Supporting Document

Mandatory Technical Document

PP-Module for Keyboard/Mouse Devices

Version: 1.0

2019-07-19

National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the Common Criteria Recognition Arrangement (CCRA).

Technical Editor:

National Information Assurance Partnership (NIAP)

Document history:

V1.0, July 2019 (Initial)

General Purpose:

The purpose of this SD is to define evaluation methods for the functional behavior of peripheral sharing devices that support keyboard and/or mouse (KM) peripherals.

Field of special use:

This Supporting Document applies to the evaluation of TOEs claiming conformance with the PP-Module for Keyboard/Mouse Devices.

Acknowledgements:

The NIAP Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia, supported the development of this SD.

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the PP-Module for Keyboard/Mouse Devices is to describe the security functionality of keyboard/mouse types of peripheral devices to be connected to Peripheral Sharing Devices in terms of [CC] and to define functional and assurance requirements for such products. The PP-Module is intended for use with the following Base-PPs:

- Protection Profile for Peripheral Sharing Devices, version 4.0 (PP_PSD_V4.0 or PSD PP)

This SD is mandatory for evaluations of TOEs that claim conformance to the following PP-Module:

- PP-Module for Keyboard/Mouse Devices (MOD_KM_V1.0)

Although Evaluation Activities (EAs) are defined mainly for the evaluators to follow, in general they will also help Developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in EAs may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for isolation documentation).

1.2 Structure of the Document

EAs can be defined for both SFRs and Security Assurance Requirements (SAR). These are defined in separate sections of the SD.

If any EA cannot be successfully completed in an evaluation then the overall verdict for the evaluation is a 'fail'. In rare cases, there may be acceptable reasons why an EA may be modified or deemed not applicable for a particular TOE, but this must be agreed with the Certification Body for the evaluation.

In general, if all EAs (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a 'pass'. To reach a 'fail' verdict when the EAs have been successfully completed would require a specific justification from the evaluator as to why the EAs were not sufficient for that TOE.

Similarly, at the more granular level of Assurance Components, if the EAs for an Assurance Component and all of its related SFR EAs successfully completed in an evaluation then it would be expected that the verdict for the Assurance Component is a 'pass'. To reach a 'fail' verdict for the Assurance Component when these EAs have been successfully completed would require a specific justification from the evaluator as to why the EAs were not sufficient for that TOE.

1.3 Terminology

1.3.1 Glossary

Reference the terms sections of the PSD PP and MOD_KM_V1.0 in addition to the terms listed below.

Term	Definition
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).

Term	Definition
BadUSB	A malicious Universal Serial Bus (USB) device that presents itself as a legitimate mass storage device that can change its USB Class.
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
NAK Transaction	A standard USB PID 1010B transaction used to indicate the receiving device cannot accept data or the transmitting device cannot send data.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent set of security requirements for a specific subset of products described by a PP.
Resistor	Limits the current flow in an electronic circuit.
Security Assurance Requirement (SAR)	A requirement for how the TOE's proper implementation of the SFRs is verified by an evaluator.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Supplementary Information	Information not necessarily included in the ST or operational guidance, and may not necessarily be public. Examples of such information would be entropy analysis, or description of a cryptographic key management architecture used in (or in support of) the TOE. The corresponding PP or PP-Module identifies the requirement for supplementary information.
USB Class	A class code sent to a USB host that defines the functionality of a USB device.
USB Dummy Load	A USB Type-A plug with resistor connected between positions 1 and 4 and used to simulate power overloading of a TOE USB peripheral device interface.
USB Protocol Analyzer Software	Software running on a computer capable of capturing, analyzing, and displaying all USB traffic passing through the computer's USB ports.
USB Rubber Ducky	A malicious USB device that presents itself as a legitimate USB-HID, which can change its USB class.
USB Sniffer	Hardware device connected between a USB interface and USB device capable of capturing, analyzing, and displaying all USB traffic passing to or from that specific USB device.

1.3.2 Acronyms

Reference the acronyms section of the PSD PP and MOD_KM_v1.0 in addition to the acronyms listed below.

Acronym	Meaning
NAK	Negative Acknowledgement

2 Evaluation Activities for SFRs

The EAs presented in this section are intended to supplement those defined in the PSD PP.

MOD_KM_V1.0 relies on several PSD PP SFRs to help in the implementation of its required functionality. These SFRs are listed in this section along with any impact to how they are to be evaluated in a TOE that includes the PP-Module. This section also defines the EAs for the mandatory SFRs that are introduced in the PP-Module.

Successful completion of these EAs assists in the completion of the relevant portions of ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1, which are required to be applied to the entire TOE as per CFG_PSD-AO-KM-UA-VI_V1.0, CFG_PSD-AO-KM-VI_V1.0, CFG_PSD-KM_V1.0, CFG_PSD-KM-UA_V1.0, CFG_PSD-KM-UA-VI_V1.0, and CFG_PSD-KM-VI_V1.0.

2.1 Test Environment for Evaluation Activities

In order to be sure the TOE demonstrates the functionality the EAs require, it is necessary for the evaluator to be sure they have appropriate equipment to conduct the required testing. The following is a list of the additional equipment needed to perform the testing described in this SD along with the purpose of each piece of equipment.

- Keyboard – used to generate text entry inputs
- Keyboard emulator software application – used to verify unidirectional communication
- Mouse – preferably an optical mouse with colored visible light – used to generate pointing device inputs
- Switchable 5 volt power supply with a USB Type-B plug – used to verify electrical signals are not sent to non-selected computers
- USB audio headset – used to verify the peripheral device connections
- USB camera – used to verify the peripheral device connections
- USB composite device evaluation board – used to verify the peripheral device connections
- USB dummy load – used to verify electrical signals are not sent to non-selected computers
- USB gaming mouse with programmable LEDs – used to verify unidirectional communication
- USB generator – used to verify emulation of keyboard and mouse functions
- USB hub – used to verify the peripheral device connections
- USB mass storage device – used to verify the peripheral device connections
- USB printer – used to verify the peripheral device connections
- USB protocol analyzer software – used to verify the presence or absence of USB traffic
- USB rubber ducky/BadUSB/Programmable Keyboard – used to verify the TOE rejects devices that re-enumerate as unauthorized devices
- USB sniffer – used to verify the presence or absence of USB traffic
- USB wireless LAN dongle – used to verify the peripheral device connections

This equipment is required in addition to that which is relevant for testing any PSD as defined in the PSD PP.

When conducting testing, the evaluator must be sure to test all combinations of switch selections. For example, if testing a device with two HID interfaces and eight computer interfaces, the evaluator may use two connected computers, but must change the connected ports several times to be sure to test each of the possible variations of switch positions.

2.2 PSD Evaluation Activities

The EAs defined in this section are additional activities for the PSD PP that the evaluator shall perform when the ST claims the PP-Module for Keyboard/Mouse Devices. The evaluator shall perform these actions in addition to those required by the PSD PP (and by any other PP-Modules in the claimed PP-Configuration).

2.2.1 Security Audit (FAU)

2.2.1.1 Security Audit Data Generation (FAU_GEN)

FAU_GEN.1 Audit Data Generation

There are no changes to the EAs for this SFR. MOD_KM_V1.0 changes this requirement from optional to selection-based, but otherwise makes no changes to it.

2.2.2 User Data Protection (FDP)

2.2.2.1 Active PSD Connections (FDP_APC_EXT)

FDP_APC_EXT.1 Active PSD Connections

Isolation Document
The evaluator shall examine the Isolation Document and verify it describes how the TOE ensures that no data or electrical signals flow between connected computers in both cases (powered on, powered off).

TSS
There are no TSS EAs for this component beyond what the PSD PP requires.

Guidance
There are no guidance EAs for this component beyond what the PSD PP requires.

Test
For tests that use the USB sniffer or USB analyzer software, the evaluator verifies whether traffic is sent or not sent by inspection of the passing USB transactions and ensuring they do not contain USB data payloads other than any expected traffic, as well as USB NAK transactions or system messages. To avoid clutter during USB traffic capture, the evaluator may filter NAK transactions and system messages.

The evaluator shall perform the following tests:

Test 1-KM – KM Switching methods

[Conditional: Perform this test if “switching can be initiated only through express user action” is selected in FDP_SWI_EXT.1.1 in the PSD PP]

While performing this test, ensure that switching is always initiated through express user action.

This test verifies the functionality of the TOE’s KM switching methods.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect an authorized peripheral device for each peripheral device type selected in FDP_PDC_EXT.3.1/KM. Run an instance of a text editor on each connected computer.

Step 2: Connect a display to each computer in order to see all computers at the same time, turn on the TOE, and enter text or move the cursor to verify which connected computer is selected.

Step 3: For each switching method selected in FDP_SWI_EXT.2.2, switch selected computers in accordance with the operational user guidance, and verify that it succeeds.

Step 4: For each peripheral device type selected in FDP_PDC_EXT.3.1/KM, attempt to switch the device to more than one computer at once and verify that the TOE ignores all such commands or otherwise prevents the operation from executing.

Step 5: [Conditional: If "keyboard" is selected in FDP_PDC_EXT.3.1/KM, then] attempt to control the computer selection using the following standard keyboard shortcuts, where '#' represents a computer channel number, and verify that the selected computer is not switched:

- Control - Control - # - Enter
- Shift - Shift - #
- Num Lock - Minus - #
- Scroll Lock - Scroll Lock - #
- Scroll Lock - Scroll Lock - Function #
- Scroll Lock - Scroll Lock - arrow (up or down)
- Scroll Lock - Scroll Lock - # - enter
- Control - Shift - Alt - # - Enter
- Alt - Control - Shift - #

Step 6: [Conditional: If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] attempt to switch to other connected computers using the pointing device and verify that it does not succeed.

Step 7: [Conditional: If "peripheral devices using a guard" is selected in FDP_SWI_EXT.2.2, then] attempt to switch to other connected computers using the peripheral device and guard by only performing some of the steps outlined in the operational user guidance, and verify that it does not succeed.

Test 2-KM – Positive and Negative Keyboard and Mouse Data Flow Rules Testing

This test verifies the functionality for correct data flows of a mouse and keyboard during different power states of the selected computer.

Step 1: Continue with the test setup from Test 1 and for each connected computer, connect a USB sniffer between it and the TOE or open the USB analyzer software. Perform steps 2-12 with each connected computer as the selected computer.

Step 2: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer.

[Conditional: Perform steps 3-10 if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.]

Step 3: [If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] switch the TOE to each connected computer, and use the mouse to position the mouse cursor at the center of each display. Switch the TOE back to the originally selected computer.

Step 4: [If “keyboard is selected in FDP_PDC_EXT.3.1/KM, then] use the keyboard to enter text into the text editor. [If “mouse” is selected in FDP_PDC_EXT.3.1/KM, then] use the mouse to move the cursor to the bottom right corner of the display.

Step 5: Switch to each connected computer and verify that the actions taken in Step 4 did not occur on any of the non-selected computers.

Step 6: Switch to the originally selected computer. Continue exercising the functions of the peripheral device(s) and examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent.

Step 7: Disconnect and reconnect the TOE interface cables connected to the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent.

Step 8: Reboot the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent.

Step 9: Enter sleep or suspend mode in the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers to verify that no traffic is sent.

Step 10: Exit sleep or suspend mode on the selected computer. Examine the USB protocol analyzers on each of the non-selected computers to verify that no traffic is sent. Ensure that any text in the Text Editor application is deleted.

Step 11: Perform step 12 when the TOE is off and then in a failure state.

Step 12: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that no results are observed on the selected computer and that no traffic is captured using the USB analyzer.

Test 3-KM – Flow Isolation and Unidirectional Rule

This test verifies that the TOE properly enforces unidirectional flow and isolation.

Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance.

Perform steps 2-12 with each connected computer as the selected computer.

Step 2: Ensure the TOE is powered on and connect a display directly to the selected computer. Open a real-time hardware information console on the selected computer.

[If “mouse” is selected in FDP_PDC_EXT.3.1/KM, then perform steps 3-4]

Step 3: Connect a gaming mouse with programmable LEDs directly to the selected computer and attempt to configure the LEDs using the mouse application running on the selected computer. Verify that the mouse programmable LEDs change state.

Step 4: Disconnect the gaming mouse from the selected computer and connect it to the TOE mouse peripheral device port through the USB sniffer. Attempt to configure the LEDs using the mouse application running on the selected computer. Verify that the mouse programmable LEDs do not change state and that no traffic is sent and captured by the USB sniffer while the evaluator is not moving the mouse.

[If “keyboard” is selected in FDP_PDC_EXT.3.1/KM, then perform step 5]

Step 5: Connect a keyboard to the peripheral device interface through the USB sniffer. Use a keyboard emulation software application running on the selected computer to turn the keyboard Num Lock, Caps Lock, and Scroll Lock LEDs on and off. Verify that the LEDs on the keyboard do not change state and that no traffic is sent and captured by the USB sniffer.

Step 6: Power down the TOE and disconnect the peripheral interface USB cable from the TOE to the selected computer and the peripheral devices from the TOE.

Step 7: Power up the TOE and ensure the selected computer has not changed (this should have no effect on the selected computer because it was disconnected in the previous step). Reconnect the peripheral devices disconnected in step 6 to the TOE.

Step 8: [If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] check that immediately following the connection, the mouse LEDs are illuminated (indicating that the peripheral devices are powered on, although the selected computer is not connected). [If "keyboard" is selected in FDP_PDC_EXT.3.1/KM, then] check that immediately following the connection, the Num Lock, Caps Lock, and Scroll Lock keyboard LEDs are blinking momentarily and then stay off (indicating that the keyboard is powered on, although the selected computer is not connected).

Step 9: Turn the TOE off and disconnect the peripheral devices connected in step 6.

Step 10: Reconnect the first computer interface USB cable to the TOE.

Step 11: Turn on the TOE and check the computer real-time hardware information console for the presence of the peripheral devices connected in step 6 and disconnected in step 9. The presence of the TOE peripheral devices in the information console when the peripheral devices are not connected to the TOE indicates that the TOE emulates the KM devices.

Step 12: [Conditional] If the TOE keyboard and mouse do not appear in the listed devices, repeat the following steps for both mouse and keyboard to simulate USB traffic:

- Connect a USB generator to the TOE peripheral device interface port.
- Configure the USB generator to enumerate as a generic HID mouse/keyboard device and then to generate a random stream of mouse/keyboard report packets.
- Connect a USB sniffer device between the TOE computer interface and the USB port on the first computer to capture the USB traffic between the TOE and the first computer.
- Turn on the TOE and verify that no packets cross the TOE following the device enumeration.

Test 4-KM – No Flow between Computer Interfaces

[Conditional: Perform this test if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP]

This test verifies correct data flow while the TOE is powered on or powered off.

Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. Connect a display directly to each connected computer. Perform steps 2-10 for each connected computer.

Step 2: Connect a USB sniffer between a non-selected TOE KM computer interface and its computer. Run USB protocol analyzer software on all remaining computers.

Step 3: Turn on the TOE and observe the TOE enumeration data flow in the protocol analyzer connected to the selected computer and is not in any other USB protocol analyzers or the USB sniffer.

Step 4: Ensure the TOE is switched to the first computer.

Step 5: Reboot the first computer. Verify that no USB traffic is captured on all non-selected computer USB protocol analyzers.

Step 6: Generate intensive USB HID traffic by moving the mouse at high speed and/or holding down the keyboard space key at the same time. Verify that no new USB traffic is captured on all non-selected computer USB protocol analyzers.

Step 7: Perform steps 8 and 9 for each TOE keyboard/mouse peripheral interface.

Step 8: Connect a USB dummy load into the TOE KM peripheral device interface. Verify that no new USB traffic is captured on all non-selected computer USB protocol analyzers. Remove the plug after the step is completed.

Step 9: Connect a switchable 5 volt power supply with a USB Type-B plug into the TOE KM peripheral device interface. Modulate the 5 volt supply (i.e., cycle on and off) manually at various speeds from approximately one cycle per five seconds to one cycle per second. Verify that no new USB traffic is captured on all non-selected computer USB analyzers.

Step 10: Turn off the TOE. Verify that no new traffic is captured.

Test 5-KM – No Flow between Connected Computers over Time

This test verifies that the TOE does not send data to different computers connected to the same interface at different times. Repeat this test for each TOE KM computer port.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect an authorized peripheral device for each peripheral device type selected in FDP_PDC_EXT.3.1/KM. Connect two computers to a different display and run an instance of a text editor and USB analyzer software on each computer.

Step 2: Connect the first computer to the TOE and ensure it is selected and that no other computers are connected.

Step 3: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer.

Step 4: Disconnect the first computer. Generate intensive USB HID traffic by moving the mouse at high speed and/or holding down the keyboard space key at the same time.

Step 5: Cease generation of the USB HID traffic, connect the second computer to the same port and ensure it is selected.

Step 6: Verify that no results from the previous use of the peripheral device are observed on the selected computer and that no traffic is sent and captured using the USB analyzer.

Step 7: Reboot the TOE and repeat step 6.

Step 8: Turn off the TOE and repeat step 6.

Step 9: Restart the TOE and repeat step 6.

Step 10: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer.

2.2.2.2 Peripheral Device Connection (FDP_PDC_EXT)

FDP_PDC_EXT.1 Peripheral Device Connection

Isolation Document
There are no Isolation Document evaluation activities for this component beyond what the PSD PP requires.
TSS
There are no TSS EAs for this component beyond what the PSD PP requires.

Guidance
The evaluator shall verify that the operational user guidance describes devices authorized for use with the TOE in accordance with the authorized peripheral device connections.

Test
Test 1-KM:

The evaluator shall verify that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections.

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, no traffic captured on the USB sniffer or analyzer software other than NAK transactions or system messages, or incompatibility of the device interface with the peripheral interface. Also verify device rejection through examination of the USB sniffer or analyzer software for no traffic captured other than NAK transactions or system messages and through examination of the real-time hardware console for no display of new USB devices (recognized or not recognized).

Repeat this test for each keyboard/mouse TOE peripheral interface.

Perform steps 1-6 for each of the following unauthorized devices:

- USB audio headset
- USB camera
- USB printer
- USB user authentication device connected to a TOE keyboard/mouse peripheral interface
- USB wireless LAN dongle

Step 1: Ensure the TOE is powered off and connected to a computer. Run USB analyzer software on the connected computer and connect a USB sniffer to the TOE keyboard/mouse peripheral interface. Open the real-time hardware information console.

Step 2: Attempt to connect the unauthorized device to the USB sniffer.

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

Step 4: Ensure the unauthorized device is disconnected from the USB sniffer, then attempt to connect it to the USB sniffer again.

Step 5: Verify the device is rejected.

Step 6: Repeat steps 1 through 5 with a USB hub connected between the USB device and USB sniffer and observe that the results are identical.

Step 7: Repeat steps 1-6 with a composite device with non-HID device classes and verify that the non-HID functions are rejected or the entire device is rejected.

Test 2-KM:

The evaluator shall verify that the TOE KM ports do not reject authorized devices and devices with authorized protocols as per the authorized peripheral device connections.

Repeat this test for each of the following four device types:

- Barcode reader;
- Keyboard or Keypad;
- Mouse, Touchscreen, Trackpad, or Trackball; and
- PS/2 to USB adapter (with a connected PS/2 keyboard or mouse).

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Run an instance of a text editor on a connected computer.

Step 2: Ensure the TOE is powered off.

Step 3: Connect the authorized device to the TOE peripheral interface.

Step 4: Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present.

Step 5: Ensure the connected computer is selected and send inputs using the authorized devices. Verify that the input is received into the text editor or on the screen of the connected computer.

Step 6: Disconnect the authorized device, and then reconnect it to the TOE KM peripheral device interface.

Step 7: Verify the TOE user indication described in the operational user guidance is not present.

Step 8: Send inputs using the authorized devices. Verify that the input is received into the text editor or on the screen of the connected computer.

2.2.2.3 PSD Switching (FDP_SWI_EXT)

FDP_SWI_EXT.2 PSD Switching Methods

Isolation Document
There are no additional Isolation Document evaluation activities for this SFR.

TSS
If “peripheral devices using a guard” is selected, the evaluator shall verify that the TSS describes the implementation of the guard function, and verify that multiple, simultaneous express user action is required to switch between connected computers using connected peripheral devices.

Guidance

If “peripheral devices using a guard” is selected, the evaluator shall verify that the user guidance describes the steps the user must take as required by the guard to switch between connected computers using a connected peripheral pointing device.

Test
The evaluator shall ensure that switching is always initiated through express user action using the selected mechanisms throughout testing for FDP_APC_EXT.1 above.

Additional tests for this SFR are performed in FDP_APC_EXT.1 test 1-KM above.

2.2.3 Identification and Authentication (FIA)

2.2.3.1 User Authentication (FIA_UAU)

FIA_UAU.2 User Authentication Before Any Action

There are no changes to the EAs for this SFR. MOD_KM_V1.0 changes this requirement from optional to selection-based, but otherwise makes no changes to it.

2.2.3.2 User Identification (FIA_UID)

FIA_UID.2 User Identification Before Any Action

There are no changes to the EAs for this SFR. MOD_KM_V1.0 changes this requirement from optional to selection-based, but otherwise makes no changes to it.

2.2.4 Security Management (FMT)

2.2.4.1 Management of Functions in TSF (FMT_MOF)

FMT_MOF.1 Management of Security Functions Behavior

There are no changes to the EAs for this SFR. MOD_KM_V1.0 changes this requirement from optional to selection-based, but otherwise makes no changes to it.

2.2.4.2 Specification of Management Functions (FMT_SMF)

FMT_SMF.1 Specification of Management Functions

There are no changes to the EAs for this SFR. MOD_KM_V1.0 changes this requirement from optional to selection-based, but otherwise makes no changes to it.

2.2.4.3 Security Management Roles (FMT_SMR)

FMT_SMR.1 Security Roles

There are no changes to the EAs for this SFR. MOD_KM_V1.0 changes this requirement from optional to selection-based, but otherwise makes no changes to it.

2.2.5 Protection of the TSF (FPT)

2.2.5.1 Time Stamps (FPT_STM)

FPT_STM.1 Reliable Time Stamps

There are no changes to the EAs for this SFR. MOD_KM_V1.0 changes this requirement from optional to selection-based, but otherwise makes no changes to it.

2.3 TOE SFR Evaluation Activities

2.3.1 User Data Protection (FDP)

2.3.1.1 Peripheral Device Connection (FDP_PDC_EXT)

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

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

TSS
TSS evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

Guidance
Guidance evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

Test
Testing of this component is performed through evaluation of FDP_PDC_EXT.1 Test 2 as specified in section 2.2.2.2 above.

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

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

TSS
The evaluator shall examine the TSS and verify it describes which types of peripheral devices that the PSD supports.

The evaluator shall examine the TSS to verify that keyboard or mouse device functions are emulated from the TOE to the connected computer.

Guidance
There are no guidance EAs for this component.

Test
Test activities for this SFR are covered under FDP_APC_EXT.1 tests 1-KM and 3-KM.

2.3.1.2 Unidirectional Data Flow (FDP_UDF_EXT)

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

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

TSS

The evaluator shall examine the TSS to verify that it describes if and how keyboard Caps Lock, Num Lock, and Scroll Lock indications are displayed by the TOE and to verify that keyboard internal LEDs are not changed by a connected computer.

The evaluator shall examine the TSS to verify that keyboard and mouse functions are unidirectional from the TOE keyboard/mouse peripheral interface to the TOE keyboard/mouse computer interface.

Guidance
There are no guidance EAs for this component.

Test
Test activities for this SFR are covered under FDP_APC_EXT.1 test 3-KM.

3 Evaluation Activities for Optional Requirements

3.1 SFR Evaluation Activities for Optional Requirements

3.1.1 User Data Protection (FDP)

3.1.1.1 Device Filtering (FDP_FIL_EXT)

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

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

TSS
The evaluator shall examine the TSS and verify that it describes whether the PSD has configurable or fixed device filtering.

[Conditional - If "configurable" is selected in FDP_FIL_EXT.1.1/KM, then:] the evaluator shall examine the TSS and verify that it describes the process of configuring the TOE for whitelisting and blacklisting KM peripheral devices, including information on how this function is restricted to administrators. The evaluator shall verify that the TSS does not allow TOE device filtering configurations that permit unauthorized devices on KM interfaces.

Guidance
[Conditional - If "configurable" is selected in FDP_FIL_EXT.1.1/KM, then:] the evaluator shall examine the guidance documentation and verify that it describes the process of configuring the TOE for whitelisting and blacklisting KM peripheral devices and the administrative privileges required to do this.

Test
Test 1

Perform the test steps in FDP_PDC_EXT.1 with all devices on the PSD KM blacklist and verify that they are rejected as expected.

Test 2

[Conditional: Perform this only if "configurable" is selected in FDP_FIL_EXT.1.1/KM]

In the following steps the evaluator shall verify that whitelisted and blacklisted devices are treated correctly.

Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance.

Step 2: Connect to the TOE KM peripheral device interface a composite device which contains a HID class and a non-HID class.

Step 3: Configure the TOE KM CDF to whitelist the composite device.

Step 4: Verify that the HID-class part is accepted and that the non-HID class part is rejected through real-time device console and USB sniffer capture, or that the entire device is rejected.

Step 5: Configure the TOE KM CDF to blacklist the device.

Step 6: Verify that both the HID-class part and the non-HID class part is rejected through real-time device console and USB sniffer capture.

3.1.1.2 Re-Enumeration Device Rejection (FDP_RDR_EXT)

FDP_RDR_EXT.1 Re-Enumeration Device Rejection

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

TSS
The evaluator shall examine the TSS to verify that it describes how the TSF identifies and rejects a device that attempts to enumerate again as a different device.

Guidance
There are no guidance EAs for this component.

Test
The evaluator shall use a BadUSB, programmable keyboard, and/or USB Rubber Ducky as a malicious USB device to perform the following test:

Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. Ensure the TOE is powered off and connect a USB sniffer between the TOE and a computer. Open the real-time hardware information console.

Step 2: Configure the malicious USB device as a HID-class device and to re-enumerate as a mass storage device.

Step 3: Connect the malicious USB device to the TOE KM peripheral interface.

Step 4: Power on the TOE and activate the re-enumeration after 1 minute.

Step 5: Verify device rejection per TOE guidance, the cessation of traffic passed in the USB sniffer, and the absence of the device and any new devices in the information console.

Step 6: Remove the malicious USB device and reconfigure as a HID-class device and to re-enumerate as a mass storage device.

Step 7: Connect the malicious USB device to the TOE KM peripheral interface and activate the re-enumeration after 1 minute.

Step 8: Verify device rejection per TOE guidance, the cessation of traffic passed in the USB sniffer, and the absence of the device and any new devices in the information console.

4 Evaluation Activities for Selection-Based Requirements

4.1 Selection-Based SFR Evaluation Activities

4.1.1 User Data Protection (FDP)

4.1.1.1 Residual Information Protection (FDP_RIP)

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

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

TSS
The evaluator shall verify that the TSS indicates whether or not the TOE has user data buffers.

The evaluator shall verify that the TSS describes how all keyboard data stored in volatile memory is deleted upon switching computers.

Guidance
There are no guidance EAs for this component.

Test
There are no test EAs for this component.

4.1.1.2 PSD Switching (FDP_SWI_EXT)

FDP_SWI_EXT.3 Tied Switching

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

TSS
The evaluator shall verify that the TSS does not indicate that keyboard and mouse devices may be switched independently to different connected computers.

Guidance
The evaluator shall verify that the guidance does not describe how to switch the keyboard and mouse devices independently to different connected computers.

Test
The evaluator shall verify that the keyboard and mouse devices are always switched together to the same connected computer throughout testing in FDP_APC_EXT.1 in section 2.2.2.1 above.

Tests for this SFR are performed in FDP_APC_EXT.1 test 1-KM in section 2.2.2.1 above.

5 Evaluation Activities for SARs

To evaluate the SARs specified by CFG_PSD-AO-KM-UA-VI_V1.0, CFG_PSD-AO-KM-VI_V1.0, CFG_PSD-KM_V1.0, CFG_PSD-KM-UA_V1.0, CFG_PSD-KM-UA-VI_V1.0, and CFG_PSD-KM-VI_V1.0, the evaluator shall perform the SAR EAs defined in the PSD PP against the entire TOE as applicable (i.e., both the generic PSD portion and the portion(s) related to support for specific peripheral types).

6 Required Supplementary Information

This Supporting Document refers in various places to the possibility that 'supplementary information' may need to be supplied as part of the deliverables for an evaluation. This term is intended to describe information that is not necessarily included in the Security Target or operational guidance, and that may not necessarily be public. Examples of such information could be a Letter of Volatility or isolation documentation. The requirement for any such supplementary information will be identified in the relevant PP, PP-Module, or Supporting Document.

The PSD PP requires an Isolation Document to be included with the TOE for evaluation of isolation requirements. The EAs the evaluator is to perform are captured under the appropriate SFR.

7 References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017
[PP_PSD_V4.0 or PSD PP]	Protection Profile for Peripheral Sharing Devices, Version 4.0, July 2019
[MOD_KM_V1.0]	PP-Module for Keyboard/Mouse Devices, Version 1.0, July 2019
[CFG_PSD-AO-KM-UA-VI_V1.0]	PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, Version 1.0, July 2019
[CFG_PSD-AO-KM-VI_V1.0]	PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, and Video/Display Devices, Version 1.0, July 2019
[CFG_PSD-KM_V1.0]	PP-Configuration for Peripheral Sharing Device and Keyboard/Mouse Devices, Version 1.0, July 2019
[CFG_PSD-KM-UA_V1.0]	PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices and User Authentication Devices, Version 1.0, July 2019
[CFG_PSD-KM-UA-VI_V1.0]	PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, Version 1.0, July 2019
[CFG_PSD-KM-VI_V1.0]	PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and Video/Display Devices, Version 1.0, July 2019