PP-Module for Enterprise Session Controller (ESC)

Version: 1.0
2020-11-19
National Information Assurance Partnership

Contents

1. Introduction

1.1 Overview

The scope of this PP-Module is to describe the security functionality of an Enterprise Session Controller (ESC) in terms of [CC] and to define functional and assurance requirements for such products. This PP-Module is intended for use with the following Base-PPs:

- collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e

This Base-PP is valid because a device that implements an ESC is a specific type of network device, and there is nothing about the implementation of an ESC that would prevent any of the security capabilities defined by the Base-PP from being satisfied. This PP-Module does not mandate a particular architecture; the TOE may be either standalone or distributed as permitted by the Base-PP.

1.2 Terms

The following sections provide both Common Criteria and technology terms used in this PP-Module.

1.2.1 Common Criteria Terms

Table 1: CC Terms and Definitions

Term	Definition
Assurance	Grounds for confidence that a TOE meets the SFRs.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.2.2 Technology Terms

Table 2: Technology Terms and Definitions

Term	Definition
Audit Log	A persistent record of security-relevant events such as administrative access, administrative actions performed, system failures, and the establishment and termination of remote communications.
Call Detail Record	A log of call metadata that can be used to determine characteristics of a call, such as its length and involved parties, without recording any of its content.
Call Processing	The act of translating a dialed phone number into an attempt to establish a connection with the appropriate party; this is in contrast to the actual transmission of voice/video media over a call.
Enterprise Session Controller	A type of network device that is responsible for establishment, processing, and termination of Voice/Video over IP (VVoIP) calls.
Service Provider	A third-party telecommunications company that is responsible for providing commercial service and connectivity to the worldwide telephone network.
Session Border Controller	A type of network device that resides on the edge of a VVoIP network that is responsible for filtering corrupted or potentially malicious traffic and preventing it from entering or leaving the network.
System Log	A live display of system characteristics that can be viewed on demand to diagnose system performance in real-time. This data is typically only stored for a short period of time if at all.
Telecommunications Device	In this PP-Module, used to refer generally to any piece of infrastructure equipment that the ESC may connect to other than a VVoIP Endpoint, which could include equipment such as a call conferencing server or Session Border Controller.
Trunking	The concept of connecting multiple networks together; analogous to the use of a T1 line in a legacy telephone network.
VVoIP Endpoint	A VVoIP-capable phone or software application that a human user can use to make or receive a voice or video call.

1.3 Compliant Targets of Evaluation

The Target of Evaluation (TOE) that is defined by the combination of the NDcPP and this PP-Module is a network device, either a dedicated appliance with a non-modifiable operating system, or a general-purpose server running an independent commercially-available operating system that provides ESC functionality. Regardless of whether the TOE is a standalone appliance or a general-purpose server that is configured to function as an ESC, the TOE must be capable of satisfying all of the mandatory requirements of the NDcPP.

An ESC is a privately-owned telecommunication switch where its primary function is to set up, process, and terminate voice and video calls over an enterprise-wide Internet Protocol (IP) network. ESC operation is analogous to the tasks of 1930's telephone switchboard-operators, which is to patch (connect) together callers to callees. But today's ESC executes switchboard operations automatically, while providing simultaneous connectivity to hundreds of callers virtually instantaneously. In addition to establishing, processing, and managing thousands of connected calls, most ESCs support auxiliary services such as VVoIP Conferencing, Voicemail, Chat, Telepresence, Encrypted Communications, and Protocol Translation for end-to-end connectivity of diverse endpoints.

ESCs are commonly known as Call Servers, Communications Servers, and Call-Processing Systems, and they vary in complexities and capabilities. The typical ESC can manage thousands of calls between diverse client devices such as VoIP-handsets, Softphones, Desktop Telepresence Systems, Room-size Video Telepresence Systems, and Mobile Devices. ESCs are normally installed within a SCIF or other entry-controlled environment, especially systems that can register numerous VVoIP endpoints. To protect the ESC, a Session Border Controller (SBC) is installed on the outer edge of the VVoIP network to help protect the ESC from external network attacks. Also note that a fairly robust ESC system includes many major components such as its own database, operating system (O/S), conferencing system, dialplan, network manager, call-signaling protocols (e.g. H.323, Session Initiation Protocol (SIP), SS7), and its own 'Operations, Administration, and Management (OA&M)' application system.

If any one of these major components is successfully attacked, then one can expect the entire ESC system to be negatively impacted. The intention of this PP-Module is to provide a list of security requirements needed by an ESC for protection of its functionality and protection of the VVoIP communications it is responsible for facilitating.

1.4 TOE Boundary

An ESC is a logical component of a physical hardware appliance that is responsible for establishing connectivity between VVoIP endpoints. The ESC is an advanced version of a legacy IP-PBX system. As a specific type of network device, an ESC TOE will be evaluated against both the NDcPP and this PP-Module. All functionality described by the SFRs are within the TOE boundary, as is the ability for the TSF to establish secure remote connections with trusted entities in the OE.

Figure 1 below shows a typical VVoIP infrastructure in which an ESC is deployed.

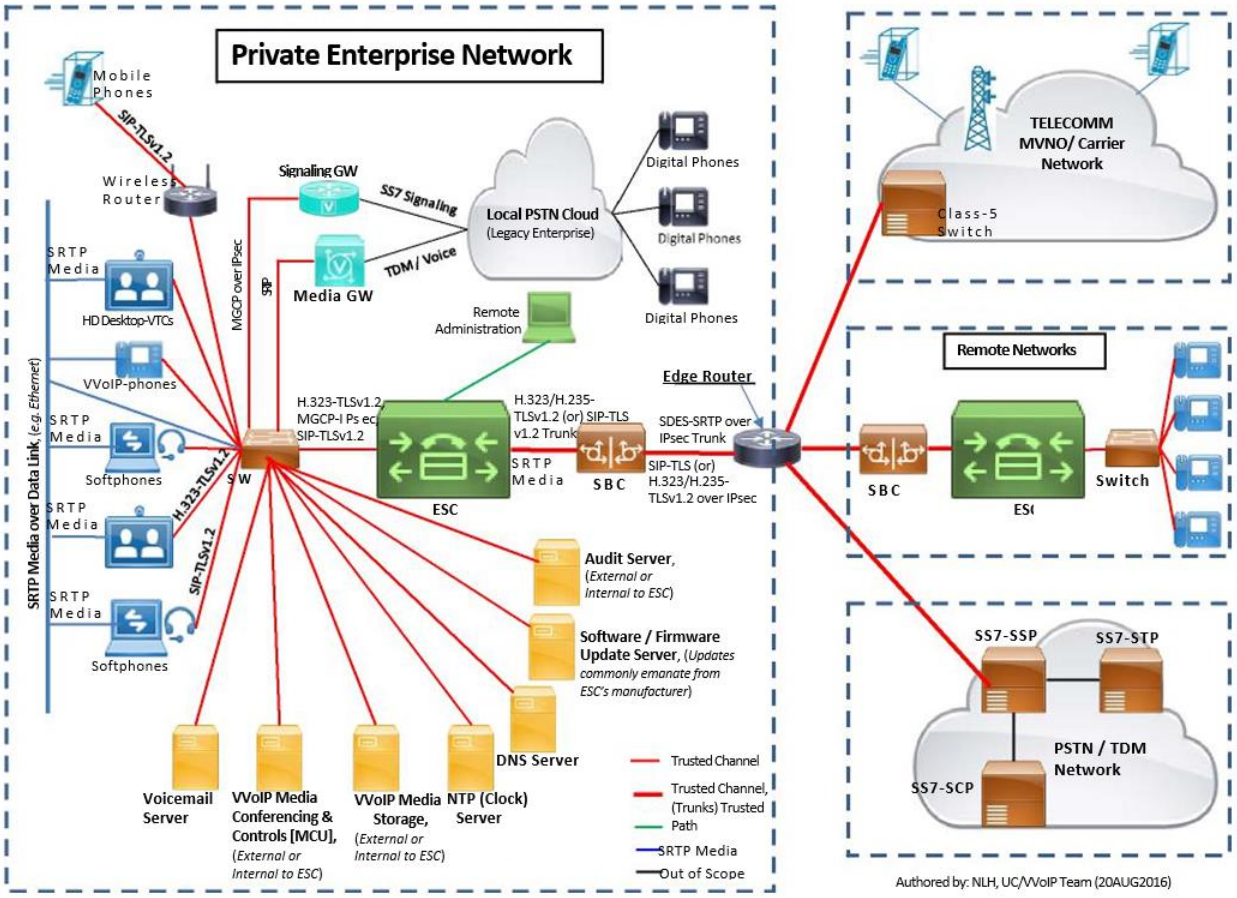


Figure 1: Representative ESC Deployment

As can be seen from this figure, the ESC's purpose is to provide an interface between VVoIP networks in order to connect calls. The ESC depends on or communicates with a number of services that are located within the internal network such as voicemail, conferencing, Network Time Protocol (NTP), Domain Name System, and software updates that are downloaded from VVoIP endpoint manufacturers and stored on the ESC for distribution to the clients.

Certain storage capabilities may be implemented exclusively within the TOE or within both the TOE and its OE (such as the TOE maintaining an internal audit log that is also written to an external audit server).

For connecting networks, the ESC relies on edge routing to handle lower-level communications between the networks and on a SBC to filter out potentially malicious activity.

The ESC itself, which can be administered locally or remotely, consists of several different logical components, as shown in Figure 2 below.

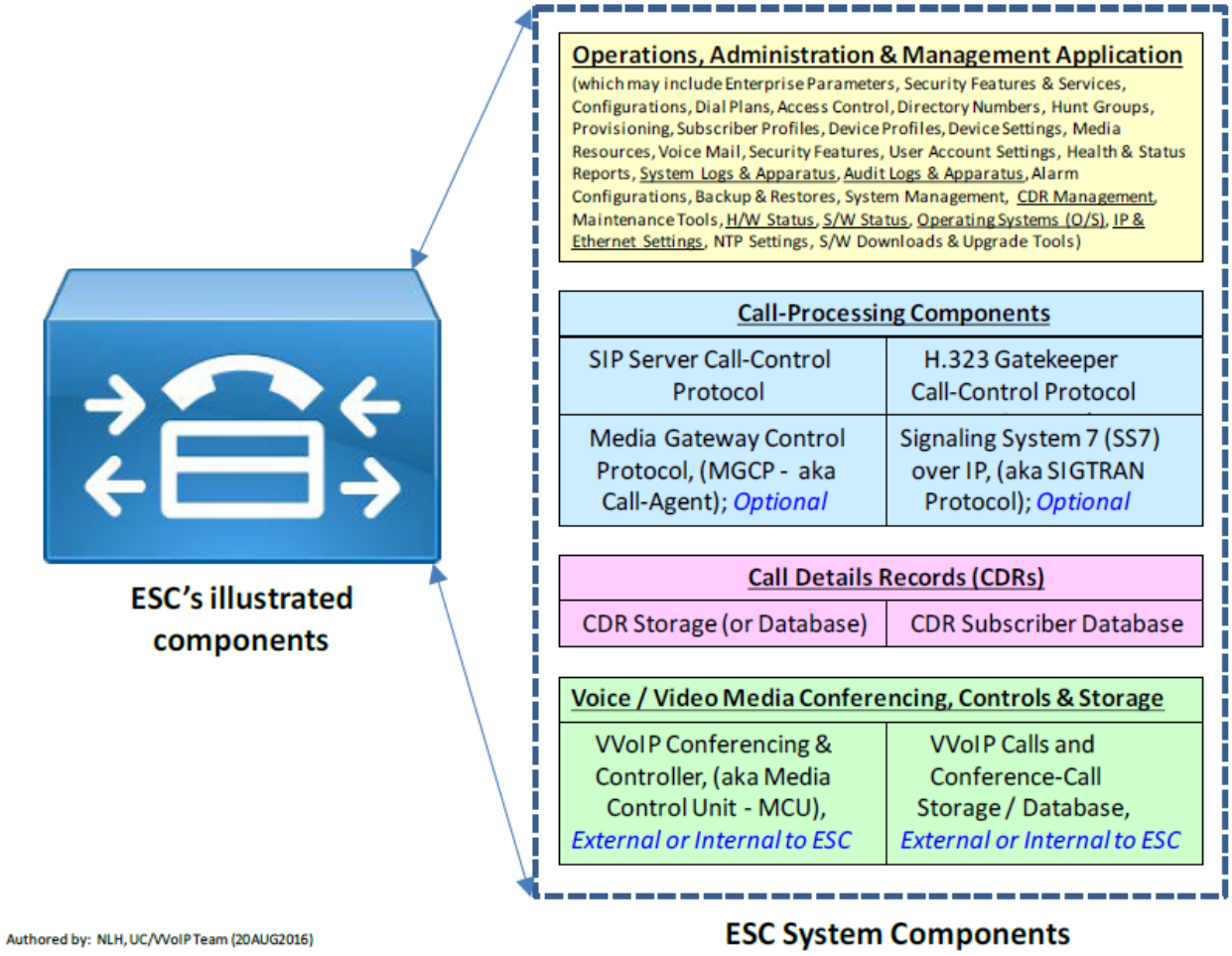


Figure 2: ESC Components

As can be seen from the figure above, the ESC provides the following logical capabilities:

- OA&M – Responsible for providing a management interface to the ESC's configuration.
- Call Processing – Responsible for setting up and tearing down calls between VVoIP endpoints using one or more call control protocols.
- Call Detail Records – Responsible for storage of call activity for auditing purposes.
- Voice/Video Media Conferencing, Controls, and Storage – responsible for establishing multi-way conference calls and storage of call recordings.

Different ESCs may implement these capabilities in different ways. This PP-Module defines a minimum baseline of capabilities that all conformant ESCs must provide.

1.5 Use Cases

Requirements in this PP-Module are designed to address the security problem in the following use cases. Use cases are not mutually exclusive; a TOE may implement more than one of these use cases. The description of these use cases provide instructions for how the TOE and its OE should be made to support the functionality required by this PP-Module.

This PP-Module defines four potential use cases for the ESC TOE:

[USE CASE 1] Dedicated Appliance

The ESC is sold and packaged as a standalone network appliance that does not have a direct interface to the underlying platform operating system, customized application, or commercial-off-the-shelf database.

[USE CASE 2] Call Processing (Connect VVoIP Calls Together)

The ESC serves as a call control system that employs multiple technologies for processing and managing voice/video calls between end-point devices. The ESC receives a call-request message from the source IP-phone (endpoint-A) and then locates and connects the call-originator to the destination device (endpoint-B). The ESC is used as a centralized system to process, manage, and connect calls between registered IP-phones. It should be noted that H.323 and SIP are the ESC's most commonly used call-processing (i.e. call control) protocols. Both H.323 and SIP are used to set up, process, and terminate voice/video calls between endpoints. Supplemental call control protocols such as Media Gateway Control Protocol (MGCP) and SS7 do not limit ESC capabilities, but instead enhances its functionality. Both H.323 and SIP provide an ESC with the capabilities required for execution of all use cases. Both H.323 and SIP provide the ESC with call control capabilities, support trunking between the ESC and Service Providers, support trunking between an array of ESCs, and can use encryption schemes that secure the ESC's call control functions.

[USE CASE 3] Trunk Calls to/from Telecommunications Service Provider

The ESC may support the ability to bundle numerous calls that originate from locally-registered VVoIP devices onto an ESC's communication trunk for connectivity through a telecommunications service provider (e.g. Verizon) to remote endpoints. In this case, the ESC supports the aggregation of traffic for all registered IP devices for the purpose of passing local calls over a single trunk to an external service provider. This allows for a simplified network deployment where a single connection from the ESC to the service provider can support a large number of devices, rather than requiring each individual device to connect to the service provider separately.

[USE CASE 4] Trunk Calls in/out to Remote ESCs

Similar to trunking calls to telecommunications service providers, the ESC can trunk a large volume of calls to other remote ESCs. An example of this deployment is a meshed configuration of trunk-connected ESCs that are deployed to support a metropolitan-sized enterprise-wide VVoIP call-processing network. This particular type of use case may not require any of the meshed ESCs to be connected to a service provider.

2. Conformance Claims

2.1 CC Conformance

Conformance Statement

This PP-Module inherits exact conformance as required from the specified Base-PP and as defined in the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

No additional PPs or PP-Modules are allowed to be specified in a PP-Configuration with this PP-Module.

CC Conformance Claims

This PP-Module is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Release 5 [CC].

Package Claim

This PP-Module does not claim conformance to any packages.

3. Security Problem Description

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its operational environment, and any organizational security policies that the TOE is expected to enforce.

The ESC is a network appliance that incorporates multiple components and protocols, and is designed with the purpose of connecting and managing calls that emanate from registered VVoIP endpoints. The ESC is also designed to provide centralized control of an enterprise-wide VVoIP communication network. As the central control system that manages and processes VVoIP calls from as many as 50,000 endpoints per node, it is critically important for the ESC to be protected because it is a single point of failure for tens of thousands of end-users.

As a centralized system the ESC is subject to attacks from the VVoIP endpoints that are registered to the ESC. Any VVoIP endpoint could be a threat to launch a malicious attack against the ESC. Therefore the ESC shall possess the security requirements needed for mitigating such a threat type.

Note that as PP-Module of the NDcPP, all threats, assumptions, and Organizational Security Policies (OSPs) defined there will also apply to an ESC TOE unless otherwise specified.

The Security Functional Requirements (SFRs) defined in this PP-Module will mitigate the threats that are defined in the PP-Module but will also mitigate some NDcPP threats in more comprehensive detail due to the specific capabilities provided by an ESC.

3.1 Threats

The following threats defined in this PP-Module extend the threats defined by the Base-PP.

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.

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.

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

All assumptions for the operational environment of the Base-PP also apply to this PP-Module. A.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.

3.3 Organizational Security Policies

The following organizational security policy is applicable to the TOE if the TOE is deployed on an independent, commercially-available operating system:

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

4.1 Security Objectives for the TOE

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)

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)

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)

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, FPT_FLS.1

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

All objectives for the operational environment of the Base-PP also apply to this PP-Module. OE.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.

This PP-Module also defines the following additional environmental objective:

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 this PP-Module.

Table 3: 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.
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

Objective	Threat or OSP	Rationale
		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.SECURITY_FUNCTIONALITY_ FAILURE (from Base-PP)	The TOE further mitigates the threat of security functionality failure defined in the Base-PP by ensuring that residual data is not preserved on the system for potential disclosure and by responding in a secure manner if a failure state is detected.
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 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

Objective	Threat or OSP	Rationale
		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. Security Requirements

The Security Functional Requirements (SFRs) included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, with additional extended functional components.

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 defined by the CC:

- Assignments are indicated with *italicized text*.
- Refinements made by the PP-Module author are indicated with **bold text**. Refinements are only applied to significant technical changes to existing SFRs; minor presentation changes with no technical impact (such as British vs American spelling differences) are not marked as refinements. Refinements are also indicated when an operation is added or substituted for an existing operation (e.g. the PP-Module completes an assignment in such a way that it introduces a selection into the assignment)
- Selections are indicated with *italicized text*.
- Iterations are indicated by appending the SFR name either with a slash and unique identifier suggesting the purpose of the iteration, e.g. '/CDR' for an SFR relating to call data records
- Extended SFRs are identified by having a label "EXT" after the SFR name.

5.1 Base-PP Security Functional Requirements Direction

This section instructs the ST author on what selections must be made to certain SFRs contained in the NDcPP in order to mitigate the threats defined in this PP-Module or to mitigate a threat from the NDcPP in a more specific or restrictive manner than what it specifies.

Full assurance activities are not repeated for the requirements in this section; only the additional testing needed to supplement what has already been captured in the Supporting Documents for the NDcPP is included.

5.1.1 Modified SFRs

FAU_GEN.1 Audit Data Generation (Audit Log)

FAU_GEN.1.1 is refined to include the following auditable events in addition to what is defined in the Base-PP.

Table 4: Audit Log Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_VVR_EXT.2 (if applicable)	Voice/video recordings of completed calls	Unique identifying data specified in FAU_VVR_EXT.2.3.
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).

Requirement	Auditable Events	Additional Audit Record Contents
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.
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).
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.
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; The exact SQL command/instruction that was executed.

Application Note: *The Base-PP version of the SFR requires "all administrative actions" to be audited. When the TOE includes this PP-Module, it is expected that this will also include the administrative actions that support the PP-Module defined in FMT_SMF.1/ESC.*

FAU_VVR_EXT.2 is a selection-based requirement. Auditing for this requirement must be performed if and only if the TOE claims it.

FAU_STG.1 Protected Audit Trail Storage

This SFR is optional in the NDcPP but is mandated by this PP-Module because the ESC is expected to maintain audit data internal to the TOE which must be protected from unauthorized access.

Application Note: *Both the "audit data" (FAU_GEN.1) and "system log" data (FAU_GEN.1/Log) are expected to be protected from unauthorized access. This SFR applies to all data related to the behavior of the TOE regardless of how it is categorized or where it is stored.*

FCS_DTLSS_EXT.1 DTLS Server Protocol without Mutual Authentication

FCS_DTLSS_EXT.1.1 The TSF shall implement [*DTLS 1.2 (RFC 6347)*)] supporting the following ciphersuites: [*selection: select supported ciphersuites from List 1* ***in the NDcPP***] and no other ciphersuites.

Application Note: *This SFR is selection-based in the NDcPP and remains selection-based in this PP-Module because DTLS may be used to secure transmitted media. In this case, it must be claimed if 'DTLS' is selected in FTP_ITC.1.1/ESC in addition to the applicable selection triggers in the Base-PP.*

This SFR is also refined from its definition in the Base-PP by requiring the use of DTLS 1.2 if this function is claimed.

FCS_DTLSS_EXT.2 DTLS Server Support for Mutual Authentication

This SFR is optional in the NDcPP but is selection-based in this PP-Module because any ESC use of DTLS requires mutually-authenticated DTLS to be implemented. Therefore, this SFR must be claimed if 'DTLS' is selected in FTP_ITC.1.1/ESC.

FCS_NTP_EXT.1 NTP Protocol

FCS_NTP_EXT.1.1 The TSF shall use only the following NTP version: [*NTP v4 (RFC 5905)*].

Application Note: *This SFR is selection-based in the Base-PP but is mandatory for a TOE that conforms to this PP-Module because the refinement to FPT_STM_EXT.1 requires this SFR to be claimed in all cases.*

This SFR has been refined from the NDcPP to permit the NTP v4 selection only. No other parts of the SFR are modified.

FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

FCS_TLSC_EXT.1.1 The TSF shall implement [*TLS 1.2 (RFC 5246)*)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [*selection: select supported ciphersuites from List 1* ***in the NDcPP***] and no other ciphersuites.

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

FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

This SFR is optional in the NDcPP but is mandated by this PP-Module because SIP and H.323 communications require mutually-authenticated TLS.

FCS_TLSS_EXT.1 TLS Server Protocol without Mutual Authentication

FCS_TLSS_EXT.1.1 The TSF shall implement [*TLS 1.2 (RFC 5246)*)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [*selection: select supported ciphersuites from List 1* ***in the NDcPP***] and no other ciphersuites.

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

FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication

This SFR is optional in the NDcPP but is mandated by this PP-Module because SIP and H.323 communications require mutually-authenticated TLS.

FIA_X509_EXT.1/Rev X.509 Certificate Validation

This SFR is selection-based in the Base-PP. It is mandatory when the TOE claims conformance to this PP-Module because X.509 certificate validation is needed when establishing TLS communications for SIP and H.323. There are no changes to the SFR otherwise.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for **TLS,** [*selection: DTLS, HTTPS, IPsec, SSH, no other protocols*], **VVoIP endpoint registration,** and [*selection: code signing for system software updates , [assignment: other uses], no additional uses*].

Application Note: *The NDcPP requires the ST author to select the protocol(s) that certificate authentication is used for. This element has been modified from its definition in the Base-PP by mandating support for TLS because FCS_TLSC_EXT.1 and FCS_TLSS_EXT.2 are mandatory SFRs for a TOE that conforms to this PP-Module. Additional protocols may or may not be selected depending on the other functionality provided by the TSF.*

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [selection: *allow the administrator to choose whether to accept the certificate in these cases, accept the certificate, not accept the certificate*].

Application Note: *This SFR is selection-based in the Base-PP but is made mandatory when this PP-Module is claimed because the ESC implements functionality that requires the use of certificate authentication.*

FIA_X509_EXT.3 X.509 Certificate Requests

This SFR is selection-based in the NDcPP but is mandated by this PP-Module because an ESC must implement security functions that require it to be issued its own X.509 certificate.

FPT_STM_EXT.1 Reliable Time Stamps

FPT_STM_EXT.1.2 The TSF shall [*synchronize time with an NTP server*].

Application Note: *This SFR has been refined from the NDcPP to permit the NTP server selection only. No other parts of the SFR are modified.*

5.2 TOE Security Functional Requirements

5.2.1 Security Audit (FAU)

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

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

FAU_GEN.1.2/CDR The TSF shall record within each **CDR** at least the following information: **[**

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

Application Note: *The TOE should be uniquely identified as part of the CDR so that there is attribution of individual CDRs in environments where multiple ESCs are feeding CDRs to a centralized server.*

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

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, [*selection: power status, fan status, no other activities*].**

FAU_GEN.1.2/Log The TSF shall record within each system log record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure of the event); and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*event details described in System Log Events table*].

Table 5: System Log Events

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).

Event	Additional System Log Record Contents
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.
Fan status (conditional)	Fan identification; Status (on or off).
Power status (conditional)	Status (on or off).

Application Note: *Unlike audit data (see FAU_GEN.1), system log data is used primarily for real-time analysis of system behavior. This data is expected to be treated as non-persistent data by the TOE.*

The ST author is expected to identify the sampling interval for the information presented in the system log so that it is clear to the evaluator how often updates to that information will be presented to an administrator.

Logging of power status is optional and is only intended for TOEs that have multiple redundant power supplies. Logging of fan status is also optional.

FAU_SAR.1/Log Audit Review (System Log)

FAU_SAR.1.1/Log The TSF shall provide [*Security Administrators*] with the capability to read [*assignment: 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**.

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

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

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

FAU_VVR_EXT.1 Recording Voice and Video Call Data

FAU_VVR_EXT.1.1 The TSF shall [selection: *have, not have*] the capability to record voice and video call data.

Application Note: *If "have" is selected, both FAU_STG.1/VVR and FAU_VVR_EXT.2 must be claimed and "Ability to enable/disable voice and video recordings for any registered VVoIP endpoint" must be selected in FMT_SMF.1.1/ESC.*

5.2.2 User Data Protection (FDP)

FDP_IFC.1 Subset Information Flow Control

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

FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [*enterprise session controller SFP*] based on the following types of subject and information security attributes: [*assignment: method by which the TSF identifies each endpoint for a call*] **using the following call control protocols: [*selection: SIP, H.323*] and [*selection: SS7, MGCP, 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: [*assignment: rules, based on security attributes, that explicitly authorize information flows*].

Application Note: *The expectation of this element is that the ST author define any explicit allowlist behavior that overrides the normal information flow handling to automatically open a communications channel through the TOE. It is acceptable to complete the assignment with "no additional rules" if there are no exceptions to the behavior defined in FDP_IFF.1.2 and 1.3.*

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*assignment: rules, based on security attributes, that explicitly deny information flows*].

Application Note: *The expectation of this element is that the ST author define any explicit denylist behavior that overrides the normal information flow handling to automatically block a communications channel through the TOE. It is acceptable to complete the assignment with "no additional rules" if there are no exceptions to the behavior defined in FDP_IFF.1.2 and 1.3.*

FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*selection: allocation of the resource to, deallocation of the resource from*] the following objects: [*assignment: disk storage location(s) erased by the TSF during factory reset or other wipe operation*].

Application Note: *The TOE is expected to follow guidelines for [NIST SP 800-88], 'Disk Storage Sanitization' as the method for ensuring that residual information is cleared from both volatile and nonvolatile memory. This involves overwriting the entire disk or disk partition with zeroes, followed by all ones, followed by all zeroes. Since it is not feasible to pause the wipe operation while in progress it is sufficient for the*

evaluator to observe during testing that the final result is all zeroes; however, the vendor-provided evidence is expected to provide a justification that [NIST SP 800-88] guidelines are being followed.

5.2.3 Identification and Authentication (FIA)

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

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**.

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

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**.

Application Note: *This includes both the establishment of voice/video calls and the TOE-initiated application of an update to the VVoIP endpoint software/firmware.*

5.2.4 Security Management (FMT)

FMT_CFG_EXT.1 Secure by Default Configuration

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.

FMT_SMF.1/ESC Specification of Management Functions (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;
- [*selection:*
  - *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;*
  - *Ability to enable/disable voice and video recordings for any registered VVoIP endpoint;*
  - *Ability to specify criteria for retention of voice and video recordings;*
  - *No other capabilities*].

Application Note: *This SFR defines additional management functions for the TOE beyond what is defined in the Base-PP as FMT_SMF.1. The TOE may have all management functionality implemented in the same logical interface; it is not necessary for*

"network device management" and "enterprise session controller management" to be implemented in separate interfaces.

The TOE developer is encouraged, but not required, to provide a more sophisticated password strength policy than what is prescribed by FIA_PMG_EXT.1 as defined in the NDcPP. This may include the ability for an administrator to configure the metrics used to define an acceptable password. At minimum, the minimum password length must be configurable. If "have" is selected in FAU_VVR_EXT.1.1, then "Ability to enable/disable voice and video recordings for any registered VVoIP endpoint" must be selected.

The selection "Ability to configure NTP" must be included in the ST if the TOE uses NTP for timestamp configuration. If selected, FCS_NTP_EXT.1 from the NDcPP must be claimed as well.

If "Ability to specify the set of audited events" is selected, FAU_SEL.1 must be claimed.

5.2.5 Protection of the TSF (FPT)

FPT_FLS.1 Failure with Preservation of a Secure State

FPT_FLS.1.1 The TSF shall preserve a secure state **through the following means: [*selection: audible alarm, visual indicator, reboot of the TOE, shutdown of the TOE, [assignment: other methods]*]** when the following types of failures occur: [*failure of self-tests defined in FPT_TST_EXT.1, failure of [assignment: hardware components that affect the proper functioning of the TOE]*].

5.2.6 Trusted Path/Channels (FTP)

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

FTP_ITC.1.1/ESC The TSF shall **be capable of using TLS and [*selection: DTLS, IPsec, 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), [*selection: VVoIP conferencing system, no other capabilities*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

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 [*assignment: list of functions for which a trusted channel is required*].

5.3 TOE Security Functional Requirements Rationale

The following rationale provides justification for each security objective for the TOE, showing that the SFRs are suitable to meet and achieve the security objectives:

Table 6: SFR-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.
	FAU_STG.1/VVR (selection-based)	This SFR supports the objective by requiring the TSF to securely store call detail records, if generated by the TSF.

Objective	Addressed By	Rationale
	FAU_VVR_EXT.2 (selection-based)	This SFR supports the objective by defining when voice and video recordings are generated by the TSF, how they are stored, and how they are uniquely identified for future access.
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_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 establishment of valid cryptographic channels.
	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.

Objective	Addressed By	Rationale
	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.
	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.

Objective	Addressed By	Rationale
	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.

5.4 TOE Security Assurance Requirements

This PP-Module does not define any additional assurance requirements above and beyond what is defined in the Base-PP. In general, application of the SARs to the TOE boundary described by both the NDcPP and this PP-Module is sufficient to demonstrate that the claimed SFRs have been implemented correctly by the TOE. However, in some cases it may be necessary to perform additional assurance activities in order to satisfy the SARs due to unique capabilities or limitations of the TOE that is specified by this PP-Module.

The Supporting Document that accompanies this PP-Module defines the additional Evaluation Activities that are to be performed.

6. Consistency Rationale

6.1 NDcPP Base

6.1.1 Consistency of TOE Type

When this PP-Module is used to extend the NDcPP, the TOE type for the overall TOE is still a network device. The TOE boundary is simply extended to include ESC functionality that is provided by the network device.

6.1.2 Consistency of Security Problem Definition

The threats defined by this PP-Module (see section 3.1) supplement those defined in the NDcPP as follows:

Table 7: Threat Consistency Rationale

PP-Module Threat	Consistency Rationale
T.MALICIOUS_TRAFFIC	The Base-PP does not define a threat for malicious traffic because all of its security-relevant external interfaces define the network device as the endpoint. This PP-Module defines interfaces where the TOE is facilitating a connection between two external entities, such that traffic between them will flow "through" the TOE as opposed to "to/from the TOE." This threat is consistent with the Base-PP because it is only applied to the interfaces defined in this PP-Module where it is relevant; it does not apply to the interfaces defined in the Base-PP.
T.NETWORK_DISCLOSURE	The Base-PP does not define a threat for access to network resources because all of its security-relevant external interfaces define the network device as the endpoint. This PP-Module defines interfaces where the TOE is facilitating a connection between two external entities, such that traffic between them will flow "through" the TOE as opposed to "to/from the TOE." This threat is consistent with the Base-PP because it is only applied to the interfaces defined in this PP-Module where it is relevant; it does not apply to the interfaces defined in the Base-PP.
T.UNAUTHORIZED_CLIENT	This threat is a specific instance of the T.WEAK_AUTHENTICATION_ENDPOINTS threat defined in the Base-PP because it refers to a scenario where an unauthorized client is able to communicate successfully with the TOE because the TSF is incapable of authenticating clients to determine which are or are not authorized.

This PP-Module does not define any assumptions beyond those defined in the NDcPP. However, it does note that A.NO_THRU_TRAFFIC_PROTECTION from the NDcPP only applies to the Base-PP external interfaces. This is because the interfaces defined by this PP-Module do enforce through-traffic protection.

The organizational security policies defined in this PP-Module are consistent with the NDcPP based on the following rationale:

Table 8: Organizational Security Policies Consistency Rationale

PP-Module Policy	Consistency Rationale
P.SECURED_PLATFORM	The Base-PP does not define any policies that expect that environmental systems are configured in any specific manner. Therefore, it is expected that

PP-Module Policy	Consistency Rationale
	requiring environmental systems to be configured in a secure manner will not prevent the TSF from being fully implemented.

6.1.3 Consistency of Objectives

The Base-PP does not define any TOE objectives; the TOE objectives that are defined by this PP-Module are all mapped to SFRs defined in the Base-PP and PP-Module. Because of this, consistency of the PP-Module's TOE objectives with the Base-PP is demonstrated in Section 6.1.4 below.

The objectives for the TOE's operational environment are consistent with the NDcPP based on the following rationale:

Table 9: Environmental Objective Consistency Rationale

PP-Module Environmental Objective	Consistency Rationale
OE.SECURED_PLATFORM	This objective expects the TOE to be configured in such a manner that the underlying OS on which the TOE runs cannot be used to alter the behavior of the TSF. This is consistent with the OE.NO_GENERAL_PURPOSE objective in the Base-PP that expects that general-purpose computing capability will be prohibited by the OS. This ensures that OE.SECURED_PLATFORM can be satisfied by the operational environment.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the NDcPP that are needed to support ESC functionality. This is considered to be consistent because the functionality provided by the network device is being used for its intended purpose. The PP-Module also identifies a number of new SFRs that are used entirely to provide ESC functionality. The rationale for why this does not conflict with SFRs defined by the NDcPP are as follows:

Table 10: SFR Consistency Rationale

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FAU_GEN.1	This PP-Module modifies the Base-PP SFR to add specific auditable events that relate to ESC functionality.
FAU_STG.1	This PP-Module mandates the inclusion of this optional SFR because it is required to implement functionality required by this PP-Module.
FCS_DTLSS_EXT.1	This PP-Module refines this selection-based SFR to a more restrictive selection if claimed. The available selection item is one of the items in the original version of the SFR. This PP-Module also specifies an additional trigger for when this SFR must be claimed.
FCS_DTLSS_EXT.2	This PP-Module conditionally mandates the inclusion of this optional SFR for any situation where DTLS is claimed, which makes this into a selection-based SFR.
FCS_NTP_EXT.1	This PP-Module requires NTP v4 to be selected, which is one of two selection options defined in the original SFR in the Base-PP. This PP-Module also

PP-Module Requirement	Consistency Rationale
	mandates the inclusion of this selection-based SFR because it is required to implement the NTP functionality prompted by the PP-Module's refinement to FPT_STM_EXT.1.
FCS_TLSC_EXT.1	This PP-Module mandates the inclusion of this selection-based SFR because it is required to implement the trusted communications required by the PP-Module.
FCS_TLSC_EXT.2	This PP-Module mandates the inclusion of this optional SFR because it is required to implement the trusted communications required by the PP-Module.
FCS_TLSS_EXT.1	This PP-Module mandates the inclusion of this selection-based SFR because it is required to implement the trusted communications required by the PP-Module.
FCS_TLSS_EXT.2	This PP-Module mandates the inclusion of this optional SFR because it is required to implement the trusted communications required by the PP-Module.
FIA_X509_EXT.1/Rev	This PP-Module mandates the inclusion of this selection-based SFR because all TOEs that conform to this PP-Module will perform functions that require certificate validation.
FIA_X509_EXT.2	This PP-Module modifies the Base-PP requirement by defining a mandatory usage of X.509 certificate authentication and to require the TOE to implement at least one trusted protocol that requires certificate validation.
FIA_X509_EXT.3	This PP-Module mandates the inclusion of this selection-based SFR because all TOEs that conform to this PP-Module will perform functions that require the TSF to have the ability to issue a certificate request to obtain its own X.509 certificate.
FPT_STM_EXT.1	This PP-Module modifies the Base-PP by requiring one of this SFR's two original selection items to be chosen.
Mandatory SFRs	
FAU_GEN.1/CDR	The PP-Module iterates an SFR defined in the Base-PP to require the TOE to generate a type of audit record that is specific to the functions defined in this PP-Module.
FAU_GEN.1/Log	The PP-Module iterates an SFR defined in the Base-PP to require the TOE to generate a type of audit record that is specific to the functions defined in this PP-Module.
FAU_SAR.1/Log	This PP-Module requires the TOE to implement a mechanism for review of system log records that are defined by this PP-Module in FAU_GEN.1/Log and does not relate to the audit records required by the Base-PP.
FAU_STG.1/CDR	The PP-Module iterates an SFR defined in the Base-PP by protecting audit data required by this PP-Module in the same manner that the Base-PP defines for its own audit records.
FAU_VVR_EXT.1	This SFR applies to recording voice and video call data, which is beyond the original scope of the Base-PP.
FDP_IFC.1	This SFR applies to the TOE's implementation of an enterprise session controller policy, which applies to the TOE's through-traffic interfaces and is therefore beyond the original scope of the Base-PP.

PP-Module Requirement	Consistency Rationale
FDP_IFF.1	This SFR applies to the TOE's implementation of an enterprise session controller policy, which applies to the TOE's through-traffic interfaces and is therefore beyond the original scope of the Base-PP.
FDP_RIP.1	This SFR applies to data wipe operations which is beyond the original scope of the Base-PP. The Base-PP defines FCS_CKM.4 for destruction of cryptographic data but this PP-Module extends the requirements for data destruction to entire disk storage locations.
FIA_UAU.2/TC	This SFR applies to authentication of external entities on the TOE's through-traffic interfaces and is therefore beyond the original scope of the Base-PP.
FIA_UAU.2/VVoIP	This SFR applies to authentication of external entities on the TOE's through-traffic interfaces and is therefore beyond the original scope of the Base-PP.
FMT_CFG_EXT.1	This SFR requires the TOE to implement a secure default configuration. There is no inconsistency here with the Base-PP because the Base-PP's functionality is not dependent on a particular default configuration.
FMT_SMF.1/ESC	This SFR requires the TOE to implement management functions that are specific to ESC functionality. This does not conflict with the Base-PP because these are all additional functions that go beyond what the Base-PP requires.
FPT_FLS.1	This SFR requires the TOE to take some specific action in the event of self-test failures or other hardware failures. This extends the functionality required by the Base-PP because the Base-PP defines the self-tests that the TOE must perform but does not define specific requirements for the TOE's behavior when a self-test fails.
FTP_ITC.1/ESC	This SFR requires the TOE to implement trusted channels for VVoIP and SIP trunking communications. This is an iteration of the same Base-PP SFR that adds new external interfaces beyond the scope of the Base-PP.
Optional SFR	
FPT_TUD_EXT.1/VVoIP	This PP-Module extends the functionality required by the Base-PP by optionally allowing the TSF to perform software update activities for connected VVoIP endpoints and not just for the TOE itself.
Selection-Based SFRs	
FAU_SEL.1	This PP-Module optionally allows a conformant TOE to claim the ability to suppress the generation of audit events based on certain factors. This does not conflict with the Base-PP because if the administrators desires all required auditable events to be audited, they can choose to disable this function.
FAU_STG.1/VVR	This PP-Module optionally allows a conformant TOE to claim the ability to securely store voice/video recordings. This does not conflict with the Base-PP because the Base-PP already has the ability to define secured storage (e.g. through FAU_STG.1) so there is no expectation of availability that is being violated if this is claimed.
FAU_VVR_EXT.2	This PP-Module optionally allows a conformant TOE to claim the ability to generate and retain voice/video recordings of calls. This does not conflict with the Base-PP because the Base-PP already defines an audit mechanism via FAU_GEN.1 and also does not define any requirements that would prevent the generation of media recordings such as unobservability of user actions.

A. Optional Requirements

As indicated in the introduction to this PP-Module, the baseline requirements (those that must be performed by the TOE) are contained in the body of this PP-Module. This Appendix contains three other types of optional requirements that may be included in the ST but are not required in order to conform to this PP-Module.

The first type (in A.1) are strictly optional requirements that are independent of the TOE implementing any function. If the TOE fulfills any of these requirements or supports a certain functionality, the vendor is encouraged but not required to add the related SFRs.

The second type (in A.2) are objective requirements that describe security functionality not yet widely available in commercial technology. The requirements are not currently mandated in the body of this PP-Module, but will be included in the baseline requirements in future versions of this PP-Module. Adoption by vendors is encouraged and expected as soon as possible.

The third type (in A.3) are implementation-dependent requirements that are dependent on the TOE implementing a particular function. If the TOE fulfills any of these requirements, the vendor must either add the related SFR or disable the functionality for the evaluated configuration.

A.1 Strictly Optional Requirements

There are currently no strictly optional requirements defined by this PP-Module.

A.2 Objective Requirements

There are currently no objective requirements defined by this PP-Module.

A.3 Implementation-Dependent Requirements

A.3.1 Protection of the TSF (FPT)

FPT_TUD_EXT.1/VVoIP Trusted Update (VVoIP Endpoints)

FPT_TUD_EXT.1.1/VVoIP The TSF shall provide [*Security Administrators*] the ability to query the currently executing version of the **registered VVoIP endpoint** firmware/software as well as the most recently installed version of the **registered VVoIP endpoint** firmware/software.

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

FPT_TUD_EXT.1.3/VVoIP The TSF shall provide means to authenticate firmware/software updates to the **registered VVoIP endpoint** using a [*selection: X.509 certificate, digital signature mechanism, published hash*] prior to installing those updates.

Application Note: *The TOE may either validate the update prior to storing it for delivery to registered VVoIP endpoints or it may provide the means to validate the update to the VVoIP endpoint itself by preserving the manufacturer's integrity/authenticity mechanism and including that information in the*

update. In other words, either the TSF itself validates the update or it facilitates the ability of the VVoIP endpoint to do this by providing all information necessary to validate the update to the client.

It is typical behavior for ESCs to push software updates to registered VVoIP endpoint devices. However, many VVoIP endpoints have the ability to receive software updates from either an ESC or third-party update server. This SFR addresses the case where it is the ESC's responsibility for delivery of software updates to registered VVoIP endpoints. For those scenarios where the VVoIP endpoint gets its upload from a separate server, then the ESC is not responsible for assuring FPT_TUD_EXT.1/VVoIP.

B. Selection-Based Requirements

As indicated in the introduction to this PP-Module, the baseline requirements (those that must be performed by the TOE) are contained in the body of the PP-Module. There are additional requirements based on selections in the body of the PP-Module: if certain selections are made, then additional requirements below will need to be included.

B.1 FAU_SEL.1 Selective Audit

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) [*selection: object identity, user identity, subject identity, host identity, event type*];
b) [*assignment: list of additional attributes that audit selectivity is based upon*]

Application Note: *This requirement must be claimed when 'Ability to specify the set of audited events' is chosen in FMT_SMF.1.1/ESC.*

B.2 FAU_STG.1/VVR Protected Audit Trail Storage (Voice/Video Recording)

FAU_STG.1.1/VVR The TSF shall protect the stored **voice and video recordings** from unauthorized **disclosure and** deletion **by encrypting voice and video recording data that is stored on the TOE using an encryption method specified in FCS_COP.1**.

FAU_STG.1.2/VVR The TSF shall be able to [*prevent*] unauthorized modifications to the stored **voice and video recordings**.

Application Note: *This requirement must be claimed if 'have' is selected in FAU_VVR_EXT.1.1.*

B.3 FAU_VVR_EXT.2 Generation of Voice and Video Recordings

FAU_VVR_EXT.2.1 The TSF shall provide the ability to retain voice and video recordings based on [*assignment: administrator-specified criteria*].

FAU_VVR_EXT.2.2 The TSF shall store voice and video recordings as [*assignment: supported file format*] data.

FAU_VVR_EXT.2.3 The TSF shall uniquely identify individual voice/video recordings using the following method: [*assignment: unique identifying data*].

Application Note: *This requirement must be claimed if 'have' is selected in FAU_VVR_EXT.1.1.*

C. Extended Component Definitions

This appendix contains the definitions for the extended requirements that are used in the PP-Module including those used in Appendices A through C.

C.1 Background and Scope

This Appendix provides a definition for all of the extended components introduced in this PP-Module. These components are identified in the following table:

Table 11: Extended Components Definitions

Functional Class	Functional Components
Security Audit (FAU)	FAU_VVR_EXT Voice and Video Recording
Security Management (FMT)	FMT_CFG_EXT Secure by Default Configuration

C.2 Extended Component Definitions

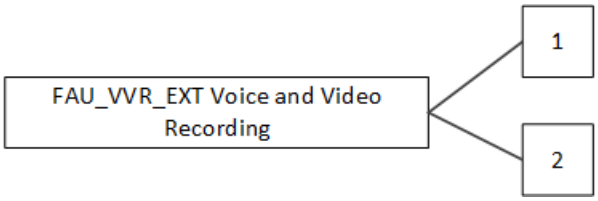
Class FAU: Security Audit

FAU_VVR_EXT Voice and Video Recording

Family Behavior

This family defines requirements for recording of voice and video data.

Component Leveling



FAU_VVR_EXT.1 Recording Voice and Video Call Data, requires the TSF to specify whether or not it records voice and video call data.

FAU_VVR_EXT.2 Generation of Voice and Video Recording, requires the TSF to store uniquely identified voice and video call recordings in a certain format and when certain conditions are met.

Management: FAU_VVR_EXT.1

The following actions could be considered for the management functions in FMT:

- Ability to enable/disable voice and video recordings

Audit: FAU_VVR_EXT.1

There are no auditable events foreseen.

Management: FAU_VVR_EXT.2

The following actions could be considered for the management functions in FMT:

- Ability to specify criteria for retention of voice and video recordings

Audit: FAU_VVR_EXT.2

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- Voice/video recordings of completed calls

FAU_VVR_EXT.1 Recording Voice and Video Call Data

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_VVR_EXT.1.1 The TSF shall [selection: *have, not have*] the capability to record voice and video call data.

FAU_VVR_EXT.2 Generation of Voice and Video Recording

Hierarchical to: No other components.

Dependencies: FAU_VVR_EXT.1 Recording Voice and Video Call Data

FAU_VVR_EXT.2.1 The TSF shall provide the ability to retain voice and video recordings based on [*assignment: administrator-specified criteria*].

FAU_VVR_EXT.2.2 The TSF shall store voice and video recordings as [*assignment: supported file format*] data.

FAU_VVR_EXT.2.3 The TSF shall uniquely identify individual voice/video recordings using the following method: [*assignment: unique identifying data*].

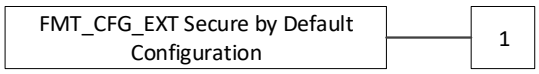
Class FMT: Security Management

FMT_CFG_EXT Secure by Default Configuration

Family Behavior

This family defines requirements for protecting the TSF and its data from unauthorized access.

Component Leveling



FMT_CFG_EXT.1 Secure by Default Configuration, requires credentials to be administratively-defined before allowing any other TSF-mediated security functionality and to enforce a deny-by-default posture on the TOE.

Management: FMT_CFG_EXT.1

No specific management functions are identified.

Audit: FMT_CFG_EXT.1

There are no auditable events foreseen.

FMT_CFG_EXT.1 Secure by Default Configuration

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of Authentication

FMT_MTD.1 Management of TSF Data

FMT_SMR.1 Security Roles

FMT_CFG_EXT.1.1 The TSF shall provide only enough functionality to set new [*assignment: administrator role*] credentials when configured with default credentials or no credentials.

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

D. Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this PP. However, these requirements are not featured explicitly as SFRs and should not be included in the ST. They are not included as standalone SFRs because it would increase the time, cost, and complexity of evaluation. This approach is permitted by [CC] Part 1, 8.2 Dependencies between components.

This information benefits systems engineering activities which call for inclusion of particular security controls. Evaluation against the PP-Module provides evidence that these controls are present and have been evaluated.

Table 12: Implicitly Satisfied Requirements Rationale

Requirement	Rationale for Satisfaction
FIA_UID.1 – Timing of Identification	FIA_UAU.2 (which is iterated in this PP-Module as FIA_UAU.2/TC and FIA_UAU.2/VVoIP) has a dependency on FIA_UID.1 because authentication of an external entity requires that entity to first identify itself so that its identity can be validated by the authentication process. This SFR has not been defined in this PP-Module because in both iterations of FIA_UAU.2, the entity being authenticated is a trusted IT product in the TOE's operational environment that communicates with the TSF over a channel specified in FTP_ITC.1/ESC. FTP_ITC.1/ESC explicitly states that the channel itself provides 'assured identification of its end points' which implies that these entities are identified prior to the authentication behavior required by the iterations of FIA_UAU.2.
FMT_MSA.3 – Static Attribute Initialization	FDP_IFF.1 has a dependency on FMT_MSA.3 to define the default security posture of security attributes for the purpose of information flow control enforcement. This SFR has not been defined by this PP-Module because the enforcement of FDP_IFF.1 is not dependent on the initial state of security attributes. For example, FDP_IFF.1.2 requires the TSF to determine if a communication attempt is valid before authorizing it. This is true regardless of whether the default value of security attributes associated with the connection attempt are permissive or restrictive; there is no difference in how the TSF determines "validity" in this case. The default values of security attributes do not cause the information flow control policy to behave differently for those rules that must always be enforced by the TSF. The ST author has the ability to define additional default-allow or default-deny rules through the assignments in

Requirement	Rationale for Satisfaction
	FDP_IFF.1.4 and 1.5. The ability to specify this behavior in the policy itself implies a default security posture of the relevant security attributes that does not need to be explicitly re-stated in a separate SFR.

E. Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy source(s) beyond the requirements outlined in the Base-PP. As with other Base-PP requirements, the only additional requirement is that the entropy documentation also applies to the specific ESC capabilities of the TOE that require random data, in addition to any functionality required by the Base-PP.

F. References

Table 13: References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2070-04-001, Version 3.1 Revision 5, April 2017 • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017 • CC and CEM addenda: Exact Conformance, Selection-Based SFRs, Optional SFRs, CCDB-2017-05-xxx, Version 0.5, May 2017
[NDcPP]	Collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020
[NIST SP 800-88]	Guidelines for Media Sanitization, Revision 1, December 2014
[SD]	Supporting Document Mandatory Technical Document, PP-Module for ESC, Version 1.0, November 19, 2020

G. Acronyms

The acronym definitions in the NDcPP should be consulted in addition to those defined here.

Table 14: Acronyms

Acronym	Meaning
CDR	Call Detail Record
ESC	Enterprise Session Controller
IP-PBX	Internet Protocol Private Branch Exchange
MGCP	Media Gateway Control Protocol
NDcPP	Collaborative Protection Profile for Network Devices
OA&M	Operations, Administration, and Management
OSP	Organizational Security Policies
SBC	Session Border Controller
SIP	Session Initiation Protocol
VVoIP	Voice/Video over IP