# PP-Module for Voice/Video over IP (VVoIP) Endpoints


Version: 1.0
2020-10-28
**National Information Assurance Partnership**

# Contents

# Tables

# 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:

- Protection Profile for Application Software, Version 1.3 (App PP)
- collaborative Protection Profile for Network Devices, Version 2.2e (NDcPP)

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

### 1.2.1 Common Criteria Terms

*Table 1: CC Terms and Definitions*

| Term | Definition |
|---|---|
| Common Criteria (CC) | Common Criteria for Information Technology Security Evaluation. |
| Common Criteria Testing Laboratory (CCTL) | 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. |
| Protection Profile (PP) | An implementation-independent set of security requirements for a specific category of technology. |
| 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 Protection Profiles. |
| Security Assurance Requirement (SAR) | A requirement for how the TOE's proper implementation of the SFRs is verified by an evaluator. |
| Supporting Document (SD) | A companion document to a PP or PP-Module that provides guidance on the specific Evaluation Activities that must be performed in order to evaluate a TOE. |

| Term | Definition |
|---|---|
| Security Functional Requirement (SFR) | A requirement for security enforcement by the TOE. |
| Security Target (ST) | A set of implementation-dependent security requirements for a specific product. |
| Target of Evaluation (TOE) | The product under evaluation. |
| TOE Security Functionality (TSF) | The security functionality of the product under evaluation. |
| TOE Summary Specification (TSS) | A description of how a TOE satisfies the SFRs in an ST. |

### 1.2.2 Technology Terms

*Table 2: Technology Terms and Definitions*

| Term | Definition |
|---|---|
| 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. |
| Session Initiation Protocol (SIP) | A communications protocol defined by IETF that is used for creating, modifying, and terminating multimedia sessions with multiple participants. |
| 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. |
| 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:<br>- Hook state: whether the endpoint is active (off-hook) or inactive (on-hook)<br>- Mute state: the endpoint is active but is deliberately not transmitting data<br>- Hold state: the endpoint is active but is deliberately not transmitting or receiving data. |
| Streaming media | The voice/video exchanged between VVoIP endpoints. |

| Term | Definition |
|---|---|
| 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

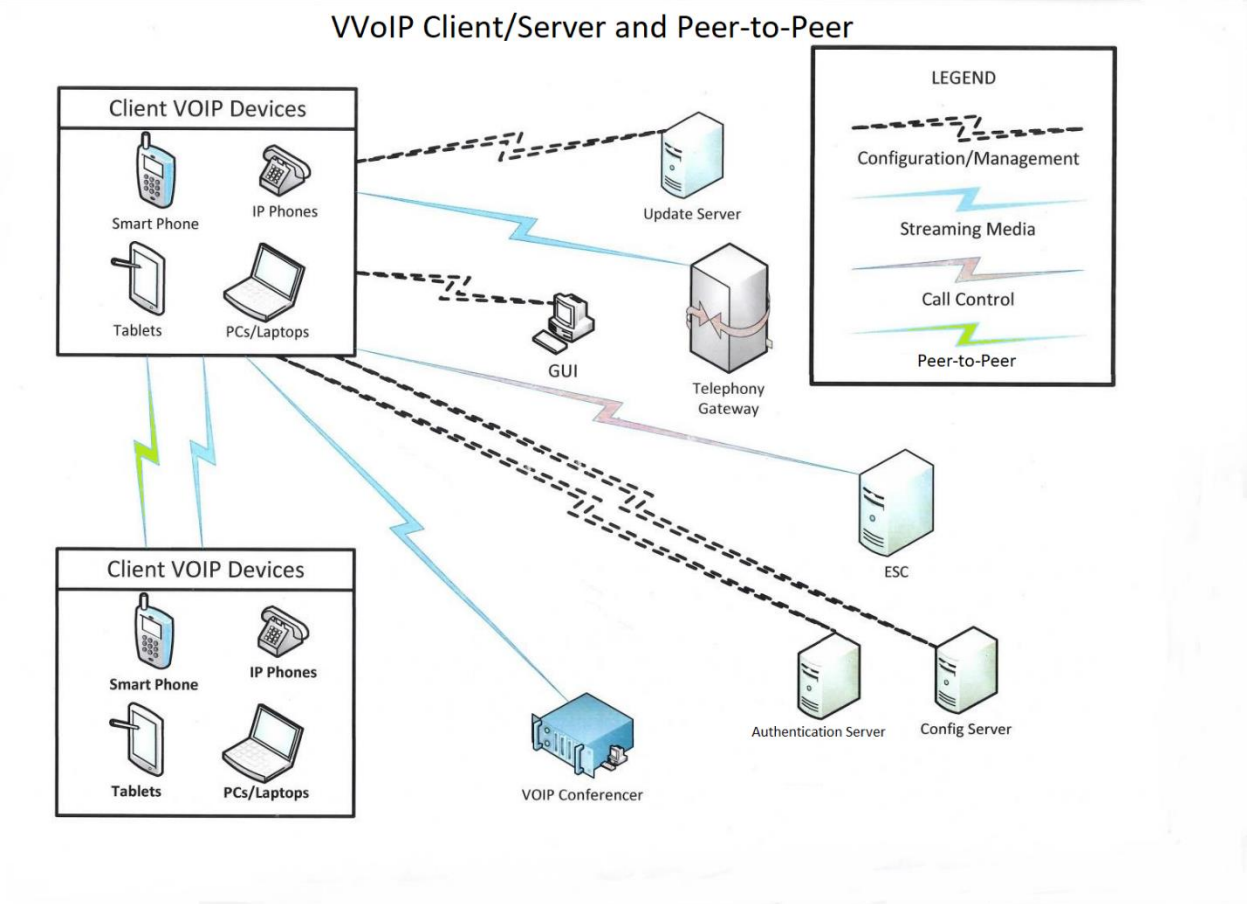
This PP-Module specifically addresses a dedicated network device or software application that facilitates the exchange of voice or video communication across an Internet Protocol (IP) network. The endpoint is a client (TOE) that communicates with a VVoIP call control server and may serve as its own call 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.

## 1.4 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.




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).

## 1.5 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.

**[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.

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.

# 2. Conformance Claims

## 2.1 CC Conformance

**Conformance Statement**

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

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

**CC Conformance Claims**

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

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

**Package Claim**

This PP-Module is TLS Package Version 1.1 Conformant when used in a PP-Configuration with the App PP.

# 3. Security Problem Description

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

## 3.1 Threats

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

**T.MEDIA_DISCLOSURE**

An attacker can use the encrypted variable rate vocoder frames to their advantage to decode transmitted data.

**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

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-Module defines no additional organizational security policies beyond those defined in the supported base PPs.

# 4. Security Objectives

## 4.1 Security Objectives for the TOE

Security objectives for the TOE are listed here. Note that TOE objectives are satisfied by SFRs defined in this PP-Module as well as those in the NDcPP, as indicated. Conformant TOE's must meet all objectives including the threats and objectives from the chosen Base-PP.

**O.ENCRYPTION**

To prevent data disclosure from decryption, conformant TOEs will transmit and store sensitive data using mechanisms that provide adequate protections.

Addressed by: FCS_NTP_EXT.1 (from NDcPP), FCS_TLSC_EXT.1 (refined from NDcPP), FCS_TLSC_EXT.2 (refined from NDcPP), FIA_X509_EXT.1/Rev (refined from NDcPP), FIA_X509_EXT.2 (refined from NDcPP), FIA_X509_EXT.3 (refined from NDcPP), FTP_ITC.1 (refined from NDcPP), FTP_DIT_EXT.1 (refined from App PP), FCO_VOC_EXT.1, FTP_ITC.1/Control, FTP_ITC.1/Media, FAU_STG_EXT.1 (optional for software-only TOEs)), FCS_COP.1/SRTP (selection-based), FCS_SRTP_EXT.1 (selection-based), FDP_IFC.1/CallControl (selection-based), FDP_IFF.1/CallControl (selection-based), FPT_STM_EXT.1/VVoIP (selection-based)

**O.NO_UNATTENDED_TRANSMISSION**

To prevent undetected transmissions, conformant TOEs will not transmit unattended voice or video data when streaming media is not in use.

Addressed by: FDP_IFC.1, FDP_IFF.1, FTA_SSL.3/Media, FAU_GEN.1/CS-Admin (optional), FAU_GEN.1/CS-VVoIP (optional), FAU_GEN.1/P2P-Admin (selection-based), FAU_GEN.1/P2P-VVoIP (selection-based), FPT_STM_EXT.1/VVoIP (selection-based)

**O.TOE_ADMINISTRATION**

To support the enforcement of other security functionality, a conformant TOE will provide a management capability that allows for configuration of the TSF.

Addressed by: FMT_SMF.1/VVoIP

## 4.2 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.

## 4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organizational security policies map to the security objectives.

*Table 3: Security Objectives Rationale*

| Threat, Assumption, or Policy | Security Objective | Rationale |
|---|---|---|
| T.MEDIA_DISCLOSURE | O.ENCRYPTION | The TOE transmits security-relevant data to environmental IT entities using cryptographic mechanisms that protect this data from unauthorized disclosure. |
| T.UNDETECTED_TRANSMISSION | O.NO_UNATTENDED_TRANSMISSION | The TOE prevents transmission of all unattended voice or video data when the streaming media is not in use, thereby ensuring that data is only transmitted when affirmatively directed by the user. Auditing (optional for software only TOE's) further assists in detecting transmission of VVOIP data. |
| | O.TOE_ADMINISTRATION | The TOE defines management functions for VVoIP connectivity and optionally allows for configuration of the idle period for calls to minimize the risk of active unattended sessions and configuration of auditing to specify how transmissions are recorded. |
| 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

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

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

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

Note that selections and assignments to be completed by the ST author are preceded with "selection:" and "assignment:". If text is italicized and does not include either of these, it means that the selection or assignment has already been completed in this PP-Module and the ST author must use the text as written.

## 5.1 NDcPP 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

#### FAU_STG_EXT.1 Protected Audit Event Storage

**FAU_STG_EXT.1.2** The TSF shall be able to store generated audit data on the TOE itself.

- [*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.*

#### 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. This is because any VVoIP TOE that can be registered to ESCs is required to use them as NTP servers.

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).

### FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

This SFR is selection-based in the NDcPP but is mandated by this PP-Module because TLS is used to secure call control and streaming media channels regardless of the application protocol used. There is no change to the SFR text itself.

### FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

This SFR is optional in the NDcPP but is mandated by this PP-Module because the TLS implementation that is used to secure call control and streaming media channels must be secured using mutual authentication. There is no change to the SFR text itself.

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

This SFR is selection-based in the NDcPP but is mandated by this PP-Module because it is a dependency on the TLS functionality that this PP-Module requires. There is no change to the SFR text itself.

### FIA_X509_EXT.2 X.509 Certificate Authentication

This SFR is selection-based in the NDcPP but is mandated by this PP-Module because it is a dependency on the TLS functionality that this PP-Module requires. There is no change to the SFR text itself.

### FIA_X509_EXT.3 X.509 Certificate Requests

This SFR is selection-based in the NDcPP but is mandated by this PP-Module because it is a dependency on the TLS functionality that this PP-Module requires. There is no change to the SFR text itself.

### 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.

### FTP_ITC.1 Inter-TSF Trusted Channel

**FTP_ITC.1.1** The TSF shall be capable of using [***TLS and*** *[selection: IPsec, SSH, DTLS, 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 that only apply when the NDcPP is the Base-PP.

## 5.2 App PP 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

#### 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. The evaluator shall ensure that the test environment is configured appropriately.

#### FTP_DIT_EXT.1 Protection of Data in Transit

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

- *encrypt all transmitted [selection: sensitive data, data] with **TLS as defined in the TLS Package and** [selection: HTTPS in accordance with FCS_HTTPS_EXT.1, DTLS as defined in the TLS Package, SSH as conforming to the Extended Package for Secure Shell, **Secure Real-Time Transport Protocol (SRTP), no other protocols**],*
- *invoke platform-provided functionality to encrypt all transmitted sensitive data with **TLS and** [selection: HTTPS, DTLS, SSH, **no other protocols**],*
- *invoke platform-provided functionality to encrypt all transmitted data with **TLS and** [selection: HTTPS, DTLS, SSH, **, no other protocols**]*

] 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 that only apply when the App PP is 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 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.*

### 5.3.2 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.*

#### 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]***].

**FDP_IFF.1.3** The TSF shall enforce [*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*].

### 5.3.3 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 the TOE claims conformance to the NDcPP and "register the TOE to an ESC…" is selected, the selection-based SFR FCS_NTP_EXT.1 must be claimed since connectivity to an ESC implies that the TSF will use it as an NTP server.*

### 5.3.4 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.*

### 5.3.5 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 Protocl (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.*

#### 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.*

**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.*

## 5.4 TOE Security Functional Requirements Rationale

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

*Table 4: SFR Rationale*

| Security Objective | SFR | Rationale |
|---|---|---|
| O.ENCRYPTION | FCS_COP.1/DataEncryption (refined from NDcPP) | This SFR supports the encryption objective by defining the AES encryption algorithm used to secure VVoIP communications. |
| | FCS_NTP_EXT.1 (from NDcPP) | This SFR supports the encryption objective by defining how accurate system time is maintained, which is used to support certain cryptographic functions. |
| | FCS_TLSC_EXT.1 (refined from NDcPP) | This SFR supports the encryption objective by defining the TLS client implementation used to secure call control and streaming media channels used for VVoIP. |
| | FCS_TLSC_EXT.2 (refined from NDcPP) | This SFR supports the encryption objective by defining the TOE's implementation of mutual authentication for its TLS client. |
| | FIA_X509_EXT.1/Rev (refined from NDcPP) | This SFR supports the encryption objective by defining requirements for the use of X.509 certificates that TLS functionality depends on. |
| | FIA_X509_EXT.2 (refined from NDcPP) | This SFR supports the encryption objective by defining requirements for the use of X.509 certificates that TLS functionality depends on. |
| | FIA_X509_EXT.3 (refined from NDcPP) | This SFR supports the encryption objective by defining requirements for the use of X.509 certificates that TLS functionality depends on. |
| | FTP_ITC.1 (refined from NDcPP) | This SFR supports the encryption objective by defining the trusted |

| Security Objective | SFR | Rationale |
|---|---|---|
| | | communications channel used for VVoIP. |
| | FTP_DIT_EXT.1 (refined from App PP) | This SFR supports the encryption objective by defining the trusted communications channel used for VVoIP. |
| | FCO_VOC_EXT.1 | This SFR supports the encryption objective by defining the use of a fixed-rate vocoder to prevent the exposure of encryption vulnerabilities that are present with variable-rate vocoders. |
| | FTP_ITC.1/Control | This SFR supports the encryption objective by defining the application-layer channel used for communications with a VVoIP call control server. |
| | FTP_ITC.1/Media | This SFR supports the encryption objective by defining the application-layer channel used for communications of media (voice and video) data. |
| | FAU_STG_EXT.1 (optional for software only TOEs) | This SFR supports the encryption objective by ensuring that audit data is securely transmitted to an external entity. |
| | FCS_COP.1/SRTP (selection-based) | This SFR supports the encryption objective by defining the implementation of encryption used for SDES-SRTP, if supported by the TOE. |
| | FCS_SRTP_EXT.1 (selection-based) | This SFR supports the encryption objective by defining the implementation of the SRTP protocol, if supported by the TOE. |
| | FDP_IFC.1/CallControl (selection-based) | This SFR supports the encryption objective 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/Call Control (selection-based) | This SFR supports the encryption objective 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. |

| Security Objective | SFR | Rationale |
|---|---|---|
| | FPT_STM_EXT.1/VVoIP (selection-based) | This SFR supports the encryption objective 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. |
| O.NO_ UNATTENDED_ TRANSMISSION | FDP_IFC.1 | This SFR supports the objective to prevent unattended transmissions by defining the existence of a media transmission policy. |
| | FDP_IFF.1 | This SFR supports the objective to prevent unattended transmissions by defining how the media transmission policy is enforced to determine when transmissions should occur. |
| | FTA_SSL.3/Media | This SFR supports the objective to prevent unattended transmissions by requiring the TSF to terminate idle sessions. |
| | FAU_GEN.1/CS-Admin (optional) | This SFR supports the objective to prevent unattended transmissions by optionally allowing a client-server TOE to provide an audit trail of administrative actions, which could diagnose mis-configuration of the TOE that could lead to unattended transmissions. |
| | FAU_GEN.1/CS-VVoIP (optional) | This SFR supports the objective to prevent unattended transmissions by optionally allowing a client-server TOE to provide an audit trail of call data, which could diagnose when unattended transmissions may be occurring. |
| | FAU_GEN.1/P2P-Admin (selection-based) | This SFR supports the objective to prevent unattended transmissions by requiring a peer-to-peer TOE to provide an audit trail of administrative actions, which could diagnose mis-configuration of the TOE that could lead to unattended transmissions. |
| | FAU_GEN.1/P2P-VVoIP (selection-based) | This SFR supports the objective to prevent unattended transmissions by requiring a peer-to-peer TOE to provide an audit trail of call data, which could diagnose when |

| Security Objective | SFR | Rationale |
|---|---|---|
| | | unattended transmissions may be occurring. |
| | FPT_STM_EXT.1/VVoIP (selection-based) | This SFR supports the encryption objective 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. |
| O.TOE_ADMINISTRATION | FMT_SMF.1/VVoIP | This SFR supports the management objective by requiring the TSF to implement certain the management functions specific to VVoIP functionality. |

In addition to the SFRs mapped to the TOE objectives listed above, this PP-Module also modifies the following Base-PP SFRs that continue to mitigate the threats defined in their respective Base-PPs:

- FPT_TUD_EXT.1 (NDcPP and App PP)

## 5.5 TOE Security Assurance Requirements

This PP-Module does not define any SARs beyond those defined by the Base-PP. It is important to note that these SARs are applied to the entire TOE and not just to the portion of the TOE defined by the Base-PP in which the SARs are located.

# 6. Consistency Rationale

## 6.1 NDcPP Base

### 6.1.1 Consistency of TOE Type

When this PP-Module is used to extend the NDcPP, the TOE type for the overall TOE is still a network device. The TOE boundary is simply extended to include 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 5: NDcPP Security Problem Definition Consistency Rationale*

| PP-Module Threat or Assumption | Consistency Rationale |
|---|---|
| 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. |
| 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. |
| 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 Objectives

The objectives defined by this PP-Module (see section 4.1) supplement those defined in the NDcPP as follows:

*Table 6: NDcPP Objective Consistency Rationale*

| PP-Module Objective | Consistency Rationale |
|---|---|
| O.NO_UNATTENDED_TRANSMISSION | The NDcPP defines objectives for secure communications and detecting activity. The objective to not transmit unattended voice or video data when streaming media is not in use supplements these objectives. |
| O.ENCRYPTION | The NDcPP defines objectives for trusted communications channels. The objective to protect media transmission from disclosure through vocoder frames is a type of side-channel that is unique to the functions of a VVoIP endpoint. However, it is consistent with the overall objective of protecting transmitted data from disclosure. |
| O.TOE_ADMINISTRATION | The NDcPP defines an objective for security management. This PP-Module supplements this by defining an objective for management of its own capabilities. |

| | |
|---|---|
| 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 network device is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the NDcPP as well as new SFRs that are used entirely to implement VVoIP functionality. The rationale for why this does not conflict with SFRs defined by the NDcPP is as follows:

*Table 7: NDcPP SFR Consistency Rationale*

| 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. The SFR is otherwise unchanged. |
| 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. |
| FCS_TLSC_EXT.1 | This PP-Module does not modify this SFR; it only forces its inclusion because a conformant TOE must implement TLS client functionality. |
| FCS_TLSC_EXT.2 | This PP-Module does not modify this SFR; it only forces its inclusion because a conformant TOE must implement a TLS client that enforces mutual authentication. |
| FIA_X509_EXT.1/Rev | This PP-Module does not modify this SFR; it only forces its inclusion because X.509 services are required to support TLS client functionality. |
| FIA_X509_EXT.2 | This PP-Module does not modify this SFR; it only forces its inclusion because X.509 services are required to support TLS client functionality. |
| FIA_X509_EXT.3 | This PP-Module does not modify this SFR; it only forces its inclusion because X.509 services are required to support TLS client functionality. |
| 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. |
| **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. |

| PP-Module Requirement | Consistency Rationale |
|---|---|
| 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/CS-Admin | 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/CS-VVoIP | 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. |
| FAU_STG_EXT.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. |
| **Selection-Based SFRs** | |
| FAU_GEN.1/P2P-Admin | 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/P2P-VVoIP | 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. |

| PP-Module Requirement | Consistency Rationale |
|---|---|
| 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 App PP Base

### 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 8: App PP Security Problem Definition Consistency Rationale*

| PP-Module Threat | Consistency Rationale |
|---|---|
| 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. |
| 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. |
| 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 Objectives

The objectives defined by this PP-Module (see section 4.1) supplement those defined in the App PP as follows:

*Table 9: App PP Objective Consistency Rationale*

| PP-Module Objective | Consistency Rationale |
|---|---|
| O.NO_UNATTENDED_TRANSMISSION | The App PP defines objectives for network attack and network eavesdropping. The objective to not transmit unattended voice or video data when streaming media is not in use supplements these objectives. |
| O.ENCRYPTION | The App PP defines an objective for network eavesdropping. The objective to protect media transmission from disclosure through vocoder frames is a type of side-channel that is unique to the functions of a VVoIP endpoint. However, it is consistent with the overall objective of protecting transmitted data from disclosure. |
| O.TOE_ADMINISTRATION | The App PP defines an objective for security management. This PP-Module supplements this by defining an objective for management of its own capabilities. |
| 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. |

### 6.2.4 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 application is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the App PP as well as new SFRs that are used entirely to implement VVoIP functionality. The rationale for why this does not conflict with the SFRs defined by the App PP is as follows:

*Table 10: App PP SFR Consistency Rationale*

| 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. |
| **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 |

| PP-Module Requirement | Consistency Rationale |
|---|---|
| | 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/CS-Admin | 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/CS-VVoIP | 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. |
| FAU_STG_EXT.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. |
| **Selection-Based SFRs** | |
| FAU_GEN.1/P2P-Admin | 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/P2P-VVoIP | 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. |

| PP-Module Requirement | Consistency Rationale |
|---|---|
| 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. |

# A. Optional Requirements

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

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

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

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

## A.1 Strictly Optional Requirements

The below requirements may optionally be claimed in any TOE that conforms to this PP-Module, regardless of which Base-PP is claimed. Note that the requirements are iterated for clarity because NDcPP already defines FAU_GEN.1.

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

**FAU_GEN.1.1/CS-Admin** The **[*selection: TSF, TOE platform*]** shall be able to generate an audit record of the following auditable events:

~~a) Start-up and shutdown of the audit functions;~~
~~b) All auditable events for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and~~
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: no other actions, [assignment: list of other uses of privileges]]*].

**FAU_GEN.1.2/CS-Admin** The TSF shall record within each audit record at least the following information:

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

***Application Note:*** *This SFR defines the same auditable events as FAU_GEN.1/P2P-Admin 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 SFR FAU_STG_EXT.1 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_EXT.1 as a mandatory requirement.*

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

**FAU_GEN.1.1/CS-VVoIP** The TSF shall be able to generate an audit record of the following auditable events:

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

**FAU_GEN.1.2/CS-VVoIP** The TSF shall record within each audit record at least the following information:

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

*Table 11: Auditable Events*

| SFR | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| FDP_IFC.1 | Call Detail Record (CDR) of VVoIP peer communications | Calling Party<br>Called Party<br>Start time of call<br>Call Duration |
| FMT_SMF.1/VVoIP | [*selection: registration of TOE to ESC, none*] | [*selection: IP Address or Identifier for the ESC, none*] |
| FTA_SSL.3/Media | Termination of call due to inactivity | Call Party Dropped Time |

| | | |
|---|---|---|
| | | Calling Party<br>Called Party<br>Start time of call<br>Call Duration |
| FTP_ITC.1/Control | Establishment of connection to VVoIP call control server<br>Termination of connection to VVoIP call control server | Calling Party<br>Called Party<br>Established Connection Time<br>Terminated Connection Time |
| FTP_ITC.1/Media | Establishment of connection to VVoIP peer<br>Termination of connection to VVoIP peer | Calling Party<br>Called Party<br>Connection Time to VVoIP Peer<br>Disconnection Time to VVoIP Peer |

***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 SFR FAU_STG_EXT.1 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_EXT.1 as a mandatory requirement.*

## A.2 Objective Requirements

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

## A.3 Implementation-Dependent Requirements

The requirement below shall be claimed by the TOE in the following implementation:

- The TOE claims conformance to the App PP; and
- The TOE claims at least one of the optional requirements FAU_GEN.1/CS-Admin or FAU_GEN.1/CS-VVoIP, or the selection-based requirements FAU_GEN.1/P2P-Admin or FAU_GEN.1/P2P-VVoIP

### FAU_STG_EXT.1 Protected Audit Event Storage

**FAU_STG_EXT.1.1** The TSF shall be able to transmit the generated audit data to **[*selection*: *an Enterprise Session Controller that the TOE is registered to, an external trusted IT entity*]** using a trusted channel **according to FTP_DIT_EXT.1**.

**FAU_STG_EXT.1.2** The TSF shall be able to store generated audit data on the [*selection: TOE, TOE platform*].

**FAU_STG_EXT.1.3** The TSF shall [*selection: drop new audit data, overwrite previous audit records according to the following rule: [assignment: rule for overwriting previous audit records], [assignment: other action]*] when the local storage space for audit data is full.

# B. Selection-Based Requirements

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

## FAU_GEN.1/P2P-Admin Audit Data Generation (Peer-to-Peer Admin Events)

The following SFR shall be claimed by the TOE if "act as a VVoIP call control server when using P2P" is selected in FMT_SMF.1.1/VVoIP or "acting as a VVoIP call control server when using P2P" is selected in FDP_IFF.1.2:

**FAU_GEN.1.1/P2P-Admin** The **[*selection: TSF, TOE platform*]** shall be able to generate an audit record of the following auditable events:

a) ~~Start-up and shutdown of the audit functions;~~
b) ~~All auditable events for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and~~
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: no other actions, [assignment: list of other uses of privileges]]*].

**FAU_GEN.1.2/P2P-Admin** The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*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 SFR FAU_STG_EXT.1 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_EXT.1 as a mandatory requirement.*

### FAU_GEN.1/P2P-VVoIP Audit Data Generation (Peer-to-Peer VVoIP Events)

The following SFR shall be claimed by the TOE if "act as a VVoIP call control server when using P2P" is selected in FMT_SMF.1.1/VVoIP or "acting as a VVoIP call control server when using P2P" is selected in FDP_IFF.1.2:

**FAU_GEN.1.1/P2P-VVoIP** The TSF shall be able to generate an audit record of the following auditable events:

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

**FAU_GEN.1.2/P2P-VVoIP** The TSF shall record within each audit record at least the following information:

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

*Table 12: Auditable Events*

| SFR | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| FDP_IFC.1 | Call Detail Record (CDR) of VVoIP peer communications | Calling Party<br>Called Party<br>Start time of call<br>Call Duration |
| FMT_SMF.1/VVoIP | [*selection: registration of TOE to ESC, none*] | [*selection: IP Address or Identifier for the ESC, none*] |
| FTA_SSL.3/Media | Termination of call due to inactivity | Call Party Dropped Time<br>Calling Party<br>Called Party<br>Start time of call<br>Call Duration |
| FTP_ITC.1/Control | Establishment of connection to VVoIP call control server<br>Termination of connection to VVoIP call control server | Calling Party<br>Called Party<br>Established Connection Time<br>Terminated Connection Time |
| FTP_ITC.1/Media | Establishment of connection to VVoIP peer | Calling Party<br>Called Party |

| SFR | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| | Termination of connection to VVoIP peer | Connection Time to VVoIP Peer<br>Disconnection Time to VVoIP Peer |

***Application Note:*** *If the TOE claims this SFR and conforms to the App PP, the implementation-dependent SFR FAU_STG_EXT.1 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_EXT.1 as a mandatory requirement.*

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

The following SFR shall be claimed by the TOE if "SRTP" is selected in FTP_DIT_EXT.1 or FPT_ITC.1/Media:

**FCS_COP.1.1/SRTP** The TSF shall perform [*encryption/decryption to support SDES-SRTP*] in accordance with a specified cryptographic algorithm [**selection**: *AES-CTR (as defined in NIST SP 800-38A), AES-GCM (as defined in NIST SP 800-38D)*] and cryptographic key sizes [**selection**: *128-bit, 256-bit*].

***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(1), 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. It is permissible for different applications of GCM to support different key sizes.*

### FCS_SRTP_EXT.1 Secure Real-Time Transport Protocol

The following SFR shall be claimed by the TOE if "SRTP" is selected in FTP_DIT_EXT.1 or FPT_ITC.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: [*selection:*

- *AES_CM_128_HMAC_SHA1_80, in accordance with RFC 4568,*
- *AES_CM_128_HMAC_SHA1_32, in accordance with RFC 4568,*
- *AES_256_CM_HMAC_SHA1_80, in accordance with RFC 6188,*
- *AES_256_CM_HMAC_SHA1_32, in accordance with RFC 6188,*
- *AEAD_AES_128_GCM, in accordance with RFC 7714,*
- *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 one of the identified cipher suites. The ST author should select any or all cipher suites supported.*

**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.*

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

The following SFR shall be claimed by the TOE if "act as a VVoIP call control server when using P2P" is selected in FMT_SMF.1.1/VVoIP or "acting as a VVoIP call control server when using P2P" is selected in FDP_IFF.1.2:

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

## FDP_IFF.1/CallControl Simple Security Attributes (for Call Control)

The following SFR shall be claimed by the TOE if "act as a VVoIP call control server when using P2P" is selected in FMT_SMF.1.1/VVoIP or "acting as a VVoIP call control server when using P2P" is selected in FDP_IFF.1.2:

**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*].

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

The following SFR shall be claimed by the TOE if "register the TOE to an ESC…" is selected in FMT_SMF.1.1/VVoIP. Note that if the TOE claims conformance to the NDcPP as its Base-PP, 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.

**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 an **ESC***].

# C. Extended Components Definition

This appendix defines the extended components used in this PP-Module.

*Table 13: Extended Components Definitions*

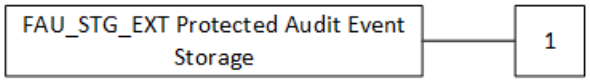
| Functional Class | Functional Components |
|---|---|
| **Security Audit (FAU)** | FAU_STG_EXT Protected Audit Event Storage |
| **Communications (FCO)** | FCO_VOC_EXT Vocoder Usage |
| **Cryptographic Support (FCS)** | FCS_SRTP_EXT Secure Real-Time Transport Protocol |
| **Protection of the TSF (FPT)** | FPT_STM_EXT Time Stamps |

## C.1 FAU_STG_EXT Protected Audit Event Storage

**Family Behavior**

Components in this family define requirements for the TSF to be able to securely transmit audit data between the TOE and an external entity.

**Component Leveling**




FAU_STG_EXT.1, Protected Audit Event Storage, requires the TSF to use a trusted channel implementing a secure protocol.

**Management: FAU_STG_EXT.1**

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

- Ability to configure the cryptographic functionality

**Audit: FAU_STG_EXT.1**

There are no auditable events foreseen.

**FAU_STG_EXT.1 Protected Audit Event Storage**

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit Data Generation

FTP_ITC.1 Inter-TSF Trusted Channel

**FAU_STG_EXT.1.1** The TSF shall be able to transmit the generated audit data to [*assignment: an external trusted IT entity*] using a trusted channel.

**FAU_STG_EXT.1.2** The TSF shall be able to store generated audit data on the [*selection: TOE, TOE platform*].

**FAU_STG_EXT.1.3** The TSF shall [*assignment: perform action*] when the local storage space for audit data is full.

## C.2 FCO_VOC_EXT Vocoder Usage

**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: No dependencies

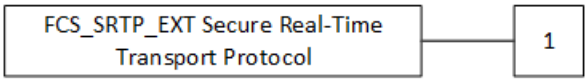
**FCO_VOC_EXT.1.1** The TSF shall transmit voice media using a constant bit rate voice vocoder.

## C.3 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: 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.

## C.4 FPT_STM_EXT Time Stamps

**Family Behavior**

Components in this family extend FPT_STM requirements by describing the source of time used in timestamps.

**Component Leveling**


FPT_STM_EXT.1, Reliable Time Stamps, requires that the TSF provide reliable time stamps for the TOE and identifies the source of the time used in those timestamps.

**Management: FPT_STM_EXT.1**

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

- Management of the time
- Administrator setting of the time

**Audit: FPT_STM_EXT.1**

There are no auditable events foreseen.

**FPT_STM_EXT.1 Reliable Time Stamps**

Hierarchical to: No other components

Dependencies: No dependencies

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

**FPT_STM_EXT.1.2** The TSF shall [*selection: allow the Security Administrator to set the time, synchronize time with an NTP server*].

# D. Implicitly Satisfied Requirements

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.

*Table 14: Implicitly Satisfied Requirements Rationale*

| 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.<br><br>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.<br><br>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.<br><br>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 |

| Requirement | Rationale for Satisfaction |
|---|---|
| | 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.<br><br>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.<br><br>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.<br><br>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.<br><br>If the TOE claims conformance to the NDcPP, the dependency is also explicitly met through FPT_STM_EXT.1, regardless of |

| Requirement | Rationale for Satisfaction |
|---|---|
| | whether the TOE is deployed in a client-server configuration (with registration to an ESC) or peer-to-peer configuration (with no ESC involved). |

# E. Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy source(s) beyond the requirements outlined in the Base-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.

# F. References

*Table 15: References*

| Identifier | Title |
|---|---|
| **[CC]** | Common Criteria for Information Technology Security Evaluation –<br>• Part 1: Introduction and General Model, CCMB-2070-04-001, Version 3.1 Revision 5, April 2017<br>• Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017<br>• Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017<br>• CC and CEM addenda: Exact Conformance, Selection-Based SFRs, Optional SFRs, CCDB-2017-05-xxx, Version 0.5, May 2017 |
| **[NDcPP]** | collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020 |
| **[App PP]** | Protection Profile for Application Software, Version 1.3, March 1, 2019 |
| **[TLS Package]** | Functional Package for Transport Layer Security (TLS), Version 1.1, February 12, 2019 |
| **[SD]** | Supporting Document Mandatory Technical Document, PP-Module for Voice/Video over IP (VVoIP) Endpoints, 28 October 2020 |

# G. Acronyms

The acronym definitions in Base-PP should be consulted in addition to those listed here.

*Table 16: Acronyms*

| Acronym | Meaning |
|---|---|
| **DHCP** | Dynamic Host Configuration Protocol |
| **ESC** | Enterprise Session Controller |
| **IETF** | Internet Engineering Task Force |
| **IP** | Internet Protocol |
| **ITU-T** | International Telegraph Union – Telecommunication Standardization Sector |
| **NTP** | Network Time Protocol |
| **PII** | Personally Identifiable Information |
| **PP** | Protection Profile |
| **P2P** | Peer-to-Peer |
| **SIP** | Session Initiation Protocol |
| **SRTP** | Secure Real-Time Transport Protocol |
| **TCP** | Transmission Control Protocol |
| **TFTP** | Trivial File Transfer Protocol |
| **UDP** | User Datagram Protocol |
| **VVoIP** | Voice/Video over IP |