Protection Profile for Peripheral Sharing Device

Version: 4.0
2019-07-19
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	8-August-2000	Initial Version
1.1	25-July-2007	Update to conform with CC V3.1
1.2	21-August-2008	Update to conform with additional parts of CC V3.1 r3
2.0	1-June-2010	Updates to assumptions, threats, and objectives
2.1	7-September-2010	Update to replace ROM requirement
3.0	13-February-2015	Update to conform with CC V3.1 r4 and substantial additional functionality
4.0	19-July-2019	Update to conform with CC V3.1 r5 and includes separation of security functionality into base Protection Profile and Protection Profile Modules based on interface type

Table of Contents

1 Introduction 5
1.1 Terms 5
1.1.1 Common Criteria Terms 5
1.1.2 Technology Terms 5
1.2 Compliant Targets of Evaluation 7
1.2.1 TOE Boundary 7
1.3 Use Cases 9

2 Conformance Claims 12

3 Security Problem Description 13
3.1 Threats 13
3.2 Assumptions 13
3.3 Organizational Security Policies 14

4 Security Objectives 15
4.1 Security Objectives for the TOE 15
4.2 Security Objectives for the Operational Environment 17
4.3 Security Objectives Rationale 17

5 Security Requirements 20
5.1 Test Environment for Evaluation Activities 20
5.2 TOE Security Functional Requirements 20
5.2.1 User Data Protection (FDP) 20
5.2.2 Protection of the TSF (FPT) 24
5.3 Security Assurance Requirements 28
5.3.1 Class ASE: Security Target 29
5.3.2 Class ADV: Development 29
5.3.3 Class AGD: Guidance Documentation 29
5.3.4 Class ALC: Life-cycle Support 30
5.3.5 Class ATE: Tests 31
5.3.6 Class AVA: Vulnerability Survey (AVA_VAN.1) 31

A Optional Requirements 33
A.1 Strictly Optional Requirements 33
A.2 Objective Requirements 33
A.3 Implementation-Dependent Requirements 33
A.3.1 TOE Capability for Configuration and Accounting 33
A.3.2 TOE Capability for Factory Reset 37
A.3.3 TOE Capability for Tamper Response 38

B Selection-Based Requirements 40
B.1 User Data Protection (FDP) 40
B.2 TOE Access (FTA) 41

C Extended Component Definitions 43
C.1 FDP_APC_EXT Active PSD Connections 43
C.2 FDP_PDC_EXT Peripheral Device Connection 44
C.3 FDP_RIP_EXT Residual Information Protection 44

C.4 FDP_SWI_EXT PSD Switching 45
C.5 FPT_FLS_EXT Failure with Preservation of Secure State 46
C.6 FPT_NTA_EXT No Access to TOE 47
C.7 FPT_TST_EXT TSF Testing 47
C.8 FTA_CIN_EXT Continuous Indications 48

D Isolation Documentation and Assessment 50
D.1 General 50
D.2 Design Description 50
D.3 Isolation Means Justification 50
D.4 Firmware Dependencies 50

E Peripheral Device Connections 51
E.1 General 51
E.2 Unauthorized Peripheral Devices 51
E.3 Unauthorized Interface Protocols 51

F Rationale 52
F.1 SFR Dependencies Analysis 52
F.2 Security Functional Requirement to Objective Mapping & Analysis 52

G References 55

H Acronyms 56

1 Introduction

This Protection Profile (PP) describes common security requirements for Peripheral Sharing Devices (PSDs). A PSD is a device that provides a mechanism for securely connecting a set of peripherals to one or more attached computers. This Base-PP may be used in conjunction with one or more PP-Modules that describe the specific functional interfaces of that PSD type (i.e., audio, video, keyboard, user authentication device, or mouse), as described in section 2.

1.1 Terms

The following sections provide both Common Criteria and technology terms used in this PP.

1.1.1 Common Criteria Terms

Term	Definition
Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	Implementation-independent documentation that describes a TOE, its Operational Environment, and its claimed security functionality.
Target of Evaluation (TOE)	A product or component, consisting of hardware, software, and/or firmware, that claims to implement certain security functionality in a specific and well-defined manner.
TOE Security Functionality (TSF)	The combined hardware, software, and firmware capabilities of a TOE that are responsible for implementation of its claimed SFRs.
TOE Security Functionality Interface (TSFI)	Any external interface between the TOE and its Operational Environment that has a security-relevant purpose or is used to transmit security-relevant data.
TOE Summary Specification (TSS)	Documentation contained within the Security Target that provides the reader with a description of how the TOE implements the claimed SFRs.

1.1.2 Technology Terms

Term	Definition
Active Interface/Connection	An Interface between a PSD and Device that currently has user data flowing through it.
Administrator	A person who administers (e.g., installs, configures, updates, audits, maintains) a PSD, Connected Peripherals, and Connections.

Term	Definition
Authorized Peripheral	A Peripheral Device that is both technically supported and administratively permitted to have an active interface with the PSD.
Configurable Device Filtration (CDF)	A PSD function that filters traffic based on properties of a connected peripheral device and criteria that are configurable by an Administrator.
Combiner (multi-viewer)	A PSD with video integration functionality. Used to simultaneously display output from multiple personal computers (PCs).
Computer Interface	The PSD's physical receptacle or port for connecting to a computer.
Connected Computer	A computing device connected to a PSD. May be a personal computer, server, tablet, or any other computing device.
Connected Peripheral	A Peripheral that is connected to a PSD.
Connection	A physical or logical conduit that enables Devices to interact through respective interfaces. May consist of one or more physical (e.g., a cable) or logical (e.g., a protocol) components.
Connector	The plug on a Connection that attaches to a Computer or Peripheral Interface.
Device	An information technology product. In the context of this PP, a Device is a PSD, a Connected Computer, or a Connected Peripheral.
Display	A device that visually outputs user data, such as a monitor.
Guard	A PSD function that requires multiple express user actions in order to switch between Connected Computers using Connected Peripherals.
Interface	A shared boundary across which two or more Devices exchange information through a Connection.
Isolator or Filter	A PSD with a single Connected Computer.
KM	A type of PSD that shares a keyboard and pointing device between Connected Computers. A KM may optionally include an analog audio device.
KVM	A type of PSD that shares a keyboard, video, and pointing device between Connected Computers. A KVM may optionally include an analog audio device and user authentication device.
Letter of Volatility	A letter issued by the manufacturer outlining whether onboard memory can store data when the device is powered off (non-volatile) or not (volatile).
Monitoring	The ability of a User to receive an indicator of the current Active Interface.
Non-Selected Computer	A Connected Computer that has no Active Interfaces with the PSD.
Peripheral/Peripheral Device	A Device with access that can be Shared or Filtered by a PSD.
Peripheral Interface	The PSD's physical receptacle or port for connecting to a Peripheral Device.
Remote Controller	Remote component of the PSD that extends the controls and indications through a cable.

Term	Definition
Secure State	An operating condition in which the PSD disables all connected peripheral and connected computer interfaces when the correctness of its functions cannot be ensured.
Selected Computer	A Connected Computer that has Active Interfaces with the PSD.
Supported Peripheral	A Peripheral Device that is technically supported by the PSD
Touch Screen	A pointing device Peripheral Device that enable users to touch one or more objects on the screen or to point the cursor device to specific locations.
User	A person that interacts with a PSD (or a process or mechanism acting on behalf of a person).
User Authentication Device	A Peripheral Device that is used to affirm the identity of a User attempting to authenticate to a computer (e.g., smart card reader, biometric authentication device, proximity card reader).
User Data	Information that the User inputs to the Connected Computer or is output to the User from the Connected Computer (and including user authentication and credential information)
Video Wall	A tiled set of displays that allow the video output from a single Selected Computer to be spanned across multiple individual displays.

1.2 Compliant Targets of Evaluation

In the context of this PP, a PSD is an IT product for connecting one or more peripheral devices to one or more computers such that data cannot flow between computers by way of the peripherals or the PSD. Examples of PSDs that can claim compliance to this PP include Keyboard, Video, Mouse (KVM) switches; Keyboard, Mouse (KM) switches; and Isolators.

A PSD may be composed of one or more hardware components or platforms, and its software or firmware. It may include cables and accessories. PSDs that support more than one computer include a user interface that includes a visible indication of the selected computer interface and a mechanism for changing the selected computer interface. The user interface can be implemented on the chassis of the PSD using, for example, a touch screen or lights and buttons, or as part of a wired remote control.

An Isolator or Filter PSD is a device that provides the same security functions as a KVM but only to a single connected computer. Isolators do not require continuous display of the active interface.

1.2.1 TOE Boundary

The TOE boundary is limited to the PSD itself. The TOE's operational environment consists of one or more connected peripherals or computers. The typical usage of a multi-computer PSD involves mapping interfaces between multiple computers such that the user is able to interact with the selected computers. In this case, the TOE includes a user interface that allows a user to select the active computer. The user interface includes an indicator identifying the currently selected computer. Typical PSD usage is illustrated in Figure 1 below.

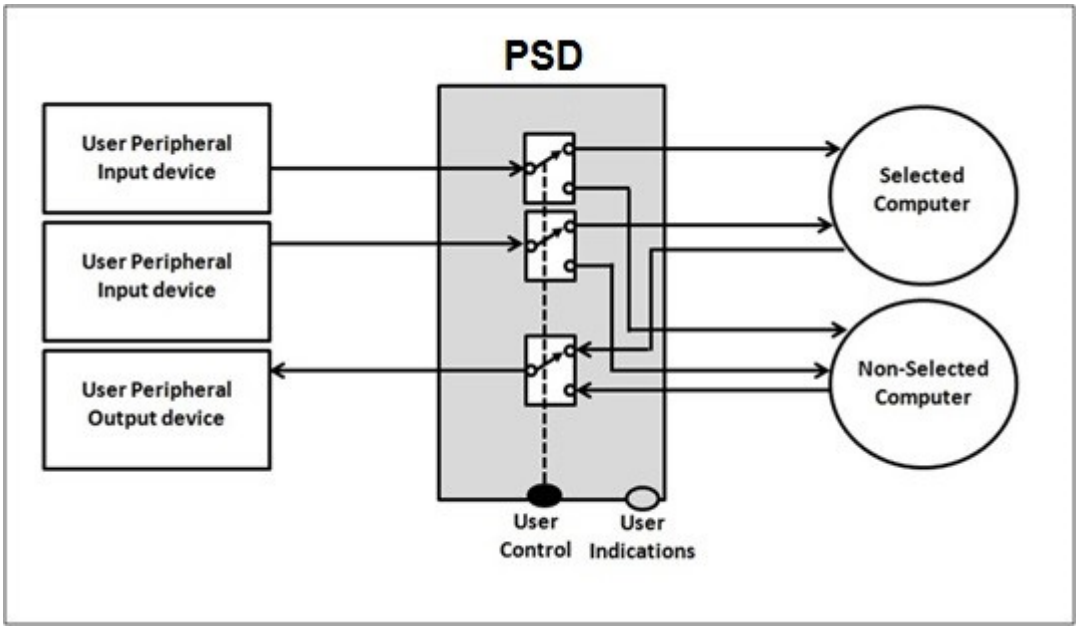


Figure 1: Simplified PSD Block Diagram

PSD Compliance Guidelines

Connected peripheral devices, computer platforms, and connecting cables are not covered under this PP, but may be addressed by another PP. Nevertheless, testing of the TOE requires a complete setup that includes computers, cables, and peripheral devices.

PSDs covered by this PP:

- May support one or more types of peripherals specified in the PP-Modules that extend this PP (e.g., video display or keyboard/mouse).
- Must be connected to one or more computers.
- May comprise one or more connected sub-systems (e.g., one KM device and one video device connected with cables or wires).
- Must not support more than one of each peripheral device type except for display or audio output devices.
- Must support only single users; a PSD may not be shared among users.

The following list includes additional characteristics that a conformant TOE must have or may have:

- PSD connected devices are limited as per the Peripheral Device Connections (Appendix E).
- A single user may use more than one PSD instance at a time.
- The PSD monitoring and control functions are optional. If supported, these functions shall be built-in to the PSD chassis or implemented as part of a wired remote control.
- PSD indicators must be implemented in such a way as to be visible to the user at all times.
- PSDs may have non-tactile user controls (e.g., multi-touch windows).
- Connected Computers may have one or more peripheral devices that bypass the PSD (i.e., peripherals that are connected directly to a computer).
- The PSD user display may present one-to-many computers' video output simultaneously if displays are a peripheral type supported by the TOE.

1.3 Use Cases

The following use cases are examples of PSDs covered by this PP:

[USE CASE 1] Single user with PSD, local monitoring, and local control

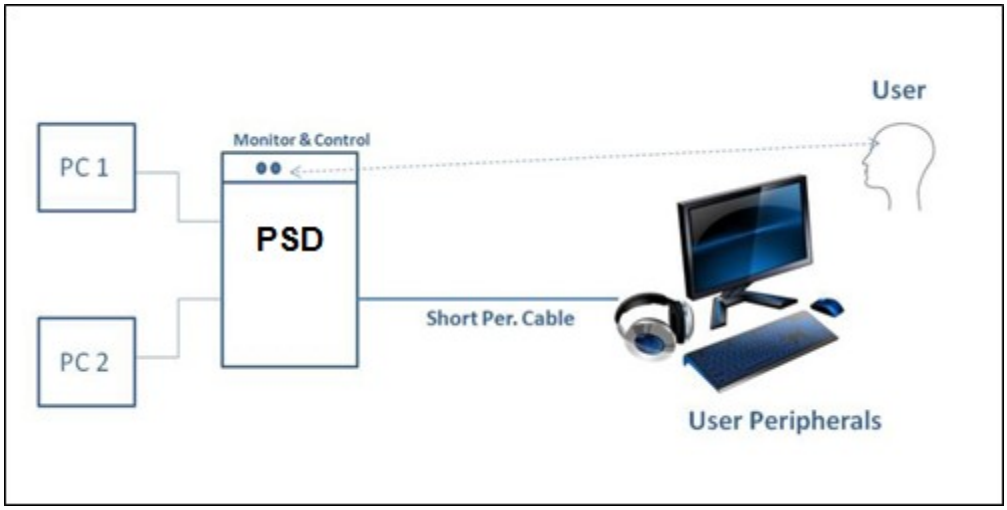


Figure 2: Single user with PSD, local monitoring, and local control

In this use case, the user controls the PSD through a user interface on the PSD itself or through a directly connected remote controller. Peripheral devices are connected directly to the PSD using cables. Since the PSD resides in close physical proximity to the user, the user is expected to have physical access and full visibility of the PSD monitoring and control functions.

PSDs implementing this use case may support any type of supported peripheral as defined in this PP and its associated PP-Modules.

Note that the Operational Environment of this PSD may include peripherals that are connected directly to the connected computers (unconnected to the PSD) and multiple peripherals of the same type (for display or audio output only) each connected to the PSD, as shown in the figures below:

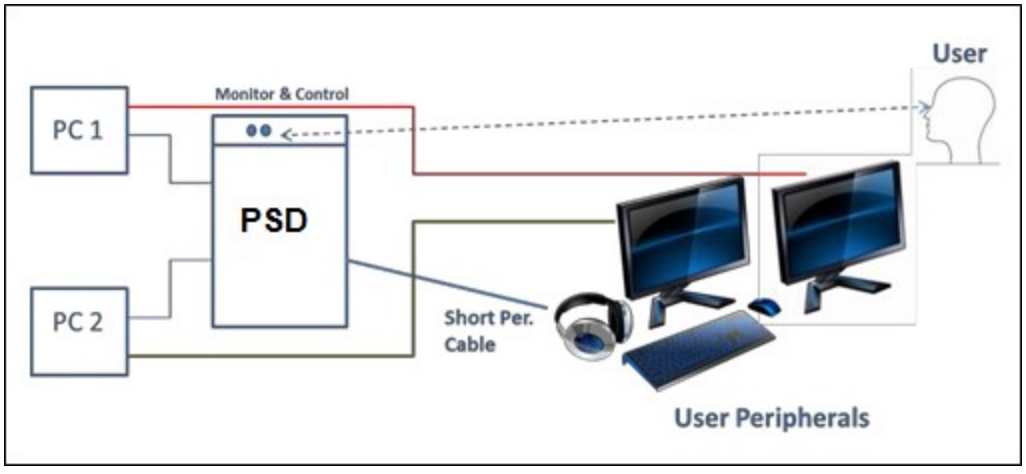


Figure 3: Single user with KM PSD and peripheral(s) connected directly to computers

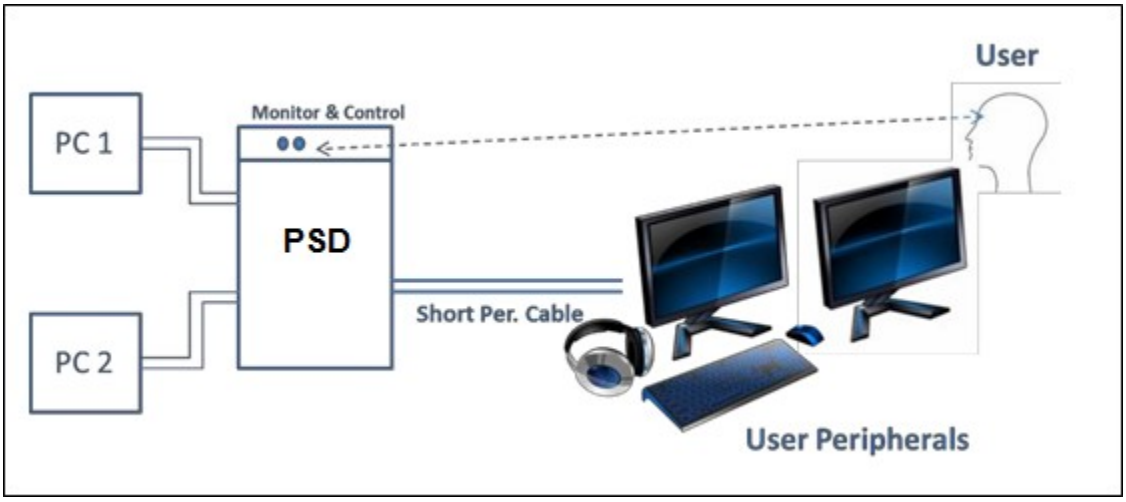


Figure 4: Single user with PSD and multiple peripherals of the same type

[USE CASE 2] Single user with PSD and a single computer (Isolator or Filter)

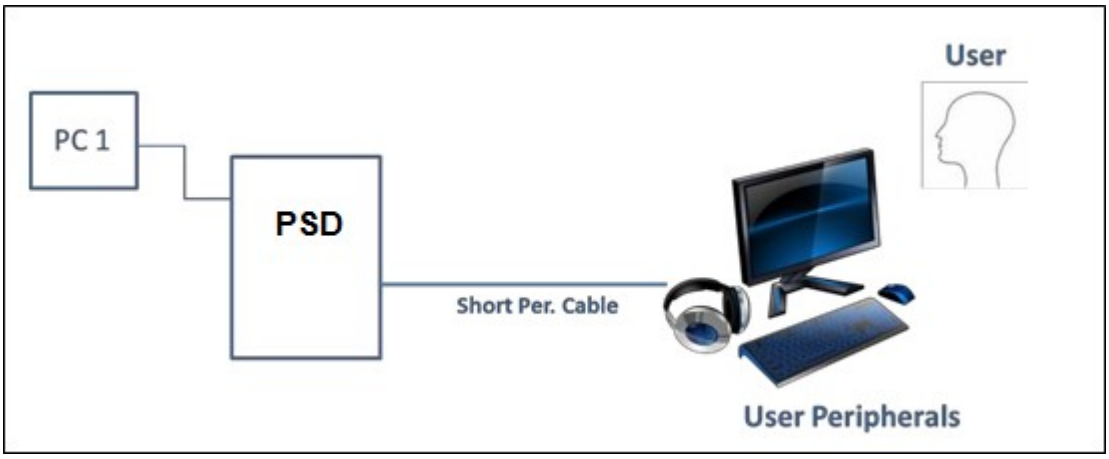


Figure 5: Single user with PSD and a single computer (Isolator or Filter)

In this use case, the PSD sits between a set of connected peripherals and a single connected computer. The connected computer may change over time, such as different laptops connected to an Isolator or Filter that persistently resides in a conference room. Once again, this use case does not specifically mandate or exclude the use of any one type of peripheral that is defined by this PP and its PP-Modules.

[USE CASE 3] PSD with single integrated video display (Combiner or Multi-Viewer)

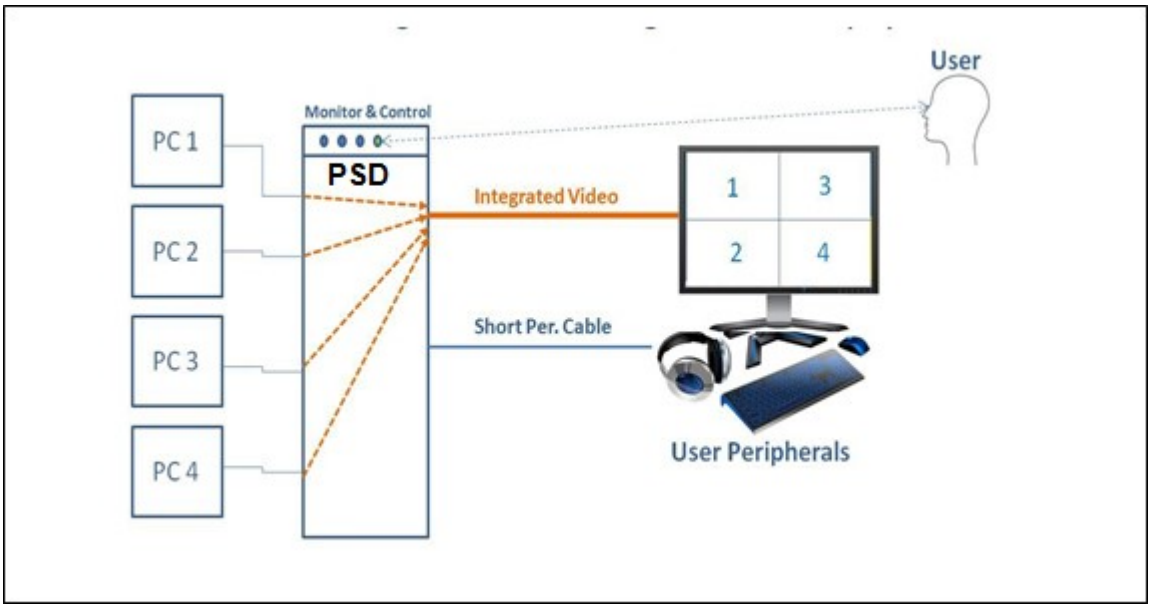


Figure 6: PSD with single integrated video display (combiner or multi-viewer)

A Combiner is used to simultaneously display output from multiple connected computers to one or more display devices. A Combiner PSD may combine the display output from multiple connected computers onto a single monitor (as shown in Figure 6 above) or output the display from one connected computer to be spanned onto multiple tiled or overlapping displays (e.g., a video wall). Any PSD TOE that claims to support this use case must have the ability to support display peripherals. Other supported peripherals can be claimed at the ST author's discretion.

2 Conformance Claims

An ST must claim exact conformance to this PP, as defined in the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

This PP is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Revision 5 [CC].

This PP does not claim conformance to any Protection Profile.

This PP does not claim conformance to any packages.

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

- PP-Module for Audio Input Devices, Version 1.0
- 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
- PP-Module for Video/Display Devices, Version 1.0

3 Security Problem Description

3.1 Threats

The threats for the PSD are listed in the sections below. The description of each threat is then followed by a rationale describing how it is addressed by the SFRs in the following chapters.

T.DATA_LEAK

A connection via the PSD between one or more computers may allow unauthorized data flow through the PSD or its connected peripherals.

T.SIGNAL_LEAK

A connection via the PSD between one or more computers may allow unauthorized data flow through bit-by-bit signaling.

T.RESIDUAL_LEAK

A PSD may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer.

T.UNINTENDED_USE

A PSD may connect the user to a computer other than the one to which the user intended to connect.

T.UNAUTHORIZED_DEVICES

The use of an unauthorized peripheral device with a specific PSD peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSD or its connected computers.

T.LOGICAL_TAMPER

An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code or data stored in the PSD's volatile or non-volatile memory to allow unauthorized information flows.

T.PHYSICAL_TAMPER

A malicious user or human agent could physically modify the PSD to allow unauthorized information flows.

T.REPLACEMENT

A malicious human agent could replace the PSD during shipping, storage, or use with an alternate device that does not enforce the PSD security policies.

T.FAILED

Detectable failure of a PSD may cause an unauthorized information flow or weakening of PSD security functions.

3.2 Assumptions

This section describes the assumptions made in identification of the threats and security requirements for PSD. The PSD is not expected to provide assurance in any of these areas, and as a result, requirements are not included to mitigate the threats associated.

A.NO_TEMPEST

Computers and peripheral devices connected to the PSD are not TEMPEST approved.

A.PHYSICAL

The environment provides physical security commensurate with the value of the TOE and the data it processes and contains.

A.NO_WIRELESS_DEVICES

The environment includes no wireless peripheral devices.

A.TRUSTED_ADMIN

PSD Administrators and users are trusted to follow and apply all guidance in a trusted manner.

A.TRUSTED_CONFIG

Personnel configuring the PSD and its operational environment follow the applicable security configuration guidance.

A.USER_ALLOWED_ACCESS

All PSD users are allowed to interact with all connected computers. It is not the role of the PSD to prevent or otherwise control user access to connected computers. Computers or their connected network shall have the required means to authenticate the user and to control access to their various resources.

3.3 Organizational Security Policies

This Protection Profile does not define any organizational security policies.

4 Security Objectives

4.1 Security Objectives for the TOE

The Security Problem described in Section 3 will be addressed by a combination of PSD capabilities, with the understanding that the PSD is installed in a manner to which it can effectively enforce its policies. Conformant PSDs will provide security functionality that addresses threats to the TOE. The following subsections provide a description of the security objectives required to meet the threats and assumptions previously discussed. Note: in each subsection below particular security objectives are identified (highlighted by O.) and they are matched with the associated security functional requirements (SFRs) that provide the mechanisms to satisfy the objectives.

O.COMPUTER_INTERFACE_ISOLATION

The PSD shall prevent unauthorized data flow to ensure that the PSD and its connected peripheral devices cannot be exploited in an attempt to leak data. The TOE-Computer interface shall be isolated from all other PSD-Computer interfaces while TOE is powered.

Addressed by: FDP_APC_EXT.1

O.COMPUTER_INTERFACE_ISOLATION_ TOE_UNPOWERED

The PSD shall not allow data to transit a PSD-Computer interface while the PSD is unpowered.

Addressed by: FDP_APC_EXT.1

O.USER_DATA_ISOLATION

The PSD shall route user data, such as keyboard entries, only to the computer selected by the user. The PSD shall provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.

Addressed by: FDP_APC_EXT.1

O.NO_USER_DATA_RETENTION

The PSD shall not retain user data in non-volatile memory after power up or, if supported, factory reset.

Addressed by: FDP_RIP_EXT.1, FDP_RIP_EXT.2 (optional)

O.NO_OTHER_EXTERNAL_INTERFACES

The PSD shall not have any external interfaces other than those implemented by the TSF.

Addressed by: FDP_PDC_EXT.1

O.LEAK_PREVENTION_SWITCHING

The PSD shall ensure that there are no switching mechanisms that allow signal data leakage between connected computers.

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

O.AUTHORIZED_USAGE

The TOE shall explicitly prohibit or ignore unauthorized switching mechanisms, either because it supports only one connected computer or because it allows only authorized mechanisms to switch between connected computers. Authorized switching mechanisms shall require express user action restricted to console buttons, console switches, console touch screen, wired remote control, and

peripheral devices using a guard. Unauthorized switching mechanisms include keyboard shortcuts, also known as “hotkeys,” automatic port scanning, control through a connected computer, and control through keyboard shortcuts. Where applicable, the results of the switching activity shall be indicated by the TSF so that it is clear to the user that the switching mechanism was engaged as intended.

A conformant TOE may also provide a management function to configure some aspects of the TSF. If the TOE provides this functionality, it shall ensure that whatever management functions it provides can only be performed by authorized administrators and that an audit trail of management activities is generated.

Addressed by: FAU_GEN.1 (optional), FDP_SWI_EXT.1, FDP_SWI_EXT.2 (selection-based), FIA_UAU.2 (optional), FIA_UID.2 (optional), FMT_MOF.1 (optional), FMT_SMF.1 (optional), FMT_SMR.1 (optional), FPT_STM.1 (optional), FTA_CIN_EXT.1 (selection-based)

O.PERIPHERAL_PORTS_ISOLATION

The PSD shall ensure that data does not flow between peripheral devices connected to different PSD interfaces.

Addressed by: FDP_APC_EXT.1

O.REJECT_UNAUTHORIZED_PERIPHERAL

The PSD shall reject unauthorized peripheral device types and protocols.

Addressed by: FDP_PDC_EXT.1

O.REJECT_UNAUTHORIZED_ENDPOINTS

The PSD shall reject unauthorized peripheral devices connected via a Universal Serial Bus (USB) hub.

Addressed by: FDP_PDC_EXT.1

O.NO_TOE_ACCESS

The PSD firmware, software, and memory shall not be accessible via its external ports.

Addressed by: FPT_NTA_EXT.1

O.TAMPER_EVIDENT_LABEL

The PSD shall be identifiable as authentic by the user and the user must be made aware of any procedures or other such information to accomplish authentication. This feature must be available upon receipt of the PSD and continue to be available during the PSD deployment. The PSD shall be labeled with at least one visible unique identifying tamper-evident marking that can be used to authenticate the device. The PSD manufacturer must maintain a complete list of manufactured PSD articles and their respective identification markings’ unique identifiers.

Addressed by: FPT_PHP.1

O.ANTI_TAMPERING

The PSD shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the PSD would be evident, and optionally thwarted through disablement of the TOE. Note: This applies to a wired remote control as well as the main chassis of the PSD.

Addressed by: FPT_PHP.1, FPT_PHP.3 (optional)

O.SELF_TEST

The PSD shall perform self-tests following power up or powered reset.

Addressed by: FPT_TST.1

O.SELF_TEST_FAIL_TOE_DISABLE

The PSD shall enter a secure state upon detection of a critical failure.

Addressed by: FPT_FLS_EXT.1, FPT_TST_EXT.1

O.SELF_TEST_FAIL_INDICATION

The PSD shall provide clear and visible user indications in the case of a self-test failure.

Addressed by: FPT_TST_EXT.1

4.2 Security Objectives for the Operational Environment

The following subsections describe objectives for the Operational Environment.

OE.NO_TEMPEST

The operational environment will not use TEMPEST approved equipment.

OE.PHYSICAL

The operational environment will provide physical security, commensurate with the value of the PSD and the data that transits it.

OE.NO_WIRELESS_DEVICES

The operational environment will not include wireless keyboards, mice, audio, user authentication, or video devices.

OE.TRUSTED_ADMIN

The operational environment will ensure that trusted PSD Administrators and users are appropriately trained.

OE.TRUSTED_CONFIG

The operational environment will ensure that administrators configuring the PSD and its operational environment follow the applicable security configuration guidance.

4.3 Security Objectives Rationale

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

Threat or Assumption	Security Objective(s)	Rationale
T.DATA_LEAK	O.COMPUTER_INTERFACE_ISOLATION	Isolation of computer interfaces prevents data from leaking between them without authorization.
	O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED	Maintaining interface isolation while the TOE is in an unpowered state ensures that data cannot leak between computer interfaces.
	O.USER_DATA_ISOLATION	The TOE's routing of data only to the selected computer ensures that it will not leak to any others.

Threat or Assumption	Security Objective(s)	Rationale
	O.NO_OTHER_EXTERNAL_INTERFACES	The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked.
	O.PERIPHERAL_PORTS_ISOLATION	Isolation of peripheral ports prevents data from leaking between them without authorization.
T.SIGNAL_LEAK	O.COMPUTER_INTERFACE_ISOLATION	Isolation of computer interfaces prevents data leakage through bit-wise signaling because there is no mechanism by which the signal data can be communicated.
	O.NO_OTHER_EXTERNAL_INTERFACES	The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked through bit-wise signaling.
	O.LEAK_PREVENTION_SWITCHING	The TOE's use of switching methods that are not susceptible to signal leakage helps mitigate the signal leak threat.
T.RESIDUAL_LEAK	O.NO_USER_DATA_RETENTION	The TOE's lack of data retention ensures that a residual data leak is not possible.
T.UNINTENDED_USE	O.AUTHORIZED_USAGE	The TOE's support for only switching mechanisms that require explicit user action to engage ensures that a user has sufficient information to avoid interacting with an unintended computer.
T.UNAUTHORIZED_DEVICES	O.REJECT_UNAUTHORIZED_ENDPOINTS	The TOE's ability to reject unauthorized endpoints mitigates the threat of unauthorized devices being used to communicate with connected computers.
	O.REJECT_UNAUTHORIZED_PERIPHERAL	The TOE's ability to reject unauthorized peripherals mitigates the threat of unauthorized devices being used to communicate with connected computers.
T.LOGICAL_TAMPER	O.NO_TOE_ACCESS	The TOE's prevention of logical access to its firmware, software, and memory mitigates the threat of logical tampering.
T.PHYSICAL_TAMPER	O.ANTI_TAMPERING	The TOE mitigates the threat of physical tampering through use of an enclosure that provides tamper detection functionality.
	O.TAMPER_EVIDENT_LABEL	The TOE mitigates the threat of physical tampering through use of tamper evident labels that reveal physical tampering attempts.
T.REPLACEMENT	O.TAMPER_EVIDENT_LABEL	The TOE's use of a tamper evident label that provides authenticity of the device mitigates the threat that it is substituted for a replacement device during the acquisition process.
T.FAILED	O.SELF_TEST	The TOE mitigates the threat of failures leading to compromise of security functions through self-tests of its own functionality.

Threat or Assumption	Security Objective(s)	Rationale
	O.SELF_TEST_FAIL_TOE_DISABLE	The TOE mitigates the threat of failures leading to compromise of security functions by disabling all data flows in the event a failure is detected.
	O.SELF_TEST_FAIL_INDICATION	The TOE mitigates the threat of failures leading to compromise of security functions by providing users with a clear indication when it is in a failure state and should not be trusted.
A.NO_TEMPEST	OE.NO_TEMPEST	If the TOE's operational environment does not include TEMPEST approved equipment, then the assumption is satisfied.
A.NO_PHYSICAL	OE.PHYSICAL	If the TOE's operational environment provides physical security, then the assumption is satisfied.
A.NO_WIRELESS_DEVICES	OE.NO_WIRELESS_DEVICES	If the TOE's operational environment does not include wireless peripherals, then the assumption is satisfied.
A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN	If the TOE's operational environment ensures that only trusted administrators will manage the TSF, then the assumption is satisfied.
A.TRUSTED_CONFIG	OE.TRUSTED_CONFIG	If TOE administrators follow the provided security configuration guidance, then the assumption is satisfied.
A.USER_ALLOWED_ACCESS	OE.PHYSICAL	If the TOE's operational environment provides physical access to connected computers, then the assumption is satisfied.

Table 1: Security Objectives Rationale

5 Security Requirements

The Security Functional Requirements 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 Security Functional Requirements: 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**) is used to add details to a requirement, and thus further restricts a requirement.
- **Selection** (denoted by italicized text): is used to select one or more options provided by the [CC] in stating a requirement. Selection operations completed in the PP are shown in brackets.
- **Assignment** operation (denoted by italicized text) is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation is identified with a slash ('/') and an identifier (e.g. "/KM").
- **Extended** SFRs are identified by having a label "EXT" after the SFR name.

5.1 Test Environment for Evaluation Activities

Test environments for each test are specified below for each SFR.

5.2 TOE Security Functional Requirements

5.2.1 User Data Protection (FDP)

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 flows between connected computers whether the TOE is powered on or powered off.

FDP_APC_EXT.1.3 The TSF shall ensure that no data transits the TOE when the TOE is powered off.

FDP_APC_EXT.1.4 The TSF shall ensure that no data transits the TOE when the TOE is in a failure state.

Evaluation Activity

Isolation Document
The evaluator shall review the Isolation Documentation and Assessment as described in Appendix D of this PP and ensure that it adequately describes the isolation concepts and implementation in the TOE and why it can be relied upon to provide proper isolation between connected computers whether the TOE is powered on or powered off.

TSS

The evaluator shall verify that the TSS describes the conditions under which the TOE enters a failure state.

Guidance
The evaluator shall verify that the operational user guidance describes how a user knows when the TOE enters a failure state.

Test
There are no test Evaluation Activities for this component.

FDP_PDC_EXT.1 Peripheral Device Connection

FDP_PDC_EXT.1.1 The TSF shall reject connections with unauthorized devices upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.1.2 The TSF shall reject connections with devices presenting unauthorized interface protocols upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.1.3 The TOE shall have no external interfaces other than those claimed by the TSF.

FDP_PDC_EXT.1.4 The TOE shall not have wireless interfaces.

FDP_PDC_EXT.1.5 The TOE shall provide a visual or auditory indication to the User when a peripheral is rejected.

Application Note: *The list of unauthorized devices is in Appendix E: Peripheral Device Connections.*

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.

Evaluation Activity

Isolation Document
There are no Isolation Document evaluation activities for this component.

TSS
The evaluator shall verify that the TSS describes the compatible devices for each peripheral port type supported by the TOE. The description must include sufficient detail to justify any PP-Modules that extend this PP and are claimed by the TOE (e.g., if the ST claims the Audio Input PP-Module, then the TSS shall reference one or more audio input devices as supported peripherals).

The evaluator shall verify that the TSS describes the interfaces between the PSD and computers and the PSD and peripherals, and ensure that the TOE does not contain wireless connections for these interfaces.

The evaluator shall verify that the list of peripheral devices and interfaces supported by the TOE does not include any prohibited peripheral devices or interface protocols specified in Appendix E.

The evaluator shall verify that the TSS describes all external physical interfaces implemented by the TOE, and that there are no external interfaces that are not claimed by the TSF.

Guidance

The evaluator shall verify that the operational user guidance provides clear direction for the connection of computers and peripheral devices to the TOE.

The evaluator shall verify that the operational user guidance provides clear direction for the usage and connection of TOE interfaces, including general information for computer, power, and peripheral devices.

The evaluator shall determine if interfaces that receive or transmit data to or from the TOE present a risk that these interfaces could be misused to import or export user data.

The evaluator shall verify that the operational user guidance describes the visual or auditory indications provided to a user when the TOE rejects the connection of a device.

Test

Test 1: The evaluator shall check the TOE and its supplied cables and accessories to ensure that there are no external wired interfaces other than computer interfaces, peripheral device interfaces, and power interfaces.

Test 2: The evaluator shall check the TOE for radio frequency certification information to ensure that the TOE does not support wireless interfaces.

Test 3: The evaluator shall verify that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections (Appendix E).

For this test, verify device rejection through TOE user indication in accordance with the operational user guidance, an immediate cessation of traffic following device detection or enumeration, or incompatibility of the device interface with the peripheral interface, and through no such device appearing in the real-time hardware information console.

Step 1: Ensure the TOE is powered off. Open a real-time hardware information console on the connected computer.

Step 2: Attempt to connect a USB mass storage device to the TOE peripheral interface.

Step 3: Power on the TOE. Verify the device is rejected.

Step 4: Ensure the USB mass storage device is disconnected, and then attempt to connect it to the TOE peripheral interface again.

Step 5: Verify the device is rejected.

Step 6: Power off the TOE. Connect an unauthorized USB device to a USB hub, and attempt to connect the USB hub to the TOE peripheral interface.

Step 7: Power on the TOE. Verify the device is rejected.

Step 8: Ensure the USB hub is disconnected, and then attempt to connect it to the TOE peripheral interface again.

Step 9: Verify the device is rejected.

Step 10: Power off the TOE. Attempt to connect any Personal System/2 (PS/2) device directly to the TOE peripheral interface.

Step 11: Power on the TOE. Verify the device is rejected.

Step 12: Ensure the PS/2 device is disconnected, and then attempt to connect it directly to the TOE peripheral interface again.

Step 13: Verify the device is rejected.

FDP_RIP_EXT.1 Residual Information Protection

FDP_RIP_EXT.1.1 The TSF shall ensure that no user data is written to TOE non-volatile memory or storage.

Evaluation Activity

Isolation Document
There are no Isolation Document evaluation activities for this component.

TSS
The evaluator shall verify that the TSS includes a Letter of Volatility that provides the following information:

- Which TOE components have non-volatile memory, the non-volatile memory technology, manufacturer/part number, and memory sizes;
- Any data and data types that the TOE may store on each one of these components;
- Whether or not each one of these parts is used to store user data and how this data may remain in the TOE after power down; and
- Whether the specific component may be independently powered by something other than the TOE (e.g., by a connected computer).

Note that user configuration and TOE settings are not considered user data for purposes of this requirement.

The evaluator shall verify that the Letter of Volatility provides assurance that user data is not stored in TOE non-volatile memory or storage.

Guidance
There are no guidance Evaluation Activities for this component.

Test
There are no test Evaluation Activities for this component.

FDP_SWI_EXT.1 PSD Switching

FDP_SWI_EXT.1.1 The TSF shall ensure that [*selection: the TOE supports only one connected computer, switching can be initiated only through express user action*].

Application Note: *If "switching can be initiated only through express user action" is selected, the ST must include the selection-based requirements FDP_SWI_EXT.2 and FTA_CIN_EXT.1.*

Evaluation Activity

Isolation Document
There are no Isolation Document evaluation activities for this component.

TSS
If the ST includes the selection *the "TOE supports only one connected computer"*, the evaluator shall verify that the TSS indicates that the TOE supports only one connected computer.

If the ST includes the selection "*switching can be initiated only through express user action"*, the evaluator shall verify that the TSS describes the TOE supported switching mechanisms and that those mechanisms can be initiated only through express user action.

Guidance
If the ST includes the selection "*switching can be initiated only through express user action*"*,* the evaluator shall verify that the operational user guidance describes the TOE supported switching mechanisms.

Test
There are no test Evaluation Activities for this component.

5.2.2 Protection of the TSF (FPT)

FPT_FLS_EXT.1 Failure with Preservation of Secure State

FPT_FLS_EXT.1.1 The TSF shall preserve a secure state when the following types of failures occur: failure of the power-on self-test and [*selection: failure of the anti-tamper function, no other failures*].

Application Note: *In the context of this PP, a 'secure state' is defined by the TOE disabling all peripheral and connected computer interfaces when the correctness of its own functions cannot be assured.*

Failure of the anti-tamper function should be selected if FPT_PHP.3 is included in the ST.

Evaluation Activity

This SFR is evaluated in conjunction with FPT_TST.1.

FPT_NTA_EXT.1 No Access to TOE

FPT_NTA_EXT.1.1 TOE firmware, software, and memory shall not be accessible via the TOE's external ports, with the following exceptions: [*selection: the **Extended Display Identification Data (**EDID**)** memory of Video TOEs may be accessible from connected computers; the configuration data, settings, and logging data that may be accessible by authorized administrators; no other exceptions*].

Evaluation Activity

Isolation Document
There are no Isolation Document evaluation activities for this component.

TSS
The evaluator shall examine the TSS to ensure that the TSS documents that connected computers and peripherals do not have access to TOE software, firmware, and TOE memory, except as described above.

Guidance
The evaluator shall check the operational user guidance to ensure any configurations required to comply with this SFR are defined.

Test
There are no test Evaluation Activities for this component.

FPT_PHP.1 Passive Detection of Physical Attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

Application Note: *FPT_PHP.1.1 include indications generated from application of optional SFR FPT_PHP.3*

Evaluation Activity

Isolation Document
There are no Isolation Document evaluation activities for this component.

TSS
The evaluator shall verify that the TSS indicates that the TOE provides unambiguous detection of physical tampering of the TOE enclosure and TOE remote controller (if applicable). The evaluator shall verify that the TSS provides information that describes how the TOE indicates that it has been tampered with.

Guidance
The evaluator shall verify that the operational user guidance describes the mechanism by which the TOE provides unambiguous detection of physical

tampering and provides the user with instructions for verifying that the TOE has not been tampered with.

Test
Test 1: The evaluator shall verify, for each tamper evident seal or label affixed to the TOE enclosure and TOE remote controller (if applicable), that any attempts to open the enclosure or remove the seal results in the seal being damaged in a manner that is consistent with the operational user guidance.

Test 2: The evaluator shall verify that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.

FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self-tests [*during initial start-up and at the conditions **[selection: upon reset button activation, no other conditions]***] to demonstrate the correct operation of [*user control functions and **[selection: active anti-tamper functionality, no other functions]***].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of [*selection: [assignment: parts of TSF data], TSF data*].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of [*selection: [assignment: parts of TSF], TSF*].

Application Note: *Reset button activation should be selected if the TOE includes such functionality.*

If "active anti-tamper functionality" is selected, portions of the evaluation activities will test functions from the optional active anti-tamper SFR FPT_PHP.3.

Anyone with physical access to the TOE can be considered an authorized user.

Evaluation Activity

Isolation Document
There are no Isolation Document evaluation activities for this component.

TSS
The evaluator shall verify that the TSS describes the self- tests that are performed on start up or on reset (if "upon reset button activation" is selected). The evaluator shall verify that the self-tests cover at least the following:

a) a test of the user interface – in particular, tests of the user control mechanism (e.g., checking that the front panel push-buttons are not jammed); and

b) if "active anti-tamper functionality" is selected, a test of any anti-tampering mechanism (e.g., checking that the backup battery is functional).

The evaluator shall verify that the TSS describes how the TOE ensures a shutdown upon a self-test failure or a failed anti-tampering function, if present. If there are instances when a shutdown does not occur (e.g., a failure is deemed non-security relevant), those cases are identified and a rationale is provided explaining why the TOE's ability to enforce its security policies is not affected.

The evaluator shall check the TSS to verify that it describes the TOE behavior in case of self-test failure. The evaluator shall verify that the described TOE behavior includes shutting down the PSD functionality once the failure is detected.

The evaluator shall examine the TSS to verify that it describes how users verify the integrity of the selections in FPT_TST.1.2 and FPT_TST.1.3. This method can include restarting the TOE, a dedicated self-test, or some other method.

Guidance
The evaluators shall verify that the operational user guidance describes how users verify the integrity of the selections in FPT_TST.1.2 and FPT_TST.1.3. This method can include restarting the TOE, a dedicated self-test, or some other method.

Test
The evaluator shall trigger the conditions specified in the TSS that are used to initiate TSF self-testing and verify that successful completion of the self-tests can be determined by following the corresponding steps in the operational guidance.

FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1 The TSF shall respond to a self-test failure by providing users with a [*selection: visual, auditory*] indication of failure and by shutdown of normal TSF functions.

Evaluation Activity

Isolation Document
There are no Isolation Document evaluation activities for this component.

TSS
The evaluator shall check the TSS to verify that it describes the TOE behavior in case of self-test failure. The evaluator shall verify that the described TOE behavior includes shutting down the PSD functionality once the failure is detected.

Guidance
The evaluator shall verify that the operational user guidance:

a) describes how the results of self-tests are indicated to the user

b) provides the user with a clear indication of how to recognize a failed self-test; and

c) details the appropriate actions to be completed in the event of a failed self-test.

The evaluator shall verify that the operational user guidance provides adequate information on TOE self-test failures, their causes, and their indications.

Test
The evaluator shall cause a TOE self-test failure and verify that the TOE responds by disabling normal functions and provides proper indications to the user.

5.3 Security Assurance Requirements

The Security Objectives for the TOE in Section 4 were constructed to address threats identified in Section 3.1. The Security Functional Requirements (SFRs) in Section 5.2 are a formal instantiation of the Security Objectives. The SARs were chosen based on the complexity of the products that are anticipated to be evaluated against this PP as well as the expected level of sophistication and access that an attacker would have if the TOE is deployed in an environment that satisfies the environmental security objectives in this PP.

This section lists the set of SARs drawn from CC Part 3 that are required in evaluations against this PP. Individual Evaluation Activities to be performed are specified both in Section 5.2 as well as in this section.

The general model for evaluation of TOEs against STs written to conform to this PP is as follows:

After the ST has been approved for evaluation, the Common Criteria Testing Laboratory (CCTL) will obtain the TOE, supporting IT environmental, and the administrative/user guides for the TOE. The CCTL is expected to perform actions mandated by the Common Evaluation Methodology (CEM) for the ASE and ALC SARs. The CCTL also performs the Evaluation Activities contained within Section 5.2, which are intended to be an interpretation of the other CEM assurance requirements as they apply to the specific technology instantiated in the TOE. The Evaluation Activities that are captured in Section 5.2 also provide clarification as to what the developer needs to provide to demonstrate the TOE is compliant with the PP.

The TOE security assurance requirements are identified in Table 3.

Assurance Class	Assurance Components
Security Target (ASE)	Conformance Claims (ASE_CCL.1)
	Extended Components Definition (ASE_ECD.1)
	ST Introduction (ASE_INT.1)
	Security Objectives (ASE_OBJ.2)
	Derived Security Requirements (ASE_REQ.2)
	Security Problem Definition (ASE_SPD.1)
	TOE Summary Specification (ASE_TSS.1)
Development (ADV)	Basic Functional Specification (ADV_FSP.1)
Guidance documents (AGD)	Operational User Guidance (AGD_OPE.1)
	Preparative Procedures (AGD_PRE.1)

Assurance Class	Assurance Components
Life cycle support (ALC)	Labeling of the TOE (ALC_CMC.1)
	TOE CM Coverage (ALC_CMS.1)
Tests (ATE)	Independent Testing – Conformance (ATE_IND.1)
Vulnerability assessment (AVA)	Vulnerability Survey (AVA_VAN.1)

Table 2: TOE Security Assurance Requirements

5.3.1 Class ASE: Security Target

The ST is evaluated as per ASE activities defined in the CEM. In addition, there may be Evaluation Activities specified within Section 5 and the relevant appendices that call for necessary descriptions to be included in the TSS that are specific to the TOE technology type.

5.3.2 Class ADV: Development

The design information about the TOE is contained in the guidance documentation available to the end user, the TSS portion of the ST, and in proprietary information contained in documents that is not to be made public (e.g., Isolation Documentation).

Basic Functional Specification (ADV_FSP.1)

The functional specification describes the Target Security Functions Interfaces (TSFIs). It is not necessary to have a formal or complete specification of these interfaces. Additionally, because TOEs conforming to this PP will necessarily have interfaces to the Operational Environment that are not directly able to be invoked by TOE users, there is little point specifying that such interfaces be described in and of themselves since only indirect testing of such interfaces may be possible. For this PP, the activities for this family should focus on understanding the interfaces presented in the TSS in response to the functional requirements and the interfaces presented in the AGD documentation. No additional "functional specification" documentation is necessary to satisfy the Evaluation Activities specified.

The interfaces that need to be evaluated are characterized through the information needed to perform the Evaluation Activities listed, rather than as an independent, abstract list.

Evaluation Activity

There are no specific Evaluation Activities associated with these SARs. The Evaluation Activities listed in this PP are associated with the applicable SFRs; since these are directly associated with the SFRs, the tracing element ADV_FSP.1.2D is implicitly already done, and no additional documentation is necessary. The functional specification documentation is provided to support the evaluation activities described in Section 5.2 and other activities described for AGD, and ATE SARs. The requirements on the content of the functional specification information are implicitly assessed by virtue of the other Evaluation Activities being performed. If the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided.

5.3.3 Class AGD: Guidance Documentation

The guidance documents will be provided with the ST. Guidance must include a description of how the authorized user verifies that the Operational Environment can fulfill its role for the security functionality. The documentation should be in an informal style and readable by the authorized user.

Guidance must be provided for every operational environment that the product supports as claimed in the ST. This guidance includes:

- Instructions to successfully and securely install the TSF in that environment; and
- Instructions to manage the security of the TSF as a product and as a component of the larger operational environment; and
- Instructions to provide a protected administrative capability.

Guidance pertaining to particular security functionality must also be provided; requirements on such guidance are contained in the Evaluation Activities specified with each requirement.

Operational User Guidance (AGD_OPE.1)

The operational user guidance does not have to be contained in a single document. Guidance to users and Administrators can be spread among documents or web pages. The developer should review the Evaluation Activities contained in Section 5.2 of this PP to ascertain the specifics of the guidance for which the evaluator will be checking. This will provide the necessary information for the preparation of acceptable guidance.

Preparative Procedures (AGD_PRE.1)

As with the operational user guidance, the developer should look to the Evaluation Activities contained in Section 5.2 of this PP to determine the required content with respect to preparative procedures.

5.3.4 Class ALC: Life-cycle Support

At the assurance level provided for TOEs conformant to this PP, life-cycle support is limited to end-user-visible aspects of the life-cycle, rather than an examination of the TOE vendor's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation at this assurance level.

Labeling of the TOE (ALC_CMC.1)

This component is targeted at identifying the TOE such that it can be distinguished from other products or versions from the same vendor and can be easily specified when being procured by an end user.

A label should consist of a "hard label" (e.g., stamped into the metal, paper label) or a "soft label" (e.g., electronically presented when queried).

The evaluator performs the CEM work units associated with ALC_CMC.1, as well as the Evaluation Activity specified below.

Evaluation Activity

The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance, the evaluator implicitly confirms the information required by this component.

TOE CM Coverage (ALC_CMS.1)

Given the scope of the TOE and its associated evaluation evidence requirements, this component's Evaluation Activities are covered by the Evaluation Activities listed for ALC_CMC.1.

5.3.5 Class ATE: Tests

Testing is specified for functional aspects of the system as well as aspects that take advantage of design or implementation weaknesses. The former is done through the ATE_IND family, while the latter is through the AVA_VAN family. For this PP, testing is based on advertised functionality and interfaces with dependency on the availability of design information. One of the primary outputs of the evaluation process is the test report as specified in the following requirements.

Independent Testing – Conformance (ATE_IND)

Testing is performed to confirm the functionality described in the TSS as well as the guidance documentation. The evaluation activities identify the specific testing activities necessary to verify compliance with the SFRs. The evaluator produces a test report documenting the plan for and results of testing, as well as coverage arguments focused on the platform/TOE combinations that are claiming conformance to this PP.

Evaluation Activity

The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the CEM and the body of this PP's Evaluation Activities. While it is not necessary to have one test case per test listed in an Evaluation Activity, the evaluator must document in the test plan that each applicable testing requirement in the PP is covered.

The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition of each platform to be tested and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test equipment or tools. For each piece of equipment or tool, an argument (not just an assertion) should be provided that the equipment or tool will not adversely affect the performance of the functionality by the TOE and its platform.

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.

5.3.6 Class AVA: Vulnerability Survey (AVA_VAN.1)

For the current generation of this PP, the evaluation lab is expected to survey open sources to discover what vulnerabilities have been discovered in these types of products and in the connected peripherals. In addition, the evaluation lab is expected to survey open sources to discover new vulnerabilities and weaknesses discovered in microcontrollers, ASICs, FPGAs, and microprocessors used in the TOE. In some cases, these vulnerabilities will require sophistication beyond that of a basic attacker. The labs will be

expected to comment on the likelihood of these vulnerabilities given the documentation provided by the vendor. This information will be used for the development of future PPs.

Evaluation Activity

As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in peripheral sharing devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.

A Optional Requirements

As indicated in the introduction to this PP, the baseline requirements (those that must be performed by the TOE) are contained in the body of this PP. 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.

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, but will be included in the baseline requirements in future versions of this PP. 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

A.3.1 TOE Capability for Configuration and Accounting

If the TSF supports activities that require the actions of an authorized administrator, the following SFRs must all be claimed or the functionality disabled:

- FAU_GEN.1 – The actions of the authorized administrator must be auditable, along with self-test failures, and peripheral device acceptance and rejections. No specific SFRs are required to detail the methods for storing and reading audit entries; however, this information must be included in the TSS.
- FIA_UID.2 and FIA_UAU.2 – Authorized administrators must be appropriately identified and authenticated to perform any action identified as an administrative activity.
- FMT_MOF.1, FMT_SMF.1 and FMT_SMR.1 – The administrative functions are described in FMT_MOF.1 and FMT_SMF.1. The administrative role or roles are described in FMT_SMR.1.
- FPT_STM.1– A reliable time stamp must be provided for use in TSF functions such as generating audit records.

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the audit functions;
b. All auditable events for the [*not specified*] level of audit; and

c. [*administrator login, administrator logout, self-test failures, peripheral device acceptance and rejections, [assignment: all administrative functions claimed in FMT_MOF.1 and FMT_SMF.1]*]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other information*].

Application Note: *If a peripheral device is rejected due to its incompatibility with the peripheral interface, then this rejection need not be audited.*

Evaluation Activity

Isolation Document
There are no Isolation Document evaluation activities for this component.

TSS
The evaluator shall verify that the TSS describes the audit functionality including which events are audited, what information is saved in each record type, how the records are stored, the conditions in which audit records are overwritten, and the means by which the audit records may be read. Although the TOE may provide an interface for an administrator to view the audit records, this is not a requirement.

Guidance
The evaluator shall verify that the operational guidance provides instructions on how the audit logs can be viewed as well as any information needed to interpret the audit logs.

Test
The evaluator shall perform each of the auditable functions to succeed, and where possible, to fail. The evaluator shall use the means described in the TSS to access the audit records and verify that each of the events has been recorded, with all of the expected information.

FIA_UAU.2 User Authentication Before Any Action

FIA_UAU.2.1 The TSF shall require each **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **administrator**.

Application Note: *This requirement expects that the authentication method(s) be described (e.g., logon credential, specially assigned key, etc.).*

Evaluation Activity

This SFR is evaluated by the Evaluation Activities in FMT_MOF.1 below.

FIA_UID.2 User Identification Before Any Action

FIA_UID.2.1 The TSF shall require each **administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that **administrator**.

Evaluation Activity

This SFR is evaluated by the Evaluation Activities in FMT_MOF.1 below.

FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [*modify the behavior of*] the functions [*assignment: list of functions*] to [*the authorized administrators*].

Evaluation Activity

Isolation Document
There are no Isolation Document evaluation activities for this component.

TSS
The evaluator shall verify that the TSS describes the mechanism for preventing non-administrators from accessing the administrative functions stated above.

If the TSF provides multiple administrative roles, the evaluator shall verify that the authorized behavior for each separate administrative role is described.

The evaluator shall check the TSS to verify that it describes at least the following:

a) Administrator name limitations and syntax requirements;
b) Administrator password limitations and syntax requirements;
c) Restoring lost name or password;
d) Initial setting of administrator credentials;
e) Logon success, fail limitations, and logging; and
f) All functions identified in the above assignment.

Guidance
The evaluator shall check the user and administrative guidance to verify that the administrative functions described above are only available to identified administrators. If the TSF provides multiple administrative roles, the evaluator shall verify that the authorized behavior for each separate administrative role is described.

Test
Step 1: Set up the TOE to enable administrator access per applicable TOE administrative guidance. Verify that the TOE is in factory default format.

Step 2: Attempt to set the initial administrator user name and password.

Step 3: Logon as a valid administrator and perform all authorized administrative functions to assure the logon was successful.

Step 4: Log off from the TOE.

Step 5: Attempt to logon with an incorrect administrator name. Verify that the logon is failing as expected and that administrative functions are unavailable.

Step 6: Attempt to access administrative functions while there is no logged on administrator. Verify that all attempts fail.

Step 7: If the TOE provides multiple administrative roles, repeat this test for each defined role to ensure that the authorizations for each role are consistent with what is described in the operational guidance.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TOE shall be capable of performing the following management functions: [*assignment: list of management functions to be provided by the TSF*].

Application Note: *Supported management functions may depend on the PP-Modules that are claimed by the TOE alongside this PP. This could include Configurable Device Filtration (CDF) for one or more supported peripheral types not defined in this PP. A management function should also be included if the optional FDP_RIP_EXT.2.1 requirement is included which specifies that the TOE shall have a purge memory or restore factory defaults function accessible to the administrator.*

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

The evaluator shall check to ensure the TSS describes the management functions available to the administrators and user TOE configurations and how they are used by the TOE.

Guidance

The evaluator shall check that every management function mandated in the ST for this requirement is described in the operational user guidance and that the description contains the information required to perform the management duties associated with each management function.

Test

The evaluator shall test the TOE's ability to provide the management functions by configuring the TOE and testing each option assigned from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.

FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [*administrators*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Note: *The intent of this SFR is to make clear the fact that the TSF is expected to provide some sort of controlled access to administrative functions such that ordinary users are not able to execute them without authorization. It does not mandate that the TSF provide a single administrative role named "administrator"; if multiple administrative roles with different authorizations are provided, then the behavior can be described in the ST and tested accordingly.*

Evaluation Activity

Refer to the Evaluation Activities of FMT_MOF.1.1 above.

FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application Note: *Reliable time stamps are expected to be used with other TSF, e.g., for the generation of audit data, to allow the Administrator to investigate incidents by checking the order of events and to determine the actual local time when events occurred. The decision about the required level of accuracy of that information is up to the Administrator*.

Evaluation Activity

Isolation Document
There are no Isolation Document evaluation activities for this component.

TSS
The evaluator shall check to ensure the TSS describes how the TOE provides reliable timestamps.

Guidance
The evaluator shall check that the operational user guidance describes how the TOE provides reliable timestamps and if there are any management functions for configuring the time.

Test
The evaluator shall test the TOE's ability to provide time stamps. It is expected that this test be performed in conjunction with FAU_GEN.1.

A.3.2 TOE Capability for Factory Reset

If the TSF provides a factory reset capability, the following SFR must be claimed or the functionality disabled.

FDP_RIP_EXT.2 Purge of Residual Information

FDP_RIP_EXT.2.1 The TOE shall have a purge memory or restore factory defaults function accessible to the administrator to delete all TOE stored configuration and settings except for logging.

Evaluation Activity

Isolation Document
There are no Isolation Document evaluation activities for this component.

TSS
The evaluator shall verify that the TSS describes the TOE's reaction to memory purge or restore factory defaults.

The evaluator shall verify that the Letter of Volatility included in the TSS describes the effect that the TOE Restore Factory Default function has on each component listed in the Letter of Volatility.

Guidance
The evaluator shall check that the operational user guidance provides a method to purge TOE memory or to restore factory default settings.

Test
Step 1: Perform the TOE memory purge or restore factory defaults according to the guidance and verify that the TOE enters a desirable secure state.

The evaluator shall check that the log record is not deleted if a logging function is supported by the TOE.

A.3.3 TOE Capability for Tamper Response

If the TSF provides resistance to physical attack via automatic response, the following SFR must be claimed or the functionality disabled.

FPT_PHP.3 Resistance to Physical Attack

FPT_PHP.3.1 The TSF shall resist [*a physical attack for the purpose of gaining access to the internal components, to damage the anti-tamper battery, to drain or exhaust the anti-tamper battery*] to the [*TOE enclosure*] by **becoming permanently disabled.**

Application Note: *'Becoming permanently disabled' is interpreted to mean that connected peripheral devices will cease to function.*

Evaluation Activity

Isolation Document
There are no Isolation Document evaluation activities for this component.

TSS
The evaluator shall verify that the TSS describes the TOE's reaction to opening the device enclosure or damaging/exhausting the anti-tampering battery associated with the enclosure.

Guidance
The evaluator shall examine the operational user guidance and verify that the guidance provides users with information on how to recognize a device where the anti-tampering functionality has been activated.

The evaluator shall verify that the operational user guidance warns the user of the actions that will cause the anti-tampering functionality to disable the device.

Test
In the following testing the evaluator shall attempt to gain physical access to the TOE internal circuitry (enough access to allow the insertion of tools to tamper with the internal circuitry). The TOE anti- tampering function is expected to trigger, causing an irreversible change to the TOE functionality. The evaluator then shall verify that the anti-tampering triggering provides the expected user indications and also disables the TOE.

TOE disabling means that the user would not be able to use the TOE for any purpose – all peripheral devices and computers are isolated.

Note that it is obvious that if the TOE was physically tampered with, then the attacker may easily circumvent the tamper indication means (for example cut the relevant TOE front panel wires). Nevertheless, the following test verifies that the user would be unable to ignore the TOE tampering indications and resume normal work.

The evaluator shall perform the following steps:

Step 1: The evaluator shall attempt to open the PSD enclosure enough to gain access to its internal circuitry and observe that the TOE is both permanently disabled and provides the proper indication that it has been tampered with in accordance with the operational user guidance.

Step 2: [conditional: this step is applicable for TOEs having a remote controller] The evaluator shall attempt to open the PSD remote controller enclosure enough to gain access to its internal circuitry and observe that the TOE is both permanently disabled and provides the proper indication that it has been tampered with in accordance with the operational user guidance.

Step 3: The evaluator shall attempt to access the TOE settings to reset the tampering state and verify that it is not possible to recover from the tampered state.

Step 4: The evaluator shall acquire a copy of the TOE that has been previously tampered with.

Step 5: The evaluator shall power on the TOE and verify that the tampering indicator is displayed.

B Selection-Based Requirements

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

B.1 User Data Protection (FDP)

FDP_SWI_EXT.2 PSD Switching Methods

FDP_SWI_EXT.2.1 The TSF shall ensure that no switching can be initiated through automatic port scanning, control through a connected computer, or control through keyboard shortcuts.

FDP_SWI_EXT.2.2 The TSF shall ensure that switching can be initiated only through express user action using [*selection: console buttons, console switches, console touch screen, wired remote control, peripheral devices using a guard*].

Application Note: *This SFR must be claimed if "switching can be initiated only through express user action" is chosen as the selection for FDP_SWI_EXT.1.1.*

If the TOE also claims conformance to the PP-Module for Video/Display Devices (Video Module) and if "peripheral devices using a guard" is selected here, the TOE must claim the selection-based requirement FDP_CDS_EXT.1 in the Video Module and select "multiple connected displays" in FDP_CDS_EXT.1.1.

Evaluation Activity

Isolation Document
There are no Isolation Document evaluation activities for this component.

TSS
The evaluator shall verify that the TSS describes the TOE supported switching mechanisms. The evaluator shall verify that the TSS does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms. The evaluator shall verify that the described switching mechanisms can be initiated only through express user action according to the selections.

Guidance
The evaluator shall verify that the operational user guidance describes the TOE supported switching mechanisms. The evaluator shall verify that the operational user guidance does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms.

Test
There are no test Evaluation Activities for this component.

B.2 TOE Access (FTA)

FTA_CIN_EXT.1 Continuous Indications

FTA_CIN_EXT.1.1 The TSF shall display a visible indication of the selected computers at all times when the TOE is powered.

FTA_CIN_EXT.1.2 The TSF shall implement the visible indication using the following mechanism: [*selection: a button, a panel with lights, a screen with dimming function, a screen with no dimming function, [assignment: description of visible indication]*].

FTA_CIN_EXT.1.3 The TSF shall ensure that while the TOE is powered the current switching status is reflected by [*selection: the indicator, multiple indicators which never display conflicting information*].

Application Note: *This SFR must be claimed if "switching can be initiated only through express user action" is chosen as the selection for FDP_SWI_EXT.1.1.*

FTA_CIN_EXT.1.3's selection of "multiple indicators which never display conflicting information" should be selected when the TOE has multiple indicators, and concerns TOEs with multiple authorized switching mechanisms that have distinct switching status indicators. Such indicators must never convey conflicting information to the user regarding the currently selected interface(s). In general, all indicators must always reflect the same status. It is permissible for the most recently used switching mechanism to reflect the current status while all other indicators to reflect no status. It is also permissible for a TOE that supports split control (i.e., different peripherals pointing to different computers) to have separate indicators for individual peripherals. Note however that a TOE that supports keyboard/mouse peripherals is not permitted to have the keyboard and mouse peripherals split in this manner, as per the requirements in the PP-Module for Keyboard/Mouse (KM) Devices.

If multiple products with single and multiple indicators are part of the TOE, then it is recommended that FTA_CIN_EXT.1.3 be iterated for each selection rather than do a different evaluation for each model.

Evaluation Activity

Isolation Document
There are no Isolation Document evaluation activities for this component.

TSS
The evaluator shall verify that the TSS describes how the TOE behaves on power up and on reset, if applicable, regarding which computer interfaces are active, if any.

The evaluator shall verify that the TSS documents the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.

Guidance

The evaluator shall verify that the operational user guidance notes which computer connection is active on TOE power up or on recovery from reset, if applicable. If a reset option is available, use of this feature must be described in the operational user guidance.

The evaluator shall verify that the operational user guidance documents the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.

Test
Step 1: The evaluator shall configure the TOE and its operational environment in accordance with the operational user guidance.

Step 2: The evaluator shall select a connected computer and power down the TOE, then power up the TOE and verify that the expected selected computer is indicated in accordance with the TSS and that the connection is active.

Step 3: The evaluator shall repeat this process for every possible selected TOE configuration.

Step 4: [Conditional] If "*upon reset button activation*" is selected in FPT_TST.1.1, then the evaluator shall repeat this process for each TOE configuration using the reset function rather than power-down and power-up.

Step 5: The evaluator shall verify that the TOE selected computer indications are always on (i.e., continuous) and fully visible to the TOE user.

Step 6: [Conditional] If the TOE allows peripherals to have active interfaces with different computers at the same time, the evaluator shall verify that each permutation has its own selection indications.

Step 7: [Conditional] If "*a screen with dimming function*" is selected, the evaluator shall verify that indications are visible at minimum brightness settings in standard room illumination conditions.

Step 8: [Conditional] If "*multiple indicators which never display conflicting information*" is selected, the evaluator shall verify that either all indicators reflect the same status at all times, or the indicator for the most recently used switching mechanism displays the correct switching status and that all other indicators display the correct status or no status.

C Extended Component Definitions

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_APC_EXT Active PSD Connections
	FDP_PDC_EXT Peripheral Device Connection
	FDP_RIP_EXT Residual Information Protection
	FDP_SWI_EXT PSD Switching
Protection of the TSF (FPT)	FPT_FLS_EXT Failure with Preservation of Secure State
	FPT_NTA_EXT No Access to TOE
	FPT_TST_EXT TSF Testing
TOE Access (FTA)	FTA_CIN_EXT Continuous Indications

C.1 FDP_APC_EXT Active PSD Connections

Family Behavior

Components in this family define the requirements for when an external interface to the TOE is authorized to transmit data related to peripheral sharing.

Component Leveling

FDP_APC_EXT.1 Active PSD Connections, restricts the flow of data through the TSF.

Management: FDP_APC_EXT.1

No specific management functions are identified.

Audit: FDP_APC_EXT.1

There are no auditable events foreseen.

FDP_APC_EXT.1 Active PSD Connections

Hierarchical to: No other components

Dependencies: No dependencies

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 flows between connected computers whether the TOE is powered on or powered off.

FDP_APC_EXT.1.3 The TSF shall ensure that no data transits the TOE when the TOE is powered off.

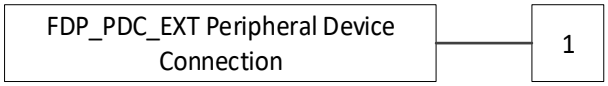
FDP_APC_EXT.1.4 The TSF shall ensure that no data transits the TOE when the TOE is in a failure state.

C.2 FDP_PDC_EXT Peripheral Device Connection

Family Behavior

Components in this family define the requirements for peripheral device connections.

Component Leveling



FDP_PDC_EXT.1 Peripheral Device Connection, requires the TSF to limit external connections to only authorized devices.

Management: FDP_PDC_EXT.1

No specific management functions are identified.

Audit: FDP_PDC_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Acceptance or rejection of a peripheral

FDP_PDC_EXT.1 Peripheral Device Connection

Hierarchical to: No other components

Dependencies: No dependencies

FDP_PDC_EXT.1.1 The TSF shall reject connections with unauthorized devices upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.1.2 The TSF shall reject connections with devices presenting unauthorized interface protocols upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.1.3 The TOE shall have no external interfaces other than those claimed by the TSF.

FDP_PDC_EXT.1.4 The TOE shall not have wireless interfaces.

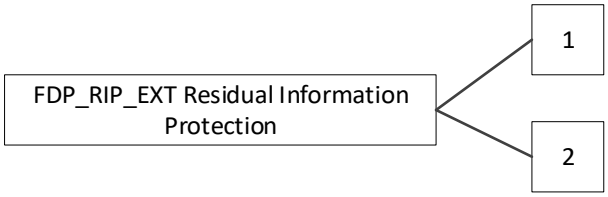
FDP_PDC_EXT.1.5 The TOE shall provide a visual or auditory indication to the User when a peripheral is rejected.

C.3 FDP_RIP_EXT Residual Information Protection

Family Behavior

Components in this family define the requirements for how the TSF prevents data disclosure from its memory.

Component Leveling



FDP_RIP_EXT.1 Residual Information Protection, requires the TSF to prevent the writing of user data to non-volatile memory.

FDP_RIP_EXT.2 Purge of Residual Information, requires the TSF to have a purge function to clear its memory of all stored non-audit data.

Management: FDP_RIP_EXT.1, FDP_RIP_EXT.2

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

- Ability to trigger the TSF's purge function

Audit: FDP_RIP_EXT.1

There are no auditable events foreseen.

Audit: FDP_RIP_EXT.2

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Purging of the TSF's memory

FDP_RIP_EXT.1 Residual Information Protection

Hierarchical to:	No other components
Dependencies:	No dependencies
FDP_RIP_EXT.1.1	The TSF shall ensure that no user data is written to TOE non-volatile memory or storage.

FDP_RIP_EXT.2 Purge of Residual Information

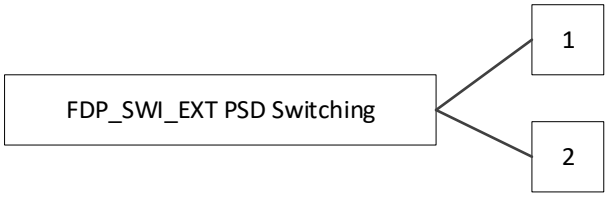
Hierarchical to:	No other components
Dependencies:	No dependencies
FDP_RIP_EXT.2.1	The TOE shall have a purge memory or restore factory defaults function accessible to the administrator to delete all TOE stored configuration and settings except for logging.

C.4 FDP_SWI_EXT PSD Switching

Family Behavior

Components in this family define the requirements for how the TSF protects against inadvertent data switching.

Component Leveling



FDP_SWI_EXT.1 PSD Switching, requires action on the part of a user in order for the TSF's switching mechanisms to be activated.

FDP_SWI_EXT.2 PSD Switching Methods, places restrictions on how the TSF's switching mechanisms can be controlled.

Management: FDP_SWI_EXT.1, FDP_SWI_EXT.2

No specific management functions are identified.

Audit: FDP_SWI_EXT.1, FDP_SWI_EXT.2

There are no auditable events foreseen.

FDP_SWI_EXT.1 PSD Switching

Hierarchical to: No other components

Dependencies: No dependencies

FDP_SWI_EXT.1.1 The TSF shall ensure that [*selection: the TOE supports only one connected computer, switching can be initiated only through express user action*].

FDP_SWI_EXT.2 PSD Switching Methods

Hierarchical to: No other components

Dependencies: FDP_SWI_EXT.1 PSD Switching

FDP_SWI_EXT.2.1 The TSF shall ensure that no switching can be initiated through automatic port scanning, control through a connected computer, or control through keyboard shortcuts.

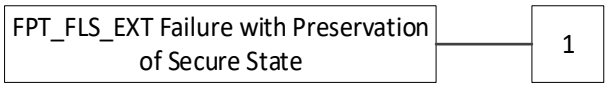
FDP_SWI_EXT.2.2 The TSF shall ensure that switching can be initiated only through express user action using [*selection: console buttons, console switches, console touch screen, wired remote control, peripheral devices using a guard*].

C.5 FPT_FLS_EXT Failure with Preservation of Secure State

Family Behavior

Components in this family define the secure failure requirements for the TSF.

Component Leveling



FPT_FLS_EXT.1 Failure with Preservation of Secure State, requires the TSF to go into a secure state upon the detection of selected failures.

Management: FPT_FLS_EXT.1

No specific management functions are identified.

Audit: FPT_FLS_EXT.1

There are no auditable events foreseen.

FPT_FLS_EXT.1 Failure with Preservation of Secure State

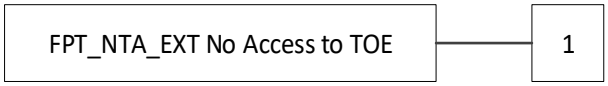
Hierarchical to:	No other components
Dependencies:	FPT_TST.1 TSF Testing
	FPT_PHP.3 Resistance to Physical Attack
FPT_FLS_EXT.1.1	The TSF shall preserve a secure state when the following types of failures occur: failure of the power-on self-test and [*selection: failure of the anti-tamper function, no other failures*].

C.6 FPT_NTA_EXT No Access to TOE

Family Behavior

Components in this family define what TSF information may be externally accessible.

Component Leveling



FPT_NTA_EXT.1 No Access to TOE, requires the TSF to block access to non-authorized TSF data via external ports.

Management: FPT_NTA_EXT.1

No specific management functions are identified.

Audit: FPT_NTA_EXT.1

There are no auditable events foreseen.

FPT_NTA_EXT.1 No Access to TOE

Hierarchical to:	No other components
Dependencies:	No dependencies
FPT_NTA_EXT.1.1	TOE firmware, software, and memory shall not be accessible via the TOE's external ports, with the following exceptions: [*selection: the EDID memory of Video TOEs may be accessible from connected computers; the configuration data, settings, and logging data that may be accessible by authorized administrators; no other exceptions*].

C.7 FPT_TST_EXT TSF Testing

Family Behavior

Components in this family define how the TSF responds to a self-test failure.

Component Leveling

FPT_TST_EXT.1 TSF Testing, requires the TSF to shutdown normal functions and provide a visual or auditory indication that a self-test has failed.

Management: FPT_TST_EXT.1

No specific management functions are identified.

Audit: FPT_TST_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Indication that the TSF self-test was completed
- Failure of self-test

FPT_TST_EXT.1 TSF Testing

Hierarchical to: No other components

Dependencies: FPT_TST.1 TSF Testing

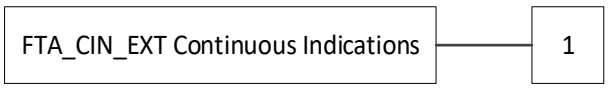
FPT_TST_EXT.1.1 The TSF shall respond to a self-test failure by providing users with a [*selection: visual, auditory*] indication of failure and by shutdown of normal TSF functions.

C.8 FTA_CIN_EXT Continuous Indications

Family Behavior

Components in this family define how the TSF displays its switching status.

Component Leveling



FTA_CIN_EXT.1 Continuous Indications, requires the TSF to display a visual indication of what computers are selected.

Management: FTA_CIN_EXT.1

No specific management functions are identified.

Audit: FTA_CIN_EXT.1

There are no auditable events foreseen.

FTA_CIN_EXT.1 Continuous Indications

Hierarchical to: No other components

Dependencies: FDP_APC_EXT.1 Active PSD Connections

FTA_CIN_EXT.1.1 The TSF shall display a visible indication of the selected computers at all times when the TOE is powered.

FTA_CIN_EXT.1.2 The TSF shall implement the visible indication using the following mechanism: [*selection: a button, a panel with lights, a screen with dimming function, a screen with no dimming function, [assignment: description of visible indication]*].

FTA_CIN_EXT.1.3 The TSF shall ensure that while the TOE is powered the current switching status is reflected by [*selection: the indicator, multiple indicators which never display conflicting information*].

D Isolation Documentation and Assessment

D.1 General

This appendix describes the required supplementary information for implementing isolation of data between connected computers.

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 between connected computers. This documentation should include three detailed sections: design description; isolation means justification; and firmware dependencies.

This documentation is not required to be part of the TSS and may be kept confidential.

D.2 Design Description

The documentation shall include the design of all user data paths inside the TOE as a whole, including the interaction between the various data paths and their primary components (microcontrollers or programmable logic). It shall have one or more block diagrams showing the different data paths in the TOE and any parts that may translate, emulate, switch, force into unidirectional flow or otherwise affect these data streams. It shall also describe the operation of each of the main components in the data paths to include how it works, how isolation is kept, and how power source or power loading may affect isolation between these data paths. The documentation should walk through the flow of each data stream (keyboard, mouse, display video, display EDID, audio etc.) and describe each component that may handle more than one path in detail. The document shall also cover the external interfaces and internal connections. In particular, the documentation shall explain how independence is maintained between the various computer interfaces from a power supply and power loading perspective.

This design must also include a description of all programmable components in the data path and how isolation is maintained in cases where the firmware has been tampered with or the firmware has failed.

D.3 Isolation Means Justification

The documentation shall include a section that refers to each one of the unauthorized data flows listed in the appropriate data flow SFRs, how isolation is provided and how the risk is mitigated by the TOE. The details shall include a description of the method used in the TOE to assure that the specific unauthorized data flow will be blocked. The document shall also provide justification for each method used based on the threats defined in Chapter 2 of this PP.

D.4 Firmware Dependencies

Documentation shall include a section dedicated to areas in the TOE where isolation strength depends on firmware functions. This shall describe how all microcontrollers or other components handle multiple data streams coupled to multiple computers. The documentation shall describe the methods used to assure that firmware failure would not result in catastrophic TOE data isolation failure.

E Peripheral Device Connections

E.1 General

This appendix provides a list of unauthorized devices and interface protocols referenced by FDP_PDC_EXT.1.

E.2 Unauthorized Peripheral Devices

The following are unauthorized devices:

- USB Mass Storage Device
- Any unauthorized device connected to the PSD through a USB hub

E.3 Unauthorized Interface Protocols

The following are unauthorized interface protocols:

- PS/2

F Rationale

F.1 SFR Dependencies Analysis

The dependencies between SFRs implemented by the TOE are addressed as follows.

SFR	Dependencies	Rationale Statement
FAU_GEN.1	FPT_STM.1	Included
FDP_APC_EXT.1	None	N/A
FDP_PDC_EXT.1	None	N/A
FDP_RIP_EXT.1	None	N/A
FDP_RIP_EXT.2	None	N/A
FDP_SWI_EXT.1	None	N/A
FDP_SWI_EXT.2	FDP_SWI_EXT.1	Included
FIA_UAU.2	FIA_UID.1	Included
FIA_UID.2	None	N/A
FMT_MOF.1	FMT SMF.1 FMT_SMR.1	Included Included
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	Included
FPT_FLS_EXT.1	FPT_TST.1 FPT_PHP.3	Included Included only if anti-tamper is selected in FPT_FLS_EXT.1.1
FPT_NTA_EXT.1	None	N/A
FPT_PHP.1	None	N/A
FPT_PHP.3	None	N/A
FPT_STM.1	Included	N/A
FPT_TST.1	None	N/A
FPT_TST_EXT.1	FPT_TST.1	Included
FTA_CIN_EXT.1	FDP_APC_EXT.1	Included

F.2 Security Functional Requirement to Objective Mapping & Analysis

The Security Functional Requirements to objectives mapping and rationale are as follows:

Security Objective(s)	Security Functional Requirement	Rationale
O.COMPUTER_INTERFACE_ISOLATION	FDP_APC_EXT.1	This prevents unauthorized data flows between the different computer interfaces in the TOE.

Security Objective(s)	Security Functional Requirement	Rationale
O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED	FDP_APC_EXT.1	This prevents data flows between the different computer interfaces in the TOE, even when the TOE itself is unpowered.
O.USER_DATA_ISOLATION	FDP_APC_EXT.1	This ensures that user data will only transit the TOE to the computer that the user has explicitly selected it to go to and provides isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
O.NO_USER_DATA_RETENTION	FDP_RIP_EXT.1, FDP_RIP_EXT.2	This mitigates the threat by preventing user data retention by the TOE when it is being powered off (i.e., user data is not stored in non-volatile memory). If a factory reset capability is provided, this is another method by which data in residual memory could be made unavailable.
O.NO_OTHER_EXTERNAL_INTERFACES	FDP_PDC_EXT.1	This ensures all unauthorized devices and external interfaces are rejected, thus ensuring no signal data can be injected into the user data.
O.LEAK_PREVENTION_SWITCHING	FDP_SWI_EXT.1, FDP_SWI_EXT.2	By preventing the use of unauthorized switching methods, signaling data leakage between connected computers is also prevented.
O.AUTHORIZED_USAGE	FAU_GEN.1, FDP_SWI_EXT.1, FDP_SWI_EXT.2, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_SMF.1, FMT_SMR.1, FPT_STM.1, FTA_CIN_EXT.1	The SFRs mapped to this objective enforce authorized usage of the TOE through ensuring that the TOE either supports only one connected computer or by ensuring users can only control the behavior of peripheral and computer interfaces using authorized mechanisms, and through ensuring that administrators can only perform management functions with proper authorization. They also ensure that unauthorized usage is detected through the use of an auditing function and that a user does not inadvertently perform an action against an unintended computer through continuous indications of the selected port(s).
O.PERIPHERAL_PORTS_ISOLATION	FDP_APC_EXT.1	This ensures that there is no method by which unauthorized data flow can occur between peripheral ports.
O.REJECT_UNAUTHORIZED_PERIPHERAL	FDP_PDC_EXT.1	This ensures the TOE rejects or otherwise prevents operation of unauthorized peripheral devices or protocols to work with the TOE.
O.REJECT_UNAUTHORIZED_ENDPOINTS	FDP_PDC_EXT.1	The PSD enforces rules for peripheral device connections by rejecting unauthorized peripheral devices connected via a USB hub.

Security Objective(s)	Security Functional Requirement	Rationale
O.NO_TOE_ACCESS	FPT_NTA_EXT.1	This ensures the PSD firmware, software, and memory is not accessible via its external ports.
O.TAMPER_EVIDENT_LABEL	FPT_PHP.1	This provides additional assurance that the physical boundary of the TOE has not been breached by ensuring the TOE provides a visible unique identifying tamper-evident label. The use of a tamper evident label provides assurance that the TOE is genuine and was not modified or substituted during shipping or storage.
O.ANTI_TAMPERING	FPT_PHP.1 FPT_PHP.3	These SFRs implement anti-tampering by providing tamper protection and potentially tamper response functionality.
O.SELF_TEST	FPT_TST_EXT.1	The PSD performs self-tests following power up or powered reset to increase the likelihood that a malfunction in the TSF is detected.
O.SELF_TEST_FAIL_TOE_DISABLE	FPT_FLS_EXT.1, FPT_TST_EXT.1	The PSD enters a secure state upon detection of a critical failure ensuring TSF functionality is not able to continue while the TOE is in a self-test failure state.
O.SELF_TEST_FAIL_INDICATION	FPT_TST_EXT.1	The PSD provides the user with a means to determine when the TOE is in a self-test failure state by providing clear and visible user indications of a self-test failure.

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

H Acronyms

Acronym	Meaning
EDID	Extended Display Identification Data
KM	Keyboard, Mouse
KVM	Keyboard, Video and Mouse
PC	Personal Computer
PSD	Peripheral Sharing Device
PS/2	Personal System/2
USB	Universal Serial Bus