Supporting Document

Mandatory Technical Document

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

Version: 1.0

2020-10-28

National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the Common Criteria Recognition Arrangement (CCRA).

Technical Editor:

National Information Assurance Partnership (NIAP)

Document history:

V1.0, 28 October 2020 (Initial)

General Purpose:

The purpose of this SD is to define evaluation methods for the functional behavior of Voice/Video over IP (VVoIP) endpoints.

Field of special use:

Voice/Video over IP (VVoIP) Endpoints, implemented as network devices or applications.

Acknowledgements:

The NIAP Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia supported the development of this SD.

Table of Contents

1 Introduction 5
1.1 Technology Area and Scope of Supporting Document 5
1.2 Structure of the Document 5
1.3 Terminology 5
1.3.1 Glossary 5
1.3.2 Acronyms 6

2 Evaluation Activities for SFRs 7
2.1 NDcPP Evaluation Activities 7
2.1.1 Security Audit (FAU) 7
2.1.1.1 Protected Audit Event Storage (FAU_STG_EXT) 7
2.1.2 Cryptographic Support (FCS) 7
2.1.2.1 NTP Protocol (FCS_NTP_EXT) 7
2.1.2.2 TLS Client Protocol (FCS_TLSC_EXT) 7
2.1.3 Identification and Authentication (FIA) 7
2.1.3.1 Authentication Using X.509 Certificates (FIA_X509_EXT) 7
2.1.4 Protection of the TSF (FPT) 8
2.1.4.1 Trusted Update (FPT_TUD_EXT) 8
2.1.5 Trusted Path/Channels (FTP) 8
2.1.5.1 Inter-TSF Trusted Channel (FTP_ITC) 8
2.1.6 Additional Requirements 8
2.2 App PP Evaluation Activities 8
2.2.1 Protection of the TSF (FPT) 9
2.2.1.1 Trusted Update (FPT_TUD_EXT) 9
2.2.2 Trusted Path/Channels (FTP) 9
2.2.2.1 Protection of Data in Transit (FTP_DIT_EXT) 9
2.2.3 Additional Requirements 9
2.3 TOE SFR Evaluation Activities 9
2.3.1 Communications (FCO) 9
2.3.1.1 Vocoder Usage (FCO_VOC_EXT) 9
2.3.2 User Data Protection (FDP) 10
2.3.2.1 Information Flow Control Policy (FDP_IFC) 10
2.3.2.2 Information Flow Control Functions (FDP_IFF) 10
2.3.3 Security Management (FMT) 13
2.3.3.1 Specification of Management Functions (FMT_SMF) 13
2.3.4 TOE Access (FTA) 13
2.3.4.1 Session Locking and Termination (FTA_SSL) 13
2.3.5 Trusted Path/Channels (FTP) 15
2.3.5.1 Inter-TSF Trusted Channel (FTP_ITC) 15

3 Evaluation Activities for Optional Requirements 18
3.1 Security Audit (FAU) 18

3.1.1 Security Audit Data Generation (FAU_GEN) 18
3.1.1.1 FAU_GEN.1/CS-Admin Audit Data Generation (Client-Server Admin Events) 18
3.1.1.2 FAU_GEN.1/CS-VVoIP Audit Data Generation (Client-Server VVoIP Events) 18
3.1.2 Protected Audit Event Storage (FAU_STG_EXT) 19
3.1.2.1 FAU_STG_EXT.1 Protected Audit Event Storage 19
4 Evaluation Activities for Selection-Based Requirements 21
4.1 Security Audit (FAU) 21
4.1.1 Security Audit Data Generation (FAU_GEN) 21
4.1.1.1 FAU_GEN.1/P2P-Admin Audit Data Generation (Peer-to-Peer Admin Events) 21
4.1.1.2 FAU_GEN.1/P2P-VVoIP Audit Data Generation (Peer-to-Peer VVoIP Events) 21
4.2 Cryptographic Support (FCS) 22
4.2.1 Cryptographic Operation (FCS_COP) 22
4.2.1.1 FCS_COP.1/SRTP Cryptographic Operation (Encryption/Decryption for SRTP) 22
4.2.2 Secure Real-Time Transport Protocol (FCS_SRTP_EXT) 23
4.2.2.1 FCS_SRTP_EXT.1 Secure Real-Time Transport Protocol 23
4.3 User Data Protection (FDP) 24
4.3.1 Information Flow Control Policy (FDP_IFC) 24
4.3.1.1 FDP_IFC.1/CallControl Subset Information Flow Control (for Call Control) 24
4.3.2 Simple security attributes (FDP_IFF) 24
4.3.2.1 FDP_IFF.1/CallControl Simple Security Attributes (for Call Control) 24
4.4 Protection of the TSF (FPT) 26
4.4.1 Time Stamps (FPT_STM_EXT) 26
5 Evaluation Activities for SARs 27
6 Required Supplementary Information 28
7 References 29

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the PP-Module for Voice/Video over IP (VVoIP) Endpoints is to describe the security functionality of VVoIP endpoints (whether hardware or software) in terms of [CC] and to define functional and assurance requirements for such products. The PP-Module is intended for use with the following Base-PPs:

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

The PP-Module is also conformant to the Functional Package for Transport Layer Security (TLS), Version 1.1 (TLS Package) when used in a PP-Configuration with the App PP.

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the following PP-Module:

- PP-Module for Voice/Video over IP (VVoIP) Endpoints, Version 1.0

Although Evaluation Activities (EAs) are defined mainly for the evaluators to follow, in general they will also help Developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in EAs may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy documentation).

1.2 Structure of the Document

EAs can be defined for both SFRs and Security Assurance Requirements (SAR). These are defined in separate sections of the SD.

If any EA cannot be successfully completed in an evaluation then the overall verdict for the evaluation is a 'fail'. In rare cases, there may be acceptable reasons why an EA may be modified or deemed not applicable for a particular TOE, but this must be agreed to by the Certification Body for the evaluation.

In general, if all EAs (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a 'pass'. To reach a 'fail' verdict when the EAs have been successfully completed would require a specific justification from the evaluator as to why the EAs were not sufficient for that TOE.

Similarly, at the more granular level of Assurance Components, if the EAs for an Assurance Component and all of its related SFR EAs successfully completed in an evaluation then it would be expected that the verdict for the Assurance Component is a 'pass'. To reach a 'fail' verdict for the Assurance Component when these EAs have been successfully completed would require a specific justification from the evaluator as to why the EAs were not sufficient for that TOE.

1.3 Terminology

1.3.1 Glossary

For definitions of standard CC terminology, see [CC] part 1.

Reference the terms sections of the PP-Module.

1.3.2 Acronyms

Reference the acronyms section of the PP-Module.

2 Evaluation Activities for SFRs

The EAs presented in this section are intended to supplement those defined in the NDcPP and App PP.

The PP-Module relies on several SFRs from the supported Base-PPs to help in the implementation of its required functionality. These SFRs are listed in this section along with any impact to how they are to be evaluated in a TOE that includes this PP-Module. This section also defines the EAs for the mandatory SFRs that are introduced in the PP-Module.

Successful completion of these EAs assists in the completion of the relevant portions of ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1, which are required to be applied to the entire TOE.

2.1 NDcPP Evaluation Activities

In addition to the EAs required by the Base-PP, the evaluator shall perform the following additional EAs to ensure that the Base-PP's security functionality is maintained by the addition of the PP-Module.

2.1.1 Security Audit (FAU)

2.1.1.1 Protected Audit Event Storage (FAU_STG_EXT)

FAU_STG_EXT.1 Protected Audit Event Storage

There is no change to the EAs specified for this SFR in the NDcPP Supporting Document.

2.1.2 Cryptographic Support (FCS)

2.1.2.1 NTP Protocol (FCS_NTP_EXT)

FCS_NTP_EXT.1 NTP Protocol

There is no change to the EAs specified for this SFR in the NDcPP Supporting Document, except to note that the evaluator shall use ESCs as NTP servers for all required test EAs.

2.1.2.2 TLS Client Protocol (FCS_TLSC_EXT)

FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

There is no change to the EAs specified for this SFR in the NDcPP Supporting Document.

FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

There is no change to the EAs specified for this SFR in the NDcPP Supporting Document.

2.1.3 Identification and Authentication (FIA)

2.1.3.1 Authentication Using X.509 Certificates (FIA_X509_EXT)

FIA_X509_EXT.1/Rev X.509 Certificate Validation

There is no change to the EAs specified for this SFR in the NDcPP Supporting Document.

FIA_X509_EXT.2 X.509 Certificate Authentication

There is no change to the EAs specified for this SFR in the NDcPP Supporting Document.

FIA_X509_EXT.3 X.509 Certificate Requests

There is no change to the EAs specified for this SFR in the NDcPP Supporting Document.

2.1.4 Protection of the TSF (FPT)

2.1.4.1 Trusted Update (FPT_TUD_EXT)

FPT_TUD_EXT.1 Trusted Update

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

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

2.1.5 Trusted Path/Channels (FTP)

2.1.5.1 Inter-TSF Trusted Channel (FTP_ITC)

FTP_ITC.1 Inter-TSF Trusted Channel

There is no change to the EAs specified for this SFR in the NDcPP Supporting Document.

2.1.6 Additional Requirements

The PP-Module does not define any additional requirements that apply solely when the NDcPP is the Base-PP for the TOE.

2.2 App PP Evaluation Activities

In addition to the EAs required by the Base-PP, the evaluator shall perform the following additional EAs to ensure that the Base-PP's security functionality is maintained by the addition of the PP-Module.

2.2.1 Protection of the TSF (FPT)

2.2.1.1 Trusted Update (FPT_TUD_EXT)

FPT_TUD_EXT.1 Trusted Update

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

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

2.2.2 Trusted Path/Channels (FTP)

2.2.2.1 Protection of Data in Transit (FTP_DIT_EXT)

FTP_DIT_EXT.1 Protection of Data in Transit

If "SRTP" is selected in FTP_DIT_EXT.1.1, reference the EAs for FCS_SRTP_EXT.1. Otherwise, there are no EAs for this component beyond what the App PP requires.

2.2.3 Additional Requirements

The PP-Module does not define any additional requirements that apply solely when the App PP is the Base-PP for the TOE.

2.3 TOE SFR Evaluation Activities

This section defines the EAs for the mandatory SFRs that are introduced in the PP-Module.

2.3.1 Communications (FCO)

2.3.1.1 Vocoder Usage (FCO_VOC_EXT)

FCO_VOC_EXT.1 Fixed-Rate Vocoder

TSS

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

Guidance

There are no guidance EAs for this component.

Test

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

The evaluator shall then perform the following test:

1. The evaluator shall ensure the TOE and the second VVoIP endpoint are registered to a call control server or are using P2P.
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 captured traffic to verify that a fixed rate vocoder is used.

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

2.3.2 User Data Protection (FDP)

2.3.2.1 Information Flow Control Policy (FDP_IFC)

FDP_IFC.1 Subset Information Flow Control

TSS

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

Guidance

There are no guidance EAs for this component.

Test

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

2.3.2.2 Information Flow Control Functions (FDP_IFF)

FDP_IFF.1 Simple Security Attributes

TSS

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

Guidance

There are no guidance EAs for this component.

Test

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

The evaluator shall then perform the following tests:

Test 1-ND (conditional – physical TOE):

1. The evaluator shall place the TOE into the on-hook state without registering it to the call control server or using P2P. The evaluator shall use the traffic capture tool to verify that the TOE does not transmit any streaming media traffic.
2. The evaluator shall place the TOE into the off-hook state and use the traffic capture tool to verify that the TOE does not transmit any streaming media traffic.

Test 1-App (conditional – software application TOE):

1. The evaluator shall execute the VVoIP application without registering it to the call control server or using P2P. The evaluator shall use the traffic capture tool to verify that the TOE does not transmit any streaming media traffic
2. The evaluator shall place the TOE into the off-hook state (e.g., by performing a call without specifying any destination data). The evaluator shall use the traffic capture tool to verify that the TOE does not transmit any streaming media traffic.

Test 2:

1. The evaluator shall ensure the TOE is using P2P or register the TOE with the call control server and verify that the TOE is registered by checking the call control server screen with current TOE connections and by viewing the call control path traffic using the traffic capture tool.
2. The evaluator shall place the TOE into the on-hook state and verify using the traffic capture tool that no streaming media traffic is transmitted by the TOE.
3. The evaluator shall place the TOE into the off-hook state. The evaluator shall then verify that the TOE continues to not transmit streaming media traffic.

Test 3:

1. The evaluator shall ensure the TOE is using P2P or shall register the TOE with the call control server and verify that it is registered by checking the call control server with current connections and using the traffic capture tool to verify the call control path traffic.
2. The evaluator shall ensure the TOE is using P2P or shall register the second VVoIP endpoint with the call control server and verify that it has been registered by checking the call control server with current connections and using the traffic capture tool to verify the call control path traffic.
3. The evaluator shall use the TOE to dial the second VVoIP endpoint and connect a call. The evaluator shall verify that the connection is made by having a voice/video conversation with the endpoint and using the traffic capture tool to verify that a steady stream of traffic is being transmitted between the two endpoints over the media channel.
4. The evaluator shall use the TOE to put the call on mute and verify that no traffic is transmitted from the TOE over the media channel to the second VVoIP endpoint. If the TOE is registered to a call control server, the evaluator shall also verify that a mute control message is sent to the call control server and it responds.
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 4:

1. The evaluator shall ensure the TOE is using P2P or register the TOE to the call control server and place it in the on-hook state.
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 5:

1. The evaluator shall ensure the TOE and the second VVoIP endpoint are registered to a call control server or are using P2P.
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 capture 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 6 (conditional – "The TOE is not in the hold state" is selected in FDP_IFF.1.2):

1. The evaluator shall use the TOE to put the call on hold and verify that no streaming media traffic is transmitted from the TOE over the media channel. If the TOE is registered to a call control server, the evaluator shall also verify that the VVoIP endpoint on-hold call control is sent to the call control server and it responds.
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.

2.3.3 Security Management (FMT)

2.3.3.1 Specification of Management Functions (FMT_SMF)

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

TSS

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

Guidance

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

Test

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

Test 1 (conditional – "register the TOE to an ESC [manually]" is selected):

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 (conditional – "register the TOE to an ESC [via DHCP server]" is selected):

1. On the TOE, input the DHCP server address.
2. Save configuration.
3. Verify by traffic capture 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.

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

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

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

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

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

2.3.4 TOE Access (FTA)

2.3.4.1 Session Locking and Termination (FTA_SSL)

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

TSS

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

Guidance

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

Test

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

The evaluator shall then perform the following tests:

Test 1:

1. Deploy the TOE in a default configuration (i.e. without any administrative override applied to the idle timeout value).
2. Ensure the TOE is using P2P or register the TOE with the call control server and verify that it is registered by viewing its status on the ESC and capturing the call control path traffic.
3. Ensure the second VVoIP endpoint is using P2P or register the second VVoIP endpoint with the call control server and verify that it is registered by viewing its status on the call control server and capturing the call control path traffic.
4. Use the TOE to dial the second VVoIP endpoint and establish a call. Verify the call was established by holding a conversation between the two peers and capturing the streaming media traffic that is transmitted between them.
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 (conditional – "an administrator-configurable interval" is selected in FTA_SSL.3.1/Media):

1. Deploy the TOE in a default configuration (i.e. without any administrative override applied to the idle timeout value).
2. Ensure the TOE is using P2P or register the TOE with the call control server and verify that it is registered by viewing its status on the call control server and capturing the call control path traffic.
3. Configure the TOE's idle timeout period for the shortest period of time that is supported.
4. Ensure the second VVoIP endpoint is using P2P or register the second VVoIP endpoint with the call control server and verify that it is registered by viewing its status on the call control server and capturing the call control path traffic.
5. Use the TOE to dial the second VVoIP endpoint and establish a call. Verify the call was established by holding a conversation between the two peers and capturing the streaming media traffic that is transmitted between them.

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 (conditional – "an administrator-configurable interval" is selected in FTA_SSL.3.1/Media):

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

2.3.5 Trusted Path/Channels (FTP)

2.3.5.1 Inter-TSF Trusted Channel (FTP_ITC)

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

TSS

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

Guidance

There are no guidance EAs for this component.

Test

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

The evaluator shall perform the following tests:

Test 1: The evaluators shall ensure that communications using each protocol with a call control server is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.

Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE.

Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.

Test 4: Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities.

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

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

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

Further EAs are associated with the specific protocols.

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

TSS

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

Guidance

There are no guidance EAs for this component.

Test

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

The evaluator shall perform the following tests:

Test 1: The evaluators shall ensure that communications using each protocol with another VVoIP endpoint is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.

Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE.

Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.

Test 4: Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities.

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

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

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

Further EAs are associated with the specific protocols.

3 Evaluation Activities for Optional Requirements

3.1 Security Audit (FAU)

3.1.1 Security Audit Data Generation (FAU_GEN)

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

TSS

There are no TSS EAs for this component.

Guidance

The evaluator shall make a determination of the administrative actions related to TSF data related to configuration changes. The evaluator shall examine the guidance documentation and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in MOD_VVOIP_V1.0. The evaluator shall document the methodology or approach taken to TSF data related to configuration changes. The evaluator may perform this activity as part of the activities associated with ensuring that the corresponding guidance documentation satisfies the requirements related to it.

Test

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

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

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

TSS

There are no TSS EAs for this component.

Guidance

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

Test

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

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

3.1.2 Protected Audit Event Storage (FAU_STG_EXT)

3.1.2.1 FAU_STG_EXT.1 Protected Audit Event Storage

TSS

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

The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; whether that data is stored by the TOE or through the TOE's invocation of a platform auditing mechanism; what happens when the local audit data store is full; and how these records are protected against unauthorized access.

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

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

Guidance

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

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

The evaluator shall also ensure that the guidance documentation describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. The description of possible configuration options and resulting behavior shall correspond to those described in the TSS.

Test

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

Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing. The evaluator shall verify that the TOE is capable of transferring audit data to an external audit server automatically without administrator intervention.

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

Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behavior defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that:

- The audit data remains unchanged with every new auditable event that should be tracked but that the audit data is recorded again after the local storage for audit data is cleared (for the option 'drop new audit data' in FAU_STG_EXT.1.3).
- The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option 'overwrite previous audit records' in FAU_STG_EXT.1.3).
- The TOE behaves as specified (for the option 'other action' in FAU_STG_EXT.1.3).

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

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

4 Evaluation Activities for Selection-Based Requirements

4.1 Security Audit (FAU)

4.1.1 Security Audit Data Generation (FAU_GEN)

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

TSS

There are no TSS EAs for this component.

Guidance

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

Test

For each administrative action identified in FAU_GEN.1.1/P2P-Admin, the evaluator shall perform an action either on the TOE or on the operational environment that causes the event to occur. The evaluator shall verify in each case that an auditable event was generated in a format consistent with the guidance documentation and that all audit record details specified in the SFR are present.

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

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

TSS

There are no TSS EAs for this component.

Guidance

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

Test

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

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

4.2 Cryptographic Support (FCS)

4.2.1 Cryptographic Operation (FCS_COP)

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

TSS

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

Guidance

There are no guidance EAs for this component.

Test
The evaluator shall perform the following tests:

AES-CTR Tests (Conditional – If "AES-CTR (as defined in NIST SP 800-38A)" is selected in FCS_COP.1.1/SRTP):

The Counter (CTR) mode is a confidentiality mode that features the application of the forward cipher to a set of input blocks, called counters, to produce a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa. Since the Counter Mode does not specify the counter that is used, it is not possible to implement an automated test for this mode. The generation and management of the counter is tested through FCS_SSH*_EXT.1.4. If CBC and/or GCM are selected in FCS_COP.1/DataEncryption, the test activities for those modes sufficiently demonstrate the correctness of the AES algorithm. If CTR is the only selection in FCS_COP.1/DataEncryption, the AES-CBC Known Answer Test, AESGCM Known Answer Test, or the following test shall be performed (all of these tests demonstrate the correctness of the AES algorithm):

AES-CTR Known Answer Tests

There are four Known Answer Tests (KATs) described below to test a basic AES encryption operation (AES-ECB mode). For all KATs, the plaintext, IV, and ciphertext values shall be 128-bit blocks. The results from each test may either be obtained by the validator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

KAT-1 To test the encrypt functionality, the evaluator shall supply a set of 5 plaintext values for each selected keysize and obtain the ciphertext value that results from encryption of the given plaintext using a key value of all zeros.

KAT-2 To test the encrypt functionality, the evaluator shall supply a set of 5 key values for each selected keysize and obtain the ciphertext value that results from encryption of an all zeros plaintext using the given key value

KAT-3 To test the encrypt functionality, the evaluator shall supply a set of key values for each selected keysize as described below and obtain the ciphertext values that result from AES encryption of an all zeros plaintext using the given key values. A set of 128 128-bit keys, a set of 192 192-bit keys, and/or a set of 256 256-bit keys. Key_i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1, N].

KAT-4 To test the encrypt functionality, the evaluator shall supply the set of 128 plaintext values described below and obtain the ciphertext values that result from encryption of the given plaintext using each selected keysize with a key value of all zeros (e.g. 256 ciphertext values will be generated if 128 bits and 256 bits are selected and 384 ciphertext values will be generated if all keysizes are selected). Plaintext value i in each set shall have the leftmost bits be ones and the rightmost 128-i bits be zeros, for i in [1, 128].

AES-CTR Multi-Block Message Test

The evaluator shall test the encrypt functionality by encrypting an i-block message where 1 less-than i less-than-or-equal to 10 (test shall be performed using AES-ECB mode). For each i the evaluator shall choose a key and plaintext message of length i blocks and encrypt the message, using the mode to be tested, with the chosen key. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key using a known good implementation. The evaluator shall perform this test using each selected keysize.

AES-CTR Monte Carlo Test

The evaluator shall test the encrypt functionality using 100 plaintext/key pairs. The plaintext values shall be 128-bit blocks. For each pair, 1000 iterations shall be run as follows:

```
# Input: PT, Key
for I = 1 to 1000:
CT[i] = AES-ECB-Encrypt(Key, PT) PT = CT[i]
```

The ciphertext computed in the 1000th iteration is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation. The evaluator shall perform this test using each selected keysize.

There is no need to test the decryption engine.

AES-GCM Tests (Conditional – If "AES-GCM (as defined in NIST SP 800-38D)" is selected in FCS_COP.1.1/SRTP):

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

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

4.2.2 Secure Real-Time Transport Protocol (FCS_SRTP_EXT)

4.2.2.1 FCS_SRTP_EXT.1 Secure Real-Time Transport Protocol

TSS

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

Guidance

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

Test

The evaluator shall follow the procedure for initializing their device so that they are ready to receive and place calls. For each cipher suite selected in FCS_SRTP_EXT.1.2, the evaluator shall configure the SIP server to only allow that cipher suite to be used. The evaluator shall then both place and receive a call and determine that the traffic sent and received by the TOE is encrypted using SRTP with that cipher suite. The evaluator may choose one of the below two options to ensure that the call is being encrypted and to view the cipher suite being used.

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

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

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

4.3 User Data Protection (FDP)

4.3.1 Information Flow Control Policy (FDP_IFC)

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

TSS

There are no TSS EAs for this component.

Guidance

There are no guidance EAs for this component.

Test

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

4.3.2 Simple security attributes (FDP_IFF)

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

TSS

The evaluator shall examine the TSS to verify that it describes the call control protocol(s) used by the TOE and any explicit circumstances under which the TSF will and will not transmit call control data as defined in FDP_IFF.1.4/CallControl and FDP_IFF.1.5/CallControl. The TSF should only transmit call control data using the protocol(s) and method(s) of endpoint identification as indicated in FDP_IFC.1/CallControl or if defined any explicit allow/deny rules in FDP_IFF.1.4/CallControl and FDP_IFF.1.5/CallControl.

Guidance

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

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

Test 1 (Conditional – If "SIP" is selected in FDP_IFF.1.1/CallControl):

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

Test 2 (Conditional – If "H.323" is selected in FDP_IFF.1.1/CallControl):

1. Ensure the TOE is configured to use P2P and act as a call control server using the H.323 protocol.
2. Use a traffic capture tool to capture call-signaling packets traversing the TOE.
3. Place a call to the TOE from another VVoIP endpoint using the H.323 call control protocol to the TOE and observe via packet capture that the TSF established a connection between itself and the peer.
4. Repeat step 3 with a call placed from the TOE to the other VVoIP endpoint.
5. (Conditional – if the ST claims any additional rules in FDP_IFF.1.4/CallControl) Implement any rules assigned in FDP_IFF.1.4/CallControl and verify that the specified authorized information flows occur.

6. (Conditional – if the ST claims any additional rules in FDP_IFF.1.5/CallControl) Implement any rules assigned in FDP_IFF.1.5/CallControl and verify that the specified information flows do not occur.

7. Repeat steps 1-6 for each method of endpoint identification.

4.4 Protection of the TSF (FPT)

4.4.1 Time Stamps (FPT_STM_EXT)

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

TSS

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

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

Guidance

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

Test

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

5 Evaluation Activities for SARs

To evaluate the SARs specified by the Base-PP and this PP-Module, the evaluator shall perform the SAR EAs defined in Base-PP against the entire TOE as applicable.

6 Required Supplementary Information

This document has no required supplementary information beyond the ST, operational guidance, and testing.

7 References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020
[NDcPP SD]	Evaluation Activities for Network Device cPP Version 2.2, December 2019
[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
[VVoIP Module]	PP-Module for Voice/Video over IP (VVoIP) Endpoints, Version 1.0, October 28, 2020