PP-Module for VVoIP

Version: 2.0
2026-03-17
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2020-10-28	Initial publication
2.0	2026-03-17	CC:2022 updates, incorporation of TDs

Contents

1 Introduction

1.1 Overview

The scope of this PP-Module is to describe the security functionality of a Voice/Video over IP (VVoIP) endpoint 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: f

- Protection Profile for Application Software, Version 2.0
- Network Device collaborative Protection Profile, Version 4.0

These Base-PPs are both valid because a VVoIP endpoint is a specific type of network device or software application that carries sensitive data over remote channels and uses protocols to do so that a typical network device or software application does not implement. Therefore, additional security requirements are necessary to ensure that sensitive communications are not subject to unauthorized disclosure to unintended recipients.

Note that the NDcPP defines an optional architecture for a "distributed TOE" that allows for security functionality to be spread across multiple distinct components. However, a TOE that conforms to the NDcPP and this PP-Module will not be a distributed TOE. All security functionality will be contained within a single physical device.

1.2 Terms

The following sections list Common Criteria and technology terms used in this document.

1.2.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.

Direct Rationale	A type of Protection Profile, PP-Module, or Security Target in which the security problem definition (SPD) elements are mapped directly to the SFRs and possibly to the security objectives for the operational environment. There are no security objectives for the TOE.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Functional Package (FP)	A document that collects SFRs for a particular protocol, technology, or functionality.
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 (PP-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-PPs.
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 Technical Terms

Basic telephony functions	The basic functions a VVoIP phone must provide – pick up, dial tone, dial, talk.
Call control	The packets exchanged between devices to establish, maintain, and tear down a telephony call.
Client	A VVoIP endpoint.
Enterprise Session Controller (ESC)	A VVoIP call control server for VVoIP devices.
H.323	A communications protocol defined by ITU-T that is used for creating, modifying, and terminating multimedia sessions with multiple participants.

Peer-to-Peer (P2P)	A VVoIP architecture that forces each peer to be a server and client at the same time.
SDES-SRTP	A method of key negotiation for SRTP.
Secure Real-Time Transport Protocol (SRTP)	A protocol that is used to provide multimedia (voice/video) streaming services with added security of encryption, message authentication and integrity, and replay protection.
Sensitive Data	Call control/signal data, media data, and audit/management data that must be protected while in transit to prevent unauthorized disclosure.
Session Initiation Protocol (SIP)	A communications protocol defined by IETF that is used for creating, modifying, and terminating multimedia sessions with multiple participants.
Software/firmware update delivery channel	A trusted channel between a client and file server (which may be the same server as the call control server) for secure file download of software/firmware updates.
State	A configuration of a VVoIP endpoint based on how the user is currently using or not using the endpoint. Examples include: • Hook state: whether the endpoint is active (off-hook) or inactive (on-hook) • Mute state: the endpoint is active but is deliberately not transmitting data • Hold state: the endpoint is active but is deliberately not transmitting or receiving data
Streaming media	The voice/video exchanged between VVoIP endpoints.
VVoIP Call Control Server	A VVoIP infrastructure device that performs call control functions between a client and other VVoIP endpoints; this may be either a dedicated device such as an ESC or a VVoIP device itself when using P2P.

1.3 Compliant Targets of Evaluation

This PP-Module specifically addresses a dedicated network device or software application that facilitates the exchange of voice or video communication across an Internet Protocol (IP) network. The endpoint is a client (TOE) that communicates with a VVoIP call control server and may serve as its own call control server when using P2P. The VVoIP endpoint shall be able to secure file download from a file server to update VVoIP endpoint software and configuration, to establish secure communication for call control with the call control server, and to secure streaming media to other devices.

The combination of the NDcPP and this PP-Module is a network device that provides VVoIP endpoint functionality in addition to all of the security functionality expected of a network device as mandated by the NDcPP. The combination of the App PP and this PP-Module is a software application running on a general-purpose operating system that includes VVoIP endpoint capabilities in addition to all of the security functionality expected of a software application as mandated by the App PP.

This PP-Module describes the functional requirements and threats specific to the VVoIP endpoint. The most notable additions are requirements for the call control protocol (SIP, H.323) and streaming media protocol (SRTP, RTP). A conformant TOE is expected to be a standalone device or application; distributed TOE's are not permitted.

1.3.1 TOE Boundary

The TOE boundary includes the VVoIP-capable device or application (VVoIP endpoint). A VVoIP-capable device is a dedicated phone whereas a VVoIP endpoint application is just one of many applications that runs on a general-

purpose device such as a smartphone, tablet, or PC. Regardless of whether the TOE is a hardware appliance or a client application on an operating system, it will be deployed in the same environment. The figure below shows a typical VVoIP infrastructure from the perspective of the TOE. Many of the environmental components have direct connections between one another, but since these are not visible to the TOE, these connections have not been depicted.

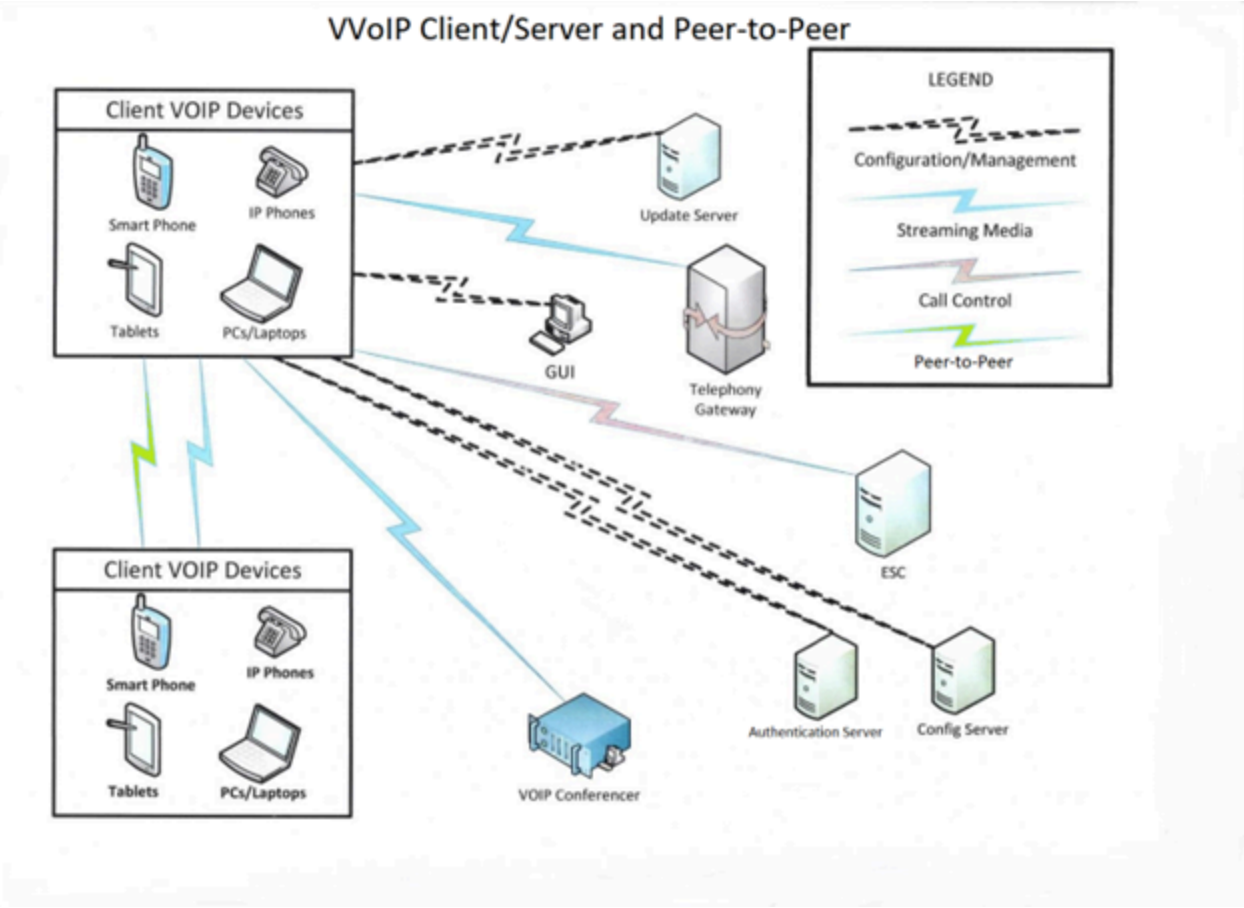


Figure 1: Typical VVoIP Deployment

The TOE uses a VVoIP call control server, either by connecting to an ESC or acting as one itself when using P2P, in order to set up connections with other VVoIP endpoint devices or other telephony equipment such as a conference bridge. The call control server also may have the ability to deliver software/firmware updates to the TOE, but this can alternatively be performed by a file server. The TOE must be able to process Internet Protocol version 4 (IPv4) and/or IPv6 packets.

To be able to initiate communications in a client-server architecture, the TOE needs at minimum an IP address, network mask, gateway address, configuration server address, update server address (or may rely on platform for updates if it is a software application configured to do so), and call control server address. The address may be obtained by Dynamic Host Configuration Protocol (DHCP), manually entered on the VVoIP endpoint, or inherited from the device the TOE resides on (if it is a software application); addresses can belong to the same device if it performs multiple functions (such as an ESC which also performs updates). The TOE should allow basic telephony functions. Once the IP addresses are obtained, the TOE downloads any VVoIP application updates, downloads VVoIP endpoint configuration, and connects to the call control server as a VVoIP client. When a call is finished or the line is otherwise not in use, the TOE will ensure that streaming media communication paths/ports are closed while call control remains open.

To be able to initiate communications in P2P, the TOE needs at minimum an IP address, network mask, gateway address, and update server address (or may rely on platform for updates if it is a software application configured to do so). The address may be obtained by DHCP, manually entered on the VVoIP endpoint, or inherited from the device the TOE resides on (if it is a software application). The TOE should allow basic telephony functions. Once the IP addresses are obtained, the TOE downloads any VVoIP application updates. The endpoint configuration for P2P TOE of telephony functions is local. When the TOE initiates a call, the TOE connects to the other peer's call

control (which is active) and the TOE is a client. When the TOE receives a call, the other peer acts as a client and connects to the TOE's call control. When a call is finished or the line is otherwise not in use, the TOE will ensure that streaming media communication paths/ports are closed while call control remains open.

The TOE has three paths for three different functions that need to execute: streaming media path that contains voice, video, and session control (endpoint to endpoint); call control path to control the endpoint (endpoint to VVoIP call control server), and configuration/management path to configure and manage the TOE (software/firmware updates, configuration updates, audit).

1.4 Use Cases

This PP-Module defines four potential use cases for the VVoIP TOE, defined below. The first two use cases define the physical embodiment of the TOE, while the latter two define its role in a telecommunications deployment.

Regardless of the physical embodiment of the TOE, the expected functional capabilities are similar. However, when the TOE is deployed in a peer-to-peer architecture, it must perform auditing and call control functions that a client-server TOE does not need to perform because the Enterprise Session Controller provides those functions in that architecture. A client-server TOE may also perform its own auditing, but it is not required.

[USE CASE 1] Dedicated Appliance

The VVoIP endpoint is sold and packaged as a standalone network appliance that does not have a direct interface to the underlying platform operating system. In this use case, conformance to the NDcPP and this PP-Module is sufficient to ensure security. Note that the NDcPP defines optional functionality for "distributed TOEs" – for a TOE to conform to this PP-Module, it must be a single device and not a distributed TOE.

[USE CASE 2] Software Application

The VVoIP endpoint is sold and packaged as an application that is installed on a general-purpose computer or mobile device running a modifiable operating system (such as Windows or Linux). This computer may run end user applications above and beyond those used for VVoIP communications since it functions as a user workstation. In this case, the VVoIP endpoint application is expected to conform to both this PP-Module and the App PP.

[USE CASE 3] Client-Server Architecture

The VVoIP endpoint, whether hardware or software, is deployed in an environment where it interacts with an Enterprise Session Controller to facilitate call control functions.

[USE CASE 4] Peer-to-Peer Architecture

The VVoIP endpoint, whether hardware or software, is deployed in an environment where it interacts directly with other VVoIP endpoints without the use of an Enterprise Session Controller as an intermediary.

1.5 Package Usage

This section contains selections and assignments that are required when the listed Functional Packages are claimed by this PP-Module.
Package Usage guidance defined in the TOE's relevant Base-PP applies to the usage of the packages for this module, unless explicitly stated otherwise in this section.

Functional Package for X.509, Version 1.0

Certificate Verification and Assertion Required in FIA_XCU_EXT.1.1

Because this PP-Module mandates support for mutual authentication for media channels, the ST author shall select the options to both verify and assert certificate identities in FIA_XCU_EXT.1.1.

Limitations on Signature Algorithms in FIA_X509_EXT.1.1

The TOE must utilize appropriate cryptographic algorithms that conform to CNSA standards. Thus, the TOE shall utilize no other algorithms outside of those specified in RFC 8603 for certificate or CRL signatures. Additionally, the TOE shall not use ECDSA with SHA-512 signatures for OCSP responses, and shall utilize no other algorithms for OCSP responses.

Required Extension Processing for FIA_X509_EXT.1.2

The ST author shall select the options to process the basicConstraints and extendedKeyUsage extensions. Other extensions may be selected as appropriate without restriction.

CRL or OCSP-based Revocation Required for FIA_X509_EXT.1.3

The TOE must support revocation that only involves CRL or OCSP. Accordingly, the TOE shall select only from options involving CRL or OCSP in FIA_X509_EXT.1.3 (e.g., the selection to treat all certificates older than a given short timeframe is not an acceptable substitute or alternative for supporting CRL or OCSP).

Connections to CRL or OCSP Servers Required for FIA_X509_EXT.1.4

Because the TOE is required to support CRL or OCSP, the TSF shall support an appropriate mechanism for obtaining revocation status information. In the case of CRL, the ST author shall claim that revocation status information is obtained via network connection to a CRL distribution point. In the case of OCSP, the ST author shall claim that revocation status information is obtained via network connection to an OCSP responder, via OCSP stapling, or via OCSP multi-stapling.

Restrictions on Acceptable Key Usage Values for FIA_X509_EXT.1.5

The TOE will always support the use of extendedKeyUsage values to verify that X.509 certificates are used in accordance with their intended purpose. Accordingly, the ST author shall claim that the TOE supports the processing of extendedKeyUsage fields in the leaf certificate (as opposed to application of trust store context rules or passing the certification path or other supported context information to an external function) and shall select all values that are relevant to the claimed uses of X.509 in the ST. In particular, since the PP does not define any functions that require the use of S/MIME, the ST author shall not select this as an extendedKeyUsage value to be validated.

Requirements on Functions for FIA_X509_EXT.2.1

The ST author shall additionally ensure that the selections and assignments in this requirement reflect the TOE's usage of X.509 certificate validation for TLS. Other assignments and selections may be made as applicable for other TOE functions.

Functional Package for Transport Layer Security (TLS), Version 2.1

DTLS or TLS Server and Client Functionality Required

The ST author shall select the option to utilize TLS as a client. The ST author shall additionally select the option to utilize DTLS as a client if support for DTLS is claimed in FTP_ITC.1.

DTLS or TLS Mutual Authentication Required

The ST shall select the option to support mutual authentication in FCS_TLSC_EXT.1 and FCS_TLSS_EXT.1, or FCS_DTLSC_EXT.1 and FCS_DTLSS_EXT.1, according with the protocol support claimed in FTP_ITC.1.

1.6 Implementation-Based Features

The following features of the TOE are implementation-based. A TOE is not required to implement these features to conform to this PP-Module, but if the feature is implemented, it is expected that associated implementation-based requirements are claimed as part of the TSF.

1.6.1 Software Application with Logging

The TOE is a software application and claims the App-PP as the Base-PP. The TOE additionally implements logging features (i.e. includes one or more of the following SFRs in the ST: FAU_GEN.1/CSADMIN, FAU_GEN.1/CSVVOIP, FAU_GEN.1/P2PADMIN, FAU_GEN.1/P2PVVOIP).

If this feature is implemented by the TOE, the following requirements must be claimed in the ST:

- **FAU_STG.1**
- **FAU_STG.5**

2 Conformance Claims

Conformance Statement

An ST must claim exact conformance to this PP-Module.

The evaluation methods used for evaluating the TOE are a combination of the workunits defined in [CEM] as well as the Evaluation Activities for ensuring that individual SFRs and SARs have a sufficient level of supporting evidence in the Security Target and guidance documentation and have been sufficiently tested by the laboratory as part of completing ATE_IND.1. Any functional packages this PP claims similarly contain their own Evaluation Activities that are used in this same manner.

CC Conformance Claims

This PP-Module is conformant to Part 2 (extended) and Part 3 (extended) of Common Criteria CC:2022, Revision 1.

PP Claim

This PP-Module does not claim conformance to any Protection Profile.

The following PPs and PP-Modules are allowed to be specified in a PP-Configuration with this PP-Module:

- Network Device collaborative Protection Profile Version 4.0
- Protection Profile for Application Software Version 2.0

Package Claim

- This PP-Module is Functional Package for TLS, version 2.0 conformant.
- This PP-Module does not conform to any assurance packages.

The functional packages to which the PP conforms may include SFRs that are not mandatory to claim for the sake of conformance. An ST that claims one or more of these functional packages may include any non-mandatory SFRs that are appropriate to claim based on the capabilities of the TSF and on any triggers for their inclusion based inherently on the SFR selections made.

3 Security Problem Definition

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.

3.1 Threats

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

T.MEDIA_DISCLOSURE

An attacker can use the encrypted variable rate vocoder frames to their advantage to decode transmitted data. An attacker can also use improperly protected data to discern sensitive information.

T.UNDETECTED_TRANSMISSION

An attacker may cause the TOE to exfiltrate audio or video media over a remote channel while in a state where the user has a reasonable expectation that no media is being transmitted.

3.2 Assumptions

These assumptions are made on the Operational Environment (OE) in order to be able to ensure that the security functionality specified in the PP-Module can be provided by the TOE. If the TOE is placed in an OE that does not meet these assumptions, the TOE may no longer be able to provide all of its security functionality.

The following assumptions that are defined in this PP-Module extend the assumptions that are defined by the Base-PPs.

A.UPDATE_SOURCE

It is assumed that TOE software/firmware updates will be made available on either the call control server that the TOE connects to or a separate file server managed by the organization.

Note that because this PP-Module specifically disallows distributed TOEs, a conformant TOE will not claim A.COMPONENTS_RUNNING when NDcPP is the Base-PP.

3.3 Organizational Security Policies

This PP defines no Organizational Security Policies beyond those defined in the claimed Base-PP(s).

4 Security Objectives

4.1 Security Objectives for the Operational Environment

The following environmental security objectives that are defined in this PP-Module extend the objectives that are defined by the Base-PPs.

OE.UPDATE_SOURCE

The operational environment will have TOE software/firmware made available on either the call control server that the TOE connects to or a separate file server managed by the organization.

Note that because this PP-Module specifically disallows distributed TOEs, a conformant TOE will not claim OE.COMPONENTS_RUNNING when NDcPP is the Base-PP.

4.2 Security Objectives Rationale

This section describes how the assumptions and organizational security policies map to operational environment security objectives.

Table 1: Security Objectives Rationale

Assumption or OSP	Security Objectives	Rationale
A.UPDATE_SOURCE	OE.UPDATE_SOURCE	The objective satisfies the assumption by ensuring that TOE updates are made available in the intended location.

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following conventions are used for the completion of operations:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): Is used to add details to a requirement or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): Is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): Is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: Is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."

5.1 Collaborative Protection Profile for Network Devices Security Functional Requirements Direction

In a PP-Configuration that includes the NDcPP, the VVoIP client is expected to rely on some of the security functions implemented by the network device as a whole and evaluated against the NDcPP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the NDcPP in addition to what is mandated by section 5.3.

5.1.1 Modified SFRs

The SFRs listed in this section are defined in the NDcPP and relevant to the secure operation of the TOE.

5.1.1.1 Security Audit (FAU)

FAU_STG_EXT.1: Protected Audit Event Storage

This SFR is modified to prohibit the selection of distributed TOE options. Any element not specified in this section is unchanged from its definition in the Base-PP.

The text of FAU_STG_EXT.1.2 is replaced with:

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*].

Application Note: This PP-Module modifies the existing FAU_STG_EXT.1 SFR in the NDcPP to prohibit the selection of any “distributed TOE” behavior in FAU_STG_EXT.1.2. The SFR is otherwise unchanged.

5.1.1.2 Cryptographic Support (FCS)

FCS_NTP_EXT.1: NTP Protocol

This SFR is selection-based in the NDcPP and remains selection-based in this PP-Module. However, an additional trigger for this SFR's inclusion is added for the selection of "register the TOE to an ESC…" in FMT_SMF.1/VVoIP if the TOE is a hardware device. This is because any hardware-based VVoIP TOE that can be registered to an ESC is required to use the ESC as an NTP time source.

If the TOE is not registered to an ESC, it is not relevant to this PP-Module whether or not NTP is implemented, and in this case this SFR remains selection-based on FPT_STM_EXT.1.2, which is not modified by this PP-Module (i.e. a peer-to-peer TOE does not register to an ESC but may still receive time data from a separate NTP source).

5.1.1.3 Protection of the TSF (FPT)

FPT_TUD_EXT.1: Trusted Update

This PP-Module does not modify this SFR as it is defined in the NDcPP. However, note that this PP-Module expects that either the call control server or a separate file server managed by the organization to function as the source of TOE software/firmware updates. The evaluator shall ensure that the test environment is configured appropriately.

Evaluation Activities:

There is no change to the EAs specified for this SFR in the NDcPP Supporting Document. Note however that the following additional configuration steps are necessary in order for this testing to be performed:

- The evaluator shall deploy a call control server or dedicated file server in the TOE's operational environment
- The evaluator shall load valid and invalid candidate updates to the call control server or dedicated file server
- The evaluator shall configure the TOE to use the call control server or dedicated file server as its source for software/firmware updates

5.1.1.4 Trusted Path (FTP)

FTP_ITC.1: Inter-TSF Trusted Channel

This SFR is modified to mandate the inclusion of TLS. Any other protocols may additionally be claimed. Any element that is not included in this section is unchanged from its definition in the Base-PP.

The text of the requirement is replaced with:

FTP_ITC.1.1 The TSF shall be capable of using **TLS as defined in the Functional Package for TLS and** [**selection:** *IPsec, SSH as defined in the Functional Package for SSH, DTLS as defined in the Functional Package for TLS, HTTPS,* ***no other protocols***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, **streaming media channel, call control channel, software/firmware update delivery channel,** [**selection:** *authentication server, [****assignment:*** *other capabilities], 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 disclosure and detection of modification of the channel data.

Application Note: The NDcPP provides the ability for the ST author to specify the protocols used to establish trusted communications in FTP_ITC.1.1. This PP-Module mandates the inclusion of TLS because it is the underlying protocol used to secure communications with the ESC and other VVoIP endpoints. Additional protocols should be selected if they are used for securing other trusted channels. For example, the TSF may communicate with an ESC using TLS for call control functions but some other

protocol for remote transmission of audit data. This PP-Module also specifies additional uses for the trusted channel beyond what the NDcPP defines. The remainder of the SFR is unchanged from its definition in the Base-PP.

5.1.2 Additional SFRs

This PP-Module does not define any additional SFRs for any PP-Configuration where the NDcPP is claimed as the Base-PP.

5.2 Protection Profile for Application Software Security Functional Requirements Direction

In a PP-Configuration that includes the App PP, the VVoIP client is expected to rely on some of the security functions implemented by the software application as a whole and evaluated against the App PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the App PP in addition to what is mandated by section 5.3.

5.2.1 Modified SFRs

The SFRs listed in this section are defined in the APP PP and relevant to the secure operation of the TOE.

5.2.1.1 Protection of the TSF (FPT)

FPT_TUD_EXT.1: Trusted Update

This PP-Module does not modify this SFR as it is defined in the App PP. However, note that this PP-Module expects that either the call control server or a separate file server managed by the organization to function as the source of TOE software/firmware updates. A vendor provided source should only be used if a call control server or separate file server cannot be configured.

Evaluation Activities:

There is no change to the EAs specified for this SFR in the App PP. Note however that the following additional configuration steps may be necessary when relying on a call control server or dedicated file server in order for this testing to be performed:

- The evaluator shall deploy a call control server or dedicated file server in the TOE's operational environment
- The evaluator shall load valid and invalid candidate updates to the call control server or dedicated file server
- The evaluator shall configure the TOE or its operational environment (whichever is selected to implement the security functions) to use the call control server or dedicated file server as its source for software/firmware updates.

5.2.1.2 Trusted Path/Channel (FTP)

FTP_DIT_EXT.1: Protection of Data in Transit

This SFR is modified from its definition in the Base-PP to mandate the inclusion of TLS as a method to protect data and to add support for the use of SRTP to protect data in transit.

The text of the requirement is replaced with:

FTP_DIT_EXT.1.1 The application shall [**selection:**

- *not transmit any [**selection, choose one of:** data, sensitive data*]
- *encrypt all transmitted [**selection, choose one of:** sensitive data, data] with **TLS as a server as defined in the Functional Package for Transport Layer Security (TLS), version 2.1 and also supports functionality for [selection: mutual authentication, none] and TLS as a client as defined in the Functional Package for Transport Layer Security (TLS), version 2.1** and **[selection:***
  - *HTTPS as a client in accordance with FCS_HTTPS_EXT.1 and FCS_HTTPS_EXT.2*
  - *HTTPS as a server in accordance with FCS_HTTPS_EXT.1*
  - *HTTPS as a server with support for mutual authentication in accordance with FCS_HTTPS_EXT.1 and FCS_HTTPS_EXT.2*
  - *DTLS as a server defined in the Functional Package for Transport Layer Security (TLS), version 2.1 and also supports functionality for [**selection:** mutual authentication, none]*
  - *DTLS as a client defined in the Functional Package for Transport Layer Security (TLS), version 2.1*
  - *SSH as defined in the Functional Package for Secure Shell (SSH), version 2.0*
  - *IPsec as defined in the VPN Client PP-Module, version 3.0*
  - ***Secure Real-Time Transport Protocol (SRTP)***

  *] for [**assignment:** function(s)] using certificates as defined in the Functional Package for X.509*
- *invoke platform-provided functionality to encrypt all transmitted sensitive data with **TLS and** [**selection:** HTTPS, DTLS, SSH, IPsec] for [**assignment:** function(s)] using certificates as defined in the Functional Package for X.509*
- *invoke platform-provided functionality to encrypt all transmitted data with **TLS and** [**selection:** HTTPS, DTLS, SSH, IPsec] for [**assignment:** function(s)] using certificates as defined in the Functional Package for X.509*

] between itself and another trusted IT product.

Application Note: The App PP provides the ability for the ST author to specify the protocols used to establish trusted communications and the behavior that trusted communications are used to protect. This PP-Module mandates the inclusion of TLS because it is the underlying protocol used to secure communications with a VVoIP call control server and other VVoIP endpoints. Additional protocols may be selected if they are used for securing other channels. For example, the TSF may communicate with an ESC using TLS for call control functions but some other protocol for remote transmission of audit data.

Since the App PP does not define separate SFRs for trusted channel (TOE to trusted third party) and trusted path (administrator to TOE), FTP_DIT_EXT.1 is expected to cover both use cases. The proper protocols should be selected accordingly.

Sensitive data includes at minimum call control/signal data, media data, and audit/management data.

If "SRTP" is selected in FTP_DIT_EXT.1.1, the selection-based SFRs FCS_COP.1/SRTP and FCS_SRTP_EXT.1 must be claimed.

5.2.2 Additional SFRs

This PP-Module does not define any additional SFRs for any PP-Configuration where the APP PP is claimed as the Base-PP.

5.3 TOE Security Functional Requirements

The following section describes the SFRs that must be satisfied by any TOE that claims conformance to this PP-Module. These SFRs must be claimed regardless of which PP-Configuration is used to define the TOE.

5.3.1 Auditable Events for Mandatory SFRs

Table 2: Auditable Events for Mandatory Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FCO_VOC_EXT.1	No events specified	N/A
FDP_IFC.1	Call Detail Record (CDR) of VVoIP peer communications.	• Calling party • Called party • Start time of call • Call duration
FDP_IFF.1	No events specified	N/A
FMT_SMF.1/VVoIP	[**selection**: *Registration of TOE to ESC.*, *None*]	[**selection, choose one of**: *IP address or identifier for the ESC*, *No additional information*]
FTA_SSL.3/MEDIA	Termination of a call due to inactivity.	Call party dropped time
FTP_ITC.1/CONTROL	Establishment of connection to VVoIP call control server	• Called party • Calling party • Established connection time
	Termination of connection to VVoIP call control server	• Called party • Calling party • Terminated connection time
FTP_ITC.1/MEDIA	Establishment of connection to VVoIP peer	• Called party • Calling party • Connection time to VVoIP peer
	Termination of connection to VVoIP peer	• Called party • Calling party • Disconnection time to VVoIP peer

5.3.2 Communications (FCO)

FCO_VOC_EXT.1 Fixed-Rate Vocoder

FCO_VOC_EXT.1.1

The TSF shall transmit voice media using a constant bit rate voice vocoder.

Application Note: A constant bit rate vocoder provides a constant output length that does not have the vulnerabilities that a variable bit rate vocoder contains when encrypted.

Evaluation Activities

FCO_VOC_EXT.1
TSS
The evaluator shall verify that the TSS specifies each vocoder used. The evaluator shall then examine the specification for each vocoder in order to verify that no variable rate vocoders are claimed by the TSF.

Guidance
There are no additional Guidance evaluation activities for this component.

Tests
The evaluator shall set up a test environment that contains the TOE, a call control server (which may be the TOE itself), a network switch, a packet capture tool, and a second VVoIP endpoint. The evaluator shall then perform the following test:

- *Test FCO_VOC_EXT.1:1:*
  - ***Step 1:*** *The evaluator shall ensure the TOE and the second VVoIP endpoint are registered to a call control server or are using P2P.*
  - ***Step 2:*** *.The evaluator shall use the TOE to dial the second VVoIP endpoint to establish a call and verify the call is established by holding a voice conversation.*
  - ***Step 3:*** *The evaluator shall review the captured traffic to verify that a fixed rate vocoder is used.*

  If multiple vocoders are supported, the evaluator shall reconfigure the TOE to use each individual vocoder and repeat steps 1-3 for each vocoder.

5.3.3 User Data Protection (FDP)

FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1

The TSF shall enforce the [*media transmission policy*] on [*voice/video media transmitted by the TOE*].

Application Note: There are states when on-hook voice and video must not stream from the TOE.

Evaluation Activities

FDP_IFC.1
TSS
The evaluator shall verify that the TSS describes how streaming media is not transmitted when not in a streaming media state.

Guidance
There are no additional Guidance evaluation activities for this component.

Tests
Testing of this component is performed through evaluation of FDP_IFF.1.

FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1

The TSF shall enforce the [*media transmission policy*] based on the following types of subject and information security attributes: [*TOE hook state, VVoIP call connection status, and VVoIP call control server status*].

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: [

- *The TOE is [**selection**: registered with a VVoIP call control server, acting as a VVoIP call control server when using P2P],*
- *A call has been established with a telephony device (VVoIP endpoint),*
- *The TOE is in the off-hook state,*
- *The TOE is not in the mute state,*
- *[**selection**: The TOE is not in the hold state, no other rules]*

].

Application Note: If "acting as a VVoIP call control server when using P2P" is selected, the ST must include the selection-based SFRs FAU_GEN.1/P2PADMIN, FAU_GEN.1/P2PVVOIP, FDP_IFC.1/CALLCONTROL, and FDP_IFF.1/CALLCONTROL.

FDP_IFF.1.3

The TSF shall enforce ~~the~~ [*no additional information flow control policy rules*].

FDP_IFF.1.4

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

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [*all TCP and UDP ports used by the TOE are closed when not in active use*].

Evaluation Activities

FDP_IFF.1

TSS

The evaluator shall verify that the TSS describes the TOE's enforcement of the media transmission policy and describes the conditions that are necessary for the TSF to transmit voice/video data to the operational environment.

Guidance

There are no additional Guidance evaluation activities for this component.

Tests

The evaluator shall set up a test environment that contains the TOE, a call control server (which may be the TOE itself), a network switch, a traffic capture tool, and a second VVoIP endpoint. The evaluator shall then perform the following tests:

- *Test FDP_IFF.1:1: (Conditional - physical TOE)*
  - ***Step 1:** The evaluator shall place the TOE into the on-hook state without registering it to the call control server or using P2P. The evaluator shall use the traffic capture tool to verify that the TOE does not transmit any streaming media traffic.*

- ***Step 2:*** *The evaluator shall place the TOE into the off-hook state and use the traffic capture tool to verify that the TOE does not transmit any streaming media traffic.*

- *Test FDP_IFF.1:2: (Conditional - software application TOE)*
  - ***Step 1:*** *The evaluator shall execute the VVoIP application without registering it to the call control server or using P2P. The evaluator shall use the traffic capture tool to verify that the TOE does not transmit any streaming media traffic.*
  - ***Step 2:*** *The evaluator shall place the TOE into the off-hook state (e.g., by performing a call without specifying any destination data). The evaluator shall use the traffic capture tool to verify that the TOE does not transmit any streaming media traffic.*
- *Test FDP_IFF.1:3:*
  - ***Step 1:*** *The evaluator shall ensure the TOE is using P2P or register the TOE with the call control server and verify that the TOE is registered by checking the call control server screen with current TOE connections and by viewing the call control path traffic using the traffic capture tool.*
  - ***Step 2:*** *The evaluator shall place the TOE into the on-hook state and verify using the traffic capture tool that no streaming media traffic is transmitted by the TOE.*
  - ***Step 3:*** *The evaluator shall place the TOE into the off-hook state. The evaluator shall then verify that the TOE continues to not transmit streaming media traffic.*
- *Test FDP_IFF.1:4:*
  - ***Step 1:*** *The evaluator shall ensure the TOE is using P2P or shall register the TOE with the call control server and verify that it is registered by checking the call control server with current connections and using the traffic capture tool to verify the call control path traffic.*
  - ***Step 2:*** *The evaluator shall ensure the TOE is using P2P or shall register the second VVoIP endpoint with the call control server and verify that it has been registered by checking the call control server with current connections and using the traffic capture tool to verify the call control path traffic.*
  - ***Step 3:*** *The evaluator shall use the TOE to dial the second VVoIP endpoint and connect a call. The evaluator shall verify that the connection is made by having a voice/video conversation with the endpoint and using the traffic capture tool to verify that a steady stream of traffic is being transmitted between the two endpoints over the media channel.*
  - ***Step 4:*** *The evaluator shall use the TOE to put the call on mute and verify that no traffic is transmitted from the TOE over the media channel to the second VVoIP endpoint. If the TOE is registered to a call control server, the evaluator shall also verify that a mute control message is sent to the call control server and it responds.*
  - ***Step 5:*** *The evaluator shall use the TOE to take the call off mute and verify that the streaming media traffic between the TOE and the second VVoIP endpoint is resumed.*
- *Test FDP_IFF.1:5:*
  - ***Step 1:*** *The evaluator shall ensure the TOE is using P2P or register the TOE to the call control server and place it in the on-hook state.*
  - ***Step 2:*** *The evaluator shall use a fuzzing tool to attempt to connect to the TOE on the full range of TCP ports used by the TSF. All ports used by the TOE should be closed except for the port that is used to communicate with the ESC.*
- *Test FDP_IFF.1:6:*
  - ***Step 1:*** *The evaluator shall ensure the TOE and the second VVoIP endpoint are registered to a call control server or are using P2P.*
  - ***Step 2:*** *The evaluator shall place the TOE in the on-hook state.*
  - ***Step 3:*** *The evaluator shall use a fuzzing tool to attempt to connect to the TOE on the full range of UDP ports used by the TSF. All ports used by the TOE should be closed.*
  - ***Step 4:*** *The evaluator shall place a call to the second VVoIP endpoint and verify the call is established. The evaluator shall capture the traffic to determine the port used by the*

TOE to carry the media traffic.
    - ***Step 5:*** *The evaluator shall hang up the call and verify that the TOE has returned to the on-hook state.*
    - ***Step 6:*** *The evaluator shall perform fuzzing activities to verify that the port used to carry media traffic in step 4 has been closed.*
- *Test FDP_IFF.1:7: (Conditional - "The TOE is not in the hold state" is selected in FDP_IFF.1.2)*
    - ***Step 1:*** *The evaluator shall use the TOE to put the call on hold and verify that no streaming media traffic is transmitted from the TOE over the media channel. If the TOE is registered to a call control server, the evaluator shall also verify that the VVoIP endpoint on-hold call control is sent to the call control server and it responds.*
    - ***Step 2:*** *The evaluator shall use the TOE to take the call off hold and verify that the streaming media traffic between the TOE and the second VVoIP endpoint is resumed.*

5.3.4 Security Management (FMT)

FMT_SMF.1/VVoIP Specification of Management Functions (VVoIP Communications)

FMT_SMF.1.1/VVoIP

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

- *Ability to [**selection**:*
    - *register the TOE to an ESC [**selection**: manually, via DHCP server]*
    - *act as a VVoIP call control server when using P2P*

];

*[**selection**:*

- *Ability to configure audit behavior (e.g., changes to storage locations for audit; changes to behavior when local audit storage space is full);*
- *Ability to modify the behavior of the transmission of audit data to an external IT entity;*
- *Ability to configure the termination period for idle calls;*
- *Ability to specify the vocoder used;*
- *Ability to disable SRTP NULL algorithm;*
- *Ability to specify the ports to be used for SRTP communications;*
- *no other capabilities*

]].

Application Note: This SFR defines additional management functions for the TOE beyond what is defined in each of the supported Base-PPs as FMT_SMF.1. The TOE may have all management functionality implemented in the same logical interface; it is not necessary for the Base-PP management functions and the PP-Module's management functions to be implemented separately.

The audit-related sections are duplicates of those in the NDcPP's definition of FMT_SMF.1. If the VVoIP audit functionality is configurable separately from the auditing for the device as a whole, the relevant selections should be made or omitted in each iteration as needed.

If "register the TOE to an ESC..." is selected, regardless of Base-PP selection, the ST must include the selection-based SFR FPT_STM_EXT.1/VVoIP.

If the TOE claims conformance to the NDcPP and “register the TOE to an ESC…” is selected, the selection-based NDcPP SFR FCS_NTP_EXT.1 must additionally be claimed since connectivity to an ESC implies that the TSF will use it as an NTP server. In this case, the TOE does not need to implement two distinct time services for different purposes. The same time service defined by FPT_STM_EXT.1 may be used here as well. Note however, for this PP-Module, the TOE must use ESCs to which it is registered as its NTP time sources.

If "act as a VVoIP call control server when using P2P" is selected, the ST must include the selection-based SFRs FAU_GEN.1/P2PADMIN, FAU_GEN.1/P2PVVOIP, FDP_IFC.1/CALLCONTROL, and FDP_IFF.1/CALLCONTROL.

Evaluation Activities

FMT_SMF.1/VVoIP

TSS

The evaluator shall verify that the TSS provides a description of the TOE initial configuration and describes the ability of the TSF to manage the functions that are defined in the SFR, including how each function is managed (e.g., manually configured, applied via downloaded configuration file).

Guidance

The evaluator shall verify that the operational guidance provides instructions on configuring any functionality specifically related to VVoIP.

Tests

The evaluator shall perform the following tests, depending on the selections made:

- *Test FMT_SMF.1/VVoIP:1: (Conditional - "register the TOE to an ESC [manually]" is selected)*
  - ***Step 1:** On the TOE, input IP address, gateway address, and subnet mask.*
  - ***Step 2:** If the operational environment is deployed in a manner such that the configuration server and ESC are two distinct servers, input the addresses for each; otherwise, input the ESC address.*
  - ***Step 3:** Save the configuration.*
  - ***Step 4:** Verify the TOE registers to the ESC.*
- *Test FMT_SMF.1/VVoIP:2: (Conditional - "register the TOE to an ESC [via DHCP server]" is selected*
  - ***Step 1:** On the TOE, input the DHCP server address.*
  - ***Step 2:** Verify by traffic capture that the TOE receives all needed IP addresses.*
  - ***Step 3:** Verify by examining the IP address on the TOE.*
  - ***Step 4:** Verify the TOE registers to the ESC.*

Test EAs to verify that the TOE can act as a VVoIP call control server when using P2P (if it is selected) are performed as part of testing for FDP_IFF.1/CALLCONTROL.

Test EAs to verify the configuration of audit behavior are performed as part of testing for FAU_STG.1 and FAU_STG.5.

Test EAs to verify the modification of transmission of audit data to an external IT entity are performed as part of testing for FAU_STG.1.

Test EAs to verify that the idle call termination period can be specified are performed as part of testing for FTA_SSL.3/MEDIA, specifically Test 2 and Test 3.

Test EAs to verify that the vocoder can be specified are performed as part of testing for FCO_VOC_EXT.1.

5.3.5 TOE Access (FTA)

FTA_SSL.3/MEDIA TSF-Initiated Termination (Media Channel)

FTA_SSL.3.1/MEDIA

The TSF shall terminate **voice/video transmission** after [*inactivity longer than [**selection**: [**assignment**: default number of seconds] seconds, an administrator-configurable interval]*].

Application Note: This SFR is intended to mitigate the potential unauthorized disclosure of media data in the case where connectivity with the peer is lost. The ST author should choose one or both selections if applicable. Note that if "an administrator-configurable interval" is selected, the ST author must select "configure the termination period for idle calls" in FMT_SMF.1.1/VVoIP.

Evaluation Activities

FTA_SSL.3/MEDIA

TSS

The evaluator shall verify that the TSS specifies whether idle calls are terminated by default after a certain amount of time or by an administrator-configurable interval.

Guidance

If the idle call timeout period is administrator-configurable, the evaluator shall verify that the operational guidance includes instructions for how to configure this, as well as what the minimum and maximum allowed values are.

Tests

The evaluator shall set up a test environment that contains the TOE, a call control server (which may be the TOE itself), a configuration server (if used to communicate configuration changes to idle timeout period), a network switch, a traffic capture tool, and a second VVoIP endpoint. The evaluator shall then perform the following tests:

- *Test FTA_SSL.3/MEDIA:1:*
  - ***Step 1:** Deploy the TOE in a default configuration (i.e. without any administrative override applied to the idle timeout value).*
  - ***Step 2:** Ensure the TOE is using P2P or register the TOE with the call control server and verify that it is registered by viewing its status on the ESC and capturing the call control path traffic.*
  - ***Step 3:** Ensure the second VVoIP endpoint is using P2P or register the second VVoIP endpoint with the call control server and verify that it is registered by viewing its status on the call control server and capturing the call control path traffic.*
  - ***Step 4:** Use the TOE to dial the second VVoIP endpoint and establish a call. Verify the call was established by holding a conversation between the two peers and capturing the streaming media traffic that is transmitted between them.*
  - ***Step 5:** Power down the second VVoIP endpoint while the call is active. Observe that the TOE stops transmitting media after the default period of time specified in the ST.*

- *Test FTA_SSL.3/MEDIA:2: (Conditional - "an administrator-configurable interval is selected in FTA_SSL.3.1/MEDIA)*
  - ***Step 1:** Deploy the TOE in a default configuration (i.e. without any administrative override applied to the idle timeout value).*
  - ***Step 2:** Ensure the TOE is using P2P or register the TOE with the call control server and verify that it is registered by viewing its status on the call control server and capturing the call control path traffic.*
  - ***Step 3:** Configure the TOE's idle timeout period for the shortest period of time that is supported.*
  - ***Step 4:** Ensure the second VVoIP endpoint is using P2P or register the second VVoIP endpoint with the call control server and verify that it is registered by viewing its status on the call control server and capturing the call control path traffic.*
  - ***Step 5:** Use the TOE to dial the second VVoIP endpoint and establish a call. Verify the call was established by holding a conversation between the two peers and capturing the streaming media traffic that is transmitted between them.*
  - ***Step 6:** Power down the second VVoIP endpoint while the call is active. Observe that the TOE stops transmitting media after the period of time configured in Step 3.*
- *Test FTA_SSL.3/MEDIA:3: (Conditional - "an administrator-configurable interval" is selected in FTA_SSL.3.1/MEDIA)*

  Repeat Test 2 but in Step 3, configure the idle timeout value to be the longest period of time that is supported as opposed to the shortest.

5.3.6 Trusted Path/Channels (FTP)

FTP_ITC.1/CONTROL Inter-TSF Trusted Channel (Signaling Channel)

FTP_ITC.1.1/CONTROL

The TSF shall **be capable of using [selection: *Session Initiation Protocol (SIP), H.323*] to** provide a **trusted** communication channel between itself and **a VVoIP call control server** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

Application Note: Both the SIP and H.323 protocols rely on TLS. This SFR defines the application layer protocol used to secure call control functions.

FTP_ITC.1.2/CONTROL

The TSF shall permit [*the TSF, **the VVoIP call control server***] to initiate communication via the trusted channel.

FTP_ITC.1.3/CONTROL

The TSF shall initiate communication via the trusted channel for [*establishment of call control*].

Application Note: The call control channel is secured with TLS as specified in FTP_DIT_EXT.1 from App PP or FTP_ITC.1 from NDcPP.

Evaluation Activities

FTP_ITC.1/CONTROL

TSS
The evaluator shall verify that the TSS describes the ability of the TOE to use SIP and/or H.323 with TLS.

Guidance
There are no additional Guidance evaluation activities for this component.

Tests
The vendor shall provide to the evaluator application layer configuration settings for all secure communication mechanisms specified by the FTP_ITC.1/CONTROL requirement. This information should be sufficiently detailed to allow the evaluator to determine the application layer timeout settings for each cryptographic protocol. There is no expectation that this information must be recorded in any public-facing document or report.

The evaluator shall perform the following tests:

- *Test FTP_ITC.1/CONTROL:1: The evaluators shall ensure that communications using each protocol with a call control server is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.*
- *Test FTP_ITC.1/CONTROL:2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE.*
- *Test FTP_ITC.1/CONTROL:3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.*
- *Test FTP_ITC.1/CONTROL:4:*

  Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities.

  The evaluator shall, for a connection to a call control server using each claimed protocol, physically interrupt the connection to the call control server for the following durations: i) a duration that exceeds the TOE's application layer timeout setting, ii) a duration shorter than the application layer timeout but of sufficient length to interrupt the MAC layer.

  The evaluator shall ensure that, when the physical connectivity is restored, communications are appropriately protected and no TSF data is sent in plaintext.

  In the case where the TOE is able to detect when the cable is removed from the device, another physical network device (e.g., a core switch) shall be used to interrupt the connection between the TOE and the call control server. The interruption shall not be performed at the virtual node (e.g., virtual switch) and must be physical in nature.

  Further EAs are associated with the specific protocols.

FTP_ITC.1/MEDIA Inter-TSF Trusted Channel (Media Channel)

FTP_ITC.1.1/MEDIA

The TSF shall **be capable of using [selection: *SRTP, H.235/H.323*] to** provide a trusted communication channel between itself and **another VVoIP endpoint or other telephony device** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

Application Note: This SFR defines the application layer protocol used to secure voice/video transmissions once a call is established between another VVoIP endpoint

or other telephony device such as a call conference device.

If "SRTP" is selected, the selection-based SFRs FCS_COP.1/SRTP and FCS_SRTP_EXT.1 must be claimed.

FTP_ITC.1.2/MEDIA

The TSF shall permit [*the TSF, **another VVoIP endpoint or other telephony device***] to initiate communication via the trusted channel.

FTP_ITC.1.3/MEDIA

The TSF shall initiate communication via the trusted channel for [*transmission of voice/video media*].

Application Note: The corresponding trusted media channel must be chosen to match the trusted control channel: SIP – SRTP, H.323 – H.235/H.323.

If "SRTP" is selected in FTP_ITC.1.1/Media, the selection-based SFRs FCS_COP.1/SRTP and FCS_SRTP_EXT.1 must be claimed.

Evaluation Activities

FTP_ITC.1/MEDIA

TSS

The evaluator shall verify that the trusted channel will use SRTP or H.323/H.235 in accordance with the selections made in the SFR.

Guidance

There are no additional Guidance evaluation activities for this component.

Tests

The vendor shall provide to the evaluator application layer configuration settings for all secure communication mechanisms specified by the FTP_ITC.1/MEDIA requirement. This information should be sufficiently detailed to allow the evaluator to determine the application layer timeout settings for each cryptographic protocol. There is no expectation that this information must be recorded in any public-facing document or report.

The evaluator shall perform the following tests:

- *Test FTP_ITC.1/MEDIA:1: The evaluators shall ensure that communications using each protocol with another VVoIP endpoint is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.*
- *Test FTP_ITC.1/MEDIA:2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE.*
- *Test FTP_ITC.1/MEDIA:3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.*
- *Test FTP_ITC.1/MEDIA:4:*

  Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities.

  The evaluator shall, for a connection to another VVoIP endpoint device using each claimed protocol, physically interrupt the connection to that remote endpoint for the following durations: i) a duration that exceeds the TOE's application layer timeout setting, ii) a duration shorter than the application layer timeout but of sufficient length to interrupt the MAC layer.

The evaluator shall ensure that, when the physical connectivity is restored, communications are appropriately protected and no TSF data is sent in plaintext.

In the case where the TOE is able to detect when the cable is removed from the device, another physical network device (e.g., a core switch) shall be used to interrupt the connection between the TOE and the call control server. The interruption shall not be performed at the virtual node (e.g., virtual switch) and must be physical in nature.

Further EAs are associated with the specific protocols.

5.4 TOE Security Functional Requirements Rationale

The following rationale provides justification for each SFR for the TOE, showing that the SFRs are suitable to address the specified threats:

Table 3: SFR Rationale

Threat	Addressed by	Rationale
T.MEDIA_ DISCLOSURE	FAU_STG_EXT.1 (modified from NDcPP)	Mitigates the threat by ensuring that audit data is securely stored locally and transmitted to an external entity.
	FAU_STG.1 (optional for software-only TOEs)	Mitigates the threat by ensuring that audit data is securely transmitted to an external entity.
	FAU_STG.5 (optional for software-only TOEs)	Mitigates the threat by defining behavior for response to log space overruns.
	FCO_VOC_EXT.1	Mitigates the threat by defining the use of a fixed-rate vocoder to prevent the exposure of encryption vulnerabilities that are present with variable-rate vocoders.
	FCS_COP.1/SRTP (selection-based)	Mitigates the threat by defining the implementation of encryption used for SDES-SRTP, if supported by the TOE.
	FCS_NTP_EXT.1 (modified from NDcPP)	Mitigates the threat by defining how accurate system time is maintained, which is used to support certain cryptographic functions.
	FCS_SRTP_EXT.1 (selection-based)	Mitigates the threat by defining the implementation of the SRTP protocol, if supported by the TOE.
	FDP_IFC.1/CALLCONTROL (selection-based)	Mitigates the threat by defining a policy for protection of call control information in cases where the TOE can act as a VVoIP call control server in a peer-to-peer configuration.

	FDP_IFF.1/CALLCONTROL (selection-based)	Mitigates the threat by defining the implementation of the call control policy in cases where the TOE can act as a VVoIP call control server in a peer-to-peer configuration.
	FPT_STM_EXT.1/VVoIP (selection-based)	Mitigates the threat by defining how the TSF obtains system time in certain cases, which is then used as an input to other functions that support this objective.
	FPT_TUD_EXT.1 (modified from NDcPP and App PP)	Mitigates the threat by ensuring the cryptographic functions or other TSF can be updated to remain secure.
	FTP_DIT_EXT.1 (modified from App PP)	Mitigates the threat by defining the trusted communications channel used for VVoIP.
	FTP_ITC.1 (modified from NDcPP)	Mitigates the threat by defining the trusted communications channel used for VVoIP
	FTP_ITC.1/CONTROL	Mitigates the threat by defining the application-layer channel used for communications with a VVoIP call control server.
	FTP_ITC.1/MEDIA	Mitigates the threat by defining the application-layer channel used for communications of media (voice and video) data.
T.UNDETECTED_TRANSMISSION	FAU_GEN.1/CSADMIN (optional)	Mitigates the threat by optionally allowing a client-server TOE to provide an audit trail of administrative actions, which could diagnose misconfiguration of the TOE that could lead to unattended transmissions.
	FAU_GEN.1/P2PADMIN (selection-based)	Mitigates the threat by requiring a peer-to-peer TOE to provide an audit trail of administrative actions, which could diagnose misconfiguration of the TOE that could lead to unattended transmissions.
	FDP_IFC.1	Mitigates the threat by defining the existence of a media transmission policy.
	FDP_IFF.1	Mitigates the threat by defining how the media transmission policy is enforced to determine when transmissions should occur.
	FMT_SMF.1/VVoIP	Mitigates the threat by requiring the TSF to implement certain the management functions specific to VVoIP functionality.

FPT_STM_EXT.1/VVoIP (selection-based)	Mitigates the threat by requiring the TSF to specify how it obtains system time in certain cases, which is then used as an input to other functions that support this objective.
FTA_SSL.3/MEDIA	Mitigates the threat by requiring the TSF to terminate idle sessions.

6 Consistency Rationale

6.1 Collaborative Protection Profile for Network Devices

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 VVoIP endpoint functionality that is provided by the network device.

6.1.2 Consistency of Security Problem Definition

The threats and assumptions defined by this PP-Module (see sections 3.1 and 3.2) supplement those defined in the NDcPP as follows:

Table 4: Consistency of Security Problem Definition (NDcPP base)

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.MEDIA_DISCLOSURE	The NDcPP defines a threat for untrusted communications channels. The threat of media disclosure through vocoder frames is a type of side channel attack that is unique to the functions of a VVoIP endpoint. However, it is consistent with the overall threat of unintended disclosure of sensitive data.
T.UNDETECTED_TRANSMISSION	The NDcPP defines threats for insecure communications and undetected activity. Unauthorized and undetected use of a communications channel is consistent with these threats.
A.UPDATE_SOURCE	The NDcPP does not have any assumptions for the source of TOE updates, only that the updates have adequate integrity protections. There is no conflict with this Module assuming that TOE updates will be retrieved from a particular location.

6.1.3 Consistency of OE Objectives

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

Table 5: Consistency of OE Objectives (NDcPP base)

PP-Module OE Objective	Consistency Rationale
OE.UPDATE_SOURCE	The NDcPP requires the TOE to be able to apply software/firmware updates but does not define any specific way that these updates need to be made available. This PP-Module defines an objective that allows for an assumption that TOE updates will be made available in a specific location. A.UPDATE_SOURCE is consistent with the Base-PP objectives for the same reason.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the NDcPP that are needed to support VVoIP functionality. This is considered to be consistent because the functionality provided by the NDcPP is being used for its intended purpose. The rationale for why this does not conflict with the claims defined by the NDcPP are as follows:

Table 6: Consistency of Requirements (NDcPP base)

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FAU_STG_EXT.1	This PP-Module modifies this SFR to prohibit the selection of any "distributed TOE" behavior in FAU_STG_EXT.1.2.
FCS_NTP_EXT.1	This PP-Module does not modify this SFR; it only modifies the circumstances that trigger its inclusion in the TOE's logical boundary.
FPT_TUD_EXT.1	This PP-Module does not modify this SFR; it only specifies that the source of TOE software/firmware updates must be a specific type of server.
FTP_ITC.1	This PP-Module restricts the Base-PP SFR to a subset of existing permissible functionality and does not introduce any new behavior.
Additional SFRs	
This PP-Module does not add any requirements when the NDcPP is the base.	
Mandatory SFRs	
FCO_VOC_EXT.1	The use of a fixed-rate vocoder relates to application-layer communications that are not within the scope of the NDcPP.
FDP_IFC.1	This SFR defines a policy for when data will or will not be transmitted by the TSF. The NDcPP defines requirements for how data is transmitted but a policy governing when an external interface may be invoked is beyond its scope.
FDP_IFF.1	This SFR defines the rules for a policy for when data will or will not be transmitted by the TSF. The NDcPP defines requirements for how data is transmitted but a policy governing when an external interface may be invoked is beyond its scope.
FMT_SMF.1/VVoIP	This PP-Module defines a new iteration of FMT_SMF.1 to add additional management functions that relate specifically to VVoIP functionality. The addition of these functions does not prevent any of the original functions from being implemented. This iteration does include two duplicates of management functions specified in the Base-PP; this is consistent because it is possible that auditing is handled differently for the VVoIP functionality as it is for the rest of the TOE's auditing. These functions are also selectable so it is not required that a conformant TOE implement this.
FTA_SSL.3/MEDIA	This SFR defines session termination behavior for the TOE's media channel. This interface is specific to this PP-Module and is not within the scope of the NDcPP.
FTP_ITC.1/CONTROL	This SFR defines the trusted communications protocol used by the TOE's signaling channel, which is specific to the VVoIP technology and does not

	conflict with the functionality defined in the NDcPP.
FTP_ITC.1/MEDIA	This SFR defines the trusted communications protocol used by the TOE's media channel, which is specific to the VVoIP technology and does not conflict with the functionality defined in the NDcPP.
Optional SFRs	
FAU_GEN.1/CSADMIN	The NDcPP already defines an audit generation function. This PP-Module adds redundant audit events for administrative actions (with respect to those defined in the NDcPP) to be required for software-only TOEs. A TOE that conforms to the NDcPP satisfies this SFR by default.
FAU_GEN.1/CSVVOIP	The NDcPP already defines an audit generation function. This PP-Module adds an iteration of FAU_GEN.1 for the auditable events that relate specifically to VVoIP endpoint behavior that may apply for client-server TOEs.
Objective SFRs	
This PP-Module does not define any Objective requirements.	
Implementation-dependent SFRs	
FAU_STG.1	This SFR is implementation-dependent and is explicitly not claimed when the NDcPP is the Base-PP. Therefore there is no conflict between this SFR and the NDcPP.
FAU_STG.5	This SFR is implementation-dependent and is explicitly not claimed when the NDcPP is the Base-PP. Therefore there is no conflict between this SFR and the NDcPP.
Selection-based SFRs	
FAU_GEN.1/P2PADMIN	The NDcPP already defines an audit generation function. This PP-Module adds redundant audit events for administrative actions (with respect to those defined in the NDcPP) to be required for software-only TOEs. A TOE that conforms to the NDcPP satisfies this SFR by default.
FAU_GEN.1/P2PVVOIP	The NDcPP already defines an audit generation function. This PP-Module adds an iteration of FAU_GEN.1 for the auditable events that relate specifically to VVoIP endpoint behavior that must apply for peer-to-peer TOEs.
FCS_COP.1/SRTP	This SFR defines the AES functionality used to support SRTP. This does not conflict with the NDcPP because the TOE can still use FCS_COP.1/DataEncryption to make claims related to all other uses of AES.
FCS_SRTP_EXT.1	This SFR defines support for the SRTP protocol, which is specific to VVoIP technology. The TSF's implementation of this protocol does not prevent the enforcement of any NDcPP SFRs.
FDP_IFC.1/CALLCONTROL	This SFR defines VVoIP call control policy. The TSF's implementation of this protocol does not prevent the enforcement of any NDcPP SFRs.
FDP_IFF.1/CALLCONTROL	This SFR defines VVoIP call control policy. The TSF's implementation of this protocol does not prevent the enforcement of any NDcPP SFRs.

FPT_STM_EXT.1/VVoIP	This SFR defines the TOE's reliance on ESCs to act as its NTP servers in deployments where the TOE is registered to them. It is duplicative of the FPT_STM_EXT.1 SFR defined in the Base-PP but is refined to identify the use of the ESC as a specific NTP server, which is a restriction not present in the Base-PP.

6.2 Protection Profile for Application Software

6.2.1 Consistency of TOE Type

When this PP-Module is used to extend the App PP, the TOE type for the overall TOE is still a software application. The TOE boundary is simply extended to include the VVoIP endpoint functionality that is supported by the application.

6.2.2 Consistency of Security Problem Definition

The threats and assumptions defined by this PP-Module (see sections 3.1 and 3.2) supplement those defined in the App PP as follows:

Table 7: Consistency of Security Problem Definition (APP PP base)

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.MEDIA_DISCLOSURE	The App PP defines a threat for network eavesdropping. The threat of media disclosure through vocoder frames is a type of side-channel attack that is unique to the functions of a VVoIP endpoint. However, it is consistent with the overall threat of unintended disclosure of sensitive data.
T.UNDETECTED_TRANSMISSION	The App PP defines threats for network attack and network eavesdropping. Unauthorized and undetected use of a communications channel is consistent with these threats.
A.UPDATE_SOURCE	The App PP does not have any assumptions for the source of TOE updates, only that the updates have adequate integrity protections. There is no conflict with this Module assuming that TOE updates will be retrieved from a particular location.

6.2.3 Consistency of OE Objectives

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

Table 8: Consistency of OE Objectives (APP PP base)

PP-Module OE Objective	Consistency Rationale
OE.UPDATE_SOURCE	The App PP requires the TOE to be able to apply software/firmware updates but does not define any specific way that these updates need to be made available. This PP-Module defines an objective that allows for an assumption that TOE updates will be made available in a specific location. A.UPDATE_SOURCE is consistent with the Base-PP objectives for the same reason.

6.2.4 Consistency of Requirements

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

Table 9: Consistency of Requirements (APP PP base)

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FPT_TUD_EXT.1	This PP-Module does not modify this SFR; it only specifies that the source of TOE software/firmware updates must be a specific type of server.
FTP_DIT_EXT.1	This PP-Module modifies the App PP SFR by mandating the use of trusted communications to secure transmitted data, mandating support for TLS, and permitting support for SRTP. The first two modifications are derived from selections that are already present in the App PP version of the SFR. The addition of SRTP does not prevent any of the other protocols from being used if supported.
Additional SFRs	
This PP-Module does not add any requirements when the APP PP is the base.	
Mandatory SFRs	
FCO_VOC_EXT.1	The use of a fixed-rate vocoder relates to application-layer communications that are not within the scope of the App PP.
FDP_IFC.1	This SFR defines a policy for when data will or will not be transmitted by the TSF. The App PP defines requirements for how data is transmitted but a policy governing when an external interface may be invoked is beyond its scope.
FDP_IFF.1	This SFR defines the rules for a policy for when data will or will not be transmitted by the TSF. The App PP defines requirements for how data is transmitted but a policy governing when an external interface may be invoked is beyond its scope.
FMT_SMF.1/VVoIP	This PP-Module defines a new iteration of FMT_SMF.1 to add additional management functions that relate specifically to VVoIP functionality. The addition of these functions does not prevent any of the original functions from being implemented. This iteration does include two duplicates of management functions specified in the Base-PP; this is consistent because it is possible that auditing is handled differently for the VVoIP functionality as it is for the rest of the TOE's auditing. These functions are also selectable so it is not required that a conformant TOE implement this.
FTA_SSL.3/MEDIA	This SFR defines session termination behavior for the TOE's media channel. This interface is specific to this PP-Module and is not within the scope of the App PP.
FTP_ITC.1/CONTROL	This SFR defines the trusted communications protocol used by the TOE's signaling channel, which is specific to the VVoIP technology and does not

	conflict with the functionality defined in the App PP.
FTP_ITC.1/MEDIA	This SFR defines the trusted communications protocol used by the TOE's media channel, which is specific to the VVoIP technology and does not conflict with the functionality defined in the App PP.
Optional SFRs	
FAU_GEN.1/CSADMIN	This PP-Module specifies an iteration of FAU_GEN.1 for the auditable events that relate specifically to the administration of the VVoIP endpoint. The App PP does not mandate that the TOE include an audit function but it is not prohibited by the PP.
FAU_GEN.1/CSVVOIP	This PP-Module specifies an iteration of FAU_GEN.1 for the auditable events that relate specifically to VVoIP endpoint behavior. The App PP does not mandate that the TOE include an audit function but it is not prohibited by the PP.
Objective SFRs	
This PP-Module does not define any Objective requirements.	
Implementation-dependent SFRs	
FAU_STG.1	This SFR defines the ability of the TOE to protect, store, and transmit audit data to a remote server using a secure channel. The App PP does not define its own requirements for auditing but it does not prohibit audit functionality, so this PP-Module's inclusion of an audit function does not conflict with the PP.
FAU_STG.5	This SFR defines the ability of the TOE to handle log space overruns in a defined manner. The App PP does not define its own requirements for auditing but it does not prohibit audit functionality, so this PP-Module's inclusion of an audit function does not conflict with the PP.
Selection-based SFRs	
FAU_GEN.1/P2PADMIN	This PP-Module specifies an iteration of FAU_GEN.1 for the auditable events that relate specifically to the administration of the VVoIP endpoint. The App PP does not mandate that the TOE include an audit function but it is not prohibited by the PP.
FAU_GEN.1/P2PVVOIP	This PP-Module specifies an iteration of FAU_GEN.1 for the auditable events that relate specifically to VVoIP endpoint behavior. The App PP does not mandate that the TOE include an audit function but it is not prohibited by the PP.
FCS_COP.1/SRTP	This SFR defines the AES functionality used to support SRTP. This does not conflict with the App PP because the TOE can still use FCS_COP.1/DataEncryption to make claims related to all other uses of AES.
FCS_SRTP_EXT.1	This SFR defines support for the SRTP protocol, which is specific to VVoIP technology. The TSF's implementation of this protocol does not prevent the enforcement of any App PP SFRs.

FDP_IFC.1/CALLCONTROL	This SFR defines VVoIP call control policy. The TSF's implementation of this protocol does not prevent the enforcement of any App PP SFRs.
FDP_IFF.1/CALLCONTROL	This SFR defines VVoIP call control policy. The TSF's implementation of this protocol does not prevent the enforcement of any App PP SFRs.
FPT_STM_EXT.1/VVoIP	This SFR defines the TOE's reliance on ESCs to act as its NTP servers in deployments where the TOE is registered to them. The App PP does not define a specific method for how a conformant TOE is expected to receive time data so there is no contradiction here.

Appendix A - Optional SFRs

A.1 Strictly Optional Requirements

A.1.1 Security Audit(FAU)

FAU_GEN.1/CSADMIN Audit Data Generation (Client-Server Admin Events)

FAU_GEN.1.1/CSADMIN

The **[selection: *TSF, TOE platform*]** shall be able to generate audit data of the following auditable events:

a. ~~Start-up and shutdown of the audit functions;~~
b. ~~All auditable events for the [**selection, choose one of**: *minimum*, *basic*, *detailed*, *not specified*] level of audit;~~
c. [*All administrative actions comprising:*
   i. *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).*
   ii. *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).*
   iii. *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).*
   iv. *Resetting passwords (name of related user account shall be logged).*
   v. *[**selection**: [**assignment**: list of other uses of privileges], no other actions]*

   ].

Application Note: This SFR defines the same auditable events as FAU_GEN.1/P2PADMIN in Appendix B below. It is defined as a separate iteration because when the TOE is deployed in a client-server architecture, the Enterprise Session Controller is expected to be responsible for the relevant auditing, so this capability is optional when the TOE is not peer-to-peer.

If the TOE claims this SFR and conforms to the App PP, the implementation-dependent SFRs FAU_STG.1 and FAU_STG.5 must also be claimed. This does not need to be claimed when the TOE conforms to the NDcPP because that PP already defines FAU_STG.1 as a mandatory requirement.

FAU_GEN.1.2/CSADMIN

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

a. Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;
b. For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [*no additional information*].

Evaluation Activities

FAU_GEN.1/CSADMIN
TSS
There are no additional TSS evaluation activities for this component.

Guidance
The evaluator shall make a determination of the administrative actions related to TSF data related to configuration changes. The evaluator shall examine the guidance documentation and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP-Module. The evaluator shall document the methodology or approach taken to TSF data related to configuration changes. The evaluator may perform this activity as part of the activities associated with ensuring that the corresponding guidance documentation satisfies the requirements related to it.

Tests
For each administrative action identified in FAU_GEN.1.1/CSADMIN, the evaluator shall perform an action either on the TOE or on the operational environment that causes the event to occur. The evaluator shall verify in each case that an auditable event was generated in a format consistent with the guidance documentation and that all audit record details specified in the SFR are present.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.

FAU_GEN.1/CSVVOIP Audit Data Generation (Client-Server VVoIP Events)

FAU_GEN.1.1/CSVVOIP

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

a. ~~Start-up and shutdown of the audit functions;~~
b. ~~All auditable events for the [**selection, choose one of**: *minimum*, *basic*, *detailed*, *not specified*] level of audit;~~
c. [*auditable events defined in the Auditable Events for Mandatory SFRs table (Table 2)*].

FAU_GEN.1.2/CSVVOIP

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

a. Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;
b. For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [*information specified in column three of the Auditable Events table in which the event was defined*].

Application Note: This SFR defines the same auditable events as FAU_GEN.1/P2P-VVoIP in Appendix B below. It is defined as a separate iteration because when the TOE is deployed in a client-server architecture, the Enterprise Session Controller is expected to be responsible for the relevant auditing, so this capability is optional

when the TOE is not peer-to-peer.

If the TOE claims this SFR and conforms to the App PP, the implementation-dependent SFRs FAU_STG.1 and FAU_STG.5 must also be claimed. This does not need to be claimed when the TOE conforms to the NDcPP because that PP already defines FAU_STG.1 as a mandatory requirement.

Evaluation Activities

FAU_GEN.1/CSVVOIP

TSS

There are no additional TSS evaluation activities for this component.

Guidance

The evaluator shall check the guidance documentation and ensure that it provides an example of each auditable event required by the PP-Module (i.e. at least one instance of each auditable event – comprising the mandatory, optional and selection-based SFR sections as applicable – shall be provided from the actual audit record).

Tests

For each administrative action identified in the Auditable Events table in the PP-Module, the evaluator shall perform an action on the TOE that causes the event to occur. The evaluator shall verify in each case that an auditable event was generated in a format consistent with the guidance documentation and that all audit record details specified in the SFR are present.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.

A.2 Objective Requirements

This PP-Module does not define any Objective SFRs.

A.3 Implementation-dependent Requirements

A.3.1 Security Audit (FAU)

FAU_STG.1 Audit data storage location

This component must be included in the ST if the TOE implements any of the following features:

- ***Software Application with Logging***

FAU_STG.1.1

The TSF shall be able to store generated audit data on the [***[selection: TOE itself, TOE platform]***, *transmit the generated audit data to* ***[selection: an Enterprise Session Controller that the TOE is registered to, an external IT entity]*** *using a trusted channel according to* ***FTP_DIT_EXT.1.***]

Application Note: This SFR is modified from its definition in [CC] Part 2 to define storage for audit data. Specifically, it is required that this data be stored both on the TOE itself and that it be transmitted securely to an external entity. Note that this SFR is only applicable for software application TOEs that implement logging, because the NDcPP specifies log data storage requirements itself. This SFR should not be claimed when the NDcPP is the Base-PP.

Evaluation Activities

FAU_STG.1

TSS

The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided.

The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally and whether that data is stored by the TOE or through the TOE's invocation of a platform auditing mechanism.

The evaluator shall examine the TSS to ensure that it details whether the transmission of audit information to an external IT entity can be done in real-time or periodically. In case the TOE does not perform transmission in real-time the evaluator needs to verify that the TSS provides details about what event stimulates the transmission to be made as well as the possible acceptable frequency for the transfer of audit data.

Guidance

The evaluator shall examine the guidance documentation to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.

The evaluator shall also examine the guidance documentation to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.

Tests

Testing of the trusted channel mechanism for audit will be performed as specified in the associated EAs for the particular trusted channel mechanism. The evaluator shall perform the following additional tests for this requirement:

- *Test FAU_STG.1:1:*

  The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing. The evaluator shall verify that the TOE is capable of transferring audit data to an external audit server automatically without administrator intervention.

If the ability to modify this behavior is configurable (e.g., if the TOE can be configured to transmit audit data either to an ESC to which it is registered or to an external trusted IT entity that is not an ESC), the evaluator shall repeat this test as necessary to show that changing the available configuration options will result in the TOE performing the expected behavior in each case.

FAU_STG.5 Prevention of audit data loss

This component must be included in the ST if the TOE implements any of the following features:

- ***Software Application with Logging***

FAU_STG.5.1

The TSF shall [**selection**: *ignore audited events, overwrite the oldest stored audit records, [**assignment**: other actions to be taken in case of audit storage failure and conditions for the actions]*] if the audit data storage is full.

Application Note: Note that this SFR is only applicable for software application TOEs that implement logging, because the NDcPP specifies log data storage requirements itself. This SFR should not be claimed when the NDcPP is the Base-PP.

Evaluation Activities

FAU_STG.5
TSS
The evaluator shall examine the TSS to ensure it describes what happens when the local audit data store is full; and how these records are protected against unauthorized access.

The evaluator shall examine the TSS to ensure that it details the behavior of the TOE when the storage space for audit data is full. When the option 'overwrite the oldest stored audit records' is selected this description should include an outline of the rule for overwriting audit data. If 'other actions...' are chosen such as sending the new audit data to an external IT entity, then the related behavior of the TOE shall also be detailed in the TSS.

Guidance
The evaluator shall ensure that the guidance documentation describes all possible configuration options for FAU_STG.5 and the resulting behavior of the TOE for each possible configuration. The description of possible configuration options and resulting behavior shall correspond to those described in the TSS.

Tests

- *Test FAU_STG.5:1:*
  The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behavior defined in FAU_STG.5. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that:

- *The audit data remains unchanged with every new auditable event that should be tracked but that the audit data is recorded again after the local storage for audit data is cleared (for the option 'ignore audited events' in FAU_STG.5).*
- *The oldest audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option 'overwrite the oldest stored audit records' in FAU_STG.5).*
- *The TOE behaves as specified (for the option 'other action' in FAU_STG.5).*

If the behavior of the TOE when the local audit storage space is full is configurable, the evaluator shall repeat this test for each configuration option and observe that the intended result occurs.

If the local storage location of the audit data is configurable, the evaluator shall repeat this test as needed to demonstrate that specifying a new location for storage of audit data results in audit data being stored to the desired location.

Appendix B - Selection-based Requirements

B.1 Security Audit (FAU)

FAU_GEN.1/P2PADMIN Audit Data Generation (Peer-to-Peer Admin Events)

The inclusion of this selection-based component depends upon selection in FDP_IFF.1.2, FMT_SMF.1.1/VVoIP.

FAU_GEN.1.1/P2PADMIN

The **[selection: *TSF*, *TOE platform*]** shall be able to generate audit data of the following auditable events:

a. ~~Start-up and shutdown of the audit functions;~~
b. ~~All auditable events for the [**selection, choose one of**: *minimum*, *basic*, *detailed*, *not specified*] level of audit;~~
c. [*All administrative actions comprising:*
   i. *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).*
   ii. *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).*
   iii. *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).*
   iv. *Resetting passwords (name of related user account shall be logged).*
   v. *[**selection**: [**assignment**: list of other uses of privileges], no other actions]*

].

FAU_GEN.1.2/P2PADMIN

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

a. Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;
b. For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [*no additional information*].

Application Note: If the TOE is a hardware device and claims this SFR, this is inherently satisfied through FAU_GEN.1 as defined by the NDcPP. Any other relevant auditable events for the functionality described in the NDcPP is defined there (the App PP does not include any auditing requirements).

If the TOE claims this SFR and conforms to the App PP, the implementation-dependent SFRs FAU_STG.1 and FAU_STG.5 must also be claimed. This does not need to be claimed when the TOE conforms to the NDcPP because that PP already defines FAU_STG.1 as a mandatory requirement.

Evaluation Activities

FAU_GEN.1/P2PADMIN

TSS

There are no additional TSS evaluation activities for this component.

Guidance

The evaluator shall make a determination of the administrative actions related to TSF data related to configuration changes. The evaluator shall examine the guidance documentation and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP-Module. The evaluator shall document the methodology or approach taken to TSF data related to configuration changes. The evaluator may perform this activity as part of the activities associated with ensuring that the corresponding guidance documentation satisfies the requirements related to it.

Tests

For each administrative action identified in FAU_GEN.1.1/P2PADMIN, the evaluator shall perform an action either on the TOE or on the operational environment that causes the event to occur. The evaluator shall verify in each case that an auditable event was generated in a format consistent with the guidance documentation and that all audit record details specified in the SFR are present.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.

FAU_GEN.1/P2PVVOIP Audit Data Generation (Peer-to-Peer VVoIP Events)

The inclusion of this selection-based component depends upon selection in FDP_IFF.1.2, FMT_SMF.1.1/VVoIP.

FAU_GEN.1.1/P2PVVOIP

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

a. ~~Start-up and shutdown of the audit functions;~~
b. ~~All auditable events for the [**selection, choose one of**: *minimum*, *basic*, *detailed*, *not specified*] level of audit;~~
c. [*auditable events defined in the Auditable Events for Mandatory SFRs table (Table 2)*].

FAU_GEN.1.2/P2PVVOIP

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

a. Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;
b. For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [*information specified in column three of the Auditable Events table in which the event was defined*].

Application Note: If the TOE claims this SFR and conforms to the App PP, the implementation-dependent SFRs FAU_STG.1 and FAU_STG.5 must also be claimed. This does not need to be claimed when the TOE conforms to the NDcPP because that PP already defines FAU_STG.1 as a mandatory requirement.

Evaluation Activities

FAU_GEN.1/P2PVVOIP
TSS
There are no additional TSS evaluation activities for this component.

Guidance
The evaluator shall check the guidance documentation and ensure that it provides an example of each auditable event required by the PP-Module (i.e. at least one instance of each auditable event – comprising the mandatory, optional and selection-based SFR sections as applicable – shall be provided from the actual audit record).

Tests
For each administrative action identified in the Auditable Events table in the PP-Module, the evaluator shall perform an action on the TOE that causes the event to occur. The evaluator shall verify in each case that an auditable event was generated in a format consistent with the guidance documentation and that all audit record details specified in the SFR are present.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.

B.2 Cryptographic Support (FCS)

FCS_COP.1/SRTP Cryptographic Operation (Encryption/Decryption for SRTP

The inclusion of this selection-based component depends upon selection in FTP_DIT_EXT.1.1, FTP_ITC.1.1/MEDIA.

FCS_COP.1.1/SRTP

The TSF shall perform [*encryption/decryption to support SDES-SRTP*] in accordance with a specified cryptographic algorithm [*AES-GCM*] and cryptographic key sizes [*256-bit*] that meet the following: [*NIST SP 800-38D*].

Application Note: The NDcPP and App PP each define their own iteration of FCS_COP.1 for AES encryption and decryption (FCS_COP.1/DataEncryption and FCS_COP.1/SKC, respectively). The encryption and decryption used specifically for SRTP has been broken out into a separate iteration for readability purposes; the same cryptographic library that implements the AES algorithms claimed in the Base-PP requirements can be used here. Note that GCM is a supported AES mode both in this iteration and in the Base-PPs.

Evaluation Activities

FCS_COP.1/SRTP

TSS

The evaluator shall examine the TSS to determine that it claims the use of GCM. The evaluator shall verify that the TSS notes the GCM key sizes that the TOE supports for each use of GCM. If GCM is supported for other uses, the evaluator shall ensure that the specific key sizes supported for each use of GCM are identified.

Guidance

There are no additional Guidance evaluation activities for this component.

Tests

If the TOE claims the App PP as its Base-PP, the evaluator shall perform the AES-GCM test activities identified for FCS_COP.1/SKC in the Base-PP.

If the TOE claims the NDcPP as its Base-PP, the evaluator shall perform the AES-GCM test activities identified for FCS_COP.1/DataEncryption in the Base-PP.

FCS_SRTP_EXT.1 Secure Real-Time Transport Protocol

The inclusion of this selection-based component depends upon selection in FTP_DIT_EXT.1.1, FTP_ITC.1.1/MEDIA.

FCS_SRTP_EXT.1.1

The TSF shall implement the Secure Real-Time Transport Protocol (SRTP) that complies with RFC 3711, and use Security Descriptions for Media Streams (SDES) in compliance with RFC 4568 to provide key information for the SRTP connection.

FCS_SRTP_EXT.1.2

The TSF shall implement SDES-SRTP supporting the following cipher suites: [*AEAD_AES_256_GCM, in accordance with RFC 7714*].

Application Note: This requirement specifies that the SRTP session that will be used to carry the VVoIP traffic will be keyed according to an SDES dialogue using the identified cipher suite.

FCS_SRTP_EXT.1.3

The TSF shall ensure the SRTP NULL algorithm can be disabled.

FCS_SRTP_EXT.1.4

The TSF shall allow the SRTP ports to be used for SRTP communications to be specified by an Authorized Administrator.

Application Note: This requirement specifies that the SRTP session that will be used to carry the VoIP traffic will be keyed according to an SDES dialog using the identified cipher suite.

Evaluation Activities

FCS_SRTP_EXT.1

TSS
The evaluator shall examine the TSS to verify that it describes how the SRTP session is negotiated for both incoming and outgoing calls. This includes how the keying material is established, as well has how requests to use the NULL algorithm or other unallowed cipher suites are rejected by the TSF.

Guidance
The evaluator shall examine the operational guidance to determine that it includes instructions for how to disable the use of the SRTP NULL algorithm and how to specify the ports to be used for SRTP communications.

Tests
The evaluator shall follow the procedure for initializing their device so that they are ready to receive and place calls. The evaluator shall then both place and receive a call and determine that the traffic sent and received by the TOE is encrypted using SRTP with the specified cipher suite. The evaluator may choose one of the below two options to ensure that the call is being encrypted and to view the cipher suite being used.

Option 1: The evaluator shall configure the SIP server to report whether SRTP is being used, and if so, print the negotiated SRTP cipher suite. The evaluator shall confirm that SRTP was used for the calls and that the correct cipher suite was negotiated.

Option 2: A packet capture tool should be used with the SIP server's private key loaded in. The evaluator shall decrypt the TLS-SIP traffic, view the SDES negotiation, and ensure that the correct cipher suite was negotiated.

Option 3: The evaluator shall inspect the VVoIP endpoint's audit or system log to ensure that the correct cipher suite was negotiated.

Next, the evaluator shall configure the SIP server to only allow the SRTP NULL cipher suite. The evaluator shall attempt to both place and receive a call and confirm that both attempts failed.

B.3 User Data Protection (FDP)

FDP_IFC.1/CALLCONTROL Subset Information Flow Control (for Call Control)

The inclusion of this selection-based component depends upon selection in FDP_IFF.1.2, FMT_SMF.1.1/VVoIP.

FDP_IFC.1.1/CALLCONTROL
The TSF shall enforce the [*call control policy*] on [*call control information transmitted by the TOE*].

Evaluation Activities

FDP_IFC.1/CALLCONTROL
TSS
There are no additional TSS evaluation activities for this component.

Guidance
There are no additional Guidance evaluation activities for this component.

Tests
Testing of this component is performed through evaluation of FDP_IFF.1/CALLCONTROL.

FDP_IFF.1/CALLCONTROL Subset Information Flow Control (for Call Control)

The inclusion of this selection-based component depends upon selection in FDP_IFF.1.2, FMT_SMF.1.1/VVoIP.

FDP_IFF.1.1/CALLCONTROL

The TSF shall enforce the [*call control policy*] 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*]**.

Application Note: The ST author should complete the assignment with an endpoint identifier (i.e. how the TSF identifies the endpoints each endpoint for a call). For example, the endpoint could be identified by an IP address, a phone number, or a username.

FDP_IFF.1.2/CALLCONTROL

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 with the TOE is attempted, the TSF will establish a connection between itself and the peer*].

Application Note: The validity of a call is determined by the protocol and the identifier of the endpoint.

FDP_IFF.1.3/CALLCONTROL

The TSF shall enforce ~~the~~ [*no additional information flow control policy rules*].

FDP_IFF.1.4/CALLCONTROL

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

FDP_IFF.1.5/CALLCONTROL

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

Evaluation Activities

FDP_IFF.1/CALLCONTROL
TSS
The evaluator shall examine the TSS to verify that it describes the call control protocol(s) used by the TOE and any explicit circumstances under which the TSF will and will not transmit call control data as defined in FDP_IFF.1.4/CALLCONTROL and FDP_IFF.1.5/CALLCONTROL. The TSF

should only transmit call control data using the protocol(s) and method(s) of endpoint identification as indicated in FDP_IFC.1/CALLCONTROL or if defined any explicit allow/deny rules in FDP_IFF.1.4/CALLCONTROL and FDP_IFF.1.5/CALLCONTROL.

Guidance
If any aspects of the TOE's call control functionality are configurable (such as the specific call control protocol used or the circumstances in which the TSF will or will not transmit call control data), the evaluator shall examine the guidance documentation to verify that instructions for configuring this behavior are provided.

Tests
The evaluator shall perform one or more of the following tests depending on the protocols that the TOE claims to support.

- *Test FDP_IFF.1/CALLCONTROL:1: (Conditional - if "SIP" is selected in FDP_IFF.1.1/CALLCONTROL)*
  - ***Step 1:** Ensure the TOE is configured to use P2P and act as a call control server using the SIP protocol.*
  - ***Step 2:** Use a traffic capture tool to capture call-signaling packets traversing the TOE.*
  - ***Step 3:** Place a call to the TOE from another VVoIP endpoint using the SIP call control protocol to the TOE and observe via packet capture that the TSF established a connection between itself and the peer.*
  - ***Step 4:** Repeat step 3 with a call placed from the TOE to the other VVoIP endpoint.*
  - ***Step 5:** (Conditional - if the ST claims any additional rules in FDP_IFF.1.4/CALLCONTROL) Implement any rules assigned in FDP_IFF.1.4 and verify that the specified authorized information flows occur.*
  - ***Step 6:** (Conditional - if the ST claims any additional rules in FDP_IFF.1.5/CALLCONTROL) Implement any rules assigned in FDP_IFF.1.5 and verify that the specified information flows do not occur.*
  - ***Step 7:** Repeat steps 1-6 for each method of endpoint identification.*
- *Test FDP_IFF.1/CALLCONTROL:2: (Conditional - if "H.323" is selected in FDP_IFF.1.1/CALLCONTROL)*
  - ***Step 1:** Ensure the TOE is configured to use P2P and act as a call control server using the H.323 protocol.*
  - ***Step 2:** Use a traffic capture tool to capture call-signaling packets traversing the TOE.*
  - ***Step 3:** Place a call to the TOE from another VVoIP endpoint using the H.323 call control protocol to the TOE and observe via packet capture that the TSF established a connection between itself and the peer.*
  - ***Step 4:** Repeat step 3 with a call placed from the TOE to the other VVoIP endpoint.*
  - ***Step 5:** (Conditional - if the ST claims any additional rules in FDP_IFF.1.4/CALLCONTROL) Implement any rules assigned in FDP_IFF.1.4/CallControl and verify that the specified authorized information flows occur.*
  - ***Step 6:** (Conditional - if the ST claims any additional rules in FDP_IFF.1.5/CALLCONTROL) Implement any rules assigned in FDP_IFF.1.5 and verify that the specified information flows do not occur.*
  - ***Step 7:** Repeat steps 1-6 for each method of endpoint identification.*

B.4 Protection of the TSF (FPT)

FPT_STM_EXT.1/VVoIP Reliable Time Stamps (VVoIP Communications)

The inclusion of this selection-based component depends upon selection in FMT_SMF.1.1/VVoIP.

FPT_STM_EXT.1.1/VVoIP

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

FPT_STM_EXT.1.2/VVoIP

The TSF shall [*synchronize time with* ***[selection: an ESC, the TOE platform]***].

Application Note: The selection made for this requirement depends on the TOE type. If the TOE is a hardware device, "an ESC" must be selected. If the TOE is a software application, "the TOE platform" must be selected. If the TOE is a software VVoIP application, FMT_SMF.1.1/VVoIP is not required as the TOE relies upon the platform for time.

Evaluation Activities

FPT_STM_EXT.1/VVoIP

TSS

The evaluator shall examine the TSS to ensure that it lists each security function that makes use of time, and that it provides a description of how the time is maintained and considered reliable in the context of each of the time related functions.

If an ESC is selected in FPT_STM_EXT.1.1, the evaluator shall also verify that the TSS describes the ability of the TOE to support NTP synchronization with an ESC.

Guidance

The evaluator shall review the guidance to confirm that it provides instructions for how to synchronize the time. If an ESC is selected in FPT_STM_EXT.1.1, this should include instructions on how to enable NTP synchronization with an ESC.

Tests

(Conditional - "an ESC" is selected in FPT_STM_EXT.1.2/VVoIP)

The evaluator shall use the guidance documentation to configure the NTP client on the TOE and set up a communication path with the ESC. The evaluator will observe that the ESC has set the time to what is expected.

Appendix C - Extended Component Definitions

This appendix contains the definitions for all extended requirements specified in the PP-Module.

C.1 Extended Components Table

All extended components specified in the PP-Module are listed in this table:

Table 10: Extended Component Definitions

Functional Class	Functional Components
Communications (FCO)	FCO_VOC_EXT Fixed-Rate Vocoder
Cryptographic Support (FCS)	FCS_SRTP_EXT Secure Real-Time Transport Protocol

C.2 Extended Component Definitions

C.2.1 Communications (FCO)

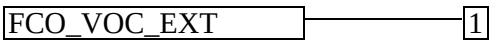
This PP-Module defines the following extended components as part of the FCO class originally defined by CC Part 2:

C.2.1.1 FCO_VOC_EXT Fixed-Rate Vocoder

Family Behavior

Components in this family define the use of vocoders in audio transmission.

Component Leveling



FCO_VOC_EXT.1, Fixed-Rate Vocoder, requires the TSF to use a constant bit rate vocoder as opposed to a variable one.

Management: FCO_VOC_EXT.1

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

- Ability to specify the vocoder used

Audit: FCO_VOC_EXT.1

There are no auditable events foreseen.

FCO_VOC_EXT.1 Fixed-Rate Vocoder

Hierarchical to: No other components.

Dependencies to: No dependencies.

FCO_VOC_EXT.1.1

The TSF shall transmit voice media using a constant bit rate voice vocoder.

C.2.2 Cryptographic Support (FCS)

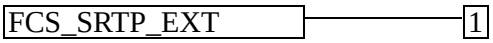
This PP-Module defines the following extended components as part of the FCS class originally defined by CC Part 2:

C.2.2.1 FCS_SRTP_EXT Secure Real-Time Transport Protocol

Family Behavior

Components in this family define the implementation of the Secure Real-Time Transport Protocol (SRTP).

Component Leveling



FCS_SRTP_EXT.1, Secure Real-Time Transport Protocol, requires the TSF to implement SRTP and defines conditions on its use.

Management: FCS_SRTP_EXT.1

No specific management functions are identified.

Audit: FCS_SRTP_EXT.1

There are no auditable events foreseen.

FCS_SRTP_EXT.1 Secure Real-Time Transport Protocol

Hierarchical to: No other components.

Dependencies to: FCS_COP.1 Cryptographic Operation

FCS_SRTP_EXT.1.1

The TSF shall implement the Secure Real-Time Transport Protocol (SRTP) that complies with RFC 3711, and use Security Descriptions for Media Streams (SDES) in compliance with RFC 4568 to provide key information for the SRTP connection.

FCS_SRTP_EXT.1.2

The TSF shall implement SDES-SRTP supporting the following cipher suites: [**assignment**: *list of permitted SDES-SRTP cipher suites*].

FCS_SRTP_EXT.1.3

The TSF shall ensure the SRTP NULL algorithm can be disabled.

FCS_SRTP_EXT.1.4

The TSF shall allow the SRTP ports to be used for SRTP communications to be specified by an Authorized Administrator.

Appendix D - Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this PP-Module. 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, 8.3 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.

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this PP-Module. 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.

Requirement	Rationale for Satisfaction
FAU_GEN.2 – User identity association	The iterations of FAU_GEN.1.2 explicitly requires that the OS record any user account associated with each event; therefore, it is duplicative to include a separate requirement to associate a user account with each event. If the TOE claims conformance to the NDcPP, the dependency is explicitly met through FAU_GEN.2.
FIA_UID.1 – Timing of Identification	For the purpose of logging and processing VVoIP telephony functions, the TOE is identified solely by underlying system or configuration characteristics (e.g., IP address, phone number) independent of the identity of the user interacting with the TOE. When the TOE is a software application, neither this PP-Module nor the Base-PP (App PP) define a separate identification and authentication mechanism for the software application to interact with its management interface. The software application assumes that accessing the OS platform itself is sufficient to grant access to the application. For accountability purposes, the user of the TOE is identified as the user that logged in to the OS platform and subsequently interacted with the TSF.
FMT_MSA.1 – Management of Security Attributes	This SFR defines the TOE security attributes that can be managed and what management role can administer them. Specifically, this is indirectly dependent on FDP_IFF.1. The PP-Module defines two iterations of FDP_IFF.1. Each of these iterations define explicit rules that determine when the TSF transmits call control and media data. The relevant attributes are either directly under the control of an ordinary user, such that no specific security authorization is needed, or they are entirely under the control of the TSF and cannot be influenced by the user regardless of privilege. An example of the first case in that in FDP_IFF.1.2, whether or not the TOE is in the off-hook state or the mute state is controllable by a user with physical access to the TOE and does not require the assumption of an administrative role. An example of the second case is in FDP_IFF.1.2/CallControl, where the TSF will determine if the other end of the connection is a valid VVoIP endpoint, which is something the user has no ability to configure or influence.

FMT_MSA.3 – Static Attribute Initialization	This SFR is a dependency on FDP_IFF.1. The PP-Module defines two iterations of FDP_IFF.1. Each of these iterations define explicit rules that determine when the TSF transmits call control and media data. FMT_MSA.3 has not been specified because the default state of the attributes used to determine if data flow is authorized is not relevant to enforcement of the rules. For example, FDP_IFF.1.2 states that the TSF will not transmit media data within a call if the TOE is in the mute state. Whether the call starts with the mute state active or inactive does not affect the enforcement of the rule, and requiring the ST to state this information does not affect the security of the TSF.
FMT_SMR.1 – Security Roles	When the TOE is a software application, neither this PP-Module nor the Base-PP (App PP) define security roles that are authorized to perform management functionality on the TSF. For user access, the TOE does not require separate authentication to the TSF because authentication to the OS platform on which the TOE is installed is sufficient user access control; a user logged in to the OS platform is assumed to be a valid user of the TOE. If the TOE is registered to an ESC, the ESC may be able to issue management commands to the TOE. No separate ‘user role’ is needed to define this because the ESC is not a ‘user’ and so FMT_SMR.1.2 is not applicable in this context. The ESC’s authorization to manage the TSF is implicitly granted through the user registering the TOE to the ESC.
FPT_STM.1 – Reliable time stamps	The iterations of FAU_GEN.1.2 explicitly requires that the software application TSF associate timestamps with audit records; therefore it is duplicative to include a separate timestamp requirement. Additionally, the App PP has an assumption of relying upon a trustworthy computing platform with a reliable time clock for its execution, so the dependency is also met through the assumption. Alternatively, if the TOE is registered to an ESC, the selection-based requirement FPT_STM_EXT.1/VVoIP must be claimed, which is sufficient to address the dependency as the TSF will receive time data from the operational environment that is assumed to be reliable. If the TOE claims conformance to the NDcPP, the dependency is also explicitly met through FPT_STM_EXT.1, regardless of whether the TOE is deployed in a client-server configuration (with registration to an ESC) or peer-to-peer configuration (with no ESC involved).

Appendix E - Entropy Documentation and Assessment

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

Appendix F - Acronyms

Table 11: Acronyms

Acronym	Meaning
Base-PP	Base Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
cPP	Collaborative Protection Profile
DHCP	Dynamic Host Configuration Protocol
ESC	Enterprise Session Controller
FP	Functional Package
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU-T	International Telegraph Union – Telecommunication Standardization Sector
NTP	Network Time Protocol
OE	Operational Environment
P2P	Peer-to-Peer
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SIP	Session Initiation Protocol
SRTP	Secure Real-Time Transport Protocol
ST	Security Target
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol

TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification
UDP	User Datagram Protocol
VVoIP	Voice/Video over IP

Appendix G - Bibliography

Table 12: Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and general model, CCMB-2022-11-001, CC:2022, Revision 1, November 2022. • Part 2: Security functional requirements, CCMB-2022-11-002, CC:2022, Revision 1, November 2022. • Part 3: Security assurance requirements, CCMB-2022-11-003, CC:2022, Revision 1, November 2022. • Part 4: Framework for the specification of evaluation methods and activities, CCMB-2022-11-004, CC:2022, Revision 1, November 2022. • Part 5: Pre-defined packages of security requirements, CCMB-2022-11-005, CC:2022, Revision 1, November 2022.
[CEM]	Common Methodology for Information Technology Security Evaluation - • Evaluation methodology, CCMB-2022-11-006, CC:2022, Revision 1, November 2022.
[AppPP]	Protection Profile for Application Software, Version 2.0, June 16, 2025
[NDcPP]	collaborative Protection Profile for Network Devices, Version 4.0, December 22, 2025