Supporting Document

Mandatory Technical Document

PP-Module for User Authentication 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 video output peripherals.

Field of special use:

This Supporting Document applies to the evaluation of TOEs claiming conformance with the PP-Module for User Authentication Devices, Version 1.0, July 2019 (MOD_UA_V1.0).

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 User Authentication Devices is to describe the security functionality of user authentication devices, external or internal, used with 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 User Authentication Devices (MOD_UA_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

For definitions of standard CC terminology, see [CC] part 1.

Reference the terms sections of PSD PP and MOD_UA_V1.0.

1.3.2 Acronyms

Reference the acronyms section of PSD PP and MOD_UA_V1.0 in addition to the acronyms listed below.

Acronym	Meaning
DVM	Digital Voltmeter
LED	Light Emitting Diode
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_UA_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 this 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-UA_V1.0, CFG_PSD-KM-UA-VI_V1.0, CFG_PSD-KM-UA_V1.0, or CFG_PSD-AO-KM-UA-VI_V1.0.

2.1 Test Environment for Evaluation Activities

In order to ensure that the TOE demonstrates the functionality required by the EAs, it is necessary for the evaluator to ensure that 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 Supplementary Document along with the purpose of each piece of equipment:

- Digital voltmeter – used to verify power flow to the user authentication device; must have a time lapse feature
- 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 hub – used to verify the peripheral device connections
- USB keyboard – used to verify the peripheral device connections and that the user authentication function is isolated from other USB functions
- USB printer – used to verify the peripheral device connections
- USB protocol analyzer software – used to verify the presence or absence of USB traffic
- USB sniffer – used to verify the presence or absence of USB traffic; may be used in place of the USB analyzer
- USB Type-C with DisplayPort as alternate function monitor – used to verify the user authentication function is isolated from other USB functions
- USB user authentication device with power LED – used to connect authenticate sessions
- USB wireless LAN dongle – used to verify the peripheral device connections

When conducting testing, the evaluator must ensure that all device configuration combinations are tested. For example, if testing a device with two peripheral device interfaces and eight computer interfaces, the evaluator may use two connected computers, but must change the selected peripheral several times to ensure that each of the possible device configuration permutations is tested.

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 User Authentication 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_UA_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
There are no Isolation Document EAs 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
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.

Test Setup

For each of the below tests the evaluator shall perform the following test set up:

1. Configure the TOE and the operational environment in accordance with the operational guidance.
2. Connect a computer to each TOE UA computer interface and a display to each connected computer.
3. Open a real-time hardware information console and USB protocol analyzer software on each connected computer.
4. Ensure the user authentication application and driver for the authorized user authentication device used for testing is installed.
5. [Conditional: if “external” is selected in FDP_PDC_EXT.4.1, then:] connect an authorized user authentication device with a power LED and a connected DVM to each PSD UA peripheral device interface.

Test 1-UA: UA 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]

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

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

Step 1. Turn on the TOE and ensure computer #1 is selected.

Step 2: Verify that the real-time hardware information console on computer #1 indicates the presence of the user authentication device. [Conditional: if “external” is selected in FDP_PDC_EXT.4.1, then:] verify the UA device power LED is illuminated and the DVM reads between 4.75 and 5.25 VDC.

Step 3: Perform steps 4-6 for each connected computer.

Step 4: For each switching method selected in FDP_SWI_EXT.2.2, switch selected computers in accordance with the operational guidance.

Step 5: [Conditional: if “external” is selected in FDP_PDC_EXT.4.1, then:] verify that the LED for the UA device is not illuminated for at least one second while the DVM reads 0.5 VDC or less for at least one second.

Step 6: Verify that the real-time hardware console on the newly selected computer indicates the presence of the user authentication device. [Conditional: if “external” is selected in FDP_PDC_EXT.4.1, then:] verify the UA device power LED is illuminated and the DVM reads between 4.75 and 5.25 VDC.

Test 2-UA: Positive and Negative UA Data Flow Rules Testing

This test verifies correct data flows of a UA device during different power states of the selected computer.

Step 1: For each connected computer, connect a USB sniffer between it and the TOE or ensure the USB analyzer software is opened. Perform steps 2-14 with each connected computer as the selected computer.

Step 2: Connect an authentication session and verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer.

Step 3: Remove the authentication element and verify the session is terminated on the selected computer.

Step 4: Insert the authentication element. Reconnect an authentication session, verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer

[Conditional: Perform steps 5-6 if “external” is selected in FDP_PDC_EXT.4.1.]

Step 5: Disconnect the UA device and verify the session is terminated on the selected computer and that the real-time hardware console does not show the device and that no traffic is sent on the USB analyzer.

Step 6: Reconnect the UA device. Reconnect an authentication session, verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer.

[Conditional: Perform steps 7-14 if “switching can be initiated only through express user action” is selected in FDP_SWI_EXT.1.1 in the PSD PP.]

Step 7: Verify that the real-time hardware console on each of the non-selected computers does not show the UA device and that no traffic is sent on the other USB analyzers.

Step 8: Switch to another connected computer. Verify that the authentication session on the previously selected computer is terminated, the real-time hardware console on each non-selected computer does not show the UA device, and that no traffic is sent on the other USB analyzers.

Step 9: Connect an authentication session and verify that the session is connected on the selected computer, the expected traffic is sent and captured using the USB analyzer, and no traffic is sent on the other USB analyzers.

Step 10: Switch to the originally selected computer. Verify the authentication session is still terminated, and reconnect an authentication session. Verify that no traffic is sent on the other USB analyzers.

Step 11: Disconnect and reconnect the TOE interface cables connected to the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent.

Step 12: Reconnect an authentication session and verify that no traffic is sent on the other USB analyzers. Reboot the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent.

Step 13: Reconnect an authentication session and verify that no traffic is sent on the other USB analyzers. Enter sleep or suspend mode in the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent.

Step 14: Exit sleep or suspend mode in the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent.

Step 15: Perform steps 16-17 when the TOE is off and then in a failure state.

Step 16: Verify that for each connected computer, no real-time hardware console shows the device and no traffic is sent on the USB analyzer.

Step 17: Verify the authentication session is terminated on the selected computer.

Test 3-UA: No Electrical 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 no electrical signals flow between connected computers when the TOE is powered on or off.

Perform this test for each TOE UA computer interface. Perform this test when the TOE is powered on and off.

Step 1: Disconnect the first computer and replace it with a switchable 5 volt power supply with a USB Type-B plug. Modulate the 5 volt supply 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 the non-selected USB analyzers.

[Conditional: Perform steps 2-4 if “external” is selected in FDP_PDC_EXT.4.1.]

Step 2: Disconnect the power supply and replace it with the computer.

Step 3: Connect the USB dummy load into the TOE UA peripheral device interface. Examine the USB analyzers on all non-selected computers and verify that no new USB traffic is captured.

Step 4: Disconnect the USB dummy load and replace it with a switchable 5 volt power supply with a USB Type-B plug. Modulate the 5 volt supply 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 the non-selected USB analyzers.

Test 4-UA: 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 UA computer port.

Note that instead of the session ID, the evaluator may substitute authentication element or other unique session identification characteristic detectable by the USB analyzer.

Step 1: Ensure only one computer is connected to the TOE and it is selected.

Step 2: Connect an authentication session and record the authentication session ID using the USB analyzer.

Step 3: Disconnect the first computer, connect the second computer to the same port, connect an authentication session, and record the authentication session ID in less time than the authentication device timeout.

Step 4: Verify that the authentication session ID is different.

Step 5: Disconnect the second computer, connect the first computer to the same port, reconnect the authentication session, and record the authentication session ID in less time than the authentication device timeout.

Step 6: Verify that the authentication session ID is different from the first two.

2.2.2.2 Peripheral Device Connection (FDP_PDC_EXT)

FDP_PDC_EXT.1 Peripheral Device Connection

Isolation Document
There are no Isolation Document EAs 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-UA: Unauthorized Device Rejection

[Conditional: Perform this test if “external” is selected in FDP_PDC_EXT.4.1]

This test verifies 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).

Perform this test for an unauthorized device presenting itself as a composite device, a USB camera, a USB audio headset, a USB printer, a USB keyboard, a USB wireless dongle, and any device listed on the PSD UA blacklist.

Repeat this for each user authentication TOE peripheral interface.

Step 1: Ensure the TOE is powered off and connected to a computer. Run USB analyzer software and open the real-time hardware console on the connected computer, and connect a USB sniffer to the unauthorized device.

Step 2: Attempt to connect the unauthorized device via the USB sniffer to the TOE UA peripheral interface.

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

Step 4: Ensure the unauthorized device is disconnected from the TOE UA peripheral interface, then attempt to connect it again.

Step 5: Verify the device is rejected.

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

Test 2-UA: Authorized Device Acceptance

[Conditional: Perform this test if "external" is selected in FDP_PDC_EXT.4.1]

This test verifies that the TOE ports do not reject authorized devices and devices with authorized protocols as per the Peripheral Device Connection Policy.

Perform this test for a USB device identified as User Authentication and any device listed on the PSD UA whitelist:

Step 1: Ensure the TOE is powered off.

Step 2: Connect the authorized device to the TOE peripheral interface.

Step 3: Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present.

Step 4: Ensure the connected computer is selected and attempt to connect an authentication session. Verify that the authentication session is successfully connected on the connected computer.

Step 5: Disconnect the authorized device, then reconnect it to the TOE peripheral interface.

Step 6: Verify the TOE user indication described in the operational user guidance is not present.

Step 7: Attempt to start an authentication session. Verify that the authentication session begins on the connected computer.

2.2.2.3 PSD Switching (FDP_SWI_EXT)

FDP_SWI_EXT.2 PSD Switching Methods

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

Test
Test performed in FDP_APC_EXT.1 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_UA_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_UA_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_UA_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_UA_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_UA_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_UA_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 Device Filtering (FDP_FIL_EXT)

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

Note: if "configurable" is selected in FDP_FIL_EXT.1.1/UA, the evaluator shall perform these activities in conjunction with the FMT_MOF.1 and FMT_SMF.1 evaluation activities specified in the PSD PP because configuring the device filtration rules involves use of the TOE's management functionality.

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

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/UA, then:] The evaluator shall examine the TSS and verify that it describes the process of configuring the TOE for whitelisting and blacklisting UA peripheral devices, including information on how this function is restricted to administrators.

Guidance
[Conditional – If "configurable" is selected in FDP_FIL_EXT.1.1/UA, then:] the evaluator shall examine the guidance documentation and verify that it describes the process of configuring the TOE for whitelisting and blacklisting UA 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 UA 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/UA]

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

Step 1: Configure the TOE UA CDF to whitelist an authorized user authentication device, connect it to the TOE UA peripheral device interface, and verify that the device is accepted through real-time device console and USB sniffer capture.

Step 2: Configure the TOE UA CDF to blacklist the device and verify that the device is rejected through real-time device console and USB sniffer capture.

Step 3: Attempt to configure the TOE UA CDF to both whitelist and blacklist the device and verify that the device is rejected through real-time device console and USB sniffer capture.

Test 3

[Conditional – Perform this only if “fixed” is selected in FDP_FIL_EXT.1.1/UA]

The evaluator shall examine the PSD UA whitelist and verify that all devices are authorized devices.

2.3.1.2 Peripheral Device Connection (FDP_PDC_EXT)

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

The EAs for this SFR are performed as part of activities for FDP_PDC_EXT.1 above.

FDP_PDC_EXT.4 Supported Authentication Device

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

TSS
The evaluator shall examine the TSS and verify that it describes whether the PSD has internal or external authentication devices.

Additional evaluation activities for STs that include the selection “external” are performed under FDP_PDC_EXT.1 in PSD PP.

Guidance
There are no guidance evaluation activities for this component.

Test
There are no test evaluation activities for this component.

2.3.1.3 Powered by Computer (FDP_PWR_EXT)

FDP_PWR_EXT.1 Powered by Computer

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

TSS
The evaluator shall examine the TSS and verify that the connected computer does not power the TOE.

Guidance
There are no guidance EAs for this component.

Test
The evaluator shall perform the following test for each connected computer:

Step 1: Ensure the power source is disconnected from the TOE.

Step 2: Connect a USB sniffer between a TOE UA computer interface and its computer, attempt to turn on the TOE, and verify the TOE is not powered on, the user authentication device is not present in the real time hardware console, and no traffic is captured in the USB sniffer.

2.3.1.4 Session Termination (FDP_TER_EXT)

FDP_TER_EXT.1 Session Termination

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

TSS
The evaluator shall examine the TSS and verify that the TOE terminates an open session upon removal of the authentication element.

Guidance
The evaluator shall examine the guidance documentation and verify that the TOE terminates an open session upon removal of the authentication element.

Test
Testing for this component is performed as part of FDP_APC_EXT.1 test 2-UA.

2.3.1.5 User Authentication Isolation (FDP_UAI_EXT)

FDP_UAI_EXT.1 User Authentication Isolation

Isolation Document
The evaluator shall examine the Isolation Documentation and verify that it describes how the TOE enforces user authentication isolation from other TOE USB functions.

TSS
The evaluator shall examine the TSS and verify that it states that the TOE has separate USB connections for user authentication functions and any other USB functions.

Guidance
The evaluator shall examine the guidance and verify that it states that the TOE has separate USB connections for user authentication functions and any other USB functions.

Test
Test 1

This test verifies that UA functionality is not sent to other USB interfaces.

Perform this test for each computer interface.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect a display directly to each connected computer. Run USB protocol analyzer software and open a real-time hardware information console and a text editor on each connected computer. Ensure an authorized user authentication device is connected.

Perform steps 2-4 for each TOE USB peripheral interface other than UA.

Step 2: Connect a USB sniffer to the TOE USB peripheral interface.

Step 3: Connect an authentication session and verify no traffic is captured on the USB sniffer.

Step 4: Disconnect the USB sniffer and the authentication session.

Perform steps 5-7 for each TOE USB computer interface other than UA.

Step 5: Connect a USB sniffer to the TOE USB computer interface and ensure that computer is selected.

Step 6: Connect an authentication session and verify no traffic is captured on the USB sniffer.

Step 7: Disconnect the USB sniffer and the authentication session.

Step 8: Power down the TOE.

Step 9: For each TOE USB interface (peripheral device and computer) other than UA, connect the USB sniffer and verify no traffic is captured.

Test 2

[Conditional: Perform this test only if the TOE supports KM functionality.]

This test verifies that KM functionality is not sent to UA interfaces.

Perform this test while the TOE is powered on and powered off.

Step 1: Connect a KM device to the TOE KM peripheral interface.

Perform steps 2-3 for each TOE UA computer interface.

Step 2: Connect a USB sniffer to the TOE UA computer interface.

Step 3: Exercise the functions of the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM in MOD_KM_V1.0 and verify that no traffic is sent and captured on the USB sniffer.

[Conditional: Perform steps 4-5 only if “external” is selected in FDP_PDC_EXT.4.1]

Step 4: Disconnect the USB sniffer and connect it to the TOE UA peripheral device interface.

Step 5: Exercise the functions of the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM in MOD_KM_V1.0 and verify that no traffic is sent and captured on the USB sniffer.

Test 3

[Conditional: Perform this test only if the TOE supports video functionality and “USB Type-C with DisplayPort as alternate function” is selected in FDP_PDC_EXT.3.1/VI in MOD_VI_V1.0.]

This test verifies that USB video functionality is not sent to UA interfaces.

Perform this test while the TOE is powered on and powered off.

Perform steps 1-3 for each TOE UA computer interface and TOE USB type-C video peripheral interface.

Step 1: Connect a USB sniffer to the TOE UA computer interface.

Step 2: Connect a monitor to the TOE USB type-C video peripheral interface and verify that no traffic is sent and captured on the USB sniffer.

Step 3: Play a video on the selected computer and verify that no traffic is sent and captured on the USB sniffer.

[Conditional: Perform steps 4-7 only if “external” is selected in FDP_PDC_EXT.4.1]

Step 4: Disconnect the monitor.

Step 5: Disconnect the USB sniffer and connect it to the TOE UA peripheral device interface.

Step 6: Reconnect the monitor to the TOE USB type-C video peripheral interface and verify that no traffic is sent and captured on the USB sniffer.

Step 7: Play a video on the selected computer and verify that no traffic is sent and captured on the USB sniffer.

3 Evaluation Activities for Optional Requirements

MOD_UA_V1.0 does not define any optional requirements.

4 Evaluation Activities for Selection-Based Requirements

4.1 User Data Protection (FDP)

4.1.1 Session Termination (FDP_TER_EXT)

FDP_TER_EXT.2 Session Termination of Removed Devices

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

TSS

The evaluator shall examine the TSS and verify that the TOE terminates an open session upon removal of the authentication device.

Guidance
The evaluator shall examine the guidance documentation and verify that the TOE terminates an open session upon removal of the authentication device.

Test
Testing for this component performed as part of FDP_APC_EXT.1 test 2-UA.

FDP_TER_EXT.3 Session Termination upon Switching

Isolation Document
The evaluator shall examine the isolation document and verify that it describes how power is reset to the user authentication device upon switching.

TSS
The evaluator shall examine the TSS and verify that the TOE terminates an open session upon switching to a different computer.

Guidance
The evaluator shall examine the guidance documentation and verify that the TOE terminates an open session upon switching to a different computer.

Test
Testing for this component is performed as part of FDP_APC_EXT.1 test 2-UA.

5 Evaluation Activities for SARs

To evaluate the SARs specified by CFG_PSD-UA_V1.0, CFG_PSD-KM-UA-VI_V1.0, CFG_PSD-KM-UA_V1.0, or CFG_PSD-AO-KM-UA-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_UA_V1.0]	PP-Module for User Authentication Devices, Version 1.0, July 2019
[MOD_KM_V1.0]	PP-Module for Keyboard/Mouse Devices, Version 1.0, July 2019
[MOD_VI_V1.0]	PP-Module for Video/Display Devices, Version 1.0, July 2019
[CFG_PSD-UA_V1.0]	PP-Configuration for Peripheral Sharing Device and User Authentication 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-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, July 2019