PP-Module for Audio Input Devices

Version: 1.0

2019-07-19

National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2019-07-19	Initial draft

Table of Contents

1 Introduction

1.1 Overview

The scope of this PP-Module is to describe the security functionality of a specific type of Peripheral Sharing Device (PSD) product in terms of [CC] and to define functional and assurance requirements for such products. A TOE that claims compliance to this PP-Module must claim conformance to a PP-Configuration containing this PP-Module and the Protection Profile for Peripheral Sharing Device (PSD PP). This is because the PSD PP is a generic Protection Profile aimed at defining baseline requirements and assurance activities for a wide variety of PSD products but more specific requirements and assurance activities apply depending on the types of physical and logical interfaces provided by a PSD. Therefore, additional Security Functional Requirements (SFR) have been defined in this PP-Module to define security functionality that is unique to a PSD that provides the ability to support peripheral audio input devices.

1.2 Terms

Term	Definition
Analog Audio	Data stream that uses voltage to describe a sound wave.
Analog Audio Input Computer Interface, or Computer Interface	The connector on a PSD through which analog audio data exits the PSD bound for a connected computer.
Analog Audio Input Peripheral Interface, or Peripheral Interface	The connector on a PSD through which analog audio data enters the PSD from a microphone or other analog audio device.
Analog Microphone	Computer audio peripheral device that converts sound waves into analog data stream
Audio Input Peripheral Device	Microphone, headset microphone.
Digital audio	Data stream that uses digital values to describe sound waves.
Extended Audio Frequency Range	The range from 1Hz to 60 kHz.
Microphone Bias	Microphone peripheral interface line that provides power to supply the microphone built-in preamplifier.

1.3 Compliant Targets of Evaluation

A compliant Target of Evaluation (TOE) for this PP-Module is any PSD that supports **analog audio input peripheral devices**. All of the requirements and restrictions that are defined in the PSD PP apply to a conformant TOE. A conformant TOE satisfies all of the specific data protection/isolation capabilities that are required by the PSD PP. A conformant TOE embodies one or more of the use cases defined in the PSD PP.

In general, computer audio may be routed in various ways:

- Analog audio signals
- Digital audio embedded in the video stream or independent digital audio (e.g., Sony/Philips Digital Interface Format, or S/PDIF)
- USB digital audio

Analog audio input requires special attention during TOE design as it may introduce analog leakage concerns. To be compliant with this PP, **only** analog audio input data may transit the TOE. The PSD may not support other kinds of data, including keyboard, mouse, analog audio output, and video. The TOE must be a dedicated analog audio input device.

A TOE with an analog audio input function shall enforce unidirectional flow of analog signals from the TOE peripheral device analog audio input interface to the TOE connected computer analog audio output interface.

Digital audio embedded in a video stream or passed through separate lines is not addressed in this PP-Module. The capability for such audio is addressed in the PP-Module for Video/Display Devices.

USB digital audio input devices are not authorized for use with TOEs conformant to this Module.

1.3.1 TOE Boundary

The TOE boundary is the same as for a PSD in general. Refer to the PSD PP for an outline of the TOE boundary. Note that a TOE that claims compliance to this PP-Module must specifically include support for analog audio input peripherals. A TOE that claims compliance to this PP-Module may not claim compliance with other PSD PP-Modules.

1.4 Use Cases

No additional use cases are defined for this PP-Module. The TOE is expected to embody one or more use cases as defined by the PSD PP. The functionality defined by this PP-Module is implementation-independent (i.e. not tied to any specific use cases) and is related entirely to the specific security requirements related to security of the physical and logical interfaces for analog audio input devices.

2 Conformance Claims

This PP-Module inherits exact conformance as required from the specified Base-PP and as defined in the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017). This PP-Module is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Revision 5 [CC].

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

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

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

- Protection Profile for Peripheral Sharing Device, Version 4.0

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 a PP-Module of the PSD PP, all threats, assumptions, and Organizational Security Policies (OSPs) defined in the PSD PP will also apply to the TOE unless otherwise specified.

3.1 Threats

This PP-Module defines no additional threats beyond those defined in the PSD PP.

The SFRs defined in this PP-Module are intended to mitigate the T.DATA_LEAK and T.SIGNAL_LEAK threats defined in the PSD PP. Specifically, this PP-Module must ensure that analog audio input data intended for one connected computer cannot leak to another connected computer. This also requires that any data from one connected computer cannot reach another connected computer by way of the PSD.

3.2 Assumptions

This PP-Module defines no additional assumptions beyond those defined in the PSD PP.

3.3 Organizational Security Policies

This PP-Module defines no OSPs.

4 Security Objectives

4.1 Security Objectives for the TOE

Because this PP-Module does not define any additional threats or organizational security policies beyond what is defined by the PSD PP, there are no additional security objectives for the TOE to satisfy.

A TOE that conforms to this PP-Module must address O.COMPUTER_INTERFACE_ISOLATION, O.COMPUTER_INTERFACE_ISOLATION_UNPOWERED, and O.USER_DATA_ISOLATION specifically for analog audio input peripherals.

In addition to the SFRs in the PSD PP, these objectives are addressed by the refined FDP_APC_EXT.1 and FDP_PDC_EXT.1, and FDP_PDC_EXT.2/AI and FDP_UDF_EXT.1/AI as defined in this PP-Module.

4.2 Security Objectives for the Operational Environment

Because this PP-Module does not define any additional assumptions or organizational security policies beyond what is defined by the PSD PP, there are no additional security objectives for the Operational Environment to satisfy.

4.3 Security Objectives Rationale

Because this PP-Module does not define any additional security objectives, there is no additional rationale beyond what is provided by the PSD PP.

5 Security Requirements

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

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

- **Refinement** operation (denoted by **bold text** for insertions and ~~strikethrough text~~ for deletions) is used to add details to a requirement in a way that further restricts a requirement.
- **Selection** operation (denoted by *italicized text*) is used where an SFR component contains an element where a choice from several items has to be made by the ST author.
- **Assignment** operation (denoted by *italicized text*) is used where an SFR component contains an element with a value that must be chosen by the ST author but does not provide a pre-determined list of acceptable values as with a selection.
- **Iteration** operation, denoted by a slash followed by a unique text string (e.g. "/AI"), is used to create copies of an SFR so that similar functionality can be applied to different parts of the TSF in different ways.
- **Extended SFRs** are identified by having a label "EXT" after the SFR name.

5.1 PSD PP Security Functional Requirements Direction

When a TOE claims compliance to this PP-Module, it is necessary to make claims in the PSD PP requirements that are consistent with the functionality provided by the PP-Module. The following sections describe any PSD PP claims that must be made when the TOE boundary includes the functionality described by this PP-Module. Note that for some requirements, only certain individual elements within the SFR have been modified for this PP-Module. Any SFR elements that were omitted from the selections below are to be included in a conformant ST unmodified from their definition in the PSD PP.

5.1.1 Applicable Unmodified SFRs

The SFRs listed in this section are defined in the PSD PP and relevant to the secure operation of the TOE. The ST author may complete all selections and assignments in these SFRs without any additional restrictions.

- FDP_RIP_EXT.1
- FDP_SWI_EXT.1
- FPT_FLS_EXT.1
- FPT_NTA_EXT.1
- FPT_PHP.1
- FPT_TST.1
- FPT_TST_EXT.1

5.1.2 Applicable Modified SFRs

The SFRs listed in this section are defined in the PSD PP and relevant to the secure operation of the PSD. When the TOE boundary includes this PP-Module, the modifications listed below will be made to the PSD PP SFRs so that they are thoroughly applicable to this particular technology type.

FDP_APC_EXT.1 Active PSD Connections

FDP_APC_EXT.1.1 The TSF shall route user data only to ~~or from~~ the interfaces selected by the user.

FDP_APC_EXT.1.2 The TSF shall ensure that no data **or electrical signals** flows between connected computers whether the TOE is powered on or powered off.

Application Note *This SFR is refined from the PSD PP for this PP-Module to include further restrictions for electrical signals. It is very unlikely that this element can be satisfied unless all unselected computer interfaces are shorted to ground by the TSF.*

If computer interface supports right and left audio, or audio and microphone bias, then all those supported signals should comply with the above SFRs.

FDP_PDC_EXT.1 Peripheral Device Connection

There is no modification to this SFR in this PP-Module. However, there are additions to the supported peripheral device connections (see Appendix E) that are associated with this SFR.

5.2 TOE Security Functional Requirements

The SFRs included in this section are those that the TOE Security Functionality (TSF) is expected to satisfy.

5.2.1 User Data Protection (FDP)

FDP_PDC_EXT.2/AI Authorized Devices (Analog Audio Input)

FDP_PDC_EXT.2.1/AI The TSF shall allow connections with authorized devices as defined in [*Appendix E*] and [*no other devices*] on power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.2.2/AI The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*Appendix E*] and [*no other devices*] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

Application Note: *A TOE that claims conformance to this PP-Module is not permitted to conform to any other PP-Modules that extend the PSD PP. Therefore, no other devices or protocols will be supported beyond those that are defined in this PP-Module.*

FDP_UDF_EXT.1/AI Unidirectional Data Flow (Analog Audio Input)

FDP_UDF_EXT.1.1/AI The TSF shall ensure that [*analog audio input data*] transits the TOE unidirectionally from the [*TOE analog audio input peripheral interface*] to the [*TOE analog audio input computer interface*].

Application Note*:* *This SFR applies to all types of analog audio input data (e.g., if the computer interface supports left and right audio, or audio and microphone bias).*

For audio signals, the TOE analog audio input peripheral interface is considered to be unidirectional if it receives no signal greater than 45 decibels (dB) of attenuation at the extended audio frequency range.

5.3 TOE Security Assurance Requirements

The PSD PP lists the SARs from Part 3 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5. As a PP-Module of the PSD PP, this PP-Module does not prescribe any SARs beyond those defined in the PSD PP. The evaluator shall ensure that the SARs defined in the PSD PP are assessed against the entire TSF as appropriate.

6 Consistency Rationale

6.1 PSD Base

6.1.1 Consistency of TOE Type

The PSD PP defines the boundaries of a PSD—a device that provides a mechanism for securely connecting a set of peripherals to one or more attached computers. This PP-Module builds on this by defining functional capabilities that are specific to audio input devices. One of the functions of the device must be the ability for it to act as an audio input device. The requirements of this PP do not prevent a conformant TOE from implementing mandatory requirements of the PSD PP.

6.1.2 Consistency of Security Problem Definition

This PP-Module does not define any additional threats beyond those defined in the PSD PP. Therefore, there is no inconsistency between the threats defined in the PSD PP and this PP-Module.

6.1.3 Consistency of Objectives

The PSD PP does not define any TOE objectives; therefore, there is no inconsistency between it and this PP-Module. The requirements defined in this PP-Module are intended to satisfy objectives already defined in the PSD PP in a more specific manner.

6.1.4 Consistency of Requirements

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

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FDP_APC_EXT.1	This refined SFR accounts for analog and electrical signals which are not listed in the PSD PP.
FDP_PDC_EXT.1	This SFR is not modified, but it references Appendix E which is modified in this PP-Module to apply to audio input devices which are not listed in the PSD PP.
Mandatory SFRs	
FDP_PDC_EXT.2/AI	This SFR defines the devices that are authorized by this PP-Module. This is dependent on the other PP-Modules that are claimed in the TOE's ST. The Base-PP is written specifically not to discuss the supported device types, instead leaving it to the various PP-Modules to define what they support.
FDP_UDF_EXT.1/AI	This SFR applies to unidirectional audio communications which are not listed in the PSD PP.
Optional SFRs	
N/A	N/A

PP-Module Requirement	Consistency Rationale
Selection-Based SFRs	
N/A	N/A

A Optional Requirements

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

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

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

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

A.1 Strictly Optional Requirements

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

A.2 Objective Requirements

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

A.3 Implementation-Dependent Requirements

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

B Selection-Based Requirements

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

Currently, no selection-based requirements specific to this product type have been identified.

C Extended Components Definition

This appendix provides a definition for all of the extended components introduced in this PP-Module. The families to which these components belong are identified in the following table:

Functional Class	Functional Families
User Data Protection (FDP)	FDP_PDC_EXT Peripheral Device Connection
	FDP_UDF_EXT Unidirectional Data Flow

C.1 FDP_PDC_EXT Peripheral Device Connection

This family is defined in the PSD PP. This PP-Module augments the extended family by adding one additional component, FDP_PDC_EXT.2. This new component and its impact on the extended family's component leveling are shown below; reference the PSD PP for all other definitions for this family.

Component Leveling

FDP_PDC_EXT.2 Authorized Devices, defines the types of physical devices that the TSF will permit to connect to it.

Management: FDP_PDC_EXT.2

No specific management functions are identified.

Audit: FDP_PDC_EXT.2

There are no specific auditable events foreseen.

FDP_PDC_EXT.2 Authorized Devices

Hierarchical to: No other components

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

FDP_PDC_EXT.2.1 The TSF shall allow connections with authorized devices as defined in [*assignment: devices specified in the PP or PP-Module in which this SFR is defined*] and [*assignment: devices specified in another PP or PP-Module that shares a PP-Configuration with the PP or PP-Module in which this SFR is defined*] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

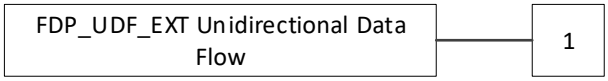
FDP_PDC_EXT.2.2 The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*assignment: devices specified in the PP or PP-Module in which this SFR is defined*] and [*assignment: devices specified in another PP or PP-Module that shares a PP-Configuration with the PP or PP-Module in which this SFR is defined*] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

C.2 FDP_UDF_EXT Unidirectional Data Flow

Family Behavior

Components in this family define unidirectional transmission of user data.

Component Leveling



FDP_UDF_EXT.1 Unidirectional Data Flow, requires the TSF to provide unidirectional (one-way) communications between a given pair of interface types.

Management: FDP_UDF_EXT.1

No specific management functions are identified.

Audit: FDP_UDF_EXT.1

There are no auditable events foreseen.

FDP_UDF_EXT.1 Unidirectional Data Flow

Hierarchical to: No other components

Dependencies: FDP_APC_EXT.1 Active PSD Connections

FDP_UDF_EXT.1.1 The TSF shall ensure [*assignment: type of data*] data transits the TOE unidirectionally from the [*assignment: origin point of* data] interface to the [*assignment: destination point of* data] interface.

D Isolation Documentation and Assessment

The TOE does not require any additional supplementary information to describe its isolation concepts beyond the requirements outlined in the 'Isolation Documentation and Assessment' sections in Appendix D of the PSD PP. As with other PSD PP requirements, the only additional requirement is that the isolation documentation also applies to the specific isolation and data flow SFRs in this PP-module in addition to the functionality required by the PSD PP.

E Peripheral Device Connections

E.1 General

This appendix expands the PSD PP Peripheral Device Connections appendix, and offers additional direction on peripheral devices and interface protocols with TOEs claiming compliance with this PP-Module. This appendix is in conjunction with the PSD PP's appendix and does not replace it.

E.2 Unauthorized Peripheral Devices

The following are unauthorized devices and device classes:

- Digital microphone
- Keyboard
- Mouse
- Any device not specifically authorized

E.3 Unauthorized Interface Protocols

The following are unauthorized interface protocols:

- Digital audio
- Digital video
- USB
- Any other protocol not specifically authorized

E.4 Authorized Peripheral Devices

The following are authorized devices and functions:

- Analog microphone

E.5 Authorized Interface Protocols

The following are authorized interface protocols:

- Analog audio input

F Interactions between PP-Modules

This appendix is not applicable to this PP-Module because there are no PP-Configurations that permit its use with other PP-Modules.

G References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2072-04-001, 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
[PP_PSD_V4.0 or PSD PP]	Protection Profile for Peripheral Sharing Device, Version: 4.0, 2019-07-19

H Acronyms

Acronym	Meaning
dB	Decibel
S/PDIF	Sony/Philips Digital Interface Format
PSD	Peripheral Sharing Device