PP-Module for Keyboard/Mouse Devices

Version: 1.0

2019-07-19

National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2019-07-19	Initial version

Table of Contents

1 Introduction 5
1.1 Overview 5
1.2 Terms 5
1.3 Compliant Targets of Evaluation 6
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 9
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 14
5.3 TOE Security Assurance Requirements 15
6 Consistency Rationale 16
6.1 PSD Base 16
6.1.1 Consistency of TOE Type 16
6.1.2 Consistency of Security Problem Definition 16
6.1.3 Consistency of Objectives 16
6.1.4 Consistency of Requirements 16
A Optional Requirements 19
A.1 Strictly Optional Requirements 19
A.2 Objective Requirements 19
A.3 Implementation-Dependent Requirements 19
A.3.1 TOE Capability for Device Filtering 19
A.3.2 TOE Capability for Rejection of Re-Enumerated Devices 20
B Selection-Based Requirements 21
B.1 User Data Protection (FDP) 21
C Extended Components Definition 22
C.1 FDP_FIL_EXT Device Filtering 22
C.2 FDP_PDC_EXT Peripheral Device Connection 23
C.3 FDP_RDR_EXT Re-Enumeration Device Rejection 24
C.4 FDP_SWI_EXT PSD Switching 24
C.5 FDP_UDF_EXT Unidirectional Data Flow 25

D Isolation Documentation and Assessment 26

E Peripheral Device Connections 27

E.1 General 27

E.2 Unauthorized Peripheral Devices 27

E.3 Unauthorized Interface Protocols 27

E.4 Authorized Peripheral Devices 27

E.5 Authorized Interface Protocols 27

F Interactions between PP-Modules 28

F.1 PP-Module for Audio Output Devices 28

F.2 PP-Module for User Authentication Devices 28

F.3 PP-Module for Video/Display Devices 28

G References 30

H Acronyms 31

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 includes the ability to manipulate or assign human interface devices (HIDs) (e.g., keyboard and pointing device) to one or more computers connected to the PSD.

1.2 Terms

Term	Definition
Blacklist	List containing one or more device attributes that will cause the PSD to reject the devices having that attribute.
Composite Device (USB)	A peripheral device that supports more than one device class.
Configurable Device Filtration (CDF)	PSD function that accepts or rejects peripheral devices based on field-configurable parameters or whitelist and blacklist.
Emulate	Imitate the behavior of a device or a function in a device.
Fixed Device Filtration (FDF)	PSD function that accepts or rejects peripheral devices based on fixed parameters loaded during production.
Endpoint (USB)	A source or a sink of data. Universal Serial Bus (USB) host is centric; endpoints occur at the end of the communications channel at the USB function.
Enumeration (USB)	A process that starts as soon as a device connects to the USB host. In this process, the host and the device jointly define the communications and power settings.
Guard	A PSD function that requires multiple express user actions to switch between connected computers using connected peripheral devices.
Interface (USB)	Groups of endpoints. Each interface relates with a single device function. An exception to this is endpoint zero, which is for device configuration and not associated with any interface.
HID	A device that allows input from, or sends output to human users.
Host (USB)	Initiates all communication on the USB and numbers the connected devices.
USB Device	USB devices are leafs in the USB tree that are connected to the host.

Term	Definition
USB Hub	A device that expands a single USB port into several so there are more ports available to connect devices to a host system.
Whitelist	List containing one or more device attributes that will cause the TOE to accept the devices having that attribute.

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 **HID peripheral devices**, in particular USB devices. Specifically, the TOE may support keyboard and/or pointing devices. As the most common pointing device expected for use with the TOE is a mouse, this term will be used throughout this PP-Module to refer to all pointing devices collectively. 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 keyboard and/or mouse connected peripherals (KM). In particular, a conformant TOE should support one or more USB keyboard and/or mouse devices.

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

Note that this PP-Module covers PSD functionality supporting USB peripherals only.

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 USB peripheral and USB computer interfaces that can be used to transmit human user input. 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.

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 supporting keyboard and mouse 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.

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 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 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. Note however that the SFRs defined in this PP-Module are intended to further mitigate the following PSD PP threats specifically for keyboard/mouse data in particular:

- T.DATA_LEAK, T.RESIDUAL_LEAK, T.SIGNAL_LEAK, T.UNINTENDED_USE (for all TOEs, because of the possibility of data being passed to an incorrect computer)
- T.UNAUTHORIZED_DEVICES (for all TOEs, because devices other than keyboards and mice can be connected to the TOE via USB)

3.2 Assumptions

This PP-Module defines no additional assumptions. Note however that the A.NO_TEMPEST assumption from the PSD PP has the following additional interpretation when the TOE claims conformance to this PP-Module:

- The TSF may or may not isolate the ground of the keyboard and mouse computer interfaces (the USB ground). The Operational Environment is assumed not to support TEMPEST red-black ground isolation.

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_TOE_UNPOWERED, O.USER_DATA_ISOLATION, O.PERIPHERAL_PORTS_ISOLATION, O.REJECT_UNAUTHORIZED_ENDPOINTS, and O.REJECT_UNAUTHORIZED_PERIPHERAL objectives from the PSD PP specifically for keyboard and/or mouse input 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 keyboard/mouse input devices:

- FDP_APC_EXT.1 (modified from PSD PP definition), FDP_FIL_EXT.1/KM (optional), FDP_PDC_EXT.1 (modified from PSD PP definition), FDP_RDR_EXT.1 (optional), FDP_SWI_EXT.3 (selection-based)

If the TOE supports configurable device filtration as specified in FDP_FIL_EXT.1/KM, it must address the O.AUTHORIZED_USAGE objective for the administrative capability to configure device filtration at minimum.

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

- FDP_PDC_EXT.2/KM, FDP_PDC_EXT.3/KM

If the TOE supports keyboard peripheral types, it must address O.NO_USER_DATA_RETENTION from the PSD PP specifically for keyboard 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 these objectives for keyboard/mouse input devices:

- FDP_RIP.1/KM (selection-based)

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

O.EMULATED_INPUT
The TOE shall emulate the keyboard and/or mouse functions from the TOE to the connected computer.

Addressed by: FDP_PDC_EXT.2/KM, FDP_PDC_EXT.3/KM

O.UNIDIRECTIONAL_INPUT

The TOE shall enforce unidirectional keyboard and/or mouse device's data flow from the peripheral device to only the selected computer.

Addressed by: FDP_UDF_EXT.1/KM

4.2 Security Objectives for the Operational Environment

All environmental security objectives from the PSD PP also apply to the TOE's environment when it includes this PP-Module in its conformance claims.

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 Objective	Rationale
T.LOGICAL_TAMPER	O.EMULATED_INPUT	The TOE's emulation of keyboard/mouse data input prevents logical tampering of the TSF ensuring that only known inputs to it are supported.
T.UNAUTHORIZED_DEVICES	O.EMULATED_INPUT	The TOE's emulation of keyboard/mouse data input ensures that a connected computer will only receive this specific type of data through a connected peripheral.
T.DATA_LEAK	O.UNIDIRECTIONAL_INPUT	The TOE's enforcement of unidirectional input for keyboard/mouse data prevents leakage of computer data through a connected peripheral interface.
T.SIGNAL_LEAK	O.UNIDIRECTIONAL_INPUT	The TOE's enforcement of unidirectional input for keyboard/mouse data prevents leakage of computer data through bit-by-bit signaling to a connected peripheral interface.

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: 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 number inside parentheses following the component or element name (e.g. "(1)") and/or a slash followed by a unique text string (e.g. "/KM"), 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 when the TOE boundary includes the functionality this PP-Module describes. For some requirements, only certain individual elements within the SFR have been modified for this PP-Module. Any SFR elements 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 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_PDC_EXT.1
- 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.

FAU_GEN.1 Audit Data Generation

This SFR is unchanged when the TOE claim includes this PP-Module. However, this SFR is an optional requirement in the PSD PP. This PP-Module defines functionality that would require this SFR to be claimed if a certain selection is made. Therefore, this PP-Module re-categorizes this optional SFR as selection-based. It shall be included in the TSF if 'configurable' is selected in FDP_FIL_EXT.1.1/KM.

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 mouse and keyboard peripheral device interfaces are electrically and logically isolated from the connected computer interfaces or through other methods, such as USB host and USB device emulation.*

For TOEs that support only a keyboard or mouse, but not both, tests and portions of tests that involve using the non-supported peripheral are considered conditional.

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/KM" 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, modifications of the application note, and additional Evaluation Activities. The application note from the PSD PP is changed to the following:

Application Note: *The Peripheral Device Connections section is in Appendix E of both the PSD PP and this PP-Module. Keyboard and mouse peripheral device ports may be specific to only one type or interchangeable between them.*

The TSF may elect to enforce rejection of unauthorized devices connected to the PSD through a USB hub by considering USB hubs as unauthorized devices, even though USB hubs are authorized devices. The TSF may elect to enforce rejection of unauthorized non-HID device classes of a composite device connected to a TOE KM peripheral interface by considering composite devices with non-HID device classes as unauthorized devices, even though the HID device classes are authorized.

FDP_SWI_EXT.2 PSD Switching

There is no modification to this SFR in this PP-Module. However, if selecting “peripheral devices using a guard,” in FDP_SWI_EXT.2.2 in the PSD PP, there are additional Evaluation Activities defined in the Supporting Document Mandatory Technical Document PP-Module for Keyboard/Mouse Input Devices.

A connected peripheral, such as a mouse or other pointing device, may be used for user selection of the connected computer if the TOE makes sure the user has taken multiple, simultaneous express actions a guard requires. An example would be if the user moved the pointing device cursor through the border between computer display areas and at the same time, the user pressed a pre-defined keyboard key or a dedicated TOE button.

FIA_UAU.2 User Authentication Before Any Action

This SFR is unchanged when the TOE claim includes this PP-Module. However, this SFR is an optional requirement in the PSD PP. This PP-Module defines functionality that would require this SFR to be claimed if a certain selection is made. Therefore, this PP-Module re-categorizes this optional SFR as selection-based. It shall be included in the TSF if ‘configurable’ is selected in FDP_FIL_EXT.1.1/KM.

FIA_UID.2 User Identification Before Any Action

This SFR is unchanged when the TOE claim includes this PP-Module. However, this SFR is an optional requirement in the PSD PP. This PP-Module defines functionality that would require this SFR to be claimed if a certain selection is made. Therefore, this PP-Module re-categorizes this optional SFR as selection-based. It shall be included in the TSF if ‘configurable’ is selected in FDP_FIL_EXT.1.1/KM.

FMT_MOF.1 Management of Security Functions Behavior

This SFR is unchanged when the TOE claim includes this PP-Module. However, this SFR is an optional requirement in the PSD PP. This PP-Module defines functionality that would require this SFR to be claimed if a certain selection is made. Therefore, this PP-Module re-categorizes this optional SFR as selection-based. It shall be included in the TSF if ‘configurable’ is selected in FDP_FIL_EXT.1.1/KM.

FMT_SMF.1 Specification of Management Functions

This SFR is unchanged when the TOE claim includes this PP-Module. However, this SFR is an optional requirement in the PSD PP. This PP-Module defines functionality that would require this SFR to be claimed if a certain selection is made. Therefore, this PP-Module re-categorizes this optional SFR as selection-based. It shall be included in the TSF if ‘configurable’ is selected in FDP_FIL_EXT.1.1/KM.

FMT_SMR.1 Security Roles

This SFR is unchanged when the TOE claim includes this PP-Module. However, this SFR is an optional requirement in the PSD PP. This PP-Module defines functionality that would require this SFR to be claimed if a certain selection is made. Therefore, this PP-Module re-categorizes this optional SFR as selection-based. It shall be included in the TSF if ‘configurable’ is selected in FDP_FIL_EXT.1.1/KM.

FPT_STM.1 Reliable Time Stamps

This SFR is unchanged when the TOE claim includes this PP-Module. However, this SFR is an optional requirement in the PSD PP. This PP-Module defines functionality that would require this SFR to be claimed if a certain selection is made. Therefore, this PP-Module re-categorizes this optional SFR as selection-

based. It shall be included in the TSF if 'configurable' is selected in FDP_FIL_EXT.1.1/KM.

5.2 TOE Security Functional Requirements

FDP_PDC_EXT.2/KM Authorized Devices (Keyboard/Mouse)

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

- ***authorized devices as defined in the PP-Module for Audio Output 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 devices***

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

FDP_PDC_EXT.2.2/KM 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 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.*

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

FDP_PDC_EXT.3/KM Authorized Connection Protocols (Keyboard/Mouse)

FDP_PDC_EXT.3.1/KM The TSF shall have interfaces for the [*selection: USB (keyboard), USB (mouse)*] protocols.

FDP_PDC_EXT.3.2/KM The TSF shall apply the following rules to the supported protocols: [*the TSF shall emulate any keyboard or mouse device functions from the TOE to the connected computer*].

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

If the TOE supports multiple connected computers (as specified by selecting "switching can be initiated only through express user action" in FDP_SWI_EXT.1.1 in the PSD PP), selections made in FDP_PDC_EXT.3.1 determine whether selection-based SFRs in Appendix B must be claimed. Specifically, selecting "USB (keyboard)" requires the TOE to claim FDP_RIP.1/KM and selecting both "USB (keyboard)" and "USB (mouse)" requires the TOE to claim FDP_SWI_EXT.3.

FDP_UDF_EXT.1/KM Unidirectional Data Flow (Keyboard/Mouse)

FDP_UDF_EXT.1.1/KM The TSF shall ensure **[*selection: keyboard, mouse*]** data transits the TOE unidirectionally from the [*TOE [selection: keyboard, mouse]*] peripheral interface(s) to the [*TOE [selection: keyboard, mouse]*] interface.

Application Note: *Caps Lock, Num Lock, and Scroll Lock indications may be displayed by the TOE while still not passing that information to the keyboard.*

5.3 TOE Security Assurance Requirements

This PP-Module does not define any 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 offers 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 specific to keyboard and mouse input devices. One of the functions of the device must be the ability for it to support keyboard and/or mouse input devices. The requirements of this PP-Module 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.EMULATED_INPUT	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 emulation of keyboard/mouse input.
O.UNIDIRECTIONAL_INPUT	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 keyboard and mouse 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 keyboard and mouse 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	
FAU_GEN.1	There is no change to this SFR in this PP-Module. However, because this PP-Module includes a condition that would require it to be included in the TOE boundary, the SFR is treated as selection-based when this PP-Module is claimed.
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.

PP-Module Requirement	Consistency Rationale
FDP_PDC_EXT.1	This SFR is not modified by the PP-Module. It adds keyboard/mouse devices to the set of authorized devices, which are specific types of peripherals not specified in the PSD PP.
FDP_SWI_EXT.2	There is no modification to this SFR in this PP-Module. However, there are additional Evaluation Activities for this SFR that are specific to keyboard and mouse devices.
FIA_UAU.2	There is no change to this SFR in this PP-Module. However, because this PP-Module includes a condition that would require it to be included in the TOE boundary, the SFR is treated as selection-based when this PP-Module is claimed.
FIA_UID.2	There is no change to this SFR in this PP-Module. However, because this PP-Module includes a condition that would require it to be included in the TOE boundary, the SFR is treated as selection-based when this PP-Module is claimed.
FMT_MOF.1	There is no change to this SFR in this PP-Module. However, because this PP-Module includes a condition that would require it to be included in the TOE boundary, the SFR is treated as selection-based when this PP-Module is claimed.
FMT_SMF.1	There is no change to this SFR in this PP-Module. However, because this PP-Module includes a condition that would require it to be included in the TOE boundary, the SFR is treated as selection-based when this PP-Module is claimed.
FMT_SMR.1	There is no change to this SFR in this PP-Module. However, because this PP-Module includes a condition that would require it to be included in the TOE boundary, the SFR is treated as selection-based when this PP-Module is claimed.
FPT_STM.1	There is no change to this SFR in this PP-Module. However, because this PP-Module includes a condition that would require it to be included in the TOE boundary, the SFR is treated as selection-based when this PP-Module is claimed.
Mandatory SFRs	
FDP_PDC_EXT.2/KM	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/KM	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/KM	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	
FDP_FIL_EXT.1.1/KM	This SFR defines specific handling for keyboard/mouse peripheral devices. This does not prevent the enforcement of any PSD PP SFRs.

PP-Module Requirement	Consistency Rationale
FDP_RDR_EXT.1	This SFR defines specific handling for keyboard/mouse peripheral devices. This does not prevent the enforcement of any PSD PP SFRs.
Selection-Based SFRs	
FDP_RIP.1/KM	This SFR defines specific handling for keyboard peripheral devices. This does not prevent the enforcement of any PSD PP SFRs.
FDP_SWI_EXT.3	This SFR defines specific handling for keyboard/mouse peripheral devices. This does not prevent the enforcement of any PSD PP 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

A.3.1 TOE Capability for Device Filtering

If the TSF supports fixed or configurable device filtration, the following SFRs must all be claimed or the functionality disabled:

- FDP_FIL_EXT.1/KM – The TSF must perform at least one of fixed or configurable device filtration, such that blacklisted devices are rejected by the TSF and whitelisted devices are accepted by the TSF unless the device is also blacklisted, in which case the blacklist takes precedent.

FDP_FIL_EXT.1/KM Device Filtering (Keyboard/Mouse)

FDP_FIL_EXT.1.1/KM The TSF shall have [*selection: configurable, fixed*] device filtering for **[*selection: keyboard, mouse*]** interfaces.

FDP_FIL_EXT.1.2/KM The TSF shall consider all [*PSD KM*] blacklisted devices as unauthorized devices for **[*selection: keyboard, mouse*]** interfaces in peripheral device connections.

FDP_FIL_EXT.1.3/KM The TSF shall consider all [*PSD KM*] whitelisted devices as authorized devices for **[*selection: keyboard, mouse*]** interfaces in peripheral device connections only if they are not on the [*PSD KM*] blacklist or otherwise unauthorized.

Application Note: *The ST author must make the selections for the device which the TOE has: configurable or fixed or both; and keyboard or mouse or both.*

A.3.2 TOE Capability for Rejection of Re-Enumerated Devices

If the TSF supports rejection of re-enumerated devices, the following SFRs must all be claimed or the functionality disabled:

- FDP_RDR_EXT.1 – The TSF must be able to reject any devices that attempt to re-enumerate as a different type of device.

FDP_RDR_EXT.1 Re-Enumeration Device Rejection

FDP_RDR_EXT.1.1 The TSF shall reject any device that attempts to enumerate again as a different unauthorized device.

Application note: *This SFR should prevent devices that change their class from authorized to unauthorized, but cannot prevent malicious devices that use an authorized HID-class.*

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_RIP.1/KM Residual Information Protection (Keyboard Data)

FDP_RIP.1.1/KM The TSF shall ensure that any **keyboard data in volatile memory** is **purged** upon **switching computers**.

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.1.1 in the PSD PP and if "USB (keyboard)" is chosen as a selection in FDP_PDC_EXT.2.1/KM.*

FDP_SWI_EXT.3 Tied Switching

FDP_SWI_EXT.3.1 The TSF shall ensure that [*connected keyboard and mouse peripheral devices*] are always switched together to the same connected computer.

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.1.1 in the PSD PP and if both "USB (keyboard)" and "USB (mouse)" are chosen as selections in FDP_PDC_EXT.2.1/KM.*

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_FIL_EXT Device Filtering
	FDP_PDC_EXT Peripheral Device Connection
	FDP_RDR_EXT Re-Enumeration Device Rejection
	FDP_SWI_EXT PSD Switching
	FDP_UDF_EXT Unidirectional Data Flow

C.1 FDP_FIL_EXT Device Filtering

Family Behavior

Components in this family define the requirements for device filtering.

Component Leveling

FDP_FIL_EXT.1 Device Filtering, requires the TSF to specify the method of device filtering used for peripheral interfaces and defines requirements for handling whitelists and blacklists.

Management: FDP_FIL_EXT.1

The following actions could be considered for the management functions in FMT:

- Ability to configure whitelist/blacklist members

Audit: FDP_FIL_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Configuration of whitelist/blacklist members

FDP_FIL_EXT.1 Device Filtering

Hierarchical to: No other components

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

FDP_FIL_EXT.1.1 The TSF shall have [*selection: configurable, fixed*] device filtering for [*assignment: list of supported peripheral interface types*] interfaces.

FDP_FIL_EXT.1.2 The TSF shall consider all [*assignment: blacklist name*] blacklisted devices as unauthorized devices for [*assignment: list of supported peripheral interface types*] interfaces in peripheral device connections.

FDP_FIL_EXT.1.3 The TSF shall consider all [*assignment: whitelist name*] whitelisted devices as

authorized devices for peripheral device connections only if they are not on the [*assignment: blacklist name*] blacklist or otherwise unauthorized.

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 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 physical/logical interfaces supported by the TOE 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.

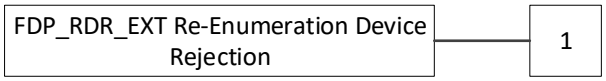
FDP_PDC_EXT.3.2 The TSF shall apply the following rules to the supported protocols: [*assignment: rules defining the handling for communications over this protocol (e.g. any processing that must be done by the TSF prior to transmitting it through the TOE, circumstances or frequency with which the protocol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

C.3 FDP_RDR_EXT Re-Enumeration Device Rejection

Family Behavior

Components in this family define requirements to reject device spoofing attempts through re-enumeration.

Component Leveling



FDP_RDR_EXT.1 Re-Enumeration Device Rejection, requires the TSF to reject re-enumeration as an unauthorized device.

Management: FDP_RDR_EXT.1

No specific management functions are identified.

Audit: FDP_RDR_EXT.1

There are no specific auditable events foreseen.

FDP_RDR_EXT.1 Re-Enumeration Device Rejection

Hierarchical to: No other components

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

FDP_RDR_EXT.1.1 The TSF shall reject any device that attempts to enumerate again as a different unauthorized device.

C.4 FDP_SWI_EXT PSD Switching

Family Behavior

This family is defined in the PSD PP. This PP-Module augments the extended family by adding one additional component, FDP_SWI_EXT.3. 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_SWI_EXT.3 Tied Switching, requires the TSF to ensure that multiple connected peripherals are always switched to the same connected computer.

Management: FDP_SWI_EXT.3

No specific management functions are identified.

Audit: FDP_SWI_EXT.3

There are no specific auditable events foreseen.

FDP_SWI_EXT.3 Tied Switching

Hierarchical to: No other components

Dependencies: FDP_SWI_EXT.1 PSD Switching,

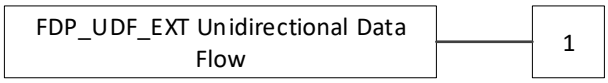
FDP_SWI_EXT.3.1 The TSF shall ensure that [*assignment: two or more tied peripheral devices*] are always switched together to the same connected computer.

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 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:

- USB audio input device connected to a KM peripheral interface
- USB audio output device connected to a KM peripheral interface
- USB camera
- USB printer
- USB user authentication device connected to a TOE keyboard/mouse peripheral interface
- USB wireless LAN dongle
- Non-HID device classes of a composite device connected to a TOE KM peripheral interface
- Any other device not specifically authorized
- Any other device class 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 and functions:

- Barcode reader
- Keyboard or keypad
- Mouse, touchscreen, trackball, or trackpad
- PS/2 to USB adapter
- USB device identified as HID class
- USB hub
- HID functions of a composite device connected to a TOE KM peripheral interface

E.5 Authorized Interface Protocols

The following are authorized interface protocols:

- USB

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 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/KM and FDP_APC_EXT.1/AO, 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.

KM functionality 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/KM 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.

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/KM 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-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
HID	Human Interface Device
OSP	Organizational Security Policies
PSD	Peripheral Sharing Device
PSD PP	Peripheral Sharing Device Protection Profile
SFR	Security Functional Requirement
USB	Universal Serial Bus