **All other configuration** – Remote Administration via SSH. **Configure ESC behaviour on self-test fail** - Remote Administration via SSH.
FMT_SMR.2	**Role-based access** – Configured in OS using user groups. The TOE maintains the Security Administrator role and the Administrators can access the TOE locally as well as remotely.
FMT_CFG_EXT.1	**Secure by Default Configuration -** No services can be started until a real Administrator account has been created. Assumes that the root user is the Administrator. The TOE will be delivered with a default Administrator account (unique to each customer) and the username and password will only be disclosed to the customer.
FPT_SKP_EXT.1	**Protected key storage** – See TSS for FCS_CKM.4 above. The TOE prevents reading of all pre-shared keys, symmetric keys, and private keys.

SFR	Measures
FPT_STM_EXT.1	**Reliable timestamp –** Managed by OS together with NTP remote time service.
FPT_TST_EXT.1	The following tests are executed by the TOE: • System Power-On Self-Test (POST) • Cryptography self-test **System POST** When the TOE powers-up, the BIOS and operating system services perform a Power-On-Self-Text (POST). During the initial BIOS tests a number of indicators on the TOE hardware panels indicate the health or failure of several internal hardware systems e.g. processors, memory, disks, and Input/Output (I/O) devices. If the TOE does not boot at all, please consult the hardware manual for information regarding the status indicators (e.g. LED's). During the BIOS POST you can interrupt the server boot-up and view health logs using the BIOS UEFI System Utilities. When the operating system boots up the Intelligent Lights Off (iLO) facility performs an orderly shutdown if a cautionary temperature level is detected. If the server hardware detects a critical temperature level before an orderly shutdown occurs, the server performs an immediate shutdown. Types of failures include hardware self-test failures (disk/memory failures). For more details, please consult the AGD. **Cryptography Self-Test** Once the system has booted completely, a Cellcrypt self-test script is automatically run during the start-up process and before any services are activated. During the execution of this script the FIPS 140-3 security module will test its algorithm integrity. Failures are recorded in the audit log and the TOE is rebooted or the service stops working. In case the failure persists after TOE reboot, the administrator should contact Cellcrypt Technical Assistance. Types of failures include cryptography (Known Answer Tests as described in NIST FIPS 140-3 requirements)).
FPT_TUD_EXT.1	**Trusted update (admin only) (digital signature)** – The TOE software is signed using a 4096-bit RSA code-signing certificate key purchased from a recognized CA (e.g. Digicert). The public key certificate can independently be verified by the customer using the CA trusted root certificate. The digital signature

SFR	Measures
	mechanism ensures that the software update files originate from Cellcrypt and have not been modified. The guidance documentation instructs the administrator on the exact steps to verify the signature. If the software package signature verification is successful the result displays “OK”, In this case the guidance instructs the administrator to continue installing the software update. If the signature verification fails, the administrator is informed to not to install the software. In this case the customer should contact Cellcrypt Technical Assistance. Software updates, together with their signatures can be delivered directly to the administrator or can be provided on a customer-specific App Store website only accessible by the administrator based on name and password. The version of the installed and running software can be viewed at any time (no delayed activation). The software version is automatically updated with each software update. The software update procedure and method to view the installed version is described in the guidance documentation.
FPT_FLS.1	**Failure with Preservation of a Secure State** – The TOE performs the following self-tests on start-up: • System POST. • Cryptography self-test. During the BIOS POST any hardware failures will result in the machine not booting up. When the operating system boots up the Intelligent Lights Off (iLO) facility performs an orderly shutdown if a cautionary temperature level is detected. If the server hardware detects a critical temperature level before an orderly shutdown occurs, the server performs an immediate shutdown. A Cellcrypt performs a cryptography self-test before starting up the normal TOE services and will not allow any services to start if it detects any cryptography failures. If the condition persists after rebooting the TOE, call Cellcrypt Technical Services.
FPT_APW_EXT.1	**Protected password storage** – Administrator and operator password are stored in OS-protected permissioned folders. The EMP admin passwords are stored Argon2 hash form. SSH passwords are OS account passwords and on RHEL9.5 these are hashed using SHA-512 together with a 64-bit salt.

<table>
<tr><th>SFR</th><th>Measures</th></tr>
<tr><td>FTA_SSL.3</td><td>Inactive session closes after pre-set time – Console inactivity session timeout is handled by the SSHD timeout (default is 60 seconds). Management Portals can also timeout inactive sessions and is configured in the EMP by a “Super Admin” (see EMP manual)
All TLS sessions will time out after 300s.</td></tr>
<tr><td>FTA_SSL.4</td><td>Admin closes session – Administrators can terminate SSH sessions as well as Management Portal sessions (EMP, MY, ECS). Administrator SSH sessions can be closed by the Administrators using the OS exit command and portal web sessions can be closed using a “Logout” button.</td></tr>
<tr><td>FTA_SSL_EXT.1</td><td>Terminate user session – Administrator console sessions can be terminated by SSHD; and management sessions using Cellcrypt Management portals (EMP, MY, ECS) can be terminated by the portals.</td></tr>
<tr><td>FTA_TAB.1</td><td>Banner display – SSHD displays the contents of a configurable banner file stored within the SSH configuration directory, and the web portals display a warning banner on the login screens.</td></tr>
<tr><td>FTP_ITC.1
FTP_ITC.1/ESC</td><td>Inter-TSF Trusted Channel – The TOE uses TLS/HTTPS for connecting with remote IT entities. A list of these entities is provided below:
Table 18 Inter-TSF and other client interfaces
<table>
<tr><th>Service</th><th>Mode</th><th>Authentication</th><th>IT Entity</th></tr>
<tr><td>SIP Server</td><td>Client</td><td>TLS with non-Mutual Authentication</td><td>ESC devices (for SIP trunking)</td></tr>
<tr><td>SIP Server</td><td>Server</td><td>TLS with Mutual Authentication</td><td>VVoIP endpoints (for protection of signaling protocols)</td></tr>
<tr><td>Conferencing Hub + Media STUN/Turn relay</td><td>N/A</td><td>SRTP</td><td>VVoIP endpoints (for protection of voice/video/media content)</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>SFR</th><th>Measures</th></tr>
<tr><td></td><td>
<table>
<tr><td>Portal service: API, Vault, Aux</td><td>Server</td><td>HTTPS, TLS non-Mutual Authentication</td><td>Cellcrypt Clients for non-VVoIP communication</td></tr>
<tr><td>Audit</td><td>Client</td><td>TLS non-Mutual Authentication</td><td>Audit Server</td></tr>
</table>
For security details see above measures for:
FCS_TLSC_EXT.2
FCS_TLSS_EXT.2
FCS_TLSS_EXT.2.1
FIA_X509_EXT.2
FIA_X509_EXT.2.2
TSF shall permit TSF or authorized TSF entities to initiate communication via trusted channel - The TOE allows VVoIP endpoints such as Cellcrypt Clients to initiate a communication channel via SIP over mutually authenticated TLS channel to protect the signalling protocols and VVoIP communication.
TSF shall initiate communication via trusted channel – The TOE initiates Normal TLS trunk mutually authenticated connection via OpenSIPS.
</td></tr>
<tr><td>FTP_TRP.1/Admin</td><td>Trusted path for administration – Secure local console and remote access for admins.
Password policy according to FIA_PMG_EXT.1, restricted to 6 bad logins before lockout and with restricted session idle time.
Password and/or public key authentication is required for remote SSH login.
Password over HTTPS for remote login to the Enterprise Management Portal (EMP).</td></tr>
<tr><td>FDP_IFC.1
FDP_IFF.1</td><td>Information Flow Control – ESC functionality enforced on all media communications. All calls managed via the ESC SIP proxy (OpenSIPS) uses the SIP protocol. The SIP protocol imposes a central signalling service on all media communications. All users must establish authorized connections with other users via the SIP server. All authorized users are registered in the ESC database and SIP registration</td></tr>
</table>

SFR	Measures
	requires a registered username and password before media communications can take place. **Enforce additional information flow rules** – Selection - No additional rules required. **TSF Explicitly authorize/deny information flow** – Handled by SIP caller registration.
FDP_RIP.1.1	When decommissioning the TOE or replacing a storage disk, keys can be erased using an appropriate file wipe utility or the TOE OS (Red Hat) “scrub” package. The scrub utility overwrites files with NNSA NAP-14.1-C patterns before deleting the file (see guidance documentation).

7.2. TOE Summary Specification Rationale

	TOE_Secure_Audit	TOE_Cryptography	TOE_Secure_Communications	TOE_Trusted_Administration	TOE_SIP_Server	TOE_Secure_Provisioning	TOE_Secure_Storage
FAU_GEN.1	X						
FAU_GEN.2	X						
FAU_SAR.1	X						
FAU_STG.1	X						X
FAU_STG_EXT.1	X						X
FAU_VVR_EXT.1	X						
FAU_SEL.1	X						
FCS_CKM.1		X					
FCS_CKM.2		X					
FCS_CKM.4		X					
FCS_COP.1		X					
FCS_RBG_EXT.1		X	X				
FCS_HTTPS_EXT.1		X	X				
FCS_SSH_EXT.1		X	X	X			
FCS_SSHS_EXT.1		X	X	X			
FCS_TLSC_EXT.1		X	X				
FCS_TLSC_EXT.2		X	X				
FCS_TLSS_EXT.1		X	X	X			
FCS_TLSS_EXT.2		X	X	X			
FCS_NTP_EXT.1	X				X		
FIA_UIA_EXT.1					X		
FIA_UAU.2/TC					X		
FIA_UAU.2/VVoIP					X		

FIA_UAU.7					X		
FIA_X509_EXT.1		X					
FIA_X509_EXT.2		X					
FIA_X509_EXT.3		X					
FIA_AFL.1					X		
FIA_PMG_EXT.1					X		
FMT_MOF.1				X	X		
FMT_MTD.1				X	X		
FMT_SMF.1				X	X		
FMT_SMR.2				X	X		
FMT_CFG_EXT.1					X		
FPT_SKP_EXT.1							X
FPT_STM.1	X						
FPT_STM_EXT.1	X						
FPT_TST_EXT.1	X						
FPT_TUD_EXT.1						X	
FPT_FLS.1					X		
FPT_APW_EXT.1							X
FTA_SSL.3			X				
FTA_SSL.4			X				
FTA_SSL_EXT.1			X				
FTA_TAB.1			X				
FTP_ITC.1			X				
FTP_TRP.1/Admin				X			
FDP_IFC.1					X		
FDP_IFF.1					X		
FDP_RIP.1				X			

8. ABBREVIATIONS AND ACRONYMS

Table 19 Abbreviations and Acronyms

AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
CA	Certificate Authority
CRL	Certificate Revocation List
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
FIPS	Federal Information Processing Standards
FlexibleLOM	Flexible LAN-on-Motherboard
GCM	Galois Counter Mode
HMAC	Keyed-Hash Message Authentication Code
HTTPS	HyperText Transfer Protocol Secure
iLO	Integrated Lights Out (HP Server Management)
IP	Internet Protocol
IPsec	Internet Protocol Security
SFF	Small Form Factor
ND	Network Device
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PAA	Processor Algorithm Accelerators
pND	Physical Network Device
POST	Power On Self-Test
PP	Protection Profile
RBG	Random Bit Generator
RSA	Rivest Shamir Adleman Algorithm

SD	Supporting Document
SHA	Secure Hash Algorithm
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
VPN	Virtual Private Network