



# **ASSURANCE ACTIVITY REPORT**

## **High Sec Labs FI11H-M, FI11D-M, FI11PH-M Firmware Version 44404- E7E7 Peripheral Sharing Devices**

**PREPARED BY**

EWA-Canada, An Intertek Company

**PREPARED FOR**

Communications Security Establishment (CSE) and  
National Information Assurance Partnership (NIAP)

**REPORT NO**

2149-002-D007-8

**DOCUMENT VERSION**

Version 1.1

**DATE**

29 April 2024





# Contents

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>INTRODUCTION .....</b>   | <b>1</b>  |
| 1.1      | EVIDENCE .....  | 1         |
| 1.2      | REFERENCES.....   | 1         |
| <b>2</b> | <b>SECURITY FUNCTIONAL REQUIREMENT ASSURANCE ACTIVITIES.....</b>        | <b>2</b>  |
| 2.1      | USER DATA PROTECTION (FDP) .....  | 2         |
| 2.1.1    | FDP_APC_EXT.1 Active PSD Connections .....                              | 2         |
| 2.1.2    | FDP_APC_EXT.1/KM Active PSD Connections .....                           | 3         |
| 2.1.3    | FDP_APC_EXT.1/VI Active PSD Connections .....                           | 11        |
| 2.1.4    | FDP_PDC_EXT.1 Peripheral Device Connection .....                        | 20        |
| 2.1.5    | FDP_PDC_EXT.2/KM Authorized Devices (Keyboard/Mouse).....               | 28        |
| 2.1.6    | FDP_PDC_EXT.2/VI Peripheral Device Connection (Video Output).....       | 29        |
| 2.1.7    | FDP_PDC_EXT.3/KM Authorized Connection Protocols (Keyboard/Mouse) ..... | 30        |
| 2.1.8    | FDP_PDC_EXT.3/VI Authorized Connection Protocols (Video Output).....    | 31        |
| 2.1.9    | FDP_RIP_EXT.1 Residual Information Protection .....                     | 32        |
| 2.1.10   | FDP_SWI_EXT.1 PSD Switching.....  | 33        |
| 2.1.11   | FDP_UDF_EXT.1/KM Unidirectional Data Flow (Keyboard/Mouse).....         | 34        |
| 2.1.12   | FDP_UDF_EXT.1/VI Unidirectional Data Flow (Video Output) .....          | 34        |
| 2.2      | PROTECTION OF THE TSF (FPT) .....                                       | 35        |
| 2.2.1    | FPT_FLS_EXT.1 Failure with Preservation of Secure State .....           | 35        |
| 2.2.2    | FPT_NTA_EXT.1 No Access to TOE .....                                    | 35        |
| 2.2.3    | FPT_PHP.1 Passive Detection of Physical Attack.....                     | 36        |
| 2.2.4    | FPT_TST.1 TSF Testing .....   | 38        |
| 2.2.5    | FPT_TST_EXT.1 TSF Testing .....   | 39        |
| <b>3</b> | <b>EVALUATION ACTIVITIES FOR OPTIONAL REQUIREMENTS.....</b>             | <b>41</b> |
| 3.1      | USER DATA PROTECTION (FDP) .....  | 41        |
| 3.1.1    | FDP_FIL_EXT.1/KM Device Filtering (Keyboard/Mouse).....                 | 41        |
| 3.1.2    | FDP_RDR_EXT.1 Re-Enumeration Device Rejection.....                      | 43        |
| <b>4</b> | <b>SELECTION-BASED REQUIREMENTS .....</b>                               | <b>44</b> |
| 4.1      | USER DATA PROTECTION (FDP) .....  | 44        |
| 4.1.1    | FDP_CDS_EXT.1 Connected Displays Supported .....                        | 44        |
| 4.1.2    | FDP_IPC_EXT.1 Internal Protocol Conversion .....                        | 45        |



|            |   |           |
|------------|---|-----------|
| 4.1.3      | FDP_RIP.1/KM Residual Information Protection (Keyboard Data)..... | 46        |
| 4.1.4      | FDP_SPR_EXT.1/DP Sub-Protocol Rules (DisplayPort Protocol) .....  | 47        |
| 4.1.5      | FDP_SPR_EXT.1/DVI-D Sub-Protocol Rules (DVI-D Protocol) .....     | 48        |
| 4.1.6      | FDP_SPR_EXT.1/HDMI Sub-Protocol Rules (HDMI Protocol) .....       | 49        |
| <b>5</b>   | <b>SECURITY ASSURANCE REQUIREMENT ACTIVITIES .....</b>            | <b>50</b> |
| <b>5.1</b> | <b>DEVELOPMENT (ADV) .....</b>                                    | <b>50</b> |
| 5.1.1      | ADV_FSP.1 Basic Functional Specifications .....                   | 50        |
| <b>5.2</b> | <b>GUIDANCE DOCUMENTS (AGD) .....</b>                             | <b>50</b> |
| 5.2.1      | AGD_OPE.1 Operational User Guidance .....                         | 50        |
| 5.2.2      | AGD_PRE.1 Preparative Procedures.....                             | 51        |
| <b>5.3</b> | <b>LIFE-CYCLE SUPPORT (ALC) .....</b>                             | <b>51</b> |
| 5.3.1      | ALC_CMC.1 Labeling of the TOE .....                               | 51        |
| 5.3.2      | ALC_CMS.1 TOE CM Coverage.....                                    | 51        |
| <b>5.4</b> | <b>TESTS (ATE) .....</b>  | <b>52</b> |
| 5.4.1      | ATE_IND Independent Testing - Conformance.....                    | 52        |
| <b>5.5</b> | <b>VULNERABILITY ANALYSIS (AVA).....</b>                          | <b>52</b> |
| 5.5.1      | AVA_VAN.1 Vulnerability Survey.....                               | 52        |



## The Developer of the TOE:

High Sec Labs Ltd.  
29 Haeshel St  
Caesarea,  
Israel 3079510

### Common Criteria Versions

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017.

### Common Evaluation Methodology Versions

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

### Protection Profiles

- Protection Profile for Peripheral Sharing Device, 2019-07-19, Version 4.0
- PP-Module for Keyboard/Mouse Devices, 2019-07-19, Version 1.0
- PP-Module for Video/Display Devices, 2019-07-19, Version 1.0
- PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and Video/Display Devices, 19 July 2019, Version 1.0

### NIAP Technical Decisions

| ITEM   | TECHNICAL DECISION TITLE                                       |
|--------|--|
| TD0506 | Missing steps to connect and reconnect display [MOD_VI_V1.0]   |
| TD0507 | Clarification on USB plug type [MOD_KM_V1.0]                   |
| TD0514 | Correction to MOD_VI FDP_APC_EXT.1 Test 3 Step 6 [MOD_VI_V1.0] |
| TD0518 | Typographical error in Dependency Table [PP_PSD_V4.0]          |
| TD0539 | Incorrect selection trigger in FTA_CIN_EXT.1 in [MOD_VI_V1.0]  |
| TD0583 | FPT_PHP.3 modified for PSD remote controllers [PP_PSD_V4.0]    |



| ITEM   | TECHNICAL DECISION TITLE   |
|--------|--|
| TD0584 | Update to FDP_APC_EXT.1 Video Tests [MOD_VI_V1.0]                  |
| TD0586 | DisplayPort and HDMI Interfaces in FDP_IPC_EXT.1 [MOD_VI_V1.0]     |
| TD0593 | Equivalency arguments for PSD [MOD_KM_V1.0], [MOD_VI_V1.0]         |
| TD0620 | EDID Read Requirements [MOD_VI_V1.0]                               |
| TD0681 | PSD purging of EDID data upon disconnect [MOD_VI_V1.0]             |
| TD0686 | DisplayPort CEC Testing [MOD_VI_V1.0]                              |
| TD0804 | Clarification regarding Extenders in PSD Evaluations [PP_PSD_V4.0] |

**Table 1 – NIAP Technical Decisions**



# 1 Introduction

This document presents assurance activity evaluation results of the TOE evaluation. There are three types of assurance activities and the following is provided for each:

1. TOE Summary Specification (TSS) - An indication that the required information is in the TSS section of the Security Target;
2. Guidance - A specific reference to the location in the guidance is provided for the required information; and
3. Test – A summary of the test procedure used and the results obtained is provided for each required test activity.

This Assurance Activity Report contains sections for each functional class and family and sub-sections addressing each of the SFRs specified in the Security Target. The SARs are also addressed.

## 1.1 Evidence

The following is a list of the documents consulted:

- [ST] High Sec Labs FI11H-M, FI11D-M, FI11PH-M Firmware Version 44404-E7E7 Peripheral Sharing Devices Security Target, Version 1.1, 29 April 2024
- [CC\_Supp] High Sec Labs FI11H-M, FI11D-M, FI11PH-M Firmware Version 44404-E7E7 Peripheral Sharing Devices Common Criteria Guidance Supplement, Version 1.5, 13 March 2024
- [Isol] High Sec Labs SC21H-4, SC82PH-4, SC162PH-4, SMX42D-M, SMX42H-M, SMX42P-M, SMX82D-M, SMX82H-M, SMX82P-M, FI11H-M, FI11D-M, FI11PH-M, FICE11PH-M, FICE11CH-M, FIFE11PH-M, CNMFE11PH-M Firmware Version 44404-E7E7 Peripheral Sharing Devices Isolation Document, version 1.2, 29 June 2020
- [19412] HSL QUICK SETUP GUIDE Secure KVM Isolators, HDC19412 Rev. 2.2
- [ETProcRes] EVALUATION TEST PLAN, PROCEDURES AND TEST RESULTS FOR PERIPHERAL SHARING DEVICE VERSION 4.0 COMMON CRITERIA EVALUATION OF HSL CFG3& CFG8\_PSD-KM-VI, version 1.2, 29 April 2024

## 1.2 References

- [PP\_PSD\_V4.0] Protection Profile for Peripheral Sharing Device, 2019-07-19, Version 4.0
- [MOD\_KM\_V1.0] PP-Module for Keyboard/Mouse Devices, 2019-07-19, Version 1.0
- [MOD\_KM\_SD] Supporting Document, PP-Module for Keyboard/Mouse Devices, 2019-07-19, Version 1.0
- [MOD\_VI\_V1.0] PP-Module for Video/Display Devices, 2019-07-19, Version 1.0
- [MOD\_VI\_SD] Supporting Document, PP-Module for Video/Display Devices, 2019-07-19, Version 1.0



## 2 Security Functional Requirement Assurance Activities

### 2.1 User Data Protection (FDP)

#### 2.1.1 FDP\_APC\_EXT.1 Active PSD Connections

##### 2.1.1.1 FDP\_APC\_EXT.1.1

*The TSF shall route user data only to or from the interfaces selected by the user.*

*Evaluation activities are detailed below.*

##### 2.1.1.2 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.*

*Evaluation activities are detailed below.*

##### 2.1.1.3 FDP\_APC\_EXT.1.3

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

*Evaluation activities are detailed below.*

##### 2.1.1.4 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.*

#### **Isolation Document Evaluator Assessment:**

[Isol] was reviewed. This document covers both CFG3 and CFG8. This document adequately describes the proper isolation whether the TOE is powered on or not. A complete review of this document is in the file "Isolation assessment of CFG3.docx".

#### **TSS Evaluator Assessment:**

[ST] TSS Section 9.2.3 discusses the conditions under which the TOE enters a failure state due to self-test failure.



### Guidance Evaluator Assessment:

[CC\_Supp] explain the possible errors and failures and the behavior of the device when in a fail state. The Guide states what causes a device to enter a fail state.

### Test Evaluator Assessment:

NA

## 2.1.1.2 FDP\_APC\_EXT.1/KM Active PSD Connections

### 2.1.1.2.1 FDP\_APC\_EXT.1.1/KM

*The TSF shall route user data only to the interfaces selected by the user.*

*Evaluation activities are detailed below.*

### 2.1.1.2.2 FDP\_APC\_EXT.1.2/KM

*The TSF shall ensure that no data or electrical signals flow between connected computers whether the TOE is powered on or powered off.*

*Evaluation activities are detailed below.*

### 2.1.1.2.3 FDP\_APC\_EXT.1.3/KM

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

*Evaluation activities are detailed below.*

### 2.1.1.2.4 FDP\_APC\_EXT.1.4/KM

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

#### **Application Note**

*This SFR is refined from the PSD PP for this PP-Module to include further restrictions for electrical signals. It is unlikely that this element can be satisfied unless mouse and keyboard peripheral device interfaces are electrically and logically isolated from the connected computer interfaces or through other methods, such as USB host and USB device emulation.*

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

*If the TOE claims conformance to multiple PP-Modules, each PP-Module modifies this SFR in a different manner for the interfaces that are unique to that module. In this case, the ST author should reference this modification of the SFR as "FDP\_APC\_EXT.1/KM" for uniqueness. Note that all elements of FDP\_APC\_EXT.1 must be included in this iteration, not just the ones that are modified by this PP-Module.*

#### **Evaluation Activity**

#### **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 nonselected 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 any compatible USB 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. **Note: TD0507 applied**



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.

#### **Isolation Document Evaluator Assessment:**

Figure 1 in [Isol] illustrates all possible data flows. Section 2.2, Table 1 Data Flow Description provides an explanation of all data flows. Figures 2 and 3 characterize the unauthorized data flows between the TOE and peripheral devices. These figures are part of the isolation justification and indicate the methods used to maintain the data separation. [Isol] Section 2.3 provides an explanation of all data flow isolation. Section 2.4 discusses power isolation. Section 3 describes the isolation enforcement policy for various aspects of the TOE. Figure 7 shows the physical characteristics. The file “Isolation assessment of CFG3.docx” is an analysis of the Isolation document. This document covers both CFG3 and CFG8.

#### **TSS Evaluator Assessment:**

NA

#### **Guidance Evaluator Assessment:**

NA

#### **Test Evaluator Assessment:**

##### **Test 1 – Not Applicable for Isolators.**

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.
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.
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.



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.
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 - #
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.
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.

The functionality of the TOE’s KM switching methods has been tested successfully. The evaluator has confirmed that the TOE prevents the user from switching between more than one computer at once.

|              |     |
|--------------|-----|
| Units Tested | N/A |
| Result       | N/A |

## Test 2

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.
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.
- ~~3. *[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.]* [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.~~
- ~~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.~~
- ~~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.~~



- ~~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.~~
- ~~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.~~
- ~~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.~~
- ~~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.~~
- ~~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.~~
11. Perform step 12 when the TOE is off and then in a failure state.
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. Correct data flows of a mouse and keyboard during different power states of the selected computer has been tested. The evaluator has confirmed that data flow is transmitted to the correct computers at the accurate times.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

### Test 3

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

9. Turn the TOE off and disconnect the peripheral devices connected in step 6.
10. Reconnect the first computer interface USB cable to the TOE.
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.
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.This test step was not performed, since the keyboard and mouse correctly appeared in the listed devices in the device manager.

Unidirectional flow and isolation of USB traffic has been tested. The evaluator has confirmed that USB traffic is enforced properly and in a single direction.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

#### Test 4 – Not Applicable for Isolators

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.
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.
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.
4. Ensure the TOE is switched to the first computer.
5. Reboot the first computer. Verify that no USB traffic is captured on all non-selected computer USB protocol analyzers.
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.
7. Perform steps 8 and 9 for each TOE keyboard/mouse peripheral interface.
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.



9. Connect a switchable 5-volt power supply with any compatible USB 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. Note: TD0507 applied
10. Turn off the TOE. Verify that no new traffic is captured.

Correct data flow while the TOE is powered on or powered off has been tested. The evaluator confirmed that USB traffic is only captured on selected authorized computers.

|              |     |
|--------------|-----|
| Units Tested | N/A |
| Result       | N/A |

### Test 5

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.
2. Connect the first computer to the TOE and ensure it is selected and that no other computers are connected.
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.
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.
5. Cease generation of the USB HID traffic, connect the second computer to the same port and ensure it is selected.
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.
7. Reboot the TOE and repeat step 6.
8. Turn off the TOE and repeat step 6.
9. Restart the TOE and repeat step 6.
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.

Data flow through the same interface has been observed and tested. The evaluator confirmed that the TOE does not send data to different computers connected to the same interface at different times.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

### 2.1.3 FDP\_APC\_EXT.1/VI Active PSD Connections

#### 2.1.3.1 FDP\_APC\_EXT.1.1/VI

*The TSF shall route user data only from the interfaces selected by the user.*





Evaluation activities are detailed below.

### 2.1.3.2 FDP\_APC\_EXT.1.2/VI

The TSF shall ensure that no data or electrical signals flow between connected computers whether the TOE is powered on or powered off.

Evaluation activities are detailed below.

### 2.1.3.3 FDP\_APC\_EXT.1.3/VI

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

Evaluation activities are detailed below.

### 2.1.3.4 FDP\_APC\_EXT.1.4/VI

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

#### Application Note

This SFR is refined from the PSD PP for this PP-Module to include further restrictions for electrical signals. It is unlikely that this element can be satisfied unless video/display peripheral device interfaces are electrically and logically isolated from the connected computer interfaces or through other methods.

If the TOE claims conformance to multiple PP-Modules, each PP-Module modifies this SFR in a different manner for the interfaces that are unique to that module. In this case, the ST author should reference this modification of the SFR as "FDP\_APC\_EXT.1/VI" for uniqueness. Note that all elements of FDP\_APC\_EXT.1 must be included in this iteration, not just the ones that are modified by this PP-Module.

#### Evaluation Activity

##### 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 guidance EAs for this component beyond what the PSD PP requires.

[Note to evaluator: This was copied directly from mod\_vi\_v1.0-sd.pdf. It is unclear whether NIAP intended no TSS EAs or whether the TSS EAs are missing.]

##### Guidance

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

##### Test

The evaluator shall perform the following tests:

#### Test 1-VI: Video Source Selection and Identification, TOE Off and Failure States

This test verifies the TOE switching function operates properly and will stop the video output display when in an OFF or FAILURE state.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance.

Step 2: Play a different video with embedded audio on a number of computers for each TOE computer video interface.

Step 3: Connect each computer to a TOE computer video interface.

Step 4: Connect a display to each TOE display interface.



Step 5: Turn on the TOE.

Step 6: For each connected computer, ensure it is selected and verify that the video and its accompanying audio from the selected computer(s) are received on the proper display(s).

Step 7: [Conditional: if the TOE claims Combiner Use Case then] verify that video generated by the TOE has clear identification marking or text to properly identify the source computer shown. **Note: TD0539 applied**

Step 8: Turn off the TOE and verify that no video appears on any connected display.

Step 9: Power on the TOE and cause the TOE to enter a failure state. Verify that the TOE provides the user with a visual indication of failure and that no usable video appears on any connected display.

Step 10: Repeat steps 3 to 9 for each unique display protocol and port type supported by the TOE.

### **Test 2-VI: Computer Video Interface Isolation**

[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 that the TOE does not transfer data to any non-selected computer video interface.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect only the first computer interface cable to one computer. Turn on the TOE.

Step 2: Switch the TOE primary display to computer #1.

Step 3: Observe the primary display to verify that the selected computer is the one that is shown.

Step 4: Remove the non-selected computer video interface cables from the TOE and connect the oscilloscope probe to the TOE #2 computer video interface to verify that no SYNC signal is passed through the TOE. Based on the connection interface protocol, this is performed as follows:

1. Video Graphics Array (VGA) – single ended probe on pins 13 and then 14;
2. High-Definition Multimedia Interface (HDMI) – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide Hot Plug Detect (HPD) signal; Check for signals - differential probe between pins 10 (+) and 12 (-);
3. Digital Visual Interface (DVI)-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-);
4. DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 23 (+) and 24 (-);
5. DisplayPort - connect pin 18 to a 3.3V power supply via 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+);
6. USB Type-C with DisplayPort as Alternate Function – connect pin A8 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals – Differential probe between pins A2 and A3, A10 and A11; B2 and B3, and B10 and B11.

Step 5: Repeat steps 3 and 4 while selecting other TOE connected computers. Verify that no SYNC signal is present.

Step 6: Repeat steps 3 to 5 with the TOE unpowered. Verify that no SYNC signal is present.

Step 7: With the probe connected to the TOE computer #2 video interface, disconnect / reconnect the computer #1 video cable. Power up the TOE and select computer #1. Attempt to detect the change in the oscilloscope at each one of the TOE #2 computer video interface pins. No changes shall be detected.

Step 8: Repeat step 7 for each one of the other TOE computer video interfaces.

Step 9: Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, disconnect and reconnect the display.

Step 10: Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, reboot the selected computer.

Step 11: Repeat steps 2 to 10 with each connected computer.

Step 12: [Conditional: if "multiple connected displays" is selected in FDP\_CDS\_EXT.1.1 then] repeat steps 3 to 10 with each other display connected to the TOE.



Step 13: Repeat this test for each unique display protocol and port type supported by the TOE.

### **Test 3-VI - Unauthorized Sub-protocols**

Note that in the following steps only native video protocol cables shall be used. No conversion from other video protocols is allowed in these tests except as directed in FDP\_IPC\_EXT.1.1.

This test verifies that unauthorized sub-protocols are blocked.

Perform this test for each of the selections in FDP\_PDC\_EXT.3.1/VI and FDP\_IPC\_EXT.1.1.

In the following steps the evaluator shall establish a verified test setup that passes video signals across the TOE.

Step 1: Connect at least one computer with a native video protocol output to the TOE computer #1 video input interface.

Step 2: Connect at least one display with native video protocol to the TOE display output.

Step 3: Power up the TOE and ensure the connected computer is selected.

Step 4: Verify that the video image is visible and stable on the user display.

In the following steps the evaluator shall verify that the test setup properly blocks the unauthorized video sub-protocol traffic.

Step 5: Open the Monitor Control Command Set (MCCS) control console program on the computer and attempt to change the display contrast and brightness. Verify that the display does not change its contrast and brightness accordingly.

Step 6: Disconnect the video cable connecting the display and the TOE and connect the display directly to the computer. Verify that the video image is visible and stable on the user display. **Note: TD0514 applied**

Step 7: Attempt to change the display contrast and brightness. Verify that the display does change its contrast and brightness accordingly.

Step 8: Connect the following testing device based on the display video protocol being tested at the peripheral display interface:

1. DisplayPort – DisplayPort AUX channel analyzer in series between the display and the TOE
2. HDMI– HDMI sink test device
3. USB Type-C with DisplayPort as Alternate Function – USB sniffer in series between the display and the TOE
4. VGA – VGA sink test device
5. DVI-I/DVI-D – DVI sink test device

### **Note: TD0584 applied**

Step 9: Attempt to change the display contrast and brightness. Verify that the testing device does not capture any MCCS commands.

Step 10: Replace the computer with a source generator for each selected protocol at the computer video interface. If DVI-I or DVI-D is selected, use an HDMI source generator.

Step 11: Run an EDID write transaction at the generator and verify in the testing device that no EDID traffic is captured.

Step 12: [Conditional, if DisplayPort (DP++ - Dual Mode Only), HDMI, or USB Type-C is the selected protocol being tested at the computer video interface, then] run Consumer Electronics Control (CEC) and High-bandwidth Digital Content Protection (HDCP) tests or commands at the generator and verify in the testing device that no CEC or HDCP traffic is captured for HDMI or USB-C, or check for an absence of power on pin 14 (CONFIG2) using an oscilloscope for DisplayPort DP++ Dual Mode. **Note: TD0686 applied.**

Step 13: [Conditional, if DVI-D, DVI-I, or HDMI is the selected protocol being tested at the computer video interface, then] run Audio Return Channel (ARC), HDMI Ethernet and Audio Return Channel (HEAC), and HDMI Ethernet Channel (HEC) tests or commands at the generator and verify in the testing device that no ARC, HEAC, or HEC traffic is captured.

Step 14: [Conditional: If “[HDMI] protocol” is selected in FDP\_IPC\_EXT.1.2, then] perform steps 15 and 16 for both pin 13 (CEC) and 14 (UTILITY).

Step 15: Turn off the TOE. Use a multi-meter to measure the resistance-to-ground of the pin at the TOE HDMI peripheral interface and verify it is greater than 2 Mega-ohms.



Step 16: Attach a single ended oscilloscope probe between the pin and the ground, turn on the TOE, and verify that no changes between 0.0v and 0.2v and between 3.0v and 3.3v are detected.

Step 17: [Conditional: if VGA is not the selected protocol being tested, then] disconnect all devices. Connect the display to a TOE computer video interface and the oscilloscope to the TOE display interface in order to verify that no HPD signal is passed by measuring a signal voltage of less than 1.0V. Based on the selected protocol being tested, this is performed as follows:

1. HDMI – connect scope to pin 19 and verify no HPD signal is detected;
2. DVI-D/DVI-I – connect scope to pin 16 and verify no HPD signal is detected;
3. DisplayPort - connect scope to pin 18 and verify no HPD signal is detected;
4. USB Type-C with DisplayPort as Alternate Function – connect scope to pin A8 and B8 and verify no HPD signal is detected.

Step 18: Repeat this test for each of the selections in FDP\_PDC\_EXT.3.1/VI and FDP\_IPC\_EXT.1.2.

#### **Test 4-VI - Video and EDID Channel Unidirectional Rule**

This test verifies that the TOE video path is unidirectional from the computer video interface to the display interface with the exception of EDID, which may be read from the display once at power up and then may be read by the connected computers. The evaluator should have at least two high-resolution displays of different models and one low-resolution display for each TOE-supported video protocol. **Note: TD0506 applied.**

In the following steps the evaluator should attempt to read display EDID after the TOE completed its self-test / power up. The TOE should not read the new display EDID.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect a computer and a high-resolution display to the TOE.

Step 2: Ensure the TOE is on, computer #1 is selected, and verify that the display shows video from computer #1 as expected.

Step 3: Turn off the TOE. Disconnect the user display from the TOE.

Step 4: Connect the low-resolution display to the TOE and turn on the TOE. After the video is shown on the display, turn off the TOE and disconnect the low-resolution display. **Note: TD0506 applied**

Step 5: Turn on the TOE. After the TOE has completed the self-test, connect the second high-resolution display of a different model to the TOE. The TOE may fail to generate video on the user display (i.e., no EDID is read at the TOE power up). If the display is showing video, then run the EDID reading and parsing software on computer #1 and check that there is no active EDID (i.e., the computer is using a default generic display or reading older display settings from the registry). **Note: TD0506 applied**

In the following steps the evaluator shall validate that the TOE video path is unidirectional from the computer video interface to the display interface.

Step 6: Perform steps 7-11 for each TOE computer video interface.

Step 7: Power off the TOE and disconnect the computer #1 video output and the display. Connect the display cable to the TOE computer #1 video interface. Connect the computer #1 video cable to the TOE display interface. This configuration will attempt to force video data through the TOE in the reverse direction.

Step 8: Power up the TOE again.

Step 9: Check that the video is not visible in the display.

Step 10: Perform steps 11 while the TOE is powered on and powered off.

Step 11: Remove the display cable from the TOE and connect the oscilloscope to verify that no SYNC signal is passed through the TOE. Based on the video protocols supported, this is performed as follows:

1. VGA – single ended probe on pins 13 and 14;
2. HDMI – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - differential probe between pins 10 (+) and 12 (-);
3. DVI-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-);



4. DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 23 (+) and 24 (-);

5. DisplayPort - connect pin 18 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+);

6. USB Type-C with DisplayPort as Alternate Function – connect pin A8 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals – Differential probe between pins A2 and A3, A10 and A11; B2 and B3, and B10 and B11.

#### **Test 5-VI – No Flow between Connected Computers over Time**

This test verifies that the TOE does not send data to different computers connected to the same TOE video interface over time. Repeat this test for each TOE Video port.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Run EDID reading and parsing software on two computers and connect a display to the TOE.

Step 2: Connect computer #1 to the TOE, ensure the TOE is on, computer #1 is selected, no other computers are connected, and verify that the display shows video from computer #1 as expected.

Step 3: Capture the TOE EDID content in the software on computer #1 and save as a file with a name that indicates capture time.

Step 4: Disconnect computer #1 and connect an I2C programmer to the same port. Attempt to write the characters “FFFF” over the entire EDID address range.

Step 5: Disconnect the I2C programmer, reconnect computer #1 to the same port, and repeat step 3.

Step 6: Reboot the TOE and repeat step 3.

Step 7: Turn off the TOE and repeat step 3.

Step 8: Restart the TOE and repeat step 3.

Step 9: Disconnect computer #1 and repeat steps 2 to 8 with computer #2 on the same port.

Step 10: Repeat steps 2 to 9 for a total of 20 EDID file captures.

Step 11: Collect all 20 captured EDID files, compare them bit-by-bit, and verify that they are identical excluding null captures recorded in Step 7. **Note: TD0584 applied**

#### **Isolation Document Evaluator Assessment:**

Figure 1 in [Isol] illustrates all possible data flows. Section 2.2, Table 1 Data Flow Description provides an explanation of all data flows. Figures 2 and 3 characterize the unauthorized data flows between the TOE and peripheral devices. These figures are part of the isolation justification and indicate the methods used to maintain the data separation. [Isol] Section 2.3 provides an explanation of all data flow isolation. Section 2.4 discusses power isolation. Section 3 describes the isolation enforcement policy for various aspects of the TOE. Figure 7 shows the physical characteristics. The file “Isolation assessment of CFG3.docx” is an analysis of the Isolation document. This document covers both CFG3 and CFG8.

#### **TSS Evaluator Assessment:**

NA

#### **Guidance Evaluator Assessment:**

NA

#### **Test Evaluator Assessment:**

##### **Test 1**

1. Configure the TOE and the Operational Environment in accordance with the operational guidance.



2. Play a different video with embedded audio on a number of computers for each TOE computer video interface.
3. Connect each computer to a TOE computer video interface.
4. Connect a display to each TOE display interface.
5. Turn on the TOE.
6. For each connected computer, ensure it is selected and verify that the video and its accompanying audio from the selected computer(s) are received on the proper display(s).
7. *[Conditional: if the TOE claims the Combiner Use Case then]* verify that video generated by the TOE has clear identification marking or text to properly identify the source computer shown. Note:TD0539 applied
8. Turn off the TOE and verify that no video appears on any connected display.
9. Power on the TOE and cause the TOE to enter a failure state. Verify that the TOE provides the user with a visual indication of failure and that no usable video appears on any connected display.
10. Repeat steps 3 to 9 for each unique display protocol and port type supported by the TOE.

The evaluator confirmed that the TOE switching function operates properly and will stop the video output display when in an OFF or FAILURE state.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

### Test 2 – Not Applicable for Isolators

1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect only the first computer interface cable to one computer. Turn on the TOE.
2. Switch the TOE primary display to computer #1.
3. Observe the primary display to verify that the selected computer is the one that is shown.
4. Remove the non-selected computer video interface cables from the TOE and connect the oscilloscope probe to the TOE #2 computer video interface to verify that no SYNC signal is passed through the TOE. Based on the connection interface protocol, this is performed as follows:

**High-Definition Multimedia Interface (HDMI)** – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide Hot Plug Detect (HPD) signal; Check for signals - differential probe between pins 10 (+) and 12 (-);

**DVI-D** - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 23 (+) and 24 (-);

**DisplayPort** - connect pin 18 to a 3.3V power supply via 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+);

5. Repeat steps 3 and 4 while selecting other TOE connected computers. Verify that no SYNC signal is present.
6. Repeat steps 3 to 5 with the TOE unpowered. Verify that no SYNC signal is present.
7. With the probe connected to the TOE computer #2 video interface, disconnect / reconnect the computer #1 video cable. Power up the TOE and select computer #1. Attempt to detect the change in the oscilloscope at each one of the TOE #2 computer video interface pins. No changes shall be detected.
8. Repeat step 7 for each one of the other TOE computer video interfaces.





9. Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, disconnect and reconnect the display.
10. Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, reboot the selected computer.
11. Repeat steps 2 to 10 with each connected computer.
12. [Conditional: if “multiple connected displays” is selected in FDP\_CDS\_EXT.1.1 then] repeat steps 3 to 10 with each other display connected to the TOE.
13. Repeat this test for each unique display protocol and port type supported by the TOE.

The evaluator confirmed that the TOE does not transfer data to any non-selected computer video interface.

|              |     |
|--------------|-----|
| Units Tested | N/A |
| Result       | N/A |

### Test 3

1. Connect at least one computer with a native video protocol output to the TOE computer #1 video input interface.
2. Connect at least one display with native video protocol to the TOE display output.
3. Power up the TOE and ensure the connected computer is selected.
4. Power up the TOE and ensure the connected computer is selected.
5. Open the Monitor Control Command Set (MCCS) control console program on the computer and attempt to change the display contrast and brightness. Verify that the display does not change its contrast and brightness accordingly.
6. Disconnect the video cable connecting the display and the TOE and connect the display directly to the computer. Verify that the video image is visible and stable on the user display. Note: TD0514 applied
7. Attempt to change the display contrast and brightness. Verify that the display does change its contrast and brightness accordingly.
8. Connect the following testing device based on the display video protocol being tested at the peripheral display interface: (Note: TD0584 applied)  
DisplayPort – DisplayPort AUX channel analyzer in series between the display and the TOE  
HDMI – HDMI sink test device
9. Attempt to change the display contrast and brightness. Verify that the testing device does not capture any MCCS commands.
10. Replace the computer with a source generator for each selected protocol at the computer video interface. If DVI-I or DVI-D is selected, use an HDMI source generator.
11. Run an EDID write transaction at the generator and verify in the testing device that no EDID traffic is captured.
12. [Conditional, if DisplayPort (DP++ - Dual Mode Only), HDMI, or USB Type-C is the selected protocol being tested at the computer video interface, then] run Consumer Electronics Control (CEC) and High-bandwidth Digital Content Protection (HDCP) tests or commands at the generator and verify in the testing device that no CEC or HDCP traffic is captured for HDMI or USB-C, or check for an absence of



power on pin 14 (CONFIG2) using an oscilloscope for DisplayPort DP++ Dual Mode. **Note: TD0686 applied.**

13. [Conditional, if DVI-D, DVI-I, or HDMI is the selected protocol being tested at the computer video interface, then] run Audio Return Channel (ARC), HDMI Ethernet and Audio Return Channel (HEAC), and HDMI Ethernet Channel (HEC) tests or commands at the generator and verify in the testing device that no ARC, HEAC, or HEC traffic is captured.
14. [Conditional: if "[HDMI] protocol" is selected in FDP\_IPC\_EXT.1.2, then] perform steps 15 and 16 for both pin 13 (CEC) and 14 (UTILITY).
15. Turn off the TOE. Use a multi-meter to measure the resistance-to-ground of the pin at the TOE HDMI peripheral interface and verify it is greater than 2 Mega-ohms.
16. Attach a single ended oscilloscope probe between the pin and the ground, turn on the TOE, and verify that no changes between 0.0v and 0.2v and between 3.0v and 3.3v are detected.
17. [Conditional: if VGA is not the selected protocol being tested, then] disconnect all devices. Connect the display to a TOE computer video interface and the oscilloscope to the TOE display interface in order to verify that no HPD signal is passed by measuring a signal voltage of less than 1.0V. Based on the selected protocol being tested, this is performed as follows:
  1. HDMI – connect scope to pin 19 and verify no HPD signal is detected;
  3. DisplayPort - connect scope to pin 18 and verify no HPD signal is detected;
  4. USB Type-C with DisplayPort as Alternate Function – connect scope to pin A8 and B8 and verify no HPD signal is detected.
18. Repeat this test for each of the selections in FDP\_PDC\_EXT.3.1/VI and FDP\_IPC\_EXT.1.2

The evaluator has confirmed that the TOE successfully blocks unauthorized sub-protocols.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

#### Test 4

1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect a computer and a high-resolution display to the TOE.
2. Ensure the TOE is on, computer #1 is selected, and verify that the display shows video from computer #1 as expected.
3. Turn off the TOE. Disconnect the user display from the TOE.
4. Connect the low-resolution display to the TOE and turn on the TOE. After the video is shown on the display, turn off the TOE and disconnect the low-resolution display. Note: TD0506 applied
5. Turn on the TOE. After the TOE has completed the self-test, connect the second high-resolution display of a different model to the TOE. The TOE may fail to generate video on the user display (i.e., no EDID is read at the TOE power up). If the display is showing video, then run the EDID reading and parsing software on computer #1 and check that there is no active EDID (i.e., the computer is using a default generic display or reading older display settings from the registry). Note: TD0506 applied
6. Perform steps 7-11 for each TOE computer video interface.
7. Power off the TOE and disconnect the computer #1 video output and the display. Connect the display cable to the TOE computer #1 video interface. Connect the computer #1 video cable to the TOE display interface. This configuration will attempt to force video data through the TOE in the reverse direction.
8. Power up the TOE again.
9. Check that the video is not visible in the display.





10. Perform steps 11 while the TOE is powered on and powered off.
11. Remove the display cable from the TOE and connect the oscilloscope to verify that no SYNC signal is passed through the TOE. Based on the video protocols supported, this is performed as follows:  
HDMI – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - differential probe between pins 10 (+) and 12 (-);

DisplayPort - connect pin 18 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+);

The evaluator confirmed the TOE video path is unidirectional from the computer video interface to the display interface except for EDID.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

### Test 5

1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Run EDID reading and parsing software on two computers and connect a display to the TOE.
2. Connect computer #1 to the TOE, ensure the TOE is on, computer #1 is selected, no other computers are connected, and verify that the display shows video from computer #1 as expected.
3. Capture the TOE EDID content in the software on computer #1 and save as a file with a name that indicates capture time.
4. Disconnect computer #1 and connect an I2C programmer to the same port. Attempt to write the characters “FFFF” over the entire EDID address range.
5. Disconnect the I2C programmer, reconnect computer #1 to the same port, and repeat step 3.
6. Reboot the TOE and repeat step 3.
7. Turn off the TOE and repeat step 3.
8. Restart the TOE and repeat step 3.
9. Disconnect computer #1 and repeat steps 2 to 8 with computer #2 on the same port.
10. Repeat steps 2 to 9 for a total of 20 EDID file captures.
11. Collect all 20 captured EDID files, compare them bit-by-bit, and verify that they are identical excluding null captures recorded in Step 7. Note: TD0584 applied

The evaluator confirmed that that the TOE does not send data to different computers connected to the same TOE video interface over time.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

### 2.1.4 FDP\_PDC\_EXT.1 Peripheral Device Connection

Note: The inclusion of [MOD\_VI\_V1.0] triggers additions to the Peripheral Device Connections Policy (see Appendix E) associated with this SFR and additional Evaluation Activities.

#### 2.1.4.1 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.

Evaluation activities are detailed below.

#### **2.1.4.2 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.

Evaluation activities are detailed below.

#### **2.1.4.3 FDP\_PDC\_EXT.1.3**

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

Evaluation activities are detailed below.

#### **2.1.4.4 FDP\_PDC\_EXT.1.4**

The TOE shall not have wireless interfaces.

Evaluation activities are detailed below.

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

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

##### **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.*

*[KM] 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.*

*[VI] 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: 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.*

#### **Test 1-AO**

*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 or an immediate cessation of traffic following device detection or enumeration, or incompatibility of the device interface with the peripheral interface.*

*Step 1: Ensure the TOE is powered off and audio analyzer software is running on the connected computer.*



*Step 2: Connect an analog microphone to the TOE analog audio output peripheral interface.*

*Step 3: Power on the TOE, speak loudly into the microphone from approximately one-inch distance, and verify no audio is present in the audio analyzer software.*

*Step 4: Disconnect the microphone and reconnect it to the TOE peripheral interface.*

*Step 5: Speak loudly into the microphone from approximately one-inch distance, and verify no audio is present in the audio analyzer software.*

#### **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.

#### **Test 1-VI**

The evaluator shall verify that the TOE ports do not reject authorized devices and devices with authorized protocols as per the Peripheral Device Connections appendix in MOD\_VI\_V1.0.

Repeat this test for each of the selected protocols in FDP\_PDC\_EXT.3.1/VI:

Step 1: Connect the authorized device with an authorized protocol directly to a computer. Display any image on the device. Disconnect the device from the computer.

Step 2: Configure the TOE and the Operational Environment in accordance with the operational guidance.

Step 3: Ensure the TOE is powered off.

Step 4: Connect the authorized device with an authorized protocol to the TOE peripheral interface.

Step 5: Power on the TOE and verify the TOE user indication described in the operational user guidance is not present.

Step 6: Ensure the connected computer is selected and verify that the device displays the same image as in step 1.

Step 7: Disconnect the authorized device, then reconnect it to the TOE peripheral interface.

Step 8: Verify the TOE user indication described in the operational user guidance is not present.

Step 9: Verify that the device displays the same image as in step 1 and 6 or that it displays a blank screen. If it displays a blank screen, reboot the TOE, select the channel that was selected prior to reboot, and verify that the device now displays the same image as in step 1 and 6. **Note: TD0681 applied.**

#### **Isolation Document Evaluator Assessment:**

NA

#### **TSS Evaluator Assessment:**

There are no wireless peripherals allowed in this configuration. [ST] TSS Section 9.1.1.2 states “There are no wireless interfaces or additional external interfaces”. The TSS section 9.1.2.3 states “The TOE does not support a wireless connection to a mouse, keyboard or USB hub ...”. Section 9.1.4 states “The TOE does not support a wireless connection to a video display.”. [ST] TSS Sections 9.1 to 9.2 describes all interfaces between the computers and the peripheral devices. The TOE is compliant with the PSD PP and does not allow non-compliant devices.



### Guidance Evaluator Assessment:

The Quick Setup Guide [19412] has instructions to install the TOE. The instructions include clear direction for connecting computers and authorized peripheral devices to the TOE as well as for usage and connection of the TOE interfaces. The input/output TOE interfaces are clearly defined, and the evaluator did not identify any method for misuse of these interfaces. The Quick Setup Guide states that the corresponding LEDs flicker when a device is rejected.

### Test Evaluator Assessment:

#### Test 1

1. Check the supplied cables and accessories to ensure there are no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.

The evaluator confirmed that all supplied cables and accessories contain no external wired interfaces. This excludes computer interfaces, peripheral device interfaces, and power interfaces.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

#### Test 2

1. Check the TOE for radio frequency certification information to ensure that the TOE does not support wireless interfaces.

The evaluator has checked the TOE for radio frequency certification information and verified the TOE does not support wireless interfaces.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

#### Test 3

1. Ensure the TOE is powered off. Open a real-time hardware information console on the connected computer.
2. Attempt to connect a USB mass storage device to the TOE peripheral interface.
3. Power on the TOE. Verify the device is rejected.
4. Ensure the USB mass storage device is disconnected, and then attempt to connect it to the TOE peripheral interface again.
5. Verify the device is rejected.
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.
7. Power on the TOE. Verify the device is rejected.
8. Ensure the USB hub is disconnected, and then attempt to connect it to the TOE peripheral interface again.
9. Verify the device is rejected.

Steps 10 -13 not performed as the TOE does not support PS/2 interfaces.



The evaluator confirmed that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections (Appendix E)

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

### Test 1 – KM

This test was repeated for each keyboard/mouse TOE peripheral interface. Steps 1-6 performed with the following unauthorized devices:

USB audio headset, USB camera, USB printer, USB authentication device connected to a TOE keyboard/mouse peripheral interface

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.
2. Attempt to connect the unauthorized device to the USB sniffer.
3. Power on the TOE. Verify the device is rejected.
4. Ensure the unauthorized device is disconnected from the USB sniffer, then attempt to connect it to the USB sniffer again.
5. Verify the device is rejected.
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.
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.

The evaluator confirmed that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

### Test 2 – KM

This test was repeated 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)

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.



2. Ensure the TOE is powered off.
3. Connect the authorized device to the TOE peripheral interface.
4. Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present.
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.
6. Disconnect the authorized device, and then reconnect it to the TOE KM peripheral device interface.
7. Verify the TOE user indication described in the operational user guidance is not present.
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.

The evaluator confirmed that the TOE KM ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

### Test 1 – VI

This test was repeated for each of the selected protocols in FDP\_PDC\_EXT.3.1/VI: HDMI, DisplayPort

1. Connect the authorized device with an authorized protocol directly to a computer. Display any image on the device. Disconnect the device from the computer.
2. Configure the TOE and the Operational Environment in accordance with the operational guidance.
3. Ensure the TOE is powered off.
4. Connect the authorized device with an authorized protocol to the TOE peripheral interface.
5. Power on the TOE and verify the TOE user indication described in the operational user guidance is not present.
6. Ensure the connected computer is selected and verify that the device displays the same image as in step 1.
7. Disconnect the authorized device, then reconnect it to the TOE peripheral interface.
8. Verify the TOE user indication described in the operational user guidance is not present.
9. Verify that the device displays the same image as in step 1 and 6 or that it displays a blank screen. If it displays a blank screen, reboot the TOE, select the channel that was selected prior to reboot, and verify that the device now displays the same image as in step 1 and 6. Note: TD0681 applied.

The evaluator confirmed that the TOE ports do not reject authorized devices and devices with authorized protocols as per the Peripheral Device Connections appendix in MOD\_VI\_V1.0.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |





## 2.1.5 FDP\_PDC\_EXT.2/KM Authorized Devices (Keyboard/Mouse)

### 2.1.5.1 FDP\_PDC\_EXT.2.1/KM

The TSF shall allow connections with authorized devices and functions as defined in [Appendix E] and [selection:

- authorized devices as defined in the PP-Module for Audio Output Devices,
- authorized devices as defined in the PP-Module for User Authentication Devices,
- authorized devices as defined in the PP-Module for Video/Display Devices,
- no other devices

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

### 2.1.5.2 FDP\_PDC\_EXT.2.2/KM

The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [Appendix E] and [selection:

- authorized devices presenting authorized interface protocols as defined in the PP-Module for Audio Output Devices,
- authorized devices presenting authorized interface protocols as defined in the PP-Module for User Authentication Devices,
- authorized devices presenting authorized interface protocols as defined in the PP-Module for Video/Display Devices,
- no other devices

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

#### **Application Note**

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

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

#### **Evaluation Activity**

#### **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 [MOD\_KM] section 2.1.7 above.

#### **Isolation Document Evaluator Assessment:**

NA



**TSS Evaluator Assessment:**

NA

**Guidance Evaluator Assessment:**

NA

**Test Evaluator Assessment:**

NA

**2.1.6 FDP\_PDC\_EXT.2/VI Peripheral Device Connection (Video Output)**

**2.1.6.1 FDP\_PDC\_EXT.2.1/VI**

*The TSF shall allow connections with authorized devices as defined in [Appendix E] and [selection:*

- *authorized devices as defined in the PP-Module for Audio Output Devices,*
- *authorized devices and functions as defined in the PP-Module for Keyboard/Mouse Devices,*
- *authorized devices as defined in the PP-Module for User Authentication Devices,*
- *no other devices*

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

**2.1.6.2 FDP\_PDC\_EXT.2.2/VI**

*The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [Appendix E] and [selection:*

- *authorized devices presenting authorized interface protocols as defined in the PP-Module for Audio Output Devices,*
- *authorized devices presenting authorized interface protocols as defined in the PP-Module for Keyboard/Mouse Devices,*
- *authorized devices presenting authorized interface protocols as defined in the PP-Module for User Authentication Devices,*
- *no other devices*

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

**Application Note**

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

*If "authorized devices presenting authorized interface protocols as defined in the PP-Module for Keyboard/Mouse" is selected and "USB Type-C with DisplayPort as alternate function" is selected in FDP\_PDC\_EXT.3.1/VI, then video devices that use USB Type-C with DisplayPort as alternate function may not be used in conjunction with touch screen devices.*

**Evaluation Activity**

**Isolation Document**

*There are no Isolation Document EAs for this component.*

**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 as specified in section 2.1.7 above.

**Isolation Document Evaluator Assessment:**

NA

**TSS Evaluator Assessment:**

NA

**Guidance Evaluator Assessment:**

NA

**Test Evaluator Assessment:**

NA

**2.1.7 FDP\_PDC\_EXT.3/KM Authorized Connection Protocols (Keyboard/Mouse)****2.1.7.1 FDP\_PDC\_EXT.3.1/KM**

The TSF shall have interfaces for the [selection: USB (keyboard), USB (mouse)] protocols.

**2.1.7.2 FDP\_PDC\_EXT.3.2/KM**

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

**Application Note**

It is expected that the ST author will make all selections in FDP\_PDC\_EXT.3.1/KM for which the TOE has an interface; the TOE boundary should encompass the entire device where possible.

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

**Evaluation Activity****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.



## Evaluator Assessment

### Isolation Document Evaluator Assessment:

NA

### TSS Evaluator Assessment:

[ST] TSS Sections 9.1 to 9.2 describes which peripherals are supported by the TOE. Section 9.1.2.2 states that "Since the keyboard and mouse function are emulated by the TOE, ...".

### Guidance Evaluator Assessment:

NA

### Test Evaluator Assessment:

NA

## 2.1.8 FDP\_PDC\_EXT.3/VI Authorized Connection Protocols (Video Output)

### 2.1.8.1 FDP\_PDC\_EXT.3.1/VI

*The TSF shall have interfaces for the [selection: VGA, DVI-D, DVI-I, HDMI, DisplayPort, USB Type-C with DisplayPort as alternate function] protocols.*

### 2.1.8.2 FDP\_PDC\_EXT.3.2/VI

*The TSF shall apply the following rules to the supported protocols: [the TSF shall read the connected display EDID information once during power-on or reboot [selection: automatically, when prompted by user intervention]]. **Note: TD0620 applied***

#### **Application Note**

*It is expected that the ST author will make all selections in FDP\_PDC\_EXT.3.1/VI for which the TOE has an interface; the TOE boundary should encompass the entire device where possible.*

*If the KM PP-Module is also claimed by the ST, "USB Type-C with DisplayPort as alternate function" may not be selected in conjunction with a touchscreen peripheral device.*

*If "DisplayPort" is selected, the ST must include the selection-based requirement FDP\_IPC\_EXT.1.*

*This PP-Module defines several iterations of FDP\_SPR\_EXT.1. Depending on the selections made in FDP\_PDC\_EXT.3.1/VI, the evaluator must include the relevant iterations.*

*If the TOE can read the connected display EDID information during power-on or reboot without human intervention, the first selection item for FDP\_PDC\_EXT.3.2/VI is selected. If the TOE requires human intervention to read the connected display EDID during power-on or reboot, the second selection item is selected. **Note: TD0620 applied***

#### **Evaluation Activity**

#### **Isolation Document**

*There are no Isolation Document EAs for this component.*

#### **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\_APC\_EXT.1 as specified in section 2.1.5 above.*

---

#### **Isolation Document Evaluator Assessment:**

NA

#### **TSS Evaluator Assessment:**

NA

#### **Guidance Evaluator Assessment:**

NA

#### **Test Evaluator Assessment:**

NA

### **2.1.9 FDP\_RIP\_EXT.1 Residual Information Protection**

#### **2.1.9.1 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.*

---

#### **Isolation Document Evaluator Assessment:**

NA

#### **TSS Evaluator Assessment:**

The Letter of Volatility is provided in Annex A of the [ST]. It lists each component and explains which have volatile or non-volatile memory. It also states whether data is retained or not. The power source for each



component is listed.

**Guidance Evaluator Assessment:**

NA

**Test Evaluator Assessment:**

NA

## 2.1.1.10 FDP\_SWI\_EXT.1 PSD Switching

### 2.1.10.1 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.*

**Isolation Document Evaluator Assessment:**

NA

**TSS Evaluator Assessment:**

[ST] TSS Section 9.1.1 states “The TOE devices only support one connected computer.”

**Guidance Evaluator Assessment:**

[19412] explains the device switching mechanisms.

**Test Evaluator Assessment:**

NA



## 2.1.1.11 FDP\_UDF\_EXT.1/KM Unidirectional Data Flow (Keyboard/Mouse)

### 2.1.1.1.1 FDP\_UDF\_EXT.1.1/KM

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

#### **Application Note**

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

#### **Evaluation Activity**

#### **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.*

#### **Isolation Document Evaluator Assessment:**

NA

#### **TSS Evaluator Assessment:**

[ST] TSS Section 9.1.2.1 explains how the flows to the keyboard/mouse are unidirectional. "The TOE uses optical data diodes to enforce a unidirectional data flow from the user peripherals to the coupled hosts and use isolated device emulators to prevent data leakage through the peripheral switching circuitry."

#### **Guidance Evaluator Assessment:**

NA

#### **Test Evaluator Assessment:**

NA

## 2.1.1.12 FDP\_UDF\_EXT.1/VI Unidirectional Data Flow (Video Output)

### 2.1.1.2.1 FDP\_UDF\_EXT.1.1/VI

*The TSF shall ensure [video] data transits the TOE unidirectionally from the [TOE computer video] interface to the [TOE peripheral device display] interface.*

#### **Evaluation Activity**

#### **Isolation Document**

*There are no Isolation Document EAs for this component.*



#### **TSS**

*There are no TSS EAs for this component.*

#### **Guidance**

*There are no guidance EAs for this component.*

#### **Test**

*This component is evaluated through evaluation of FDP\_APC\_EXT.1 as specified in section 2.1.5 above.*

#### **Isolation Document Evaluator Assessment:**

NA

#### **TSS Evaluator Assessment:**

NA

#### **Guidance Evaluator Assessment:**

NA

#### **Test Evaluator Assessment:**

NA

## **2.2 Protection of the TSF (FPT)**

### **2.2.1 FPT\_FLS\_EXT.1 Failure with Preservation of Secure State**

#### **2.2.1.1 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.*

#### **Evaluator Assessment:**

NA Tested with FPT\_TST.1

### **2.2.2 FPT\_NTA\_EXT.1 No Access to TOE**

#### **2.2.2.1 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.*

### **Isolation Document Evaluator Assessment:**

NA

### **TSS Evaluator Assessment:**

[ST] TSS Section 9.2.1 states:

“The connected computer does not have access to TOE firmware or memory, with the exception of EDID data is accessible to connected computer from the TOE”

### **Guidance Evaluator Assessment:**

NA. There are no configurations required to ensure that connected computers and peripherals do not have access to TOE software, firmware, and memory, except for EDID data.

### **Test Evaluator Assessment:**

NA

## **2.2.3 FPT\_PHP.1 Passive Detection of Physical Attack**

### **2.2.3.1 FPT\_PHP\_1.1**

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

### **2.2.3.2 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.*

**Isolation Document Evaluator Assessment:**

NA

**TSS Evaluator Assessment:**

[ST] TSS Section 9.2.2 explains the anti-tampering mechanisms and describes the holographic tamper evident labels. If a label is removed, the word VOID appears on both the label and product surface to indicate the TOE has been tampered.

**Guidance Evaluator Assessment:**

The Quick Setup Guide [19412] includes a note indicating that the devices are protected with tamper-evident labels on the product's enclosure to provide a visual indication in the event the enclosure is opened or compromised.

**Test Evaluator Assessment:**

**Test 1**

1. Removed the tamper evident seals from the TOE.

The evaluator confirmed that any attempt 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.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

**Test 2**

1. Attempt to remove the tamper evident seals from the TOE without damaging the tampering indicators.

The evaluator confirmed that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |



## 2.2.4 FPT\_TST.1 TSF Testing

### 2.2.4.1 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]].

---

### 2.2.4.2 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].

---

### 2.2.4.3 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 antitampering 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.

---



### Isolation Document Evaluator Assessment:

NA

### TSS Evaluator Assessment:

[ST] TSS Section 9.2.3 discusses the TOE self-test and what it encompasses:

“...

- Verification of the integrity of the microcontroller firmware

If the self-test fails, the LEDs on the front panel blink indicate the failure. The TOE remains in a disabled state until the self-test is rerun and passes.”

### Guidance Evaluator Assessment:

[CC\_Supp] Section 4.1 describes the self-test and failure behavior and advises the customer to contact HSL technical support if rebooting does not clear the failure.

### Test Evaluator Assessment:

1. The TOE must be powered off, ensure the power cable and display are disconnected from the TOE before proceeding.
2. Power on the TOE without the display connected for at least 5 seconds. This will cause the unit to enter a self-test failure mode where the TOE will be powered on, but unusable. The front panel lights will continue to cycle between the computers connected but the TOE remains inoperable.
3. The evaluator shall ensure no video/keyboard/mouse is being output from the TOE while it is in self-test failure state.

The evaluator confirmed that that successful completion of the self-tests can be determined by following the corresponding steps in operational guidance.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

## 2.2.5 FPT\_TST\_EXT.1 TSF Testing

### 2.2.5.1 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.

**Isolation Document Evaluator Assessment:**

NA

**TSS Evaluator Assessment:**

[ST] TSS section 9.2.3 states that the TOE front panel LEDs blink when a self-test fails. The TOE remains in a disabled state until the self-test is rerun and passes.

**Guidance Evaluator Assessment:**

[CC\_Supp] Section 4.1 describes the self-test and failure behavior and advises the customer to contact HSL technical support if rebooting does not clear the failure.

**Test Evaluator Assessment:**

**Test 1**

1. The TOE must be powered off, ensure the power cable and display are disconnected from the TOE before proceeding.
2. Power on the TOE without the display connected for at least 5 seconds. This will cause the unit to enter a Self-test failure mode where the TOE will be powered on, but unusable. The front panel lights will continue to cycle between the computers connected but the TOE remains inoperable.
3. The evaluator shall ensure no video/keyboard/mouse is being output from the TOE while it is in self-test failure state.

The evaluator confirmed that the TOE does perform a self-test failure and that the TOE responds by disabling normal functions and provides proper indications to the user.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |



## 3 Evaluation Activities for Optional Requirements

### 3.1 User Data Protection (FDP)

#### 3.1.1 FDP\_FIL\_EXT.1/KM Device Filtering (Keyboard/Mouse)

##### 3.1.1.1 FDP\_FIL\_EXT.1.1/KM

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

##### 3.1.1.2 FDP\_FIL\_EXT.1.2/KM

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

##### 3.1.1.3 FDP\_FIL\_EXT.1.3/KM

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

#### **Application Note**

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

#### **Evaluation Activity**

#### **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.*

#### **Isolation Document Evaluator Assessment:**

NA

#### **TSS Evaluator Assessment:**

[ST] Section 9.1.2.3 states that the TOE employs fixed device filtering.

#### **Guidance Evaluator Assessment:**

NA – the configuration is fixed.

#### **Test Evaluator Assessment:**

##### **Test 1**

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.
2. Attempt to connect the unauthorized device to the USB sniffer:
  - USB audio headset
  - USB camera
  - USB printer
  - USB user authentication device connected to a TOE keyboard/mouse peripheral interface
  - USB wireless LAN dongle
3. Power on the TOE. Verify the device is rejected.
4. Ensure the unauthorized device is disconnected from the USB sniffer, then attempt to connect it to the USB sniffer again.
5. Verify the device is rejected.
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.
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.

All devices on the PSD KM blacklist were tested and are rejected as expected. The evaluator confirmed that the blacklist in place rejects all devices found in step 2.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |



## Test 2

NA “Configurable” has not been selected. Therefore, this evaluation activity is not applicable.

### 3.1.2 FDP\_RDR\_EXT.1 Re-Enumeration Device Rejection

#### 3.1.2.1 FDP\_RDR\_EXT.1.1

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

##### **Application Note**

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

##### **Evaluation Activity**

##### **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 reenumeration 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.*

##### **Isolation Document Evaluator Assessment:**

NA

##### **TSS Evaluator Assessment:**

[ST] Section 9.1.2.1 discusses Keyboard and Mouse Enumeration. A USB keyboard is connected to the TOE keyboard host emulator through the console keyboard port. The keyboard host emulator is a





microcontroller which enumerates the connected keyboard and verifies that it is a permitted device type. The USB mouse is connected to the TOE mouse host emulator through the USB mouse port. The mouse host emulator is a microcontroller which enumerates the connected mouse and verifies that it is a permitted device type.

Section 9.1.2.4 states “If a connected device attempts to re-enumerate as a different USB device type, it will be rejected by the TOE.”

**Guidance Evaluator Assessment:**

NA

**Test Evaluator Assessment:**

**Test 1**

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 a real-time hardware information console.
2. Configure the malicious USB device as a HID-class device and to re-enumerate as a mass storage device.
3. Connect the malicious USB device to the TOE KM peripheral interface.
4. Power on the TOE and active the re-enumeration after 1 minute.
5. Verify device rejection per TOE guidance, the cessation traffic passed in the USB sniffer, and the absence of the device and any new device in the information console.
6. Remove the malicious USB device and reconfigure as a HID-class device and to re-enumerate as a mass storage device.
7. Connect the malicious USB device to the TOE KM peripheral interface and active the re-enumeration after 1 minute.
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.

The evaluator configured the USB device accordingly to verify device rejection and ensured the TOE properly enforced security protocols.

|              |          |
|--------------|----------|
| Units Tested | FI11PH-M |
| Result       | PASS     |

## 4 Selection-Based Requirements

### 4.1 User Data Protection (FDP)

#### 4.1.1 FDP\_CDS\_EXT.1 Connected Displays Supported

##### 4.1.1.1 FDP\_CDS\_EXT.1.1

*The TSF shall support [selection: one connected display, multiple connected displays] at a time.*

**Application Note**

*This SFR must be claimed if "switching can be initiated only through express user action" is chosen as a selection for FDP\_SWI\_EXT.1*



in the PSD PP.

If "peripheral devices using a guard" is selected in FDP\_SWI\_EXT.2.2 (from the PSD PP), then "multiple connected displays" must be selected in FDP\_CDS\_EXT.1.1.

**Evaluation Activity**

**Isolation Document**

There are no Isolation Document EAs for this component.

**TSS**

The evaluator shall examine the TSS and verify that it describes how many connected displays may be supported at a time.

**Guidance**

The evaluator shall examine the operational user guidance and verify that it describes how many displays are supported by the TOE.

**Test**

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

**Isolation Document Evaluator Assessment:**

N A

**TSS Evaluator Assessment:**

[ST] Table 2 indicates that all TOE models are single port video devices. [ST] Section 9.1.4 indicates that the TOE accepts any DVI-D, DisplayPort or HDMI display device at the video peripheral port.

**Guidance Evaluator Assessment:**

[CC\_Supp] Section 4.3 Table 2 lists each device and the number of displays per device.

**Test Evaluator Assessment:**

NA

**4.1.2 FDP\_IPC\_EXT.1 Internal Protocol Conversion**

**4.1.2.1 FDP\_IPC\_EXT.1.1**

The TSF shall convert the [DisplayPort] protocol at the [computer video interface] into the [HDMI] protocol within the TOE.

**4.1.2.2 FDP\_IPC\_EXT.1.2**

The TSF shall output the [HDMI] protocol from inside the TOE to [peripheral display interface(s)] as [selection: [DisplayPort] protocol, [HDMI] protocol].

**Application Note**

This SFR must be claimed if "DisplayPort" is chosen as a selection for FDP\_PDC\_EXT.2.1/VI.

**Evaluation Activity**

**Isolation Document**

There are no Isolation Document EAs for this component.

**TSS**

The evaluator shall examine the TSS and verify that it describes how data DisplayPort data is converted.

**Guidance**



*There are no guidance EAs for this component.*

**Test**

*Testing for this SFR is covered under FDP\_APC\_EXT.1 Test 3-VI.*

**Isolation Document Evaluator Assessment:**

NA

**TSS Evaluator Assessment:**

[ST] Section 9.1.3 discusses video data streams in detail.

It states that "For DisplayPort connections, the TOE video function filters the AUX channel by converting it to I2C EDID only. DisplayPort video is converted into an HDMI video stream, and the I2C EDID lines connected to the emulated EDID EEPROM functions...".

**Guidance Evaluator Assessment:**

NA

**Test Evaluator Assessment:**

NA

**4.1.3 FDP\_RIP.1/KM Residual Information Protection (Keyboard Data)**

**4.1.3.1 FDP\_RIP.1.1/KM**

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

**Application Note**

*This SFR must be claimed if "switching can be initiated only through express user action" is chosen as a selection for FDP\_SWI\_EXT.1.1 in the PSD PP and if "USB (keyboard)" is chosen as a selection in FDP\_PDC\_EXT.2.1/KM.*

**Evaluation Activity**

**Isolation Document**

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

**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.*

**Isolation Document Evaluator Assessment:**

NA

**TSS Evaluator Assessment:**

[ST] Section 9.1.2.1 states:



“The Static Random Access Memory (SRAM) in the host and device emulator circuitry stores USB Host stack parameters and up to the last 4 key codes. User data may be briefly retained; however, there are no data buffers. Data is erased during power off of the peripheral sharing device.”

**Guidance Evaluator Assessment:**

NA

**Test Evaluator Assessment:**

NA

**4.1.4 FDP\_SPR\_EXT.1/DP Sub-Protocol Rules (DisplayPort Protocol)**

**4.1.4.1 FDP\_SPR\_EXT.1.1/DP**

*The TSF shall apply the following rules for the [DisplayPort] protocol:*

*- block the following video/display sub-protocols:*

- o [CEC,*
- o EDID from computer to display,*
- o HDCP,*
- o MCCA]*

*- allow the following video/display sub-protocols:*

- o [EDID from display to computer,*
- o HPD from display to computer,*
- o Link Training].*

**Application Note**

*The ST author must include this SFR if "DisplayPort" is selected in FDP\_PDC\_EXT.3.1/VI.*

**Evaluation Activity**

**Isolation Document**

*There are no Isolation Document EAs for this component.*

**TSS**

*The evaluator shall examine the TSS and verify that it describes that the various sub-protocols are allowed or blocked by the TOE as described by the SFR.*

**Guidance**

*There are no guidance EAs for this component.*

**Test**

*Testing for this SFR is covered under FDP\_APC\_EXT.1 Test 3-VI and Test 4-VI.*



#### **Isolation Document Evaluator Assessment:**

NA

#### **TSS Evaluator Assessment:**

[ST] TSS Section 9.1.3 has a detailed discussion on the useable protocols by the display port.

#### **Guidance Evaluator Assessment:**

NA

#### **Test Evaluator Assessment:**

NA

### **4.1.5 FDP\_SPR\_EXT.1/DVI-D Sub-Protocol Rules (DVI-D Protocol)**

#### **4.1.5.1 FDP\_SPR\_EXT.1.1/ DVI-D**

*The TSF shall apply the following rules for the [DVI-D] protocol:*

*- block the following video/display sub-protocols:*

- o [ARC,*
- o CEC,*
- o EDID from computer to display,*
- o HDCP,*
- o HEAC,*
- o HEC,*
- o MCCS]*

*- allow the following video/display sub-protocols:*

- o [EDID from display to computer,*
- o HPD from display to computer].*

#### **Application Note**

*The ST author must include this SFR if "DVI-D" is selected in FDP\_PDC\_EXT.3.1/VI.*

#### **Evaluation Activity**

#### **Isolation Document**

*There are no Isolation Document EAs for this component.*

#### **TSS**

*The evaluator shall examine the TSS and verify that it describes that the various sub-protocols are allowed or blocked by the TOE as described by the SFR.*

#### **Guidance**

*There are no guidance EAs for this component.*



#### **Test**

Testing for this SFR is covered under FDP\_APC\_EXT.1 Test 3-VI and Test 4-VI.

#### **Isolation Document Evaluator Assessment:**

NA

#### **TSS Evaluator Assessment:**

[ST] TSS Section 9.1.3 has a discussion on the useable protocols by the DVI-D port.

#### **Guidance Evaluator Assessment:**

NA

#### **Test Evaluator Assessment:**

NA

### **4.1.6 FDP\_SPR\_EXT.1/HDMI Sub-Protocol Rules (HDMI Protocol)**

#### **4.1.6.1 FDP\_SPR\_EXT.1.1/HDMI**

The TSF shall apply the following rules for the [HDMI] protocol:

- block the following video/display sub-protocols:

- o [ARC,
- o CEC,
- o EDID from computer to display,
- o HDCP,
- o HEAC,
- o HEC,
- o MCCS]

- allow the following video/display sub-protocols:

- o [EDID from display to computer,
- o HPD from display to computer].

#### **Application Note**

The ST author must include this SFR if "HDMI" is selected in FDP\_PDC\_EXT.3.1/VI.

#### **Evaluation Activity**

#### **Isolation Document**

There are no Isolation Document EAs for this component.

#### **TSS**

The evaluator shall examine the TSS and verify that it describes that the various sub-protocols are allowed or blocked by the TOE as described by the SFR.



#### **Guidance**

There are no guidance EAs for this component.

#### **Test**

Testing for this SFR is covered under FDP\_APC\_EXT.1 Test 3-VI and Test 4-VI.

#### **Isolation Document Evaluator Assessment:**

NA

#### **TSS Evaluator Assessment:**

[ST] TSS Section 9.1.3 has a discussion on the useable protocols by the HDMI port.

#### **Guidance Evaluator Assessment:**

NA

#### **Test Evaluator Assessment:**

NA

## **5 Security Assurance Requirement Activities**

### **5.1 Development (ADV)**

#### **5.1.1 ADV\_FSP.1 Basic Functional Specifications**

##### **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.

##### **Evaluator Assessment:**

The [ST] and [CC\_Supp] were used to derive the verdicts for ADV\_FSP.1. The FDP\_PDC\_EXT.1.4 TSS Evaluation activity identifies the security relevant external interfaces of the TOE.

### **5.2 Guidance Documents (AGD)**

#### **5.2.1 AGD\_OPE.1 Operational User Guidance**

##### **Evaluation Activity**

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.



### **Evaluator Assessment:**

The Guidance documents consist of Quick Setup Guide [19412], and [CC\_Supp]. These guides provide the information to assess the AGD\_OPE.1 evaluation assessments. The guidance documents describe modes of operation, fail states, and procedures for the TOE's usage and operational environment.

### **5.2.2 AGD\_PRE.1 Preparative Procedures**

---

#### **Evaluation Activity**

*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.*

---

### **Evaluator Assessment:**

The [CC\_Supp] provides acceptance procedures and instructions for preparation of the operational environment. The Quick Setup Guide [19412] provide clear installation procedures.

## **5.3 Life-Cycle Support (ALC)**

### **5.3.1 ALC\_CMC.1 Labeling of the TOE**

---

#### **Note**

*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.*

---

### **Evaluator Assessment:**

The [ST] was used to determine the TOE identification and hence verdicts for ALC\_CMC.1. The labeling on the guidance documents and nameplate on the underside of the TOE were consistent with the identification of the TOE.

### **5.3.2 ALC\_CMS.1 TOE CM Coverage**

---

#### **Evaluation Activity**

*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.*

---

### **Evaluator Assessment:**

NA – covered under ALC\_CMC.1





## 5.4 Tests (ATE)

### 5.4.1 ATE\_IND Independent Testing - Conformance

#### **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.

#### **Evaluator Assessment:**

The evaluator tested the devices according to the tests in the PP and its modules. The setup was done according to the [19412], and [CC\_Supp] guidance. The test case results were recorded in the [ETProcRes].

## 5.5 Vulnerability Analysis (AVA)

### 5.5.1 AVA\_VAN.1 Vulnerability Survey

#### **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.

#### **Evaluator Assessment:**

The evaluator conducted a vulnerability assessment. The TOE is not connected to the Internet so no penetration tests were conducted. A vulnerability scan and search were conducted. This was recorded in the test plan [ETProcRes]. No vulnerabilities were found.