PP-Module for Analog Audio Output 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 Protection Profile (PP)-Module is to describe the security functionality of a specific type of Peripheral Sharing Device (PSD) product in terms of Common Criteria for Information Technology Security Evaluation, version 3.1, Release 5 [CC] and to define functional and assurance requirements for such products.

A Target of Evaluation (TOE) claiming conformance to this PP-Module must also claim conformance to the Peripheral Sharing Device Protection Profile (PSD PP) as its Base-PP. This is because the PSD PP is a generic Protection Profile aimed at defining baseline requirements and Evaluation Activities for a wide variety of PSD products, but more specific requirements and Evaluation Activities apply depending on the types of physical and logical interfaces a PSD includes. Therefore, this PP-Module defines additional Security Functional Requirements (SFRs) for security functionality unique to a PSD that supports peripheral audio output devices.

1.2 Terms

Term	Definition
Attenuation	A reduction in signal strength commonly occurring while transmitting analog or digital signals over long distances.
Analog Audio	Data stream that uses voltage to describe a continuous sound wave.
Analog Audio Output Computer Interface, or Computer Interface	The Connector on a PSD through which analog audio data enters the PSD from a Connected Computer.
Analog Audio Output Peripheral Interface, or Peripheral Interface	The Connector on a PSD through which analog audio data exits the PSD bound for a peripheral device.
Audio Output Peripheral Device	Speakers, handset, and earphones.
Audio codec	PC subsystem capable of encoding and decoding a digital data stream of audio.
Digital Audio	Data stream that uses digital values to describe a sound wave in sampled intervals.
Extended Audio Frequency Range	The range from 1Hz to 60 kHz.
Headphones	Computer audio peripheral device with one or more small speakers.
USB Audio codec	Computer audio peripheral device with USB digital input/output, one or more analog audio outputs and one or more analog audio inputs.

1.3 Compliant Targets of Evaluation

A compliant Target of Evaluation (TOE) for this PP-Module is any PSD that supports connectivity between one or more computers and one or more **analog audio output 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. It may also provide PSD functionality for additional types of computer interfaces (e.g., display, keyboard/mouse, user authentication device). In such a case, the TOE must claim conformance to all applicable PP-Modules to 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 audio peripheral devices

Analog audio output requires special attention during TOE design as it may introduce analog leakage concerns. There is an additional concern an attacker may be able to use an audio output device as a low-gain microphone for eavesdropping on the surrounding area or bridging an air-gap to nearby computers. Analog audio output presents few security problems with respect to switching, since the person listening to the audio must be authorized to hear the output of all the connected computers. And in some operational environments, it is required that the user be able to hear more than one channel at a time.

Digital audio embedded in a video stream or passed through separate lines is not a security concern for this PP-Module since it does not introduce analog signal leakage vulnerabilities. The capability for digital video is addressed in the PP-Module for Video/Display Devices.

USB audio devices (i.e., codecs) are not authorized for use with the TOE. USB audio codecs have configuration memory that may be exploited to enable unauthorized data flows.

1.3.1 TOE Boundary

The TOE boundary is the same as for a Peripheral Sharing Device in general. Refer to the PSD PP for an outline of the TOE boundary. Note that a TOE that claims conformance to this PP-Module must specifically include support for analog audio output peripherals. A TOE that claims conformance to this PP-Module is not prevented from claiming conformance to other PSD PP-Modules. All relevant PP-Modules must be claimed by the TOE based on the specific types of peripheral device functionality provided.

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 output 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:

- Protection Profile for Peripheral Sharing Device, Version 4.0
- PP-Module for User Authentication Devices, Version 1.0
- PP-Module for Keyboard/Mouse Devices, Version 1.0
- PP-Module for Video/Display Devices, Version 1.0

3 Security Problem Description

This PP-Module describes the security problem in terms of the threats the TOE is expected to address, assumptions about its operational environment, and any organizational security policies (OSPs) that the TOE is expected to enforce.

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

3.1 Threats

The following are the threats that exist for TOEs that conform to this PP-Module.

T.MICROPHONE_USE

A malicious agent could use an unauthorized peripheral device such as a microphone, connected to the TOE audio out peripheral device interface to eavesdrop or transfer data across an air-gap through audio signaling.

T.AUDIO_REVERSED

A malicious agent could repurpose an authorized audio output peripheral device by converting it to a low-gain microphone to eavesdrop on the surrounding audio or transfer data across an air-gap through audio signaling.

In addition to these threats, the SFRs defined in this PP-Module are intended to mitigate the **T.DATA_LEAK** and **T.SIGNAL_LEAK** threats that are defined in the PSD PP. This is because audio signal leakage is a specific type of signal leak that is applicable only when a TOE claims conformance to this PP-Module.

3.2 Assumptions

This PP-Module defines the following additional assumption beyond those defined in the PSD PP.

A.NO_MICROPHONES

Users are trained not to connect a microphone to the TOE audio output interface.

Note that this assumption is necessary despite the fact that the TSF enforces unidirectional data flow (see O.UNIDIRECTIONAL_AUDIO_OUT) below because the signals are analog and not digital. Because of this, it is not possible to make the pathway truly unidirectional; instead, the TSF can only diminish the strength of audio signals such that usable data cannot be transmitted. The assumption that microphones are prohibited is used to enforce a defense-in-depth strategy for mitigating the threat of audio reversal.

3.3 Organizational Security Policies

This PP-Module defines no OSPs.

4 Security Objectives

4.1 Security Objectives for the TOE

A TOE conforming to this PP-Module must address the O.COMPUTER_INTERFACE_ISOLATION, O.COMPUTER_INTERFACE_ISOLATION_UNPOWERED, O.USER_DATA_ISOLATION, O.PERIPHERAL_PORTS_ISOLATION, and O.REJECT_UNAUTHORIZED_PERIPHERAL objectives from the PSD PP specifically for audio output peripherals. In addition to the SFRs mapped in the PSD PP, the following SFRs defined in this PP-Module or modified from their PSD PP definition contribute to supporting these objectives for audio output devices:

- FDP_APC_EXT.1 (modified from PSD PP definition), FDP_PDC_EXT.1 (modified from PSD PP definition), FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1

The following security objectives are defined by this PP-Module for a TOE that claims conformance to this PP-Module.

O.UNIDIRECTIONAL_AUDIO_OUT

The PSD shall enforce the unidirectional flow of audio data from the analog audio computer interface to the analog audio peripheral interface.

Addressed by: FDP_APC_EXT.1 (modified from PSD PP definition), FDP_AFL_EXT.1, FDP_UDF_EXT.1/AO

O.COMPUTER_TO_AUDIO_ISOLATION

The PSD shall isolate the analog audio output function from all other TOE functions.

Addressed by: FDP_APC_EXT.1 (modified from PSD PP definition), FDP_UDF_EXT.1/AO

4.2 Security Objectives for the Operational Environment

OE.NO_MICROPHONES

The operational environment is expected to ensure that microphones are not plugged into the TOE audio output interfaces.

4.3 Security Objectives Rationale

This section describes how the assumptions and threats map to the security objectives. All mappings and rationale are included in the table below:

Threat or Assumption	Security Objective(s)	Rationale
A.NO_MICROPHONES	OE.NO_MICROPHONES	The assumption is upheld by the objective since the users in the environment are trained not to connect a microphone to the TOE audio output interface,
T.MICROPHONE_USE	O.UNIDIRECTIONAL_AUDIO_OUT	O.UNIDIRECTIONAL_AUDIO_OUT mitigates this threat by attenuating the strength of any inbound transmission of audio data through the TOE from a connected peripheral. If the TOE design ensures that analog audio reverse signal attenuation is below the noise floor

Threat or Assumption	Security Objective(s)	Rationale
		level then any audio signal should not have sufficient strength to be usable.
T.AUDIO_REVERSED	O.UNIDIRECTIONAL_AUDIO_OUT	O.UNIDIRECTIONAL_AUDIO_OUT mitigates this threat by ensuring that the TOE's audio peripheral interface(s) are exclusively used to output audio.
T.SIGNAL_LEAK	O.UNIDIRECTIONAL_AUDIO_OUT	O.UNIDIRECTIONAL_AUDIO_OUT mitigates this threat by preventing the exploitation of the analog audio output to receive signaled data from a connected computer. Analog audio output in standard computers may be exploited to become audio input in some audio codecs. Audio devices such as headphones may also be used as low -gain dynamic microphones. If the TOE design assures that analog audio reverse signal attenuation is below the noise floor level then the audio signal may not be recovered from the resultant audio stream. This prevents potential misuse of headphones connected to the TOE for audio eavesdropping.
	O.COMPUTER_TO_AUDIO_ISOLATION	O.COMPUTER_TO_AUDIO_ISOLATION mitigates this threat by ensuring that analog audio output converted to input by a malicious driver cannot pick up signals from other computer interfaces. A TOE design that ensures that audio signals are not leaked to any other TOE interface can effectively prevent a potential signaling leakage across the TOE through analog audio.

Table 1: Security Objectives Rationale

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 as assignments, selections, assignments within selections, and refinements. This document uses the following conventions to identify the operations the CC defines:

- **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 number inside parentheses following the component or element name (e.g. "(1)") and/or a slash followed by a unique text string (e.g. "/VI"), 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** flow 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 on how data may be routed in regards to interfaces selected by the user.*

This SFR is refined from the PSD PP for this PP-Module to include further restrictions for electrical signals. Electrical signals are considered not to flow between connected computers and data is considered not to transit the TOE if no signal greater than 45dB of attenuation at the extended audio frequency range is received. It is very unlikely that this element can be satisfied unless all unselected computer interfaces are shorted to ground by the TSF.

Note that the above port-to-port attenuation pass criterion is calculated based on the following: 45 dBv = 177.82 signal to voltage ratio. When the signal inserted on one TOE computer interface audio input is 2.00 V peak-to-peak sine wave, the maximum allowed output signal voltage measured at another TOE computer interface is therefore 11.2mV (or well below noise level). Negative swing is measured when the generated audio signal average voltage is 0V.

If the peripheral interface supports multiple signals (such as right and left audio, or audio bias), then all those supported signals should comply with the above SFRs.

If the TOE claims conformance to multiple PP-Modules, each PP-Module modifies this SFR in a different manner for the interfaces that are unique to that module. In this case, the ST author should reference this modification of the SFR as "FDP_APC_EXT.1/AO" for uniqueness. Note that all elements of FDP_APC_EXT.1 must be included in this iteration, not just the ones that are modified by this PP-Module.

FDP_PDC_EXT.1 Peripheral Device Connection

There is no modification to this SFR in this PP-Module. However, there are additions to the Peripheral Device Connections (see Appendix E) associated with this SFR and additional Evaluation Activities.

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_AFL_EXT.1 Audio Filtration

FDP_AFL_EXT.1.1 The TSF shall ensure outgoing audio signals are filtered as per [*Audio Filtration Specifications table*].

Frequency (kHz)	Minimum Attenuation (dB)	Maximum Voltage After Attenuation
14	23.9	127.65 mV
15	26.4	95.73 mV
16	30.8	57.68 mV
17	35.0	35.57 mV
18	38.8	22.96 mV
19	43.0	14.15 mV
20	46.0	10.02 mV
30	71.4	5.3 mV
40	71.4	5.3 mV
50	71.4	5.3 mV
60	71.4	5.3 mV

Table 2: Audio Filtration Specifications

Application note: *The above security requirement is designed to reduce the likelihood that speakers emitting a signaling event at frequencies outside the range of human hearing could be successfully used to bridge an air-gap to another computer.*

FDP_PDC_EXT.2/AO Peripheral Device Connection (Audio Output)

FDP_PDC_EXT.2.1/AO The TSF shall allow connections with authorized devices as defined in [*Appendix E*] and [***selection:***

- ***authorized devices and functions as defined in the PP-Module for Keyboard/Mouse Devices,***
- ***authorized devices as defined in the PP-Module for User Authentication Devices,***
- ***authorized devices as defined in the PP-Module for Video/Display Devices,***
- ***no other device***

] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.2.2/AO The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*Appendix E*] and [***selection:***

- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for Keyboard/Mouse Devices,***
- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for User Authentication Devices,***
- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for Video/Display Devices,***
- ***no other devices***

] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

Application Note: *The TSF must claim conformance to a PP-Configuration that includes each PP-Module contained in any selections. The ST author should select all devices and interfaces supported by the TOE.*

FDP_PUD_EXT.1 Powering Unauthorized Devices

FDP_PUD_EXT.1.1 The TSF shall not provide power to any unauthorized device connected to the analog audio peripheral interface.

FDP_UDF_EXT.1/AO Unidirectional Data Flow (Audio Output)

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

Application Note*:* *For audio signals, the TOE analog audio output computer interface is considered to be unidirectional if it receives no signal greater than 45 dB of attenuation at the extended audio frequency range. It is very unlikely that this element can be satisfied unless all unselected computer interfaces are shorted to ground by the TSF.*

If the peripheral interface supports multiple signals (such as right and left audio, or audio bias), then all those supported signals should comply with the above SFR.

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 Base-PP. The evaluator shall ensure that the SARs defined in the claimed base 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 devices that can share audio output peripherals. 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 defines threats that supplement those in the PSD PP as follows:

PP-Module Threat	Consistency Rationale
T.MICROPHONE_USE	The PSD PP does not identify any threats specific to analog audio output peripheral devices. This threat is specific to analog audio output devices and therefore is an additional threat to this module supplementing those in PSD PP.
T.AUDIO_REVERSED	The PSD PP does not identify any threats specific to analog audio output peripheral devices. This threat is specific to analog audio output devices and therefore is an additional threat to this module supplementing those in PSD PP.

6.1.3 Consistency of Objectives

This PP-Module defines TOE objectives that supplement those the PSD PP defines as follows:

PP-Module Objective	Consistency Rationale
O.UNIDIRECTIONAL_AUDIO_OUT	The PSD PP does not mandate bidirectional data flows for any interfaces so enforcement of unidirectional data flow does not prevent any PSD PP objectives from being satisfied.
O.COMPUTER_TO_AUDIO_ISOLATION	The PSD PP does not specify how peripheral devices interface logically with connected computers so there is no PSD PP function that is affected by isolating the analog audio output function from all other TOE functions.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the PSD PP needed to support audio output functionality. This is consistent because the functionality the PSD PP describes is being used for its intended purpose. When claiming conformance to a PP-Configuration that includes multiple PP-Modules, any additional guidance required to address interactions between them is provided by Appendix F: Interactions between PP-Modules. This PP-Module also identifies a number of modified SFRs from the PSD PP as well as new SFRs used entirely to supply audio output functionality. The rationale for why this does not conflict with the claims the PSD PP defines is as follows:

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FDP_APC_EXT.1	This SFR adds a requirement to block electrical signals that strengthens but does not conflict with the requirement in the PSD PP.
FDP_PDC_EXT.1	This SFR is not changed by this PP-Module and only defines existing Evaluation Activities for audio output devices, which does not conflict with the PSD PP.
Mandatory SFRs	
FDP_AFL_EXT.1	This SFR defines the filtering levels that outgoing audio signals must enforce. This function is specific to audio output devices and does not prevent the enforcement of any PSD PP SFRs.
FDP_PDC_EXT.2/AO	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_PUD_EXT.1	This SFR requires the TSF not provide power to any unauthorized device connected to the analog audio peripheral interface in addition to the PSD PP requirement of rejecting it. The PSD PP does not define any requirements to provide power to peripherals, therefore this does not conflict with the PSD PP but is supplementary to the PSD PP.
FDP_UDF_EXT.1/AO	This SFR requires the specific types of peripheral data defined in this PP-Module to flow unidirectionally. This does not prevent the enforcement of any PSD PP SFRs.
Optional SFRs	
This PP-Module defines no optional SFRs.	
Selection-Based SFRs	
This PP-Module defines no selection-based SFRs.	

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.

No selection-based requirements specific to this PP-Module 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_AFL_EXT Audio Filtration
	FDP_PDC_EXT Peripheral Device Connection
	FDP_PUD_EXT Powering Unauthorized Devices
	FDP_UDF_EXT Unidirectional Data Flow

C.1 FDP_AFL_EXT Audio Filtration

Family Behavior

Components in this family define the requirements for device filtering.

Component Leveling

FDP_AFL_EXT.1 Audio Filtration, requires the TSF to enforce outgoing audio filtration levels.

Management: FDP_AFL_EXT.1

No specific management functions are defined.

Audit: FDP_AFL_EXT.1

No specific audit functions are defined.

FDP_AFL_EXT.1 Device Filtering

Hierarchical to: No other components

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

FDP_AFL_EXT.1.1 The TSF shall ensure outgoing audio signals are filtered as per [*assignment: document reference to the table below*].

Frequency (kHz)	Minimum Attenuation (dB)	Maximum Voltage After Attenuation
14	23.9	127.65 mV
15	26.4	95.73 mV
16	30.8	57.68 mV
17	35.0	35.57 mV
18	38.8	22.96 mV
19	43.0	14.15 mV

Frequency (kHz)	Minimum Attenuation (dB)	Maximum Voltage After Attenuation
20	46.0	10.02 mV
30	71.4	5.3 mV
40	71.4	5.3 mV
50	71.4	5.3 mV
60	71.4	5.3 mV

C.2 FDP_PDC_EXT Peripheral Device Connection

Family Behavior

This family is defined in the PSD PP. This PP-Module augments the extended family by adding one additional component, FDP_PDC_EXT.2. The 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.

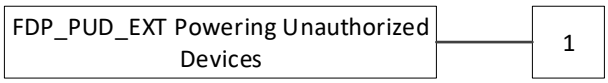
FDP_PDC_EXT.2.2 The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*assignment: devices specified in the PP or PP-Module in which this SFR is defined*] and [*assignment: devices specified in another PP or PP-Module that shares a PP-Configuration 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.3 FDP_PUD_EXT Powering Unauthorized Devices

Family Behavior

Components in this family define the requirements for unauthorized device powering.

Component Leveling



FDP_PUD_EXT.1 Powering Unauthorized Devices, requires the TSF to not power any unauthorized devices connected to the peripheral interface.

Management: FDP_PUD_EXT.1

No specific management functions are identified.

Audit: FDP_PUD_EXT.1

There are no specific auditable events foreseen.

FDP_PUD_EXT.1 Powering Unauthorized Devices

Hierarchical to: No other components

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

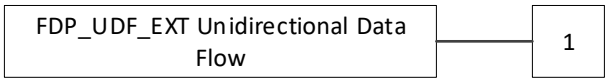
FDP_PUD_EXT.1.1 The TSF shall not provide power to any unauthorized device connected to the analog audio peripheral interface.

C.4 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's 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 peripheral devices:

- Audio input devices
- Any device not specifically authorized

E.3 Unauthorized Interface Protocols

The following are unauthorized interface protocols:

- Any protocol not specifically authorized

E.4 Authorized Peripheral Devices

The following are authorized devices:

- Analog headphones
- Analog speakers

E.5 Authorized Interface Protocols

The following are authorized interface protocols:

- Analog audio output

F Interactions between PP-Modules

This appendix provides any additional guidance required to address interactions between multiple PP-Modules when they are both contained within a PP-Configuration.

F.1 PP-Module for Keyboard/Mouse Devices

Unauthorized devices identified in both PP-Modules are considered unauthorized devices for the TOE as per FDP_PDC_EXT.1.

Authorized devices identified in both PP-Modules are considered authorized devices for the TOE as per the claimed iterations of FDP_PDC_EXT.2.

Power events at a KM interface for one connected computer cannot impact power events at an analog audio output interface for another connected computer and vice versa, as per FDP_APC_EXT.1. This evaluation activity is tested in Test 3-AO in the Supporting Document for Audio Output.

Both PP-Modules modify the Base-PP SFR FDP_APC_EXT.1 in ways that are specific to their respective peripheral types. The ST author should make two iterations of this SFR, FDP_APC_EXT.1/AO and FDP_APC_EXT.1/KM, to show the different modifications made for each specific peripheral type.

F.2 PP-Module for User Authentication Devices

Unauthorized devices identified in both PP-Modules are considered unauthorized devices for the TOE as per FDP_PDC_EXT.1.

Authorized devices identified in both PP-Modules are considered authorized devices for the TOE as per the claimed iterations of FDP_PDC_EXT.2.

Power events at a user authentication interface for one connected computer cannot impact power events at an analog audio output interface for another connected computer and vice versa, as per FDP_APC_EXT.1. This evaluation activity is tested in Test 3-AO in the Supporting Document for Audio Output.

Both PP-Modules modify the Base-PP SFR FDP_APC_EXT.1 in ways that are specific to their respective peripheral types. The ST author should make two iterations of this SFR, FDP_APC_EXT.1/AO and FDP_APC_EXT.1/UA, to show the different modifications made for each specific peripheral type.

F.3 PP-Module for Video/Display Devices

Unauthorized devices identified in both PP-Modules are considered unauthorized devices for the TOE as per FDP_PDC_EXT.1.

Authorized devices identified in both PP-Modules are considered authorized devices for the TOE as per the claimed iterations of FDP_PDC_EXT.2.

Power events at a video interface for one connected computer cannot impact power events at an analog audio output interface for another connected computer and vice versa, as per FDP_APC_EXT.1. This evaluation activity is tested in FDP_APC_EXT.1 Test 3-AO in the Supporting Document for Audio Output.

Both PP-Modules modify the Base-PP SFR FDP_APC_EXT.1 in ways that are specific to their respective peripheral types. The ST author should make two iterations of this SFR, FDP_APC_EXT.1/AO and FDP_APC_EXT.1/VI, to show the different modifications made for each specific peripheral type.

G 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
[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
dBv	A measurement of voltage ratio to 1 volt
KHz	Kilohertz
mV	Millivolt
S/PDIF	Sony/Philips Digital Interface Format
PSD	Peripheral Sharing Device