Network Device Collaborative Protection Profile (NDcPP)/Application Software Protection Profile (App PP) Extended Package Voice/Video over IP (VVoIP) Endpoint

Version: 1.0
2016-09-28
National Information Assurance Partnership

Revision History

Version	Date	Comment
v0.1	2016-08-26	Initial draft
v0.2	2016-08-26	Internal updates based on IAD feedback
v0.3	2016-09-16	Updates based on TC feedback
v0.4	2016-09-26	Updates based on TC feedback
v1.0	2016-09-28	Publishing

Table of Contents

1 Introduction

1.1 Overview

The scope of this Extended Package (EP) 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 EP is not complete in itself, but rather extends either the collaborative Protection Profile for Network Devices (NDcPP) or the Protection Profile for Application Software (App PP). This is because a VVoIP endpoint is a specific type of network device or software application that carries sensitive data over remote channels and uses protocols that are not implemented by a typical network device or software application. Therefore, additional security requirements are necessary to ensure that sensitive communications are not subject to unauthorized disclosure to unintended recipients.

1.2 Terms

The following sections provide both Common Criteria and technology terms used in this EP.

1.2.1 Common Criteria Terms

Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Extended Package (EP)	An implementation-independent set of security requirements for a specific subset of products described by a PP.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Security Assurance Requirement (SAR)	A requirement for how the TOE's proper implementation of the SFRs is verified by an evaluator.
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. In this case, a network device with Enterprise Session Controller capabilities.
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 a ST.

1.2.2 Technology Terms

Enterprise Session Controller	A VVoIP infrastructure device that is used to set up and tear down calls between VVoIP endpoints.
H.323	A communications protocol defined by ITU-T that is used for creating, modifying, and terminating multimedia sessions with multiple participants.
Session Initiation Protocol	A communications protocol defined by IETF that is used for creating, modifying, and terminating multimedia sessions with multiple participants.
Secure Real-Time Transport Protocol	A protocol that is used to provide multimedia (voice/video) streaming services with added security of encryption, message authentication and integrity, and replay protection.

1.3 Compliant Targets of Evaluation

The Target of Evaluation that is defined by this EP and either the NDcPP or the App PP is a dedicated device or software application that provides the exchange of voice and/or video communication across an Internet Protocol (IP) network. The endpoint is a client (TOE) that communicates with an Enterprise Session Controller (ESC) server. The VVoIP endpoint shall be able to secure file download from a file server to update VVoIP endpoint software and configuration, establish secure communication for call control with the ESC, and secure streaming media to other devices.

The combination of the NDcPP and this EP is a network device, either a dedicated appliance with a non-modifiable operating system, or a general-purpose server running an independent commercially-available operating system, that provides VVoIP endpoint functionality. Regardless of whether the TOE is a standalone appliance or a general-purpose device that is configured to function as a VVoIP endpoint, the TOE must be capable of satisfying all of the mandatory requirements of the NDcPP. The combination of the App PP and this EP is a software application running on a general purpose operating system that provides VVoIP endpoint capabilities in addition to all of the security functionality expected of a software application as mandated by the App PP.

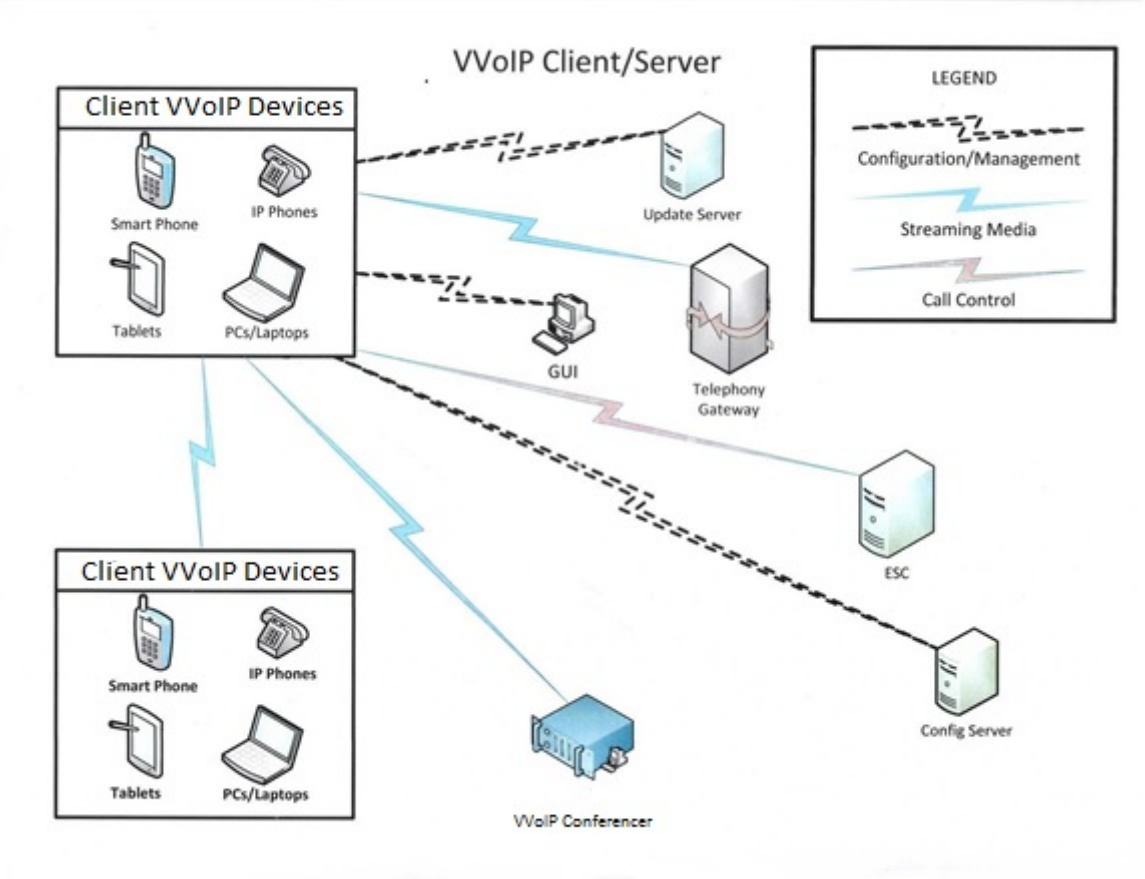
Secure File Download is the exchange of packets between the client and the file server (may be the same server as the ESC). Call Control is the packets exchanged between the ESC and client (VVoIP endpoint) to establish, maintain, and tear down a telephony call. Streaming Media is the voice/video exchanged between the endpoints.

This EP describes the functional requirements and threats specific to the VVoIP endpoint. Any requirements to the VVoIP endpoint not specified in this EP need to follow the ND cPP or App PP. The most notable additions are requirements for the call control protocol (SIP, H.323/H225.0, H.245) and streaming media protocol (SRTP, RTP).

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, they have not been depicted.



The TOE connects to an Enterprise Session Controller (ESC) in order to set up connections with other VVoIP endpoint devices or other telephony equipment such as a call conference. Additionally, the ESC is responsible for storing audit data for the TOE's operation. The ESC also has 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). To initiate communication with the ESC, the TOE needs an IP address, network mask, gateway address, configuration server address, upgrade server address, and ESC 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). 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 ESC 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 are closed.

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 ESC), and configuration/management path to configure and manage the TOE (software/firmware updates, configuration updates, audit).

1.4 Use Cases

Requirements in this EP are designed to address the security problem in the following use cases. The description of these use cases provide instructions for how the TOE and its Operational Environment should be made to support the functionality required by this EP.

[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 EP is sufficient to ensure security.

[USE CASE 2] Software Application

The VVoIP endpoint is sold and packaged as an application that is installed on a general purpose computer 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 the NIAP 'Protection Profile for Application Software'. The underlying platform is also expected to conform to the NIAP 'Protection Profile for General Purpose Operating Systems' but this is outside the scope of the EP. A conformant TOE may rely on the operating system for certain functions such as auditing or cryptography. However, any such function must be clearly identified and evidence must be provided that the operating system function meets the assurance activities specified in this EP for the relevant SFRs.

Regardless of the physical embodiment of the TOE, the expected functional capabilities are the same. This EP defines optional and selection-based requirements to allow for multiple ways to implement a given function. These differences do not constitute separate use cases because they represent the same fundamental usage of the TOE.

2 Conformance Claims

Conformance Statement

To be conformant to this EP, an ST must demonstrate Exact Conformance, a subset of Strict Conformance as defined in [CC] Part 1 (ASE_CCL). The ST must include all components in this EP that are:

- Unconditional (which are always required)
- Selection-based (which are required when certain selections are chosen in the unconditional requirements)

and may include components that are

- Optional
- Objective.

Unconditional requirements are found in the main body of the document (Section 5), while appendices contain the selection-based, optional, and objective requirements. The ST may iterate any of these components but it must not introduce any additional component (e.g. from CC Part 2 or 3) that is not defined in either the NDcPP or App PP (which this EP extends), or in this EP itself.

CC Conformance Claims

This EP is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Revision 4 [CC].

PP Claim

This EP does not claim conformance to any Protection Profile. Note that this EP extends either the NDcPP or App PP, which means that it relies on either of these PPs to provide some set of 'base' functionality which is then expanded upon by this EP. This however does not imply that the EP itself is conformant to either of these PPs.

Package Claim

This EP does not claim conformance to any packages.

3 Security Problem Description

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

Note that as an EP of the NDcPP or App PP, all threats, assumptions, and OSPs defined in the base PP will also apply to a TOE unless otherwise specified, depending on which of the base PPs it extends. The Security Functional Requirements defined in this EP will mitigate the threats that are defined in the EP but may also mitigate some threats defined in the base PPs in more comprehensive detail due to the specific capabilities provided by a VVoIP endpoint.

3.1 Threats

T.UNDETECTED_TRANSMISSION

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

T.CLOCK_DESYNC

An attacker may cause the TOE to use incorrect clock data, resulting in a denial of service from causing encryption and/or authentication connection failures.

T.MEDIA_DISCLOSURE

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

3.2 Assumptions

This EP defines no additional assumptions beyond those defined in the supported base PPs.

3.3 Organizational Security Policies

This EP defines no additional organizational security policies beyond those defined in the supported base PPs.

4 Security Objectives

4.1 Security Objectives for the TOE

This EP defines no additional TOE security objectives beyond those specified in the base PPs.

4.2 Security Objectives for the Operational Environment

Because this EP does not define any additional assumptions or organizational security policies, there are no additional security objectives for the Operational Environment to satisfy.

4.3 Security Objectives Rationale

This section is not applicable to this EP because no additional security objectives are defined.

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 4*, 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:

- **Assignment** is indicated with italicized text.
- **Refinement** is made by EP author and indicated with bold text.
- **Selection** is indicated with underlined text.
- **Assignment** within a Selection is indicated with italicized and underlined text.
- **Iteration** is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the iteration, e.g. '/CDR' for an SFR relating to call detail records.
- **Extended SFRs** is identified by having a label "EXT" after the SFR name.

5.1 NDcPP Security Functional Requirements Direction

In cases where the TOE is a physical appliance and this EP is used to extend the NDcPP, it is necessary for the ST author to make certain selections or assignments and to include certain optional requirements in order to provide the functionality required by the EP. This section provides instructions on what claims need to be made in the base PP in order to claim conformance to this EP.

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

5.1.1 Cryptographic Support (FCS)

FCS_TLSC_EXT.2 TLS Client Protocol with Authentication

This SFR is optional in the NDcPP but is mandated by this EP because TLS is used to secure call control and streaming media channels, regardless of the application layer protocol used.

Assurance Activity

No additional testing is required for this SFR beyond what is required for the NDcPP.

5.1.2 Security Management (FMT)

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;

- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates;
- **Ability to register the TOE to an ESC [*selection: manually, via TFTP server*];**
- [selection:
  - *Ability to configure audit behavior;*
  - *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;*
  - *Ability to configure the cryptographic functionality;*
  - ***Ability to configure the termination period for idle calls;***
  - ***Ability to specify the vocoder used;***
  - *No other capabilities]*

Application Note: *This EP modifies the existing FMT_SMF.1 SFR in the base PP to provide the ability of the ST author to select configurable functions related specifically to VVoIP endpoint functionality. Note that these functions may not be configurable if the TSF automatically operates in a manner that meets the SFRs by default.*

Some management functions may be implemented such that they can only be configured via an ESC/configuration server rather than through direct human interaction with the TOE. It is expected that the ST author provide information on how each management function is performed so that the evaluator can analyze the different TSF-relevant data that is transmitted to the TOE via each logical interface.

Assurance Activity

TSS In addition to the assurance activities specified in the base PP for this SFR, 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).

AGD The evaluator shall verify that the operational guidance provides instructions on configuring the TOE.

Test In addition to the assurance activities specified in the base PP for this SFR, the evaluator shall perform the following tests, depending on the method(s) supported for registering the TOE to an ESC:

Test 1 (conditional): ESC registration based on manual input:

1. On the TOE, input IP address, gateway address, and subnet mask.
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.
3. Save configuration.
4. Verify the TOE registers to the ESC.

Test 2: ESC registration based on values input from TFTP server:

1. On the TOE, input the TFTP server address.
2. Save configuration.
3. Verify by sniffing that the TOE receives all needed IP addresses.
4. Verify by examining the IP address on the TOE.
5. Verify the TOE registers to the ESC.

5.1.3 Protection of the TSF (FPT)

FPT_STM.1 Reliable Time Stamps

This EP does not modify the FPT_STM.1 SFR that is defined in the NDcPP. However, the expectation for this EP is that the TOE's time source is the ESC itself. The TOE will not rely on itself as its own definitive time source. Therefore, the additional testing described below is expected to be performed for this EP.

Assurance Activity

TSS The evaluator shall verify that the TSS describes the ability of the TOE to support NTP synchronization.

AGD The evaluator shall review the guidance to confirm that it provides instructions for how to enable NTP synchronization.

Test The evaluator shall register the TOE with the ESC and verify the TOE's clock is updated to be the same time as the ESC. The evaluator shall change the time on the time source and verify that after a short period of time, the TOE's clock is updated to be the same as what is set on the ESC.

FPT_TUD_EXT.1 Trusted Update

This SFR is unchanged from the NDcPP. However, note that this EP expects the ESC 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.

Assurance Activity

Functionally, no additional testing is required for this SFR beyond what is required for the NDcPP. The evaluator is still expected to test the ability for

the TOE to verify its current version, to apply valid updates, and to reject invalid updates. Note however that the following additional configuration steps may be necessary in order for this testing to be performed for a VVoIP endpoint TOE.

- The evaluator deploys an ESC or dedicated file server in the TOE's Operational Environment
- The evaluator loads valid and invalid candidate updates to the ESC or dedicated file server
- The evaluator configures the TOE to use the ESC or dedicated file server as its source for software/firmware updates

5.1.4 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall **be capable of using [*TLS, [selection: IPsec, SSH, HTTPS, no other protocols*]]** to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: streaming media channel, call control channel, audit channel, software/firmware update delivery channel *[selection: [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. This EP mandates the inclusion of TLS as a client for TLS because it is the underlying protocol used to secure communications with the ESC and other VVoIP endpoints. Additional protocols may 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.*

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*assignment: list of **services for which the TSF is able to initiate communications***].

Assurance Activity

No additional testing is required for this SFR beyond what is required for the NDcPP.

FTP_TRP.1 Inter-TSF Trusted Channel

FTP_TRP.1.1 The TSF shall **be capable of using [*selection: IPsec, SSH, TLS, HTTPS*] to** provide a communication path between itself and **authorized remote administrators**

that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*disclosure*] **and provides detection of modification of the channel data.**

FTP_TRP.1.2 The TSF shall permit **remote administrators** to initiate communication via the trusted channel.

FTP_TRP.1.3 The TSF shall initiate communication via the trusted channel for [*initial administrator authentication and all remote administration actions*].

Application Note: *The TOE is required to provide functionality to configure certain aspects of TOE operation that is not typically available to general users. This EP requires the TSF to provide a remote mechanism to accomplish this.*

Assurance Activity

No additional testing is required for this SFR beyond what is required for the NDcPP.

5.2 App PP Security Functional Requirements Direction

In cases where the TOE is a software application and this EP is used to extend the App PP, it is necessary for the ST author to make certain selections or assignments and to include certain optional requirements in order to provide the functionality required by the EP. This section provides instructions on what claims need to be made in the base PP in order to claim conformance to this EP.

Full assurance activities are not repeated for the requirements in this section that are references to the App PP; only the additional testing needed to supplement what has already been captured in the App PP is included.

5.2.1 Cryptographic Support (FCS)

FCS_TLSC_EXT.2 TLS Client Protocol with Authentication

This SFR is optional in the App PP but is mandated by this EP because the VVoIP communications must be secured using both encryption and authentication.

Assurance Activity

No additional testing is required for this SFR beyond what is required for the App PP.

5.2.2 Security Management (FMT)

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [selection:

- *no management functions,*

- *enable/disable the transmission of any information describing the system's hardware, software, or configuration,*
- *enable/disable the transmission of any PII,*
- *enable/disable transmission of any application state (e.g. crashdump) information,*
- *enable/disable network backup functionality to [assignment: list of enterprise or commercial cloud backup systems],*
- ***configure the termination period for idle calls,***
- ***specify the vocoder used,***
- *[assignment: list of other management functions to be provided by the TSF]]*

Application Note: *This EP modifies the existing FMT_SMF.1 SFR in the base PP to provide the ability of the ST author to select configurable functions related specifically to VVoIP endpoint functionality. Note that these functions may not be configurable if the TSF automatically operates in a manner that meets the SFRs by default.*

Assurance Activity

TSS There are no TSS activities for this SFR beyond what is required by the App PP.

AGD There are no AGD evaluation activities for this SFR beyond what is required by the App PP.

Test Compliance with the SFRs in section 5.2 and 5.3 of this EP is sufficient to demonstrate that the TOE provides sufficient means to manage its TOE functions.

5.2.3 Protection of the TSF (FPT)

FPT_TUD_EXT.1 Trusted Update

This SFR is unchanged from the App PP. However, note that this EP expects the ESC or other server to function as the source of TOE software/firmware updates. The evaluator shall ensure that the test environment is configured appropriately.

Assurance Activity

Functionally, no additional testing is required for this SFR beyond what is required for the App PP. The evaluator is still expected to test the ability for the TOE to verify its current version, to apply valid updates, to reject invalid updates, to receive updates in a format that is used by the platform-supported package manager, to remove all traces of itself upon removal, and to block modification of its own executable code. Note however that the following additional configuration steps may be necessary in order for this testing to be performed for a VVoIP endpoint TOE.

- The evaluator deploys an ESC or dedicated file server in the TOE's Operational Environment

- The evaluator loads valid and invalid candidate updates to the ESC or dedicated file server
- The evaluator configures the TOE to use the ESC or dedicated file server as its source for software/firmware updates

5.2.4 Trusted Path/Channels (FTP)

FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1 The application shall [*encrypt all transmitted data with **TLS,** [selection: HTTPS, DTLS, SSH**, SRTP, 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. This EP mandates the inclusion of TLS as a client for TLS because it is the underlying protocol used to secure communications with the ESC and other VVoIP endpoints. Additional protocols may 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.*

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 so the proper protocols should be selected accordingly.

Assurance Activity

No additional testing is required for this SFR beyond what is required for the App PP.

5.3 TOE Security Functional Requirements

The Security Functional Requirements (SFRs) included in this section are those that the TSF is expected to satisfy regardless of whether this EP is used as an extension of the NDcPP or the App PP.

The SFRs are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, with additional extended functional components.

5.3.1 Security Audit (FAU)

FAU_GEN.1/VVoIP Audit Data Generation (VVoIP)

FAU_GEN.1.1/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 Table 1*]

FAU_GEN.1.2/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 Table 1*].

SFR	Auditable Event	Additional Audit Record Contents
FDP_IFC.1	Call Detail Record (CDR) of VVoIP peer communications	Calling Party
		Called Party
		Start time of call
		Call Duration
FMT_SMF.1	Registration of TOE to ESC	Media Access Control (MAC) Address
FTA_SSL.3/Media	Termination of call due to inactivity	Call Party Dropped Time
		Calling Party
		Called Party
		Start time of call
		Call Duration
FTP_ITC.1/Control	Establishment of connection to ESC	Calling Party
		Called Party
		Established Connection Time
	Termination of connection to ESC	Terminated Connection Time
FTP_ITC.1/Media	Establishment of connection to VVoIP peer	Calling Party
		Called Party
		Connection Time to VVoIP Peer
	Termination of connection to VVoIP peer	Disconnection Time to VVoIP Peer

Table 1 – Auditable Events

Application Note: *Any relevant auditable events for the functionality described in the base PP is defined there. This SFR defines only the auditable events for VVoIP-related functions mandated by this EP.*

Assurance Activity

TSS There are no TSS assurance activities for this SFR.

AGD The evaluator shall check the guidance documentation and ensure that it lists all of the auditable events and provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the EP is described and that the description of the fields contains the information required in FAU_GEN.1.2, and the additional information specified in the table of audit events.

Test For each auditable event in Table 1, 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 AGD evidence and that all audit record details specified in the SFR are present.

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.*

Assurance Activity

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.

AGD There are no AGD evaluation activities for this SFR.

Test The evaluator shall set up a test environment that contains the TOE, an ESC, a network switch, a traffic sniffer, and a second VVoIP endpoint.

The evaluator shall then perform the following test:

1. The evaluator shall register the TOE and the second VVoIP endpoint to the ESC and verify that the registrations took place.
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.

3. The evaluator shall review the sniffed 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 shall not stream from the TOE.*

Assurance Activity

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

AGD There are no AGD evaluation activities for this SFR.

Test This SFR is evaluated in conjunction with FDP_IFF.1

FDP_IFF.1 Information Flow Control Functions

FDP_IFF.1.1 The TSF shall enforce the [*media transmission policy*] based on the following types of subject and information security attributes: [*ESC registration status and TOE hook state*].

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 registered with the ESC,*
- *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,***
- ***The TOE is in the off-hook state,***
- ***No other rules]*].**

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*].

Application Note: *Unattended voice or video should not be transmitted from the TOE when streaming media is not in use.*

Assurance Activity

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.

AGD There are no AGD evaluation activities for this SFR.

Test The evaluator shall set up a test environment that contains the TOE, an ESC, a network switch, a traffic sniffer, and a second VVoIP endpoint.

The evaluator shall then perform the following tests:

Test 1:

1. The evaluator shall place the TOE into the on-hook state without registering it to the ESC. The evaluator shall use the sniffer to observe that no streaming media traffic is transmitted by the TOE.

Test 2: The evaluator shall repeat Test 1 above with the following additional step:

1. The evaluator shall place the TOE into the off-hook state and verify that the TOE continues not transmitting any streaming media traffic.

Test 3:

1. The evaluator shall register the TOE with the ESC and verify that the TOE is registered by checking the ESC screen with current TOE connections and by viewing the call control path traffic using the sniffer.
2. The evaluator shall place the TOE into the on-hook state and verify using the sniffer that no streaming media traffic is transmitted by the TOE.

Test 4: The evaluator shall repeat Test 3 above with the following additional step:

1. 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 5:

1. The evaluator shall register the TOE with the ESC and verify that it is registered by checking the ESC with current connections and using the sniffer to verify the call control path traffic.
2. The evaluator shall register the second VVoIP endpoint with the ESC and verify that it has been registered by checking the ESC with current connections and using the sniffer to verify the call control path traffic.
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 sniffer to verify that a steady stream of traffic is being transmitted between the two endpoints over the media channel.

Test 6:

1. The evaluator shall register the TOE with the ESC and verify that it is registered by checking the ESC with current connections and using the sniffer to verify the call control path traffic.
2. The evaluator shall register the second VVoIP endpoint with the ESC and verify that it has been registered by checking the ESC with current connections and using the sniffer to verify the call control path traffic.
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 sniffer to verify that streaming media traffic is being transmitted between the TOE and other endpoint over the streaming media channel.
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. The evaluator shall also verify that a mute control message is sent to the ESC and the ESC responds.

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 7:

1. The evaluator shall register the TOE to the ESC and place it in the on-hook state.
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 8:

1. The evaluator shall register both the TOE and the second VVoIP endpoint to the ESC.
2. The evaluator shall place the TOE in the on-hook state.
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.
4. The evaluator shall place a call to the second VVoIP endpoint and verify the call is established. The evaluator shall sniff the traffic to determine the port used by the TOE to carry the media traffic.
5. The evaluator shall hang up the call and verify that the TOE has returned to the on-hook state.
6. The evaluator shall perform fuzzing activities to verify that the port used to carry media traffic in step 4 has been closed.

Test 9 (conditional):

1. If the TSF supports the use of a hold state, 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. The evaluator shall also verify that the VVoIP endpoint on-hold call control is sent to the ESC and.
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 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 [*[assignment: default number of seconds] seconds, an administrator-configurable interval on the [selection: ESC, configuration server] downloaded to the TOE during configuration*].

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.*

Assurance Activity

TSS The evaluator shall verify that the TSS specifies the default period of time that the TSF will use to terminate idle calls as well as the ability for configuration downloaded from either an ESC acting as a configuration server or a standalone configuration server.

AGD There are no AGD evaluation activities for this SFR.

Test The evaluator shall set up a test environment that contains the TOE, an ESC, a configuration server (if used to communicate configuration changes to idle timeout period), a network switch, a traffic sniffer, and a second VVoIP endpoint.

The evaluator shall then perform the following tests:

Test 1:

1. Deploy the TOE in a default configuration (i.e. without any administrative override applied to the idle timeout value).
2. Register the TOE with the ESC and verify that it is registered by viewing its status on the ESC and sniffing the call control path traffic.
3. Register the second VVoIP endpoint with the ESC and verify that it is registered by viewing its status on the ESC and sniffing the call control path traffic.
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 sniffing the streaming media traffic that is transmitted between them.
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 2:

1. Deploy the TOE in a default configuration (i.e. without any administrative override applied to the idle timeout value).
2. Register the TOE with the ESC and verify that it is registered by viewing its status on the ESC and sniffing the call control path traffic.
3. Using the ESC or configuration server (depending on what is supported by the TOE), configure the TOE's idle timeout period for the shortest period of time that is supported.
4. Register the second VVoIP endpoint with the ESC and verify that it is registered by viewing its status on the ESC and sniffing the call control path traffic.
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 sniffing the streaming media traffic that is transmitted between them.
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 3:

1. 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.

5.3.5 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: SIP, H.323*]** to provide a trusted communication channel between itself and **an Enterprise Session Controller** 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 Enterprise Session Controller*]** 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.*

Assurance Activity

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

AGD There are no AGD evaluation activities for this SFR.

Test This SFR is an iteration of FTP_ITC.1 as defined in the NDcPP. The evaluator shall repeat the assurance activities defined for FTP_ITC.1 in the NDcPP for this iteration of the SFR. Specifically, in order to demonstrate that either SIP or H.323 communications are secured, it is necessary for the evaluator to demonstrate that call setup/teardown is performed over TLS.

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 shall be chosen to match the trusted control channel: SIP – SRTP, H.323 – H.323/H.235*

Assurance Activity

TSS The evaluator shall verify that the trusted channel will use SRTP or H.323/H.235.

AGD There are no AGD evaluation activities for this SFR.

Test This SFR is an iteration of FTP_ITC.1 as defined in the NDcPP. The evaluator shall repeat the assurance activities defined for FTP_ITC.1 in the NDcPP for this iteration of the SFR.

5.4 TOE Security Assurance Requirements

As an EP of the NDcPP or the App PP, this EP does not prescribe any SARs beyond those defined in the base PPs. The evaluator shall ensure that the SARs defined in the claimed base PP are assessed against the entire TSF as appropriate.

A. Optional Requirements

As indicated in Section 2, the baseline requirements (those that must be performed by the TOE) are contained in the body of this EP. Additionally, there are three other types of requirements specified in Appendix A, Appendix B, and Appendix C. The first type (in this Appendix) are requirements that can be included in the ST, but are not required in order for a TOE to claim conformance to this EP. The second type (in Appendix B) are requirements based on selections in the body of the EP: if certain selections are made, then additional requirements in that appendix must be included. The third type (in Appendix C) are components that are not required in order to conform to this EP, but will be included in the baseline requirements in future versions of this EP, so adoption by vendors is encouraged. Note that the ST author is responsible for ensuring that requirements that may be associated with those in Appendix A, Appendix B, and Appendix C but are not listed (e.g., FMT-type requirements) are also included in the ST.

A.1 Security Audit (FAU)

FAU_STG_EXT.1 Protected Audit Event Storage

The following SFR shall be included in the ST if the TOE claims conformance to the App PP and not the NDcPP.

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to **an Enterprise Session Controller that the TOE is registered to** 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*]** itself.

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.

Application Note: *This SFR is functionally identical to FAU_STG_EXT.1 as defined in the NDcPP except that it permits the TSF to store audit data locally on its host platform (i.e. the OS file system) instead of within the TOE boundary since the App PP TOE does not include physical disk storage.*

Assurance Activity

Refer to the Assurance Activity for this SFR in the Supporting Documents for the NDcPP.

B. Selection-Based Requirements

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

FCS_SRTP_EXT.1 Secure Real-Time Transport Protocol

The following SFR shall be included in the ST if SRTP is selected in FTP_DIT_EXT.1 and/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 ciphersuites in accordance with RFC 4568: AES_CM_128_HMAC_SHA1_80.

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 ciphersuite. In the future Suite B ciphersuites will be available.*

Assurance Activity

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 ciphersuites are rejected by the TSF.

AGD There are no AGD evaluation activities for this SFR.

Test 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. To ensure that the call is being encrypted and to view the ciphersuites being used a packet capture tool should be used. In order to decrypt the TLS-SIP traffic and view the SDES negotiation the SIP server's private key needs to be loaded into the packet capture tool.

C. Objective Requirements

This Annex includes requirements that specify security functionality which also addresses threats. The requirements are not currently mandated in the body of this EP as they describe security functionality not yet widely available in commercial technology. However, these requirements may be included in the ST such that the TOE is still conformant to this EP, and it is expected that they be included as soon as possible.

Currently, no objective requirements specific to VVoIP endpoint TOEs have been identified.

D. 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 'Entropy Documentation and Assessment' section of the NDcPP/App PP. As with other base PP requirements, the only additional requirement is that the entropy documentation also applies to the specific VVoIP endpoint capabilities of the TOE in addition to the functionality required by the base PP.

E. References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012 • Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 • Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
[NDcPP]	• collaborative Protection Profile for Network Devices, Version 1.0, 27-Feb-2015
[App PP]	• Protection Profile for Application Software, Version: 1.2, 2016-04-22

F. 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
NDcPP	Collaborative Protection Profile for Network Devices
NTP	Network Time Protocol
PII	Personally Identifiable Information
PP	Protection Profile
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