PP-Module for Video/Display 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

Table of Contents 3

1 Introduction 5
- **1.1 Overview** 5
- **1.2 Terms** 5
- **1.3 Compliant Targets of Evaluation** 5
  - 1.3.1 TOE Boundary 6
- **1.4 Use Cases** 6

2 Conformance Claims 7

3 Security Problem Description 8
- **3.1 Threats** 8
- **3.2 Assumptions** 8
- **3.3 Organizational Security Policies** 8

4 Security Objectives 9
- **4.1 Security Objectives for the TOE** 9
- **4.2 Security Objectives for the Operational Environment** 10
- **4.3 Security Objectives Rationale** 10

5 Security Requirements 11
- **5.1 PSD PP Security Functional Requirements Direction** 11
  - 5.1.1 Applicable Unmodified SFRs 11
  - 5.1.2 Applicable Modified SFRs 11
- **5.2 TOE Security Functional Requirements** 13
  - 5.2.1 User Data Protection 13
- **5.3 TOE Security Assurance Requirements** 14

6 Consistency Rationale 15
- **6.1 PSD Base** 15
  - 6.1.1 Consistency of TOE Type 15
  - 6.1.2 Consistency of Security Problem Definition 15
  - 6.1.3 Consistency of Objectives 15
  - 6.1.4 Consistency of Requirements 15

A Optional Requirements 17
- **A.1 Strictly Optional Requirements** 17
- **A.2 Objective Requirements** 17
- **A.3 Implementation-Dependent Requirements** 17

B Selection-Based Requirements 18
- **B.1 User Data Protection (FDP)** 18

C Extended Components Definition 21
- **C.1 FDP_CDS_EXT Connected Displays Supported** 21
- **C.2 FDP_IPC_EXT Internal Protocol Conversion** 21
- **C.3 FDP_PDC_EXT Peripheral Device Connection** 22
- **C.4 FDP_SPR_EXT Sub-Protocol Rules** 23
- **C.5 FDP_UDF_EXT Unidirectional Data Flow** 24

D Isolation Documentation and Assessment 25

E Peripheral Device Connections 26

E.1 General 26

E.2 Unauthorized Peripheral Devices 26

E.3 Unauthorized Interface Protocols 26

E.4 Authorized Peripheral Devices 26

E.5 Authorized Interface Protocols 26

F Interactions between PP-Modules 27

F.1 PP-Module for Audio Output Devices 27

F.2 PP-Module for Keyboard/Mouse Devices 27

F.3 PP-Module for User Authentication Devices 27

G References 29

H Acronyms 30

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 additional 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 includes the ability to manipulate or assign video source inputs to video or display output devices.

1.2 Terms

Term	Definition
Combiner/Multi-viewer	A PSD that can integrate video output from multiple connected systems and output on a single display.
Display	A device such as a monitor, projector, or touchscreen, which visually outputs user data.
Guard	A PSD function that requires multiple express user actions in order to switch between Connected Computers using Connected Peripherals.
Protocol	A set of rules or procedures for transmitting data between electronic devices
Sub-Protocol	A set of common commands flowing within a protocol.
TOE Computer Video Interface	TOE port used to connect the computer or other video source.
USB Type-C	Universal Serial Bus (USB) interface that supports DisplayPort video output as an alternate mode.
Video Data	Visual and audio information presented to the user through the display device
Video Wall	A tiled or overlapping set of displays that allow the video output from a single selected computer to be spanned across multiple individual displays.

1.3 Compliant Targets of Evaluation

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

A candidate TOE for claiming conformance to this PP-Module is any TOE that conforms to the PSD PP and includes video and display functionality as connected peripherals. In particular, a conformant TOE should support one or more video sources and one or more video display devices.

The TOE may include functionality for additional types of computer interfaces (e.g. keyboard/mouse, user authentication device). When this is the case, the TOE will claim conformance to all applicable PP-Modules that extend the PSD PP.

1.3.1 TOE Boundary

The TOE boundary is a PSD. Refer to the PSD PP for an outline of the TOE boundary. When claiming conformance to this PP-Module, the TOE boundary will include one or more each of peripheral and computer interfaces that can be used to transmit video signals. It is permissible to use this PP-Module in conjunction with other PP-Modules that also extend the PSD PP by claiming conformance to a PP-Configuration that includes all applicable PP-Modules. In this manner, a single TOE may support multiple different types of peripherals.

A conformant TOE may simultaneously present the video output of one or more computers per peripheral port; it is not required to be a one-to-one relationship. Section 1.4 below defines specific methods of supported video display.

1.4 Use Cases

This PP-Module does not define additional use cases beyond what the PSD PP defines. The TOE should embody one or more use cases from the PSD PP. This PP-Module's functionality defines implementation-independent functionality (i.e., not tied to any specific use cases) and relates entirely to the specific security requirements related to security of the physical and logical interfaces for assigning video and display devices. Specifically, the TOE may perform any of the following functions:

- Display PSD – Output from one or more connected computers to be presented on a single display
- Keyboard, video, and mouse (KVM) PSD – Output from one or more connected computers to be presented on one or more displays along with keyboard and mouse user interaction—in this case, the TOE boundary would also include the requirements of the PP-Module for Keyboard/Mouse (KM) Input Devices
- Combiner/Multi-viewer – Output from multiple computers to be shown simultaneously on one or more displays along with keyboard and mouse user interaction
- Video Wall – Output from one or more computers to be shown across multiple displays

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 Analog Audio Output Devices, Version 1.0
- PP-Module for User Authentication Devices, Version 1.0
- PP-Module for Keyboard/Mouse 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 OSPs defined in the PSD PP also apply to the TOE, its usage and deployment, and its operational environment unless otherwise specified.

3.1 Threats

This PP-Module defines no additional threats. Note however that the SFRs defined in this PP-Module are intended to further mitigate the following PSD PP threats specifically for video data in particular:

- T.DATA_LEAK
- T.RESDIUAL_LEAK
- T.SIGNAL_LEAK
- T.UNAUTHORIZED_DEVICES

3.2 Assumptions

This PP-Module defines the following assumptions for a TOE claiming conformance to it.

A.NO_SPECIAL_ANALOG_CAPABILITIES

The computers connected to the TOE are not equipped with special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, digital signal processing function, or analog video capture function.

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, and O.PERIPHERAL_PORTS_ISOLATION objectives from the PSD PP specifically for video peripherals. In addition to the SFRs mapped in the PSD PP, the following SFRs modified from their PSD PP definition contribute to supporting these objectives for video devices:

- FDP_APC_EXT.1 (modified from PSD PP definition), FDP_PDC_EXT.1 (modified from PSD PP definition)

A TOE conforming to this PP-Module must address the O.REJECT_UNAUTHORIZED_PERIPHERAL objective from the PSD PP specifically for video peripherals and protocols. In addition to the SFRs mapped in the PSD PP, the following SFRs contribute to supporting these objectives for video devices:

- FDP_PDC_EXT.2/VI, FDP_PDC_EXT.3/VI, FDP_IPC_EXT.1 (selection-based), FDP_SPR_EXT.1/DP (selection-based), FDP_SPR_EXT.1/DVI-D (selection-based), FDP_SPR_EXT.1/DVI-I (selection-based), FDP_SPR_EXT.1/HDMI (selection-based), FDP_SPR_EXT.1/USB (selection-based), FDP_SPR_EXT.1/VGA (selection-based)

If the TOE supports the ability to display output from multiple connected computers (i.e., the TOE is not an isolator) it must address O.AUTHORIZED_USAGE in the PSD PP specifically for video data. In addition to the SFRs in the PSD PP, the following SFRs defined in this PP-Module or modified from their PSD PP definition contribute to supporting this objective for video devices:

- FDP_CDS_EXT.1 (selection-based); FTA_CIN_EXT.1 (modified from PSD PP definition; selection-based)

If the TOE supports DisplayPort as an authorized connection protocol, it must address O.REJECT_UNAUTHORIZED_PERIPHERAL in the PSD PP specifically for the DisplayPort protocol (which may contain non-video data and therefore represents a potential threat vector). In addition to the SFRs in the PSD PP, the following SFR defined in this PP-Module contributes to supporting these objectives for video devices:

- FDP_SPR_EXT.1/DP (selection-based)

This PP-Module also defines the following security objectives for a TOE claiming conformance to it.

O.PROTECTED_EDID

The TOE shall read the connected display Extended Display Identification Data (EDID) once during the TOE power up or reboot sequence and prevent any EDID channel write transactions that connected computers initiate.

Addressed by: FDP_PDC_EXT.2/VI, FDP_SPR_EXT.1/DP (selection-based), FDP_SPR_EXT.1/DVI-D (selection-based), FDP_SPR_EXT.1/DVI-I (selection-based), FDP_SPR_EXT.1/HDMI (selection-based), FDP_SPR_EXT.1/USB (selection-based), FDP_SPR_EXT.1/VGA (selection-based)

O.UNIDIRECTIONAL_VIDEO

The TOE shall enforce unidirectional video data flow from the connected computer video interface to the display interface only.

Addressed by: FDP_UDF_EXT.1/VI

4.2 Security Objectives for the Operational Environment

This PP-Module defines the following environmental security objectives for a TOE claiming conformance to it.

OE.NO_SPECIAL_ANALOG_CAPABILITIES

The operational environment will not have special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, or a component with digital signal processing or analog video capture functions.

4.3 Security Objectives Rationale

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

Threat or Assumption	Security Objectives	Rationale
T.DATA_LEAK	O.PROTECTED_EDID	The TOE's protection of the EDID interface prevents its use as a vector for unauthorized data leakage via this channel.
	O.UNIDIRECTIONAL_VIDEO	The TOE's enforcement of unidirectional output for video data protects against data leakage via connected computers by ensuring that no video data can be input to a connected computer through this interface.
T.RESIDUAL_LEAK	O.PROTECTED_EDID	The TOE's protection of the EDID interface prevents the leakage of residual data by ensuring that no such data can be written to EDID memory.
T.SIGNAL_LEAK	O.PROTECTED_EDID	The TOE's protection of the EDID interface prevents its use as a vector for bit-by-bit signal leakage via this channel.
	O.UNIDIRECTIONAL_VIDEO	The TOE's enforcement of unidirectional output for video data protects against signaling leakage via connected computers by ensuring that no video data can be input to a connected computer through this interface.
T.UNAUTHORIZED_DEVICES	O.UNIDIRECTIONAL_VIDEO	The TOE's limitation of supported video protocol interfaces prevents the connection of unauthorized devices.
A.NO_SPECIAL_ANALOG_ CAPABILITIES	OE.NO_SPECIAL_ANALOG_CAP ABILITIES	If administrators in the TOE's operational environment take care to ensure that computers with special analog data collection interfaces are not connected to the TOE, then the assumption that such components are not present is satisfied.

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 conformance to this PP-Module, it is necessary to make claims in the PSD PP requirements consistent with the functionality in the PP-Module. The following sections describe any PSD PP claims that must be made and any additional evaluation activities that must be performed when the TOE boundary includes the functionality this PP-Module describes.

5.1.1 Applicable Unmodified SFRs

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

Note that if only some elements of a component are modified by inclusion of this PP-Module, only the modified element(s) are included here; the remaining element(s) should be handled identically to what the PSD PP requires.

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 for electrical signals. It is unlikely that this element can be satisfied unless video/display peripheral device interfaces are electrically and logically isolated from the connected computer interfaces or through other methods.*

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/VI" 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 Policy (see Appendix E) associated with this SFR and additional Evaluation Activities.

FTA_CIN_EXT.1 Continuous Indications

This SFR is selection-based in the PSD PP. It remains selection-based when the TOE conforms to this PP-Module. However, this PP-Module adds a trigger for its selection—specifically, if "multiple connected displays" is selected in FDP_CDS_EXT.1.1, then FTA_CIN_EXT.1 is applicable to the TOE and must be claimed.

The following SFR has a specific assignment, which is a mandatory selection if selecting "multiple connected displays" in FDP_CDS_EXT.1.1.

Additionally, the SFR is refined to specify an additional display mechanism in FTA_CIN_EXT.1.2, as follows:

FTA_CIN_EXT.1.2 The TSF shall implement the visible indication using the following mechanism: **easily visible graphical and/or textual markings of each source video on the display,** [*selection: a button, a panel with lights, a screen with dimming function, a screen with no dimming function***,** *[assignment: description of visible indication]*].

5.2 TOE Security Functional Requirements

5.2.1 User Data Protection

FDP_PDC_EXT.2/VI Peripheral Device Connection (Video Output)

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

- ***authorized devices as defined in the PP-Module for Audio Output Devices,***
- ***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,***
- ***no other devices***

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

FDP_PDC_EXT.2.2/VI 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 Audio Output Devices,***
- ***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,***
- ***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.*

If "authorized devices presenting authorized interface protocols as defined in the PP-Module for Keyboard/Mouse" is selected and "USB Type-C with DisplayPort as alternate function" is selected in FDP_PDC_EXT.3.1/VI, then video devices that use USB Type-C with DisplayPort as alternate function may not be used in conjunction with touch screen devices.

FDP_PDC_EXT.3/VI Authorized Connection Protocols (Video Output)

FDP_PDC_EXT.3.1/VI The TSF shall have interfaces for the [*selection: VGA, DVI-D, DVI-I, HDMI, DisplayPort, USB Type-C with DisplayPort as alternate function*] protocols.

FDP_PDC_EXT.3.2/VI The TSF shall apply the following rules to the supported protocols: [*the TSF shall read the connected display EDID information once during power-on or reboot*].

Application Note: *It is expected that the ST author will make all selections in FDP_PDC_EXT.3.1/VI for which the TOE has an interface; the TOE boundary should encompass the entire device where possible.*

If the KM PP-Module is also claimed by the ST, "USB Type-C with DisplayPort as alternate function" may not be selected in conjunction with a touchscreen peripheral device.

If "DisplayPort" is selected, the ST must include the selection-based requirement FDP_IPC_EXT.1.

This PP-Module defines several iterations of FDP_SPR_EXT.1. Depending on the selections made in FDP_PDC_EXT.3.1/VI, the evaluator must include the relevant iterations.

FDP_UDF_EXT.1/VI Unidirectional Data Flow (Video Output)

FDP_UDF_EXT.1.1/VI The TSF shall ensure [*video*] data transits the TOE unidirectionally from the [*TOE computer video*] interface to the [*TOE peripheral device display*] interface.

5.3 TOE Security Assurance Requirements

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

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 video or display 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 does not define additional threats beyond those the PSD PP defines. Therefore, there is no inconsistency between this PP-Module and the PSD with respect to the security problem definition.

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.PROTECTED_EDID	The PSD PP does not specify how connected computers interface logically with authorized devices so the restrictions that this PP-Module places on the interaction between connected computers and the EDID of peripheral devices does not prevent any PSD PP objectives from being satisfied.
O.UNIDIRECTIONAL_VIDEO	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.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the PSD PP needed to support video and display 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 video and display 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 video/display devices, which does not conflict with the PSD PP.

FTA_CIN_EXT.1	This PP-Module adds a new display mechanism that is unique to video/display peripherals and a new trigger for when the SFR applies. Neither of these changes conflict with the original SFR definition in the PSD PP.
Mandatory SFRs	
FDP_PDC_EXT.2/VI	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_PDC_EXT.3/VI	This SFR defines the protocols that are authorized specifically by this PP-Module and the rules for handling of these protocols. This does not prevent the enforcement of any PSD PP SFRs.
FDP_UDF_EXT.1/VI	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	
FDP_CDS_EXT.1	This SFR adds support for one or multiple connected displays. It is not in the PSD PP.
FDP_IPC_EXT.1	This SFR allows for the conversion of video protocols. It is not in the PSD PP.
FDP_SPR_EXT.1/DP	This SFR describes how the TSF handles specific video sub-protocols, which is beyond the scope of the behavior described in the Base-PP.
FDP_SPR_EXT.1/DVI-D	This SFR describes how the TSF handles specific video sub-protocols, which is beyond the scope of the behavior described in the Base-PP.
FDP_SPR_EXT.1/DVI-I	This SFR describes how the TSF handles specific video sub-protocols, which is beyond the scope of the behavior described in the Base-PP.
FDP_SPR_EXT.1/HDMI	This SFR describes how the TSF handles specific video sub-protocols, which is beyond the scope of the behavior described in the Base-PP.
FDP_SPR_EXT.1/USB	This SFR describes how the TSF handles specific video sub-protocols, which is beyond the scope of the behavior described in the Base-PP.
FDP_SPR_EXT.1/VGA	This SFR describes how the TSF handles specific video sub-protocols, which is beyond the scope of the behavior described in the Base-PP.

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.

B.1 User Data Protection (FDP)

FDP_CDS_EXT.1 Connected Displays Supported

FDP_CDS_EXT.1.1 The TSF shall support [*selection: one connected display, multiple connected displays*] at a time.

Application Note: *This SFR must be claimed if "switching can be initiated only through express user action" is chosen as a selection for FDP_SWI_EXT.1 in the PSD PP.*

If "peripheral devices using a guard" is selected in FDP_SWI_EXT.2.2 (from the PSD PP), then "multiple connected displays" must be selected in FDP_CDS_EXT.1.1.

FDP_IPC_EXT.1 Internal Protocol Conversion

FDP_IPC_EXT.1.1 The TSF shall convert the [*DisplayPort*] protocol at the [*computer video interface*] into the [*HDMI*] protocol within the TOE.

FDP_IPC_EXT.1.2 The TSF shall output the [*HDMI*] protocol from inside the TOE to [*peripheral display interface(s)*] as [*selection: [DisplayPort] protocol, [HDMI] protocol*].

Application Note: *This SFR must be claimed if "DisplayPort" is chosen as a selection for FDP_PDC_EXT.2.1/VI.*

FDP_SPR_EXT.1/DP Sub-Protocol Rules (DisplayPort Protocol)

FDP_SPR_EXT.1.1/DP The TSF shall apply the following rules for the [*DisplayPort*] protocol:

- block the following video/display sub-protocols:
  - [*CEC,*
  - *EDID from computer to display,*
  - *HDCP,*
  - *MCCS*]
- allow the following video/display sub-protocols:
  - [*EDID from display to computer,*
  - *HPD from display to computer,*
  - *Link Training*].

Application Note: *The ST author must include this SFR if "DisplayPort" is selected in FDP_PDC_EXT.3.1/VI.*

FDP_SPR_EXT.1/DVI-D Sub-Protocol Rules (DVI-D Protocol)

FDP_SPR_EXT.1.1/DVI-D The TSF shall apply the following rules for the [*DVI-D*] protocol:

- block the following video/display sub-protocols:

- [*ARC,*
- *CEC,*
- *EDID from computer to display,*
- *HDCP,*
- *HEAC,*
- *HEC,*
- *MCCS*]

- allow the following video/display sub-protocols:
  - [*EDID from display to computer,*
  - *HPD from display to computer*].

Application Note: *The ST author must include this SFR if "DVI-D" is selected in FDP_PDC_EXT.3.1/VI.*

FDP_SPR_EXT.1/DVI-I Sub-Protocol Rules (DVI-I Protocol)

FDP_SPR_EXT.1.1/DVI-I The TSF shall apply the following rules for the [*DVI-I*] protocol:

- block the following video/display sub-protocols:
  - [*ARC,*
  - *CEC,*
  - *EDID from computer to display,*
  - *HDCP,*
  - *HEAC,*
  - *HEC,*
  - *MCCS*]
- allow the following video/display sub-protocols:
  - [*EDID from display to computer,*
  - *HPD from display to computer*].

Application Note: *The ST author must include this SFR if "DVI-I" is selected in FDP_PDC_EXT.3.1/VI.*

FDP_SPR_EXT.1/HDMI Sub-Protocol Rules (HDMI Protocol)

FDP_SPR_EXT.1.1/HDMI The TSF shall apply the following rules for the [*HDMI*] protocol:

- block the following video/display sub-protocols:
  - [*ARC,*
  - *CEC,*
  - *EDID from computer to display,*
  - *HDCP,*
  - *HEAC,*
  - *HEC,*
  - *MCCS*]
- allow the following video/display sub-protocols:
  - [*EDID from display to computer,*
  - *HPD from display to computer*].

Application Note: *The ST author must include this SFR if "HDMI" is selected in FDP_PDC_EXT.3.1/VI.*

FDP_SPR_EXT.1/USB Sub-Protocol Rules (USB-C Protocol)

FDP_SPR_EXT.1.1/USB The TSF shall apply the following rules for the [*USB Type-C with DisplayPort as alternate function*] protocol:

- block the following video/display sub-protocols:
  - [*CEC,*
  - *EDID from computer to display,*
  - *HDCP,*
  - *MCCS*]
- allow the following video/display sub-protocols:
  - [*EDID from display to computer,*
  - *HPD from display to computer,*
  - *Link Training*].

Application Note: *The ST author must include this SFR if "USB Type-C with DisplayPort as alternate function" is selected in FDP_PDC_EXT.3.1/VI.*

FDP_SPR_EXT.1/VGA Sub-Protocol Rules (VGA Protocol)

FDP_SPR_EXT.1.1/VGA The TSF shall apply the following rules for the [*VGA*] protocol:

- block the following video/display sub-protocols:
  - [*EDID from computer to display,*
  - *MCCS*]
- allow the following video/display sub-protocols:
  - [*EDID from display to computer*].

Application Note: *The ST author must include this SFR if "VGA" is selected in FDP_PDC_EXT.3.1/VI.*

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:

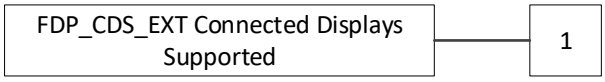
Functional Class	Functional Families
User Data Protection (FDP)	FDP_CDS_EXT Connected Displays Supported
	FDP_IPC_EXT Internal Protocol Conversion
	FDP_PDC_EXT Peripheral Device Connection
	FDP_SPR_EXT Sub-Protocol Rules
	FDP_UDF_EXT Unidirectional Data Flow

C.1 FDP_CDS_EXT Connected Displays Supported

Family Behavior

Components in this family define requirements for the number of display interfaces contained within the TOE.

Component Leveling



FDP_CDS_EXT.1, Connected Displays Supported, requires the TSF to define whether it supports one connected display at a time or multiple connected displays simultaneously.

Management: FDP_CDS_EXT.1

There are no specific management functions identified.

Audit: FDP_CDS_EXT.1

There are no auditable events foreseen.

FDP_CDS_EXT.1 Connected Displays Supported

Hierarchical to: No other components

Dependencies: No other components

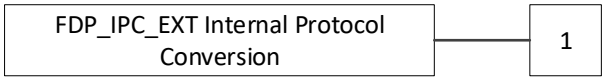
FDP_CDS_EXT.1.1 The TSF shall support [*selection: one connected display, multiple connected displays*] at a time.

C.2 FDP_IPC_EXT Internal Protocol Conversion

Family Behavior

Components in this family define requirements for the TOE's ability to convert one protocol into another for internal processing.

Component Leveling



FDP_IPC_EXT.1, Internal Protocol Conversion, requires the TSF to specify an input protocol that the TOE receives, the protocol that the TSF converts it to, and whether the data is output from the TOE as the original protocol or as the converted one.

Management: FDP_IPC_EXT.1

There are no specific management functions identified.

Audit: FDP_IPC_EXT.1

There are no auditable events foreseen.

FDP_IPC_EXT.1 Internal Protocol Conversion

Hierarchical to: No other components

Dependencies: FDP_PDC_EXT.2 Authorized Connection Protocols

FDP_IPC_EXT.1.1 The TSF shall convert the [*assignment: original protocol*] protocol at the [*assignment: TOE external interface(s)*] into the [*assignment: converted protocol*] protocol within the TOE.

FDP_IPC_EXT.1.2 The TSF shall output the [*assignment: converted protocol*] protocol from inside the TOE to [*assignment: TOE external interface(s)*] as [*selection: [assignment: original protocol] protocol], [assignment: converted protocol] protocol*].

C.3 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 two additional components, FDP_PDC_EXT.2 and FDP_PDC_EXT.3. These new components and their 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.

FDP_PDC_EXT.3, Authorized Connection Protocols, defines the protocols that the TSF will authorize over its physical/logical interfaces, as well as any rules that are applicable to these interfaces.

Management: FDP_PDC_EXT.2, FDP_PDC_EXT.3

No specific management functions are identified.

Audit: FDP_PDC_EXT.2, FDP_PDC_EXT.3

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.

FDP_PDC_EXT.3 Authorized Connection Protocols

Hierarchical to: No other components

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

FDP_PDC_EXT.3.1 The TSF shall have interfaces for the [*assignment: list of supported protocols associated with physical and/or logical TSF interfaces*] protocols.

FDP_PDC_EXT.3.2 The TSF shall apply the following rules to the supported protocols: [*assignment: rules defining the handling for communications over this protocol (e.g. any processing that must be done by the TSF prior to transmitting it through the TOE, circumstances or frequency with which the protocol is invoked)*].

C.4 FDP_SPR_EXT Sub-Protocol Rules

Family Behavior

Components in this family define the sub-protocols that the TSF allows or blocks depending on the protocols it supports.

Component Leveling

FDP_SPR_EXT.1 Sub-Protocol Rules, requires the TSF to specify the allowed and blocked sub-protocols based on the protocol it supports.

Management: FDP_SPR_EXT.1

No specific management functions are identified.

Audit: FDP_SPR_EXT.1

There are no auditable events foreseen.

FDP SPR_EXT.1 Sub-Protocol Rules

Hierarchical to: No other components

Dependencies: FDP_PDC_EXT.3 Authorized Connection Protocols

FDP_SPR_EXT.1.1 The TSF shall apply the following rules for the [*assignment: supported protocol*] protocol:

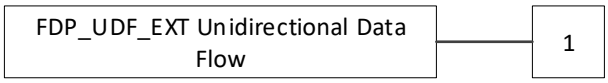
- block the following video/display sub-protocols:
  - [*assignment: list of blocked sub-protocols*]
- allow the following video/display sub-protocols:
  - [*assignment: list of allowed sub-protocols*].

C.5 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 the PSD PP requires.

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:

- Any device not specifically authorized

E.3 Unauthorized Interface Protocols

The following are unauthorized interface protocols:

- Any interface protocol not specifically authorized

E.4 Authorized Peripheral Devices

The following are authorized devices:

- Display device

E.5 Authorized Interface Protocols

The following are authorized interface protocols:

- DisplayPort
- DVI-D
- DVI-I
- HDMI
- USB Type-C with DisplayPort as alternate function
- VGA

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 Audio Output 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/VI and FDP_APC_EXT.1/AO, to show the different modifications made for each specific peripheral type.

F.2 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.

Video devices with an interface for USB Type-C with DisplayPort as alternate function may not be connected to a KM interface, and KM devices may not be connected to a video interface for USB Type-C with DisplayPort as alternate function, even though both devices are authorized devices.

Video devices with an interface for USB Type-C with DisplayPort as alternate function may not be used in conjunction with a touchscreen peripheral device, as per FDP_PDC_EXT.2/KM and FDP_PDC_EXT.3.1/Vid.

KM devices may be used with a guard in conjunction with multiple video devices, as per FDP_CDS_EXT.1 and FDP_SWI_EXT.2.

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/VI and FDP_APC_EXT.1/KM, to show the different modifications made for each specific peripheral type.

F.3 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.

Any USB-C functionality that is supported by the TOE must be isolated from user authentication functionality and vice versa as per FDP_UAI_EXT.1.

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/VI and FDP_APC_EXT.1/UA, 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-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
ARC	Audio Return Channel
CEC	Consumer Electronics Control
DVI	Digital Visual Interface (standard)
EDID	Extended Display Identification Data
HDCP	High-bandwidth Digital Content Protection
HDMI	High-Definition Multimedia Interface (standard)
HEAC	HDMI Ethernet and Audio Return Channel
HEC	HDMI Ethernet Channel
HPD	Hot Plug Detect
KVM	Keyboard, video, mouse
MCCS	Monitor Control Command Set
OSP	Organizational Security Policies
PSD	Peripheral Sharing Device
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
USB	Universal Serial Bus (standard)
VGA	Video Graphics Array (standard)