PP-Module for User Authentication Devices

Version: 1.0

2019-07-19

National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2019-07-19	Initial draft

Table of Contents

1 Introduction

1.1 Overview

The scope of this PP-Module is to describe the security functionality of a specific type of Peripheral Sharing Device (PSD) product in terms of [CC] and to define functional and assurance requirements for such products. A TOE that claims conformance to this PP-Module must also claim conformance to the Peripheral Sharing Device Protection Profile (PSD PP), Version 4.0. This is because the PSD PP is a generic Protection Profile aimed at defining baseline requirements and assurance activities for a wide variety of PSD products but more specific requirements and assurance activities apply depending on the types of physical and logical interfaces provided by a PSD. Therefore, additional Security Functional Requirements (SFRs) have been defined in this PP-Module to define security functionality that is unique to a PSD that provides the ability to support user authentication devices.

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.
Configurable Device Filtration (CDF)	PSD function that qualifies (accepts or rejects) peripheral devices based on field-configurable parameters or whitelist / blacklist.
Disconnection of authentication element	Removal of the authentication element, disconnection of a peripheral authentication device (if possible), or switching to a different connected computer (if possible).
External Authentication Device	An authentication device that has an exposed USB interface.
Fixed Device Filtration (FDF)	PSD function that qualifies (accepts or rejects) peripheral devices based on fixed parameters loaded during production.
Internal Authentication Device	An authentication device that has no exposed interface.
Removal of authentication element	Removal of smart-card, token, or proximity card from the authentication device reader.
USB Dummy Load	A USB Type A plug with resistor connected between positions 1 and 4 and used to simulate overloading a TOE USB peripheral device interface.
User Authentication Device	A peripheral device used to authenticate the identity of the user, such as a smart-card reader, biometric authentication device, or proximity card reader.
User Authentication Session	The exchange of user credentials – typically a user token presented through a User Authentication Device – and the Selected Computer.
User Authentication Session Information	User data for user authentication devices.
Whitelist	List containing one or more device attributes that will cause the TOE to accept the devices having that attribute (unless specifically blacklisted).

1.3 Compliant Targets of Evaluation

Any Target of Evaluation (TOE) that conforms to the PSD PP and includes user authentication device functionality is considered to be a candidate TOE for claiming conformance to this PP-Module. In

particular, a compliant TOE is expected to support one or more user authentication devices for one or more connected computers.

A compliant TOE will have a USB protocol connection for the TOE computer interface and can implement the TOE peripheral connection in the following ways:

- External - The TOE supports an external user authentication device with an exposed USB interface, and whose functionality may be separated from the PSD.
- Internal - The TOE implements an internal user authentication device whose functionality may not be separated from the PSD.

A compliant TOE will not emulate the user authentication device or support simultaneous user authentication sessions across multiple computers.

All of the requirements and restrictions that are defined in the PSD PP apply to a conformant TOE. A compliant TOE will also satisfy all of the specific data protection/isolation capabilities that are required by this PP-Module. A compliant TOE will embody one or more of the use cases defined in the PSD PP. It may also provide PSD functionality for additional types of computer interfaces (e.g. keyboard/mouse). In this case, the TOE will claim conformance to all applicable PP-Modules.

1.3.1 TOE Boundary

The TOE boundary is the same as that which is defined for a Peripheral Sharing Device in general. Refer to the PSD PP for an outline of the TOE boundary. A TOE that claims conformance to this PP-Module is not prevented from claiming conformance to other PSD PP-Modules; all relevant PP-Modules should be claimed by the TOE based on the specific types of functionality that it provides.

1.4 Use Cases

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

2 Conformance Claims

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

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

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

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

- Protection Profile for Peripheral Sharing Device, Version 4.0
- PP-Module for Analog Audio Output Devices, Version 1.0
- PP-Module for Keyboard/Mouse Devices, Version 1.0
- PP-Module for Video/Display Devices, Version 1.0

3 Security Problem Description

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its operational environment, and any organizational security policies that the TOE is expected to enforce.

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

3.1 Threats

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

Note however that the SFRs defined in this PP-Module are defined to mitigate the following PSD PP threats specifically for a TOE that includes this functionality:

- T.DATA_LEAK, T.RESIDUAL_LEAK, T.SIGNAL_LEAK (for all TOEs, because of the possibility of data being transmitted to an incorrect computer)
- T.UNAUTHORIZED_DEVICES (for all TOEs, because of the fact that devices other than user authentication devices can be connected to the TOE via USB)

3.2 Assumptions

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

3.3 Organizational Security Policies

This PP-Module defines no OSPs.

4 Security Objectives

4.1 Security Objectives for the TOE

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 user authentication 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 user authentication devices:

- FDP_APC_EXT.1 (modified from PSD PP definition), FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1 (modified from PSD PP definition), FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, and FDP_SWI_EXT.2 (modified from PSD PP definition).

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

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

O.USER_AUTHENTICATION_ISOLATION

The TOE shall isolate the user authentication function from all other TOE functions.

Addressed by: FDP_UAI_EXT.1

O.SESSION_TERMINATION

The TOE shall immediately terminate an open session with the selected computer upon disconnection of the authentication element.

Addressed by: FDP_TER_EXT.1, FDP_TER_EXT.2 (selection-based), FDP_TER_EXT.3 (selection-based)

4.2 Security Objectives for the Operational Environment

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

4.3 Security Objectives Rationale

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

Threat or Assumption	Security Objectives	Rationale
T.DATA_LEAK, T.RESIDUAL_LEAK, T.SIGNAL_LEAK	O.USER_AUTHENTICATION_ISOLATION	The TOE's user authentication function mitigates this threat by ensuring that the bidirectional channel between the device and the connected computer through the user authentication function is isolated from all other TOE functions.

Threat or Assumption	Security Objectives	Rationale
T.DATA_LEAK, T.RESIDUAL_LEAK, T.SIGNAL_LEAK, T.UNAUTHORIZED_DEVICES	O.SESSION_TERMINATION	The TOE mitigates the threat by ensuring that open sessions are terminated and no traffic flows upon disconnection of the authentication element.

Table 1: Security Objectives Rationale

5 Security Requirements

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

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 and refinements. This document uses the following font conventions to identify the operations defined by the CC.

- **Refinement** operation, denoted by **bold text**, 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 Base-PP requirements that are consistent with the functionality provided by the PP-Module. The following sections describe any Base-PP claims that must be made and any additional evaluation activities that must be performed when the TOE boundary includes the functionality described by this PP-Module.

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.

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/UA.

FDP_APC_EXT.1 Active PSD Connections

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 user authentication 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/UA" 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

Because of additions to the Peripheral Device Connections Policy, there is an additional application note and additional evaluation activities for this SFR.

Application Note: *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. If "internal" is the only selection made in FDP_PDC_EXT.4.1, then the TSF does not have to support USB as an authorized interface unless the KM PP-Module is also claimed by the ST author.*

FDP_SWI_EXT.2 PSD Switching Methods

There is no modification to this SFR in this PP-Module. However, there are additional Evaluation Activities defined in FDP_APC_EXT.1 in the Supporting Document Mandatory Technical Document PP-Module for User Authentication Devices.

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/UA.

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/UA.

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/UA.

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/UA.

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/UA.

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/UA.

5.2 TOE Security Functional Requirements

5.2.1 User Data Protection

FDP_FIL_EXT.1/UA Device Filtering (User Authentication Devices)

FDP_FIL_EXT.1.1/UA The TSF shall have [selection: *configurable, fixed*] device filtering for [*user authentication device*] interfaces.

Application Note: *The ST author must make the selection for the device which the TOE has: configurable, fixed or both.*

FDP_FIL_EXT.1.2/UA The TSF shall consider all [*PSD UA*] blacklisted devices as unauthorized devices for [*user authentication device*] interfaces in peripheral device connections.

FDP_FIL_EXT.1.3/UA The TSF shall consider all [*PSD UA*] whitelisted devices as authorized devices for [*user authentication device*] interfaces in peripheral device connections only if they are not on the [*PSD UA*] blacklist or otherwise unauthorized.

FDP_PDC_EXT.2/UA Authorized Devices (User Authentication Devices)

FDP_PDC_EXT.2.1/UA 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 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/UA 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 Video/Display Devices,***
- ***no other devices***

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

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

FDP_PDC_EXT.4 Supported Authentication Device

FDP_PDC_EXT.4.1 The TSF shall have an [selection: *internal, external*] user authentication device.

Application Note: *The ST author must make the selection for the device which the TOE has: internal, external or both.*

FDP_PWR_EXT.1 Powered By Computer

FDP_PWR_EXT.1.1 The TSF shall not be powered by a connected computer.

FDP_TER_EXT.1 Session Termination

FDP_TER_EXT.1.1 The TSF shall terminate an open session upon removal of the authentication element.

FDP_UAI_EXT.1 User Authentication Isolation

FDP_UAI_EXT.1.1 The TSF shall isolate the user authentication function from all other TOE USB functions.

Application Note: *This SFR requires additional information for the Isolation Documentation and Assessment. Refer to Appendix D for this information.*

5.3 TOE Security Assurance Requirements

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

6 Consistency Rationale

6.1 PSD Base

6.1.1 Consistency of TOE Type

The PSD PP defines the boundaries of a PSD – a device that 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 user authentication devices. One of the functions of the device must be the ability for it to support user authentication 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.USER_AUTHENTICATION_ISOLATION	The PSD PP does not specify how peripheral devices interface logically with connected computers so there is no PSD PP function that is affected by isolating the user authentication function from all other TOE USB.
O.SESSION_TERMINATION	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 terminating an open session with the selected computer upon disconnection of the authentication element.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the PSD PP needed to support user authentication 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 user authentication 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 modified by the PP-Module. It adds user authentication devices to the set of authorized peripherals, which are specific types of peripherals not specified in the PSD PP.

PP-Module Requirement	Consistency Rationale
FDP_SWI_EXT.2	This SFR is not modified by the PP-Module. It adds evaluation activities that are specific to this technology type but does not alter anything that the Base-PP requires.
Mandatory SFRs	
FDP_FIL_EXT.1/UA	This SFR defines device filtering specific to this PP-Module. This does not prevent the enforcement of any PSD PP SFRs.
FDP_PDC_EXT.2/UA	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.4	This SFR further defines whether the TOE includes an internal or external authentication device. This does not prevent the enforcement of any PSD PP SFRs.
FDP_PWR_EXT.1	This SFR requires the TSF not be powered by a connected computer. The Base-PP does not have any requirements for the TSF to be powered by a connected computer and therefore does not prevent the enforcement of any PSD PP SFRs.
FDP_TER_EXT.1	This SFR defines specific handling for user authentication peripheral devices. This does not prevent the enforcement of any PSD PP SFRs.
FDP_UAI_EXT.1	This SFR defines specific handling for user authentication peripheral devices. This does not prevent the enforcement of any PSD PP SFRs.
Optional SFRs	
This PP-Module defines no optional SFRs.	
Selection-Based SFRs	
FDP_TER_EXT.2	This SFR defines specific handling for user authentication devices. This does not prevent the enforcement of any PSD PP SFRs.
FDP_TER_EXT.3	This SFR defines specific handling for user authentication 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.

A.2 Objective Requirements

There are currently no objective requirements defined by this PP.

A.3 Implementation-Dependent Requirements

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

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.

FDP_TER_EXT.2 Session Termination of Removed Devices

FDP_TER_EXT.2.1 The TSF shall terminate an open session upon removal of the user authentication device.

Application Note: *This SFR must be claimed if "external" is selected in FDP_PDC_EXT.4.1/UA.*

FDP_TER_EXT.3 Session Termination upon Switching

FDP_TER_EXT.3.1 The TSF shall terminate an open session upon switching to a different computer.

FDP_TER_EXT.3.2 The TSF shall reset the power to the user authentication device for at least one second upon switching to a different computer.

Application Note: *This SFR must be claimed if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD-PP.*

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_PWR_EXT Powdered By Computer
	FDP_TER_EXT Session Termination
	FDP_UAI_EXT User Authentication Isolation

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.4. The 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.4 Supported Authentication Devices, defines whether the TSF includes an internal or external authentication device.

Management: FDP_PDC_EXT.2, FDP_PDC_EXT.4

No specific management functions are identified.

Audit: FDP_PDC_EXT.2, FDP_PDC_EXT.4

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.4 Supported Authentication Devices

Hierarchical to: No other components

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection,

FDP_PDC_EXT.2 Authorized Devices

FDP_PDC_EXT.4.1 The TSF shall have an [selection: *internal, external*] user authentication device.

C.3 FDP_PWR_EXT Powered by Computer

Family Behavior

Components in this family define the requirements for device powering.

Component Leveling

FDP_PWR_EXT.1 Powered by Computer, requires the TSF to not be powered by a connected computer.

Management: FDP_PWR_EXT.1

No specific management functions are identified.

Audit: FDP_PWR_EXT.1

There are no specific auditable events foreseen.

FDP_PWR_EXT.1 Powered by Computer

Hierarchical to: No other components

Dependencies: No dependencies

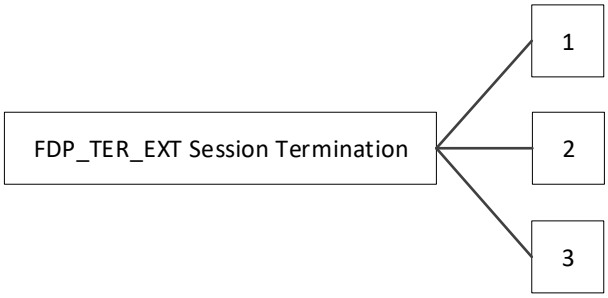
FDP_PWR_EXT.1.1 The TSF shall not be powered by a connected computer.

C.4 FDP_TER_EXT Session Termination

Family Behavior

Components in this family define the requirements for termination of open sessions.

Component Leveling



FDP_TER_EXT.1, Session Termination, requires the TSF to terminate an open session upon removal of the authentication element.

FDP_TER_EXT.2, Session Termination of Removed Devices, requires the TSF to terminate an open session upon removal of the user authentication device.

FDP_TER_EXT.3, Session Termination upon Switching, requires the TOE to terminate an open session upon switching to a different computer; and reset the power to the user authentication device for at least one second upon switching to a different computer.

Management: FDP_TER_EXT.1, FDP_TER_EXT.2, FDP_TER_EXT.3

No specific management functions are identified.

Audit: FDP_TER_EXT.1, FDP_TER_EXT.2, FDP_TER_EXT.3

There are no specific auditable events foreseen.

FDP_TER_EXT.1 Session Termination

Hierarchical to: No other components

Dependencies: No dependencies

FDP_TER_EXT.1.1 The TSF shall terminate an open session upon removal of the authentication element.

FDP_TER_EXT.2 Session Termination of Removed Devices

Hierarchical to: No other components

Dependencies: FDP_PDC_EXT.2 Authorized Devices

FDP_TER_EXT.2.1 The TSF shall terminate an open session upon removal of the user authentication device.

FDP_TER_EXT.3 Session Termination upon Switching

Hierarchical to: No other components

Dependencies: FDP_SWI_EXT.1 PSD Switching

FDP_TER_EXT.3.1 The TSF shall terminate an open session upon switching to a different computer**.**

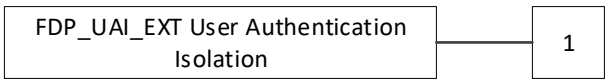
FDP_TER_EXT.3.2 The TSF shall reset the power to the user authentication device for at least one second upon switching to a different computer.

C.5 FDP_UAI_EXT User Authentication Isolation

Family Behavior

Components in this family define the requirements for user authentication isolation.

Component Leveling



FDP_UAI_EXT.1 User Authentication Isolation, requires the TSF to isolate the user authentication function from all other TOE USB functions.

Management: FDP_UAI_EXT.1

No specific management functions are identified.

Audit: FDP_UAI_EXT.1

There are no specific auditable events foreseen.

FDP_UAI_EXT.1 User Authentication Isolation

Hierarchical to: No other components

Dependencies: None

FDP_UAI_EXT.1.1 The TSF shall isolate the user authentication function from all other TOE USB functions.

D Isolation Documentation and Assessment

The TOE requires additional supplementary information to describe its isolation concepts beyond the requirements outlined in the 'Isolation Documentation and Assessment' sections in Appendix D of the Base-PP. As with other Base-PP requirements, 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 Base-PP. The following additions are included in the sections below.

D.1 General

The documentation of the isolation should be detailed enough that, after reading, the evaluator will thoroughly understand the isolation concepts and implementation in the TOE and why it can be relied upon to provide proper isolation of the user authentication function from all other TOE USB functions. The isolation documentation must be especially detailed for any internal user authentication devices.

D.2 Design Description

In addition to user authentication isolation from other TOE USB functions, if FDP_TER_EXT.3 is claimed by the ST, then when describing how power source or power loading may affect isolation between data paths, the documentation shall describe how power is reset to the user authentication device upon switching.

D.3 Isolation Means Justification

No change.

D.4 Firmware Dependencies

No change.

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:

- USB device that is black-listed
- USB audio input device connected to a user authentication peripheral interface
- USB audio output device connected to a user authentication peripheral interface
- USB camera
- USB keyboard connected to a user authentication peripheral interface
- USB printer
- USB wireless LAN dongle
- Any unauthorized device that presents itself to the PSD as a composite device and is connected to a user authentication peripheral interface
- 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 and functions:

- USB device identified as User Authentication
- USB device that is white-listed
- Internal authentication device

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

Both PP-Modules modify the Base-PP SFR FDP_APC_EXT.1 in ways that are specific to their respective peripheral types. The ST author should make two iterations of this SFR, FDP_APC_EXT.1/UA 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.

User authentication functionality must be isolated from KM 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/UA and FDP_APC_EXT.1/KM, 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.

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

G References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017
[PP_PSD_V4.0 or PSD PP]	Protection Profile for Peripheral Sharing Device, Version: 4.0, 2019-07-19

H Acronyms

Acronym	Meaning
OSP	Organizational Security Policies
PSD	Peripheral Sharing Device
PSD PP	Peripheral Sharing Device Protection Profile
SFR	Security Functional Requirement