Assurance Activities Report
for
Tripp Lite Secure KVM Switches

Version 1.1

August 20, 2018

Prepared by:

Leidos Inc.

https://www.leidos.com/civil/commercial-cyber/product-compliance

Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
Columbia, MD 21046

Prepared for:

National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:

Tripp Lite Network Services
1111 W 35th St
Chicago, IL 60609

The TOE Evaluation was Sponsored by:

Tripp Lite Network Services
1111 W 35th St
Chicago, IL 60609

Evaluation Personnel:

Greg Beaver
Cody Cummins
Justin Fisher
Gary Grainger
Allen Sant
Kevin Steiner

Common Criteria Versions

- *Common Criteria for Information Technology Security Evaluation Part 1: Introduction,* Version 3.1, Revision 4, dated: September 2012
- *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components,* Version 3.1, Revision 4, dated: September 2012
- *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components,* Version 3.1, Revision 4, dated: September 2012

Common Evaluation Methodology Versions

- *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology,* Version 3.1, Revision 4, dated: September 2012

Protection Profiles

- *Protection Profile for Peripheral Sharing Switch,* Version 3.0, 13 February 2015

Table of Contents

1 INTRODUCTION

This document presents assurance activity evaluation results of the Tripp Lite Secure KVM Switch 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
3. Test—a summary of the test procedure and result is provided for each required test activity.

This Assurance Activities Report contains sections for each functional class and family and sub-sections addressing each of the SFRs specified in the Security Target.

1.1 Evidence

[ST] *Tripp Lite Secure KVM Switch Security Target,* Document ID SST-1S0-ALL, Revision 1.05, May 10, 2018.

[Admin] *Tripp Lite Secure KVM Administration and Security Management Tool Guide,* Document ID ADG-1S0-ALL, Version 1.0, May 14, 2018

[Owner] *Owner's Manual Secure KVM Switches, NIAP Protection Profile Version 3.0,* 18-03-340-933845-EN, August 10, 2018

[Test] *TRIPP LITE Secure KVM Switch Security Common Criteria Test Report and Procedures,* Version 1.0, August 17, 2018

[VA] *Tripp Lite Secure KVM Switch Vulnerability Survey*, Version 1.2, August 20, 2018

1.2 Protection Profile

[PP PSS] Protection Profile for Peripheral Sharing Switch, Version 3.0, 13 February 2015

1.3 Technical Decisions

The following NIAP Technical Decisions were considered during the evaluation and are either satisfied or not applicable as indicated.

[TD0083] Vulnerability Survey Assurance Component (AVA_VAN.1) in PSS PP v3.0

The ST complies with TD0083 by claiming AVA_VAN.1. See ST sections 4.4 Security Assurance Requirements and 5.2 PP Conformance Claims.

[TD0086] DisplayPort to HDMI Conversion Functionality

The ST claims compliance with TD0086 in section 5.2 PP Conformance Claims. See section 2.1.4.3 below in section 2.1.4 FDP_IFF.1(2) Simple Security Attributes for the application of TD0086.

[TD0136] FDP_RIP.1.1 – Refinement

The ST complies with TD0136 by formatting FDP_RIP.1 as directed in the Technical Decision. See reference to FDP_RIP.1 in [ST] under section 4.1.3.

[TD0141] FMT_MOF.1.1 & FMT_SMF.1.1 - Test Mapping

TD0251 replaces TD0141, which NIAP has archived.

[TD0144] FDP_RIP.1.1 - Purge Memory and Restore Factory Defaults Optional

The ST complies with TD0144 by claiming FDP_RIP.1(2). See reference to FDP_RIP.1(2) in [ST] under section 4.1.3.

[TD0251] FMT_MOF.1.1 - Added Assignment

The ST complies with TD0251 by using the revised wording of FMT_MOF.1.1. See reference to FMT_MOF.1 in [ST] under section 4.1.5. Test Assurance Activities as well as AAR sections 2.1.4.3, 3.4.1.3, and 3.4.2.3.

[TD0298] Update to FDP_IFF.1 Assurance Activities

The ST compiles with TD0298 by default because the TD does not require any changes to the SFR or how the TSS is evaluated. Conformance to this TD is demonstrated in the relevant Test Assurance Activity section of this AAR.

2 Security Functional Requirement Assurance Activities

This section describes the assurance activities associated with the SFRs defined in the ST and the results of those activities as performed by the evaluation team. The assurance activities are derived from [PP PSS] as modified by NIAP Technical Decisions.

2.1 Class FDP: User Data Protection

2.1.1 FDP_IFC.1(1) Subset Information Flow Control

2.1.1.1 TSS Assurance Activities

Assurance Activities for this SFR were integrated with the Data Isolation Requirements SFR below.

See section 2.1.4.1 below in section 2.1.4 FDP_IFF.1(2) Simple Security Attributes.

2.1.1.2 Guidance Assurance Activities

Assurance Activities for this SFR were integrated with the Data Isolation Requirements SFR below.

See section 2.1.4.2 below in section 2.1.4 FDP_IFF.1(2) Simple Security Attributes.

2.1.1.3 Test Assurance Activities

Assurance Activities for this SFR were integrated with the Data Isolation Requirements SFR below.

See section 2.1.4.3 below in section 2.1.4 FDP_IFF.1(2) Simple Security Attributes.

2.1.2 FDP_IFF.1(1) Simple Security Attributes

2.1.2.1 TSS Assurance Activities

Assurance Activities for this SFR were integrated with the Data Isolation Requirements SFR below.

See section 2.1.4.1 below in section 2.1.4 FDP_IFF.1(2) Simple Security Attributes.

2.1.2.2 Guidance Assurance Activities

Assurance Activities for this SFR were integrated with the Data Isolation Requirements SFR below.

See section 2.1.4.2 below in section 2.1.4 FDP_IFF.1(2) Simple Security Attributes.

2.1.2.3 Test Assurance Activities

Assurance Activities for this SFR were integrated with the Data Isolation Requirements SFR below.

See section 2.1.4.3 below in section 2.1.4 FDP_IFF.1(2) Simple Security Attributes.

2.1.3 FDP_IFC.1(2) Subset Information Flow Control

2.1.3.1 TSS Assurance Activities

This Assurance Activity is combined with FDP_IFF.1(2).

In addition to reviewing the information in the TSS, the evaluator shall also review the Isolation Documentation and Assessment as described in Annex J of this PP.

See section 2.1.4.1 below in section 2.1.4 FDP_IFF.1(2) Simple Security Attributes.

2.1.3.2 Guidance Assurance Activities

This Assurance Activity is combined with FDP_IFF.1(2).

See section 2.1.4.2 below in section 2.1.4 FDP_IFF.1(2) Simple Security Attributes.

2.1.3.3 Test Assurance Activities

This Assurance Activity is combined with FDP_IFF.1(2).

See section 2.1.4.3 below in section 2.1.4 FDP_IFF.1(2) Simple Security Attributes.

2.1.4 FDP_IFF.1(2) Simple Security Attributes

2.1.4.1 TSS Assurance Activities

The evaluator shall verify that the TOE Summary Specification (TSS) describes all of the interfaces supported in each port group. Any options to switch peripherals independently from the keyboard and mouse must be described.

ST section 7.7 TOE User Control and Monitoring Security Functions describes switching peripherals between connected computers by push button, and when configured in KM mode, cursor control. The section does not include an option to switch peripherals independently.

ST Table 8 Peripheral Devices supported by the KVM TOE lists the types of peripheral devices the TOE supports. In section 1.6.2.1 Evaluated Products, Tables 5, 6, and 7 identify each model of the TOE. In each table, column “Description and NIAP Certification Version” identifies the peripheral interfaces each model supports. Notes following Table 7 explain how to interpret the descriptions.

Each switch has one console port group and multiple computer port groups. Tables 9, 10, and 11 identify the console port group interfaces by model. On each switch, the computer port groups are identical. Tables 12, 13, and 14 identify the computer port group interfaces by model. Paragraph "TOE External Interfaces Security Functions – KVM" in section 1.6.2.7 KVM TOE Security Functions Overview summarizes external interfaces.

The evaluator shall also verify that the TSS lists and describes all TOE control options.

ST section 7.7 TOE User Control and Monitoring Security Functions describes push button and cursor (when configured in KM mode only) control options.

To improve USB data analysis, prior to the following tests, the evaluator shall receive a full list of all USB endpoints used by the TOE, and their specific functions.

The evaluator shall verify that the TSS describes all of the external interfaces supported by the TOE and that there are no external interfaces other than computer interfaces, power interfaces and peripheral device interfaces. Any wireless or wired interface must be fully described with its intended function.

ST section 7.1 states that basic USB 1.1/2.0 devices are authorized as valid endpoints by the TOE. Devices having an integrated USB hub and composite devices are only supported if they have at least one endpoint that is a keyboard/mouse HID. In this case, all other endpoints will be disabled.

ST section 7.2 TOE External Interfaces Security Functions lists the types of external interfaces.

Table 8 Peripheral Devices supported by the KVM TOE in section 1.6.2.3 Peripheral Devices Supported by the TOE provides details of the types of peripheral devices the TOE supports. In section 1.6.2.1 Evaluated Products, Tables 5, 6, and 7 identify interfaces for each model of the TOE. In section 1.6.2.4 Protocols Supported by the KVM TOE, Tables 9, 10, and 11 identify protocols for each console peripheral port. Tables 12, 13, and 14 identify protocols for each computer port. Paragraph "TOE External Interfaces Security Functions – KVM" in section 1.6.2.7 KVM TOE Security Functions Overview summarizes external interfaces. The paragraph explicitly excludes docking protocols and analog audio input.

The evaluator shall verify that the TSS describes all of the interfaces supported in each port group.

Each switch has one console port group and multiple computer port groups. The model name of each switch summarizes the number and type of each computer video port, the type of the console port group, and whether or not the switch has a CAC port. This is described in detail in Appendix A of [ST]. The scheme for the model name is broken down as follows:

- First block: B002 for all TOE models
- Second block: five or six characters that indicate the following:
    - Characters 1 and 2: supported video in/out protocol (DV = DVI; DP = DisplayPort; HD = HDMI)
    - Character 3: whether the video in/out has single or dual monitor support (1 or 2)
    - Character 4: whether the switch supports audio switching (A or null; all claimed TOE models support audio switching so the A is present in all models)
    - Character 5: whether the switch supports CAC (C or null)

- Character 6: the number of computer ports groups (2, 4, or 8)

Section 7.1 of [ST] describes the keyboard and mouse interfaces. Section 7.3 of [ST] describes the audio interface. Section 7.4 of [ST] describes the video interfaces and specifically includes all protocols supported by the claimed TOE models (DVI, DisplayPort 1.2, HDMI 1.4). Section 7.6 of [ST] describes the CAC interface.

Tables 9, 10, and 11 describe the console port group interfaces by model. On each switch, the computer port groups are identical. Tables 12, 13, and 14 describe the computer port group interfaces by model. Paragraph "TOE External Interfaces Security Functions – KVM" in section 1.6.2.7 KVM TOE Security Functions Overview summarizes external interfaces.

ST section 7.7 TOE User Control and Monitoring Security Functions describes switching peripherals between connected computers by push button and (when configured in KM mode only) cursor control. The section does not include an option to switch peripherals independently.

[Conditional] If the TOE supports keyboard / mouse –

Any options to switch peripherals independently from the keyboard and mouse must be described.

The evaluator shall examine the TSS and verify that for any human interface device that may be switched independently from the keyboard and mouse, there is a description that explains how this interface is isolated from all other device interfaces. The evaluator shall be able to determine from this description that there are no shared components, shared lines or shared power supplies.

ST section 7.7 TOE User Control and Monitoring Security Functions describes switching peripherals between connected computers by push button and (when configured in KM mode only) cursor control. The section does not include an option to switch peripherals independently.

Conditional] If the TOE supports a user authentication device –

The evaluator shall verify that the TSS provides details about supported user authentication devices. TSS shall also indicate whether the user authentication device is emulated by the TOE or switched.

The evaluator shall examine the TSS to verify that it describes how the user authentication data path is isolated from all other data paths. This section must indicate that the data path used by the user authentication device is not shared with other transiting data. This section must also describe how the USB port for the user authentication device is powered separately from other peripheral device functions.

If the TOE includes an integrated user authentication device, the evaluator shall examine the TSS to verify that is describes:

1. *How the user authentication data path is isolated from all other data paths;*
2. *If the user authentication device is emulated by the PSS or not;*
3. *If the user authentication device is emulated, then the TSS shall include detailed information describing authentication session termination by the user, and describe how this occurs simultaneously in all connected computers.*

ST section 7.6 TOE User Authentication Device Subsystem Security Functions indicates that the TSF supports smartcard reader, PIV/CAC USB 1.1/2.0 token, or biometric reader. This is provided via a CAC port, so it is understood to be switched and not emulated.

Section 7.6 describes the isolation of the user authentication data path in paragraphs:

- [O.COMPUTER_INTERFACE_ISOLATION]: FDP_IFC.1(1) and FDP_IFF.1(1),
- [O.USER_DATA_ISOLATION]: FDP_IFC.1(1) and FDP_IFF.1, and
- [O.PERIPHERAL_PORTS_ISOLATION]: FDP_IFC.1(1) and FDP_IFF.1.

This explanation includes a description of how the data path is isolated from other peripheral interfaces and indicates that the power plane is isolated.

The TOE does not include an integrated user authentication device.

[Conditional] If the TOE supports DisplayPort video -

The evaluator shall verify that the TSS describes how the TOE video auxiliary channel (AUX) path blocks information flows other than the minimal set required to establish the video link. The description should discuss the method implemented to prevent unauthorized DisplayPort transactions:

- *The TOE prevents the DisplayPort AUX channel link from reaching speeds higher than 1 megabits per second (DisplayPort ver 1.2 or higher) while blocking MCCS transactions; or*
- *The TOE disassembles the DisplayPort AUX channel transactions to block all unauthorized transactions.*

Paragraph "[O.DISPLAYPORT_AUX_FILTERING]: FDP_IFC.1(1) and FDP_IFF.1(1)" in ST section 7.4 TOE Video Subsystem Security Functions - KVM only describes how the TOE completely disables AUX transaction between a display peripheral and a connected computer.

In addition to reviewing the information in the TSS, the evaluator shall also review the Isolation Documentation and Assessment as described in Annex J of this PP.

Tripp Lite included isolation information and assessment in ST section 7 TOE Summary Specification and Appendix B Letter of Volatility rather than in a separate document. Tripp Lite organized section 7 by TOE function. Each TOE function subsection describes the implementation of the function and then explains how the implementation meets each applicable security objective along with the corresponding security functional requirements.

Section 7.1 TOE Keyboard and Mouse Functionality covers isolation of keyboard and mouse data flows. The description addresses a number of secure objectives; those that are relevant specifically to isolation include O.COMPUTER_INTERFACE_ISOLATION, O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED, O.USER_DATA_ISOLATION, O.PERIPHERAL_PORTS_ISOLATION, and O.KEYBOARD_MOUSE_UNIDIRECTIONAL. The assurance activities for the corresponding security functional requirements confirm the objectives are met.

Sections 7.2 TOE External Interfaces Security Functions and 7.3 TOE Audio Subsystem Security Functions cover isolation of audio data flows. The descriptions address the following security objectives relevant to isolation: O.NO_ANALOG_AUDIO_INPUT, O.UNIDIRECTIONAL_AUDIO_OUT, O.COMPUTER_TO_AUDIO_ISOLATION, and O.PERIPHERAL_PORTS_ISOLATION. The assurance activates for the corresponding security functional requirement confirm the objectives are met.

Section 7.4 TOE Video Subsystem Security Functions – KVM only covers isolation of video data flows. The description addresses the following security objectives relevant to isolation: O.USER_DATA_ISOLATION, O.COMPUTER_INTERFACE_ISOLATION, O.PERIPHERAL_PORTS_ISOLATION, O.UNIDIRECTIONAL_EDID, O.UNIDIRECTIONAL_VIDEO, and O.DISPLAYPORT_AUX_FILTERING. The assurance activities for the corresponding security functional requirements confirm the objectives are met.

Section 7.6 TOE User Authentication Device Subsystem Security Functions covers isolation of user authentication device data flows. The description addresses the following security objectives relevant to isolation: O.COMPUTER_INTERFACE_ISOLATION, O.USER_DATA_ISOLATION, O.PERIPHERAL_PORTS_ISOLATION, and O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED. The assurance activities for the corresponding security functional requirements confirm the objectives are met.

Sections 7.8 TOE Tampering Protection, 7.9 TOE Self-Testing and Security Audit, and Appendix B Letter of Volatility cover firmware dependencies. Section 7.8 addresses protection of TOE firmware. Section 7.9 describes integrity testing of TOE firmware along with the TOE's response to integrity failures. Appendix B covers storage of TOE firmware. The assurance activities for the security functional requirements corresponding to the security objectives listed in section 7.8, 7.9, and Appendix B confirm the objectives are met.

With respect to the requirements from Annex J in the PP, the various sections were found to be satisfied as follows:

- J.1 General: simply summarizes the requirements of the following sections.
- J.2 Design Description: the overall presentation of the isolation documentation is separated by peripheral type. For each peripheral type, a block diagram is provided along with a description of the diagrammed behavior. The logical and electrical isolation of each of the peripheral channels is described, and the diagrammed materials are sufficient to show the internal and external interfaces of the TOE. The TSS also describes how isolation is triggered in the event of a self-test failure.
- J.3 Isolation Means Justification: The following is a list of the unauthorized data flows provided in Annex D of the PP along with references in the ST to where and how those unauthorized data flows are blocked:
    - B (selected computer to user input peripheral) – sections 7.1, 7.3, and 7.4 of the ST show how data flows are unidirectional from user input peripherals to the selected computer.
    - F (user peripheral output to user peripheral input) – sections 7.1, 7.3, 7.4, and 7.6 describe how data flows between peripheral ports are prevented through satisfaction of O.PERIPHERAL_PORTS_ISOLATION.
    - G (user peripheral input to user peripheral output) – same as data flow F.
    - I1 (user peripheral output to selected computer) – section 7.4 describes how unidirectional video flows are enforced such that the Read EDID data path is only open as part of initial link establishment.
    - I2 (user peripheral output to non-selected computer) – same as data flow I1.
    - J, K (connected computers) – the isolation between connected computers is described in sections 7.1, 7.3, 7.4, and 7.6, including information on how that isolation is maintained in the event of a self-test failure. Section 7.7 describes how the data isolation is self-tested.
    - L (user peripheral input to non-selected computer) – sections 7.1, 7.4, and 7.6 describe

how this data flow is blocked through satisfaction of the O.USER_DATA_ISOLATION objective.
    - M (selected computer to non-selected computer) – video and audio isolation between connected computers is the same as data flows J and K.
    - N (any data to external entities) – section 7.2 lists the external interfaces to the TOE and shows that there are no additional external interfaces beyond those that are authorized to transmit data.
    - P (external entities to any TSF data) – same as data flow N.
    - R (user authentication device to non-selected computer) – section 7.6 describes how user authentication data only flows to the connected computer.
    - S (user authentication device to other peripheral device) – section 7.6 describes how the CAC port is isolated from other peripheral interfaces.
    - T (other peripheral device to user authentication device) – same as data flow S.
    - U (user authentication device to other TSF data) – section 7.6 describes how the CAC interface is isolated from other TSF data.
- J.4 Firmware Dependencies: The Letter of Volatility (Appendix B) describes how all of the TOE firmware is handled. Specifically, the USB firmware exists separately from the display firmware. The self-test functionality coupled with the immutability of the firmware storage is sufficient to demonstrate that any catastrophic failure of the firmware will cause the TSF to fail closed and continue to enforce isolation.

2.1.4.2 Guidance Assurance Activities

The evaluator shall verify that the operational guidance provides clear direction for the connection of computers and peripheral devices to the TOE. Any options to switch peripheral devices independently from the keyboard and mouse must be described, including a description of how this switching is indicated on the PSS.

The [Owner] guidance document provides the following direction for connection of computers and peripheral devices to the various TOE models:

- The “System Requirements” section includes the peripherals that are supported for the various TOE models.
- The “Installation” section provides step-by-step instructions on how to connect each computer/peripheral to the TOE.
- In the “Single-Head Mode Secure KM Switching”: diagram showing how the cursor control switching process works.

The TOE does not provide any option to switch keyboard and mouse peripherals independently of one another.

The evaluator shall verify that the operational guidance provides clear direction for the usage and connection of TOE interfaces. General information may be provided for computer, power and peripheral devices. Any wireless or wired interface that receives or transmits data to or from the TOE must be described in sufficient detail to allow the evaluator to determine if there is a risk that these interfaces could be misused to import or export user data.

The [Owner] guidance document specifies in the "System Requirements" section the peripherals that are authorized for use with the TOE. The "Installation" section references the specific physical interfaces that are used to connect to the TOE (e.g. USB A/B device cables, 3.5mm stereo audio cable). At various points in the documentation the following risks/usage guidance are provided:

- Use of VGA requires a DVI-enabled KVM model and a DVI-to-VGA adapter
- Wireless keyboard and mouse are not supported
- Microphones and headsets with microphones are not supported
- CAC readers with external power sources are not supported

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

The [Owner] documentation states in the "Features" section that the triggering of the anti-tamper switches will cause the front panel LEDs to flash repeatedly. It also states that the TOE has tamper-evident seals and that attempted removal of these seals will result in visual evidence of the attempt.

The evaluator shall review the following subjects in the user and administrative guidance to verify that there are no processes or settings that may allow any forbidden data flow between objects:

a. Installation options;
b. TOE configurations:
c. TOE firmware options; or
d. Accessories supplied with TOE

The [Owner] documentation only contains information to install, configure, and use the TOE. The guidance documentation does not identify any processes or settings that may allow any forbidden data flow between objects:

a) Installation options;
b) TOE configurations:
c) TOE firmware options

The [Owner] documentation does list optional accessories in the "Optional Accessories" section. However, in each of these cases the accessories are designed to support known security-relevant interfaces (e.g. 3.5mm stereo audio cables for audio out, DVI cables, HDMI cables, USB A/B cables) and therefore these accessories cannot be used to support any forbidden data flows. Also note that these accessories are not 'supplied with the TOE' as stated in the PP; the [Owner] documentation has a "Package Includes" section which lists the only supplied components as the TOE itself, a power cable, and the owner's manual.

The evaluator shall verify that any cables or accessories supplied with the TOE (as described in the guidance) do not support computer interface types in the following prohibited protocols list:

a. Microphone audio input;
b. Line in audio input;
c. DockPort;
d. USB docking;
e. Thunderbolt; or
f. Other docking protocols.

As stated above, the [Owner] documentation has a "Package Includes" section that identifies the components that are supplied with the TOE. These components include only the TOE itself, an appropriate power cable, and the owner's manual. There are no cables or accessories supplied with the TOE that support any prohibited protocols. In addition to this, the "Optional Accessories" section of the [Owner] documentation only includes components that can be used for authorized communications channels (i.e., there are no optional accessories that can provide connectivity using any of the prohibited protocols).

The evaluator shall verify that the supported peripheral devices and protocols match the information in Annex C of this PP.
[Conditional] If the TOE supports keyboard / mouse –   *The evaluator shall examine the TOE user guidance to determine if there are any operating modes that allow peripheral devices to be switched independently from the keyboard and mouse. All such operating modes must be covered in the TSS. The evaluator shall examine the TOE guidance and verify that the TOE does not support microphone or audio line input device interfaces. The evaluator shall also examine the TOE guidance and verify that it includes an explicit warning not to use microphone, line input or headset devices with the TOE.*

The [Owner] documentation indicates the physical interfaces and peripheral types that are supported by the various TOE models. In each case, the supported interface/peripheral types are consistent with what is defined in the PP. The TOE includes the following interfaces:

- USB keyboard/mouse
- 3.5mm audio out
- (for models supporting CAC functionality) USB CAC/authentication device
- (for models supporting KVM/Matrix functionality) HDMI, DVI, or DisplayPort video

The TOE does not provide any option to switch keyboard and mouse peripherals independently from one another.

The [Owner] documentation states in the "Installation" section that "Microphones or headsets with microphones are not supported." It is understood by the evaluator that this prohibits the use of line in audio devices of any sort.

2.1.4.3 Test Assurance Activities

4.2.9. General Tests Setup Information

1. *Since a PSS typically has a large set of switched peripheral devices and connected computers, in order to prevent duplication of test setup and testing effort, several tests were grouped into larger test sets. The selection of the appropriate test set is based on the specific TOE implementation, which is based on the type of peripheral devices being supported.*
2. *Each port group switch selection must be tested for each device; however, not all port groups must be connected simultaneously. For example, if testing a 16-port device, the evaluator may use four connected computers, but must change the connected ports several times to ensure all computer port group connections and switch selections are tested. Likewise, a single USB protocol analyzer may be used, but must be moved to test each applicable port. Several of the tests are written assuming a 4 port device. Each test must be adapted to accommodate all of the ports on each tested TOE.*
3. *The tests assume the use of Windows on each connected computer. It is permissible to perform*

the tests using Linux based connected machines with similar applications installed.

4. *The evaluator is expected to prepare an image or bitmap with an easily visible number to be used as a background for each connected computer in order to identify each channel (e.g., a white background with the number 1 may serve as a desktop background for computer #1.)*
5. *Note that some of the following tests require knowledge of the USB protocol to properly configure and operate a USB protocol analyzer and USB sniffer.*

4.2.10. Test 4.1 – User Control

This test is mandatory for all TOEs claiming compliance to this PP.

The following tests assure that the TOE is compliant with the user switching rules. In this test the evaluator shall verify that switching methods supported by the TOE are those permitted by this PP.

SFRs mapped to the following test steps:

- *Switching rules: FDP_IFF.1.2(1) Rule 2*
- *Split selection: FDP_IFF.1.2(1) Rule 3*

The evaluator shall:

1. *Configure the TOE and the operational environment in accordance with the operational guidance.*
2. *Run an instance of a text editor (such as Notepad) on each connected computer to identify which computer is connected to the user keyboard by the TOE.*
3. *Connect a display to each computer in order to see all computers at the same time.*
4. *Turn on the TOE.*
5. *Test each TOE switching method and verify that all methods are authorized methods and that non-authorized methods cannot be enabled by specific TOE configuration. Verify that the TOE does not support a computer port scanning mode.*
6. *Attempt to switch the mouse/pointing device to more than one computer at once. Verify that the TOE ignores such commands. At all times, the mouse/pointing device may only be connected to a single computer.*

Note: Output peripherals such as display or audio output may be connected simultaneously to more than one computer.

7. *Attempt to switch the TOE to a computer interface that does not exist (e.g., the fifth port in a 4-port TOE) [Conditional] or to a computer channel that was previously disabled (if applicable). The TOE shall refuse to switch to such options.*
8. ***[Conditional]** If TOE enables computer channel freeze and channel disable - the evaluator shall examine these functions and verify that they operate in accordance with the operational guidance.*

The evaluator began by configuring the environment to perform this test. A keyboard and mouse were connected to the TOE via the keyboard/ mouse USB input ports. A USB was connected from each of the computer keyboard and mouse interfaces on the TOE to a USB port on each computer. Each computer was connected to its own monitor so each display could be viewed at the same time.

The evaluator verified that the only authorized method of switching on the KVM devices was by pressing in one of the buttons on the front of the TOE. The evaluator switched to each interface and moved the mouse and typed in an instance of notepad. The evaluator viewed that these actions were not replicated on the non-selected computers. The evaluator also verified an additional switching method for when the device is in KM mode. The evaluator demonstrated that in KM mode the TOE switches channels based on cursor control. Evidence for the TOE in KM mode is shown with Test 4.3 Part 5. Both instances of the TOE pass all methods of authorized switching.

The evaluator viewed that no other methods of switching were possible including switching to an unsupported channel and a port scanning mode. The evaluator attempted to switch to two channels at once. The result was either the channel did not switch at all or the channel that was pressed slightly before the other was switched to.

The overall result of Test 4.1 is a pass.

4.2.11. Test 4.2 – Keyboard Switching, Data Isolation and Device Qualification Rules

[Conditional] *The following test is mandatory for any TOE that supports one or more user keyboards.*

Test Setup

The evaluator shall:

1. *Configure the TOE and the operational environment in accordance with the operational guidance.*
2. *Run USB Protocol analyzer software in each of the connected computers.*
3. *Connect a display to each computer in order to see all computers at the same time.*
4. *Turn on the TOE.*

Part 1 - Positive and Negative Keyboard Data-flow Rules Testing

The following steps shall be run to verify that the USB keyboard traffic is properly routed to the selected computer (positive data flow rule) and no other USB traffic leaks to the non-selected computers (negative data flow rule).

SFRs mapped to the following test steps:

- *Switching rules: FDP_IFF.1.2(1) Rule 2*
- *Positive switching (allow data flow): FDP_IFF.1.2(1) Rule 1a*
- *Negative switching: FDP_IFF.1.5(1) Rule 1*
- *Multiple instances: FDP_IFF.1.2(1) Rule 4*

5. *Select computer #1.*
6. *Use the USB keyboard to type text into a text editor application running on computer #1.*
7. *Verify that the TOE sends data from the USB keyboard peripheral device to the switched computer #1 [Allowed Data Flow]. Verify that keyboard entries are visible in USB Protocol analyzer on computer #1.*
8. *Switch to each connected computer and verify that no text appears in the text editor application on any of the non-selected computers.*
9. *Continue typing on the keyboard and check each one of the non-selected computers for keyboard traffic. The only traffic visible in the USB Protocol analyzers should be USB keep-alive (NAK transactions).*

10. *Disconnect and reconnect the TOE interface cables connected to computer #1. Check each one of the non-selected computers for keyboard traffic. Verify that the only traffic visible in the USB Protocol analyzers is USB keep-alive (NAK transactions).*
11. *Reboot computer #1. Check each one of the non-selected computers for keyboard traffic. The only traffic visible in any of the non-selected computer USB Protocol analyzers is USB keep-alive traffic (NAK transactions).*
12. *Enter sleep or suspend mode in computer #1. Check each one of the non-selected computers for keyboard traffic. The only traffic visible in any of the non-selected computer USB Protocol analyzers is USB keep-alive traffic (NAK transactions).*
13. *Exit suspend mode on computer #1 and delete all of the text typed in the Text Editor application.*
14. *Repeat Steps 3 to 13 with each connected computer selected and each instance of the keyboard supported by the TOE (if applicable).*
15. ***[Conditional]** This step is applicable only for a TOE that supports PS/2 keyboards - Repeat steps 3 to 14 with a PS/2 keyboard.*

The evaluator began by configuring the environment to perform this test. A keyboard was connected to the TOE via the keyboard/ mouse USB input ports. Note that the keyboard and mouse ports are interchangeable. A USB was connected from each of the computer keyboard and mouse interfaces on the TOE to a USB port on each computer. Each computer was connected to its own monitor so each display could be viewed at the same time.

The evaluator selected computer 1 and opened up an instance of notepad. The evaluator viewed that typing in Notepad was successful on that computer but the action was not replicated on the non-selected computers. The evaluator ran a USB capture on each of the unselected computers on the USB port connected to their keyboard/mouse interface on the TOE. The evaluator continued to type with computer 1 selected and viewed that no USB data was passed on to the non-selected computers as expected. The evaluator repeated the capture process during these additional cases:

- Disconnect and reconnect the TOE interface cables connected to computer 1
- Reboot Computer 1
- Enter sleep mode on computer 1

All of the instances ended with the same result. No USB data was viewed being passed on to the unselected computers. The overall result of Test 4.2 Part 1 is a pass.

Part 2 - Keyboard Allowed Data Flow and Allowed Devices

In the following steps, the evaluator shall verify that the TOE USB keyboard device port will disable or reject a device that is not a qualified keyboard. The evaluator shall also examine the enumeration of a qualified keyboard behind a USB hub with an unauthorized device connected to another hub downstream port.

SFRs mapped to the following test steps:

- *Allowed devices: FDP_IFF.1.5(2) Rule 13*
- *Allowed data: FDP_IFF.1.5(2) Rule 2*

16. *Ensure that the USB keyboard is connected. Type on the keyboard and at the same time verify that the selected computer USB protocol analyzer does not show any USB transactions other than link maintenance messages (keep-alive NAK transactions) and keyboard keystroke*

reports (i.e., key press and key release codes).

17. *Connect a USB storage device to the USB keyboard interface (instead of the USB keyboard).*
18. *At the same time, examine the selected computer USB protocol analyzer to verify that the only captured transactions are USB keep-alive data (NAK transactions).*
19. *Verify that no new text appears in the selected computer text editor window.*
20. *Verify that the real-time hardware information console does not display any new USB devices (recognized or not recognized).*
21. *Disconnect the USB storage device and connect a USB audio device instead. Repeat steps 18 to 20 above.*
22. *Disconnect the USB audio device.*
23. *Reconnect the keyboard, this time connecting it through a USB hub. Connect the USB storage device to another downstream port of the USB hub.*
24. *Repeat steps 18 to 20. The USB storage device should not be visible in the real-time hardware information console. The keyboard may or may not be visible, depending on the TOE specific implementation.*

The evaluator began by configuring the environment to perform this test. A keyboard was connected to the TOE via the keyboard/ mouse USB input ports. Note that the keyboard and mouse ports are interchangeable. A USB was connected from each of the computer keyboard and mouse interfaces on the TOE to a USB port on each computer.

The evaluator ran a USB capture on the selected computer on the USB port connected to its keyboard/mouse interface on the TOE. The evaluator typed on the keyboard and viewed that the only data captured other than keep alive packets were the result of specific keystrokes. Each keystroke was viewed in the capture as two data packets.

The evaluator replaced the keyboard with a USB storage device. The evaluator viewed via USB capture that no USB data was sent to the selected computer. The evaluator also viewed that the TOE flashed and was not functional until the USB storage device had been removed and a reboot occurred. The evaluator viewed the same results in the following other scenarios:

- USB audio device connected
- USB storage device connected downstream of USB keyboard in USB hub.

The overall result of Test 4.2 Part 2 is a pass.

Part 3 - Keyboard Flow Isolation and Unidirectional Rule

The TOE HID data path shall not support USB traffic other than keyboard and pointing device user inputs. Therefore, in this test it is adequate to validate that the TOE keyboard device interface enumerates and supports qualified keyboard and mouse devices, but does not enumerate and support USB devices that are not HIDs.

In the following steps, the evaluator shall test the TOE to verify that it does not allow direct electrical and dataflow linkage between the computer interfaces and the connected keyboard device interfaces. In addition, the evaluator shall verify that the keyboard data flow is unidirectional.

SFRs mapped to the following test steps:

- *Unidir data flow: FDP_IFF.1.5(2) Rule 4, FDP_IFF.1.2(2)*
- *Power isolation: FDP_IFF.1.5(2) Rule 3*

- *Data types: FDP_IFF.1.5(2) Rule 2, FDP_IFF.1.2(2)*
- *Power off isolation: FDP_IFF.1.5(2) Rule 14*

25. *Power up the TOE.*
26. *Select computer #1.*
27. *Use a USB keyboard emulation software application (see additional information in Annex I) running on computer #1 to turn the keyboard Num Lock, Caps Lock and Scroll Lock LEDs on and off. LEDs on the keyboard should not illuminate. [This is true if the TOE complies with the PP requirement to prevent computer to peripheral data flow].*
28. *Power down the TOE.*
29. *Disconnect the peripheral interface USB cable connected from the TOE to computer #1. Disconnect the user keyboard.*
30. *Power up the TOE. Switch the TOE to computer #1.*
31. *Reconnect the keyboard. 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 keyboard is powered on, although the selected computer is not connected).*
32. *Turn the TOE off and disconnect the USB keyboard and mouse. Reconnect the computer #1 interface USB cable. Connect the keyboard and mouse directly to computer #1 if necessary.*
33. *Open a real-time hardware information console on computer #1.*
34. *Turn on the TOE and check the computer real-time hardware information console for the presence of the USB keyboard and mouse. If the TOE keyboard and mouse appears in the listed devices, skip directly to step 36 as the TOE has successfully passed emulated keyboard/mouse testing [keyboard and mouse are emulated and unidirectional]. If not, continue to step 35 below.*
35. *Perform simulated USB keyboard traffic testing in accordance with the following steps:*

    a. Connect a USB Generator to the TOE keyboard peripheral device interface port.

    b. Configure the USB Generator to enumerate as a generic HID keyboard device and then to generate a random stream of keyboard packets.

    c. Connect a USB protocol analyzer device (sniffer) between the TOE computer interface and the USB port on computer #1 to capture the keyboard USB traffic between the TOE and computer #1.

    d. Turn on the TOE and verify that no packets cross the TOE following the keyboard enumeration, except for keep-alive traffic (NAK transactions). If the TOE has successfully passed this test, then its keyboard path complies with the requirements by enforcing unidirectional data flow and by providing an emulated keyboard function.

The evaluator began by running a baseline test. The evaluator connected a keyboard directly to computer 2 and ran a keyboard emulator. The evaluator enabled Num Lock, Caps Lock, and Scroll Lock on the emulator. The corresponding lights were illuminated on the physical keyboard.

The evaluator then configured the environment to perform the required test. The keyboard was connected to the TOE via the keyboard/ mouse USB input ports. A USB was connected from each of the computer keyboard and mouse interfaces on the TOE to a USB port on each computer.

The evaluator powered up the TOE and selected computer 1. The evaluator ran the same keyboard emulator on the selected computer but the lights on the physical keyboard were not lit despite the same keys being selected on the emulator. The evaluator powered off the TOE and disconnected the keyboard.

The evaluator then rebooted the TOE and upon power on plugged the keyboard back in. The evaluator viewed that the lights on the keyboard did not stay illuminated. This demonstrated that keyboard traffic through the TOE was unidirectional.

The evaluator then verified that the keyboard was successfully emulated by the TOE. The evaluator powered off the TOE and disconnected the keyboard. The evaluator powered on the TOE and opened up the device manger on the selected computer. The evaluator viewed an HID Keyboard Device listed, which means the TOE emulates a keyboard correctly.

The overall result of Test 4.2 Part 3 is a pass.

Part 4 - TOE Keyboard Interface Properly Disable Unauthorized Peripheral Devices

In the following steps the evaluator shall verify that the TOE keyboard port properly disables unauthorized USB devices. This is verified through a USB protocol Analyzer device (sniffer) connected between the device and the TOE.

SFRs mapped to the following test steps:

- *Authorized devices: FDP_IFF.1.5(2) Rule 13*
- *Device rejection: FDP_ACF.1*

36. *Configure the TOE and the operational environment in accordance with the operational guidance.*
37. *Power up the TOE.*
38. *Connect the following unauthorized devices to the TOE USB keyboard peripheral interface via a USB protocol analyzer device (sniffer) to verify that the devices are rejected:*

    a. USB audio device;

    b. USB storage device;

    c. USB camera;

    d. USB user authentication device;

    e. USB printer; and

    f. USB Composite Device evaluation board with HID keyboard, Communication Device Class (CDC), and Mass Storage Class (MSC) devices. CDC and MSC shall be rejected.

Device Rejection shall be verified through:

I. The expected TOE user indication in accordance with the user guidance; and

II. An immediate cessation of captured USB traffic following device enumeration.

39. *Repeat Step 38 above with a USB hub connected between the USB protocol analyzer and the USB device. The results should be the same.*
40. *Repeat Step 38 above with the TOE powered off. The USB protocol analyzer device shall show only keep-alive traffic (NAK transactions), or no USB link at all.*

The evaluator began by configuring the environment to perform this test. A USB was connected from each of the computer keyboard and mouse interfaces on the TOE to a USB port on each computer.

A USB capture was run on the selected computer to verify that no USB data was passed to the selected computer as unauthorized devices are plugged into the keyboard/ mouse interface of the TOE. Note that the keyboard and mouse ports are interchangeable. The following unauthorized devices were tested

- USB Audio Device
- USB Storage Device
- USB Camera
- USB User Authentication Device
- USB Printer
- USB Composite Keyboard

No USB data was captured as passed to the selected computer when these devices were plugged into the keyboard/mouse interface. After each device was connected to the TOE, the TOE began to flash and lost functionality until the unauthorized device was disconnected from the TOE and the TOE was rebooted. The evaluator repeated the process with each device except the devices were plugged into a USB hub that was connected to the TOE. The results were the same. The final step was to power off the TOE and to plug each device into the TOE. The USB capture showed no data as expected.

The overall result of Test 4.2 Part 4 is a pass.

Part 5 - Keyboard User Control

[Conditional] *the following test steps are not applicable for isolators (which may not support user control).*

In the following steps, the evaluator shall use the keyboard in an attempt to perform TOE switching operations that are not authorized.

SFRs mapped to the following test steps:

- *No unauthorized keyboard data flow: FDP_IFF.1.5(2) rule 2*

41. Attempt to control the TOE computer selection using the following standard keyboard shortcuts (# denotes computer channel number):

a. Control – Control – # - Enter

b. Shift-Shift-#

c. Num Lock – Minus - #

d. Scroll Lock – Scroll Lock - #

e. Scroll Lock – Scroll Lock – Function #

f. Scroll Lock – Scroll Lock – arrow (up or down)

g. Scroll Lock – Scroll Lock – a - Enter

h. Control – Shift – Alt - # - Enter

i. Alt – Control – Shift #

The TOE shall not respond to such commands by switching channels. (It should be noted that keyboard shortcuts may be used to perform other functions, such as TOE configuration).

42. Attempt to switch the keyboard/s to more than one computer at once. The TOE shall ignore

such commands / prevent such options. At all times, the keyboard/s shall only be connected to a single selected computer.

43. ***[Conditional]*** *If the device allows for peripheral switching independent of the keyboard and mouse - the evaluator must verify that the switching function behaves in accordance with the guidance, and that the device provides a clear indication of the connection for each peripheral. The evaluator must also verify that the keyboard and mouse are always switched together.*

Notes:

1. *The USB protocol analyzer shall indicate no USB data payloads while the computer is not selected. No USB packets are allowed other than standard USB keep-alive traffic (NAK transactions).*
2. *The NAK transaction is a standard USB PID 1010B transaction used to indicate that the receiving device cannot accept data or the transmitting device cannot send data.*
3. *To comply with the USB standard, immediately before or following TOE (not computer) power state change (power off or on), the TOE may send a small number of packets to the connected computer.*

The evaluator began by configuring the environment to perform this test. A keyboard was connected to the TOE via the keyboard/ mouse USB input ports. A USB was connected from each of the computer keyboard and mouse interfaces on the TOE to a USB port on each computer. Each computer was connected to its own monitor so each display could be viewed at the same time.

The evaluator selected computer 1 and opened up an instance of notepad. The evaluator typed each of the standard keyboard shortcuts and then typed a corresponding letter in notepad to verify the TOE had not switched channels. The following shortcuts were tested:

a. Control – Control – # - Enter

b. Shift-Shift-#

c. Num Lock – Minus - #

d. Scroll Lock – Scroll Lock - #

e. Scroll Lock – Scroll Lock – Function #

f. Scroll Lock – Scroll Lock – arrow (up or down)

g. Scroll Lock – Scroll Lock – a - Enter

h. Control – Shift – Alt - # - Enter

i. Alt – Control – Shift #

As expected none of the standard keyboard shortcuts resulted in channel switching. The evaluator also verified that it was not possible to switch to two channels at once in Test 4.1.

The TOE does not support peripheral switching independent of the keyboard and mouse.

The overall result of Test 4.2 Part 5 is a pass.

4.2.12. Test 4.3 – Mouse Switching, Data Isolation and Device Qualification Rules

[Conditional] *The following test is mandatory for a TOE that supports one or more user mouse, or other pointing device.*

Test Setup

The evaluator shall:

1. *Configure the TOE and the operational environment in accordance with the operational guidance.*
2. *Run USB Protocol analyzer software in each of the connected computers.*
3. *Connect one display per computer in order to see all computers at the same time.*
4. *Turn on the TOE.*

Part 1 - Positive and Negative Mouse Data-flow Rules Testing

The following steps shall verify that the USB mouse traffic is properly routed to the selected computer (positive data flow rule), and no other USB traffic leaks to the non-selected computers (negative data flow rule).

SFRs mapped to the following test steps:

- *Switching rules: FDP_IFF.1.2(1) Rule 2*
- *Positive switching (allow data flow): FDP_IFF.1.2(1) Rule 1b*
- *Negative switching: FDP_IFF.1.5(1) Rule 1*
- *Multiple instances: FDP_IFF.1.2(1) Rule 4*

5. *Switch the TOE to each connected computer and using a USB mouse, position the mouse cursor at the center of each display. Switch the TOE to computer #1 and move the cursor to the bottom right corner of the display.*
6. *Use the USB mouse to move the cursor on computer #1.*
7. *Switch the TOE to each connected computer and verify that the cursor is still located at the center of the display. Verify that the TOE sends data from the USB mouse peripheral device to the switched computer #1 [Allowed Data Flow]. Verify that mouse movement and button reports are visible in the computer #1 USB Protocol analyzer software.*
8. *Switch to each connected computer and verify that no cursor movements are indicated on any of the non-selected computers.*
9. *Continue moving the cursor and check each one of the non-selected computers for mouse traffic. The only traffic visible in the USB Protocol analyzers should be USB keep-alive (NAK transactions).*
10. *Disconnect and reconnect the computer #1 TOE interface cables. Check each one of the non-selected computers for mouse traffic. The only traffic visible in the USB Protocol analyzers is USB keep-alive traffic (NAK transactions).*
11. *Reboot computer #1. Check each one of the non-selected computers for mouse traffic. The only traffic visible in all the non-selected computer USB Protocol analyzers is USB keep-alive traffic (NAK transactions).*
12. *Enter sleep or suspend mode in computer #1. Check each one of the non-selected computers for mouse traffic. The only traffic visible in all the non-selected computer USB Protocol analyzers is USB keep-alive traffic (NAK transactions).*

13. *Switch back to computer #1.*
14. *Repeat Steps 3 to 13 with each connected computer selected.*
15. ***[Conditional]** This step is applicable only for a TOE that supports a PS/2 mouse - Repeat steps 3 to 14 with a PS/2 mouse.*

The evaluator began by configuring the environment to perform this test. A mouse was connected to the TOE via the keyboard/ mouse USB input ports. A USB was connected from each of the computer keyboard and mouse interfaces on the TOE to a USB port on each computer. Each computer was connected to its own monitor so each display could be viewed at the same time. The evaluator set the mouse pointer to the center of the display on each computer.

The evaluator ran a USB capture on the selected computer and moved/clicked the mouse. The evaluator viewed the USB data captured was as a result of the mouse movement and clicks and no other reason. The evaluator verified that the mouse movement was not replicated on any of the non-selected computers. The evaluator ran an USB capture on each of the non-selected computers on USB port connected to their keyboard/mouse interface on the TOE. The evaluator continued to move the mouse on the TOE and viewed that no USB data was passed on to the non-selected computers. The mouse movement was not replicated on the non-selected computers.

The evaluator continued to verify that no data was passed on to the non-selected computers in the following scenarios:

- Disconnect and Reconnect Computer 1
- Reboot Computer 1
- Enter sleep mode in computer 1

All of the scenarios resulted in the same successful results. The overall result of Test 4.3 Part 1 is a pass.

Part 2 - Mouse Allowed Data Flow and Allowed Devices

In the following steps the evaluator shall verify that the TOE USB mouse device port will disable or reject devices that are not a qualified pointing device. The evaluator shall also test the enumeration of a qualified mouse behind USB hub having an unauthorized device connected to another hub downstream port.

SFRs mapped to the following test steps:

- *Allowed devices: FDP_IFF.1.5(2) Rule 13*
- *Allowed data: FDP_IFF.1.5(2) Rule 2*

16. *Reconnect the USB mouse. Move the mouse cursor from side to side and at the same time verify that the selected computer USB protocol analyzer does not show any USB transactions other than link maintenance messages (keep-alive NAK transactions) and mouse reports.*
17. *Connect a USB storage device instead of the USB mouse.*
18. *At the same time, check the selected computer USB protocol analyzer to verify that the only captured transactions are USB keep-alive traffic (NAK transactions).*
19. *Verify that the mouse cursor is no longer moving.*
20. *Verify that the real-time hardware information console does not display any new USB devices (recognized or not recognized).*
21. *Disconnect the USB storage device and connect a USB audio device instead. Repeat steps 18 to 20 above.*

22. *Disconnect the USB audio device.*
23. *Reconnect the mouse, this time through a USB hub. Connect a USB storage device to another downstream port of the USB hub.*
24. *Repeat steps 18 to 20. The USB storage device should not be visible in the real-time hardware information console. The mouse device may or may not be visible, depending on the TOE specific implementation.*

The TOE does not have distinct USB ports for keyboard or mouse peripherals. There are two available USB ports that can be used interchangeably for these types of devices. However, any non-keyboard/ mouse USB device will be rejected. The testing of allowed data flow for non-keyboard/mouse USB devices was successfully demonstrated in Test 4.2 Part 2.

Part 3 - Mouse Flow Isolation and Unidirectional Rule

The TOE HID data path shall not support USB traffic other than keyboard and pointing device user inputs. Therefore, in this test it is adequate to validate that the TOE mouse device interfaces enumerate and support qualified mouse devices, but do not enumerate and support USB devices that are not HIDs.

In the following steps, the evaluator shall test the TOE to verify that it does not allow direct electrical and dataflow linkage between the computer interfaces and the connected mouse device interfaces. In addition, the evaluator shall verify that the mouse data flow is unidirectional.

SFRs mapped to the following test steps:

- *Unidir data flow: FDP_IFF.1.5(2) Rule 4, FDP_IFF.1.2(2)*
- *Power isolation: FDP_IFF.1.5(2) Rule 3*
- *Data types: FDP_IFF.1.5(2) Rule 2, FDP_IFF.1.2(2)*
- *Power off isolation: FDP_IFF.1.5(2) Rule 14*

25. *Power up the TOE.*
26. *Select computer #1.*
27. *Use a USB gaming mouse with programmable LEDs and attempt to configure the LEDs using the mouse application running on computer #1. The mouse programmable LEDs should not change state [This demonstrates that the TOE complies with the PP requirement to prevent computer to peripheral data flow].*
28. *Power down the TOE.*
29. *Disconnect the peripheral interface USB cable connected to computer #1 from the TOE. Disconnect the user mouse.*
30. *Power up the TOE. Switch the TOE to computer #1.*
31. *Reconnect the mouse. Verify that immediately following the connection, the mouse is illuminated (i.e. powered on, although the selected computer is not connected).*
32. *Turn the TOE off and disconnect the USB keyboard and mouse. Reconnect the computer #1 interface USB cable. Connect the keyboard and mouse directly to computer #1 if necessary.*
33. *Open a real-time hardware information console on computer #1.*
34. *Turn on the TOE and check the computer real-time hardware information console for the presence of a USB keyboard and mouse. If the TOE keyboard and mouse appears in the listed devices, skip directly to step 36 as the TOE has successfully passed emulated keyboard/mouse testing [i.e. the keyboard and mouse are emulated and unidirectional]. If not, continue to step 35 below.*

35. Perform simulated USB mouse traffic testing in accordance with the following steps:

a. Connect a USB Generator to the TOE mouse peripheral device interface port.

b. Configure the USB Generator to enumerate as a generic HID mouse device and then to generate random stream of mouse report packets.

c. Connect a USB protocol analyzer device (sniffer) between the TOE computer interface and the USB port on computer #1 to capture the mouse USB traffic between the TOE and computer #1.
d. Turn on the TOE and verify that no packets cross the TOE following mouse enumeration, except for keep-alive traffic (NAK transactions). If TOE has successfully passed this test, then its mouse path complies with the requirements by enforcing unidirectional data flow and by providing an emulated mouse function.

The evaluator then configured the environment to perform the required test. The gaming mouse was connected to the TOE via the keyboard/ mouse USB input ports. A USB was connected from each of the computer keyboard and mouse interfaces on the TOE to a USB port on each computer.

The user opened up the Logitech software on computer 1 but the mouse was not recognized to be configured. The evaluator then powered down the TOE and disconnected the mouse and computer 1's interface cable from the TOE. The evaluator powered the TOE back on, switched to computer 1, and plugged the mouse back into the TOE's keyboard/mouse interface. The evaluator viewed the lights on the mouse were illuminated despite computer 1's interface cable not being connected.

The evaluator verified that the TOE properly emulated a mouse device in conjunction with Test 4.2 Part 3. The evaluator unplugged the mouse from the TOE and plugged computer 1's interface cable back into the TOE. The evaluator opened up the device manager on the selected computer and still viewed a HID-complaint mouse. The TOE successfully emulated a mouse device.

The overall result of Test 4.3 Part 3 is a pass.

Part 4 - TOE Mouse Interface Properly Disable Unauthorized Peripheral Devices

In the following steps the evaluator shall verify that the TOE mouse port properly disables unauthorized USB devices. This is verified through a USB protocol Analyzer device (sniffer) connected between the device and the TOE.

SFRs mapped to the following test steps:

- *Allowed devices: FDP_IFF.1.5(2) Rule 13*
- *Device rejection: FDP_ACF.1*

36. Reconfigure the TOE and the operational environment in accordance with the operational guidance.
37. Power up the TOE.
38. Connect the following unauthorized devices to the TOE USB mouse peripheral interface via a USB protocol analyzer device (sniffer) to verify that the devices are rejected:

a. USB audio device;
b. USB storage device;
c. USB camera;

d. USB user authentication device;
e. USB printer; and
f. USB Composite Device evaluation board with HID keyboard, Communication Device Class (CDC), and Mass Storage Class (MSC) devices. CDC and MSC devices shall be rejected.

Device rejection shall be verified through:

I. TOE user indication in accordance with the user guidance; and
II. An immediate cessation of captured USB traffic following device enumeration.

39. *Repeat Step 38 above with a USB hub connected between the USB protocol analyzer and the USB device. The results should be the same as above.*
40. *Repeat Step 38 above with the TOE powered off. The USB protocol analyzer device shall show only keep-alive traffic (NAK transactions) or no USB link at all.*

The TOE does not have distinct USB ports for keyboard or mouse peripherals. There are two available USB ports that can be used interchangeably for these types of devices. However, any non-keyboard/ mouse USB device will be rejected. The testing of proper disabling for unauthorized peripheral devices was successfully demonstrated in Test 4.2 Part 4.

Part 5 - Mouse User Control

In the following steps the evaluator shall use the mouse in an attempt to perform TOE switching operations that are not authorized.

SFRs mapped to the following test steps:

- *No unauthorized mouse data flow: FDP_IFF.1.5(2) Rule 2*

41. *Attempt to switch the mouse to more than one computer at once. The TOE shall ignore such commands / prevent such options. At all times, the mouse shall only be connected to a single selected computer.*
42. ***[Conditional]** If the device allows for peripheral switching independent of the keyboard and mouse, the evaluator must verify that the switching function behaves in accordance with the guidance, and that the device provides a clear indication of the connection for each peripheral. The evaluator must also verify that the keyboard and mouse are always switched together.*
43. ***[Conditional]** If the TOE supports cursor control of selected channels then – The evaluator shall repeat steps 41 to 43 with the cursor control.*

Notes:

1. *The USB protocol analyzer shall indicate no USB data payloads while the computer is not selected. No USB packets are allowed other than standard USB keep-alive traffic (NAK transactions).*
2. *The NAK transaction is a standard USB PID 1010B transaction used to indicate that the receiving device cannot accept data or the transmitting device cannot send data.*

To comply with the USB standard, immediately before or following TOE (not computer) power state change (power off or on), the TOE may send a small number of packets to the connected computer.

The unsuccessful attempt to switch to multiple computers at once was demonstrated in Test 4.1. The TOE supports a KM mode that allows switching via cursor control. The evaluator verified that the TOE did not switch to more than one computer using this method. The TOE does not support switching independent of the keyboard and mouse. The overall result of Test 4.3 Part 5 is a pass.

Test 4.4 – Display Switching, Data Isolation and Unidirectional Flow Rules

[Conditional] *The following test is mandatory for a TOE that supports one or more user displays.*

Test Setup

The evaluator shall:

1. Configure the TOE and the operational environment in accordance with the operational guidance.

Part 1 - Display Positive and Negative Switching Rules

The following steps evaluate the TOE compliance with the allowed data flow as it is applied to the user display data. This test verifies that the TOE does not transfer display or computer state change data to any non-selected computer.

This test requires the use of an Oscilloscope with a proper set of probes to test the presence of video signals. The type of oscilloscope and probes required depend upon the type and speed of the video interface supported by the TOE. For additional information see Annex I of this PP.

Additionally, in the following steps the evaluator shall verify that the video signal does not leak to other computer interfaces while the TOE is unpowered.

SFRs mapped to the following test steps:

- *Switching rules: FDP_IFF.1.2(1) Rule 2*
- *Positive switching (allow data flow): FDP_IFF.1.2(1) Rule 1c*
- *Negative switching: FDP_IFF.1.5(1) Rule 1*
- *Multiple instances: FDP_IFF.1.2(1) Rule 4*
- *Unpowered isolation: FDP_IFF.1.5(2) Rule 14*

2. *Turn on the TOE.*
3. *Switch the TOE primary display to computer #1.*
4. *Observe the primary display to verify that the selected computer is the one that is actually shown.*
5. *Remove the non-selected computer display interface cables from TOE and connect them, one at a time, to the oscilloscope to verify that no SYNC signal is passed through the TOE:*

    a. VGA – single ended probe on pins 13 and then 14;

    b. HDMI – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide HOT PLUG DETECT signal; Check for signals - differential probe between pins 10 (+) and 12 (-);

    c. DVI-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HOT PLUG DETECT signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-);

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

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

6. *Repeat steps 4 to 5 while selecting other TOE connected computers. Verify that no SYNC signal is present.*
7. *Repeat steps 4 to 6 with the TOE unpowered. Verify that no SYNC signal is present.*
8. *With the scope connected to the computer #2 video interface signals, 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 #2 computer interface pins. No changes shall be detected.*
9. *Repeat step 8 for each one of the other computer interfaces (#3 and 4).*
10. *Repeat steps 8 and 9, but instead of disconnecting / reconnecting the computer, disconnect and reconnect the display.*
11. *Repeat steps 8 and 9, but instead of disconnecting / reconnecting the computer, reboot the selected computer.*
12. *Repeat Steps 2 to 11 with each connected computer.*
13. ***[Conditional]** If a secondary (or other additional) display is supported - repeat Steps 3 to 11 with the secondary or other display connected to the TOE.*
14. *Turn the TOE off by removing power. Verify that no connected display shows any video.*
15. *Repeat step 5 above to verify that no video signal is present while the TOE is unpowered.*
16. *Repeat steps 2 to 15 with each type of display supported by the TOE (DVI, HDMI, DisplayPort etc.)*

The evaluator first tested the B002-DV1AC8. The evaluator began by configuring the TOE in preparation for the test. A DVI cable was run from computer 1to the corresponding video input interface on the TOE. Another DVI cable was run from the TOE video output interface to a display monitor. The evaluator powered on the TOE.

The evaluator verified that computer 1 was selected when the TOE powered up and that the display showed computer 1.

A DVI cable was connected to the computer 2 interface on the TOE. The evaluator connected the free end of the DVI-D cable to a generic DVI-D board so that the pins could be easily measured by an oscilloscope. A power supply was used to send 3.3V signal was sent to pin 16 through a 100 Ohm resistor to create a hot plug. Pins 23 and 24 were probed and verified that no difference was measured between the two. Single ended probes were attached to pins 8 and C4. This demonstrated that no sync signal was present. The evaluator powered off the TOE and repeated the process to measure with the oscilloscope that no sync signal was present. The evaluator also confirmed that no sync signale was present while disconnecting/reconnecting the computer interface cable, disconnecting/reconnecting the display interface cable, and rebooting the computer.

The evaluator repeated the test on the B002-DP2AC4 and B002-HD2AC4. The B002-HD2AC4 supports DisplayPort input and HDMI output and the B002-DP2AC4 supports DisplayPort input and output. The B002-DP2AC4 also supports secondary displays. The pins measured by the oscilloscope to verify signal

were different for each test. In the case of a DisplayPort input, pins 3 and 1 and then 10 and 12 were probed. Additionally all the steps were performed again for the secondary display.

The overall result of Test 4.4 Part 1 is a pass.

Part 2 - DisplayPort Auxiliary (AUX) Channel Data Handling

[TD0086]: DisplayPort to HDMI Conversion Functionality

[TD0298]: Update to FDP_IFF.1 Assurance Activities

Test 4.4, Part 2, Steps 17-32

An alternate testing approach for TOEs that do not support the AUX channel on both the computer and peripheral interfaces is to verify that the HDMI Consumer Electronic Control (CEC - pin 13) and HDMI Ethernet Audio Control (HEAC - pin 14) cannot be used to pass signals. The evaluators will test that the AUX channel related path through the TOE is floating (disconnected) by measuring the resistance-to-ground of the pins at the HDMI end and verify that the measured resistance-to-ground is unlimited. In addition, the absence of any signal on these pins can be verified using an oscilloscope.

[Conditional] This test shall be performed only on a TOE that supports native DisplayPort video.

A TOE that supports DisplayPort through conversion to other video formats through an external cable or dongle should not be tested using these procedures. These procedures are applicable to a TOE that supports DisplayPort video format passed through the switch.

Note that in the following steps only DisplayPort cables shall be used. No conversion from other video protocols is allowed in these tests.

SFRs mapped to the following test steps:

- *AUX filtering: FDP_IFF.1.5(2) Rule 10*

17. *Connect at least one computer with a native DisplayPort video output capable of supporting DisplayPort version 1.2 or higher standard. This computer shall be connected to the TOE computer #1 video input interface.*
18. *Connect at least one display with native DisplayPort input capable of supporting the DisplayPort version 1.2 or higher standard to the TOE display output.*
19. *Power up the TOE and select computer #1.*
20. *Verify that the video image is visible and stable on the user display.*
21. *Power off the TOE.*

In the following steps the evaluator shall verify that the test setup excluding the TOE is capable of supporting the DisplayPort version 1.2 or higher protocol.

22. *Disconnect the DisplayPort video cable connecting the display and the TOE and insert a DisplayPort AUX channel analyzer in series. Bypass the TOE and connect the video cable directly to the computer.*
23. *Change the computer display resolution beyond high definition (HD) (i.e., 1920x1200). Verify that the image is still shown on the display.*
24. *Verify in the AUX channel analyzer that the AUX channel has switched to version 1.2 or higher.*

In the following steps the evaluator shall verify that the test setup including the TOE blocks DisplayPort version 1.2 or higher protocol (675/720 Mbps Fast AUX channel speed).

25. *Disconnect the video cable from the computer video output and connect it to the TOE video output. Reconnect the TOE video input on computer #1 to the video output on computer #1, using a second DisplayPort AUX channel analyzer. If a second AUX channel analyzer is not available, steps 25 to 27 must be repeated with the single AUX channel analyzer between the TOE and the display and between the TOE and computer #1. For simplicity, two AUX channel analyzers are recommended.*
26. *Turn on the TOE and check that there is a stable image shown on the user display.*
27. *Check the AUX channel analyzer(s) to verify that the link is forced to version 1.1 only. If confirmed, then the test is successfully completed (no further testing required – continue to step 33 below). If version 1.2 or higher is detected, then continue with test steps 28 to 38.*

In the following steps the evaluator shall verify that a TOE capable of transferring DisplayPort version 1.2 and higher protocol properly blocks unauthorized transactions.

28. *Replace computer #1 with a DisplayPort source device capable of generating version 1.2 or higher traffic.*
29. *Connect the AUX channel analyzer between the TOE and the display. If a second AUX channel analyzer was used in step 25, disconnect the video input to the TOE and connect it to the AUX analyzer input. Connect the AUX analyzer output to the TOE video input.*
30. *Program the DisplayPort source device to simulate multiple display interactions. As a minimum, the evaluator shall simulate: HDMI Ethernet Audio Control (HEAC), Ethernet and USB.*
31. *Verify at the AUX channel analyzer that all transactions except for link negotiation, link training and EDID reading are blocked by the TOE. (These are the minimal set of DisplayPort transaction types required to establish video display link. All other transaction types must be blocked by the TOE). Note that detailed information regarding these transactions can be found in VESA DisplayPort standard version 1.3 or higher.*
32. *Repeat Steps 28 to 31 for each TOE computer video interface.*

The AUX channel between the PC and the monitor is completely disconnected in all TOEs that support DisplayPort video. Instead of DisplayPort AUX being passed through the switch, the TOE uses an simulated AUX to emulate a monitor on the connected computer. Therefore, the tests for AUX data filtering through the switch are not applicable but rather it was necessary to confirm the TOE simulates AUX data.

To verify that the TOE was using simulated AUX data to emulate a monitor on the connected computer the evaluator first connected the computer directly to a Samsung monitor with a DisplayPort cable. The DisplayPort cable was cut and a dip switch was connected between the AUX+ and AUX- pins (pins 15 and 17). In a normal DisplayPort video transmission, a successful AUX connection will exist if the switches on both pins are closed. This should result in a successful sending of EDID information and resolution settings from the monitor to the computer. The evaluator viewed that with the switches closed the computer received the correct EDID and that the resolution could be set.

The next step was to open the switches connected to the AUX pins, thus breaking the AUX connection from the monitor to the computer. In a normal DisplayPort video transmission, the breaking of the AUX channel communication should result in the loss of EDID information and resolution settings. When

opening the switches connected to the AUX pins the evaluator viewed that no EDID was collected by the connected computer.

The evaluator connected the display and computer through the TOE and powered on the TOE. With the switches to the AUX pins closed, the evaluator viewed that the computer received an emulated monitor EDID of an HP monitor and that the resolution was forced to 1920x1080. The final step was to open the switches connected to the AUX pins while the display monitor and computer were connected through the TOE. As stated previously in a normal DisplayPort video transmission, no EDID would be collected by the connected computer and an error would occur when trying to resolve a resolution. However, by maintaining emulated AUX+/AUX- channels on all ports during KVM operation, the physical AUX channels are not required to display video. Therefore the evaluator viewed that the computer still received an emulated monitor EDID of an HP monitor and that the resolution was forced to 1920x1080. This successfully demonstrates that the TOE provides simulated AUX data.

The evaluator also the HDMI probed pins 13 and 14 on the B002-HD2AC4 to test DisplayPort to HDMI instance as defined in TD0086. The evaluator found no signal on either of the pins.

The overall result of Test 4.4 Part 2 is a pass.

Part 3 - Video and EDID Channel Unidirectional Rule

In the following steps the evaluator shall validate that the TOE video path is unidirectional from the computer 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 shall also verify that the TOE does not pass MCCS transactions to the connected display.

SFRs mapped to the following test steps:

- *Unidir flow: FDP_IFF.1.5(2) Rule 12*
- *EDID once: FDP_IFF.1.5(2) Rule 11*
- *Unpowered isolation: FDP_IFF.1.5(2) Rule 14*

33. *Run a MCCS control console on computer #1 (see more information in Annex I of this PP). Bypass the TOE and attempt to control the display brightness to confirm that the setup is operating properly.*
34. *Reconnect the TOE between the computer and the display.*
35. *Turn on the TOE and verify that a stable image is shown on the user display.*
36. *Attempt to control the display brightness from computer #1. This control attempt should fail. Failure of the control indicates that the TOE has effectively filtered the MCCS commands issued by the computer.*
37. *Switch to the other computers and repeat Step 36 for each TOE video interface.*
38. *Repeat Steps 36 to 37 with the TOE powered off and verify that the MCCS control attempt fails.*
39. *Select computer #1 and verify that the display shows video from computer #1 as expected.*
40. *Turn off the TOE. Disconnect the user display from the TOE.*
41. *Turn on the TOE. After the TOE has completed the self-test, reconnect the user display 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).*
42. *Turn off the TOE. Connect the display directly to the video output of computer #1.*

43. *On computer #1, run the MCCS software and attempt to control the display brightness. The display brightness should be changed. [This is a control test to validate that the setup properly handles MCCS].*
44. *Disconnect the display from the computer and reconnect to the TOE. Reconnect the video output of computer #1 to the TOE.*
45. *Turn on the TOE.*
46. *Select computer #1.*
47. *Attempt to change the display brightness again using the MCCS software on computer #1. This time the display brightness must stay fixed (i.e., the MCCS commands are blocked by the TOE).*
48. *Power off the TOE.*
49. *Repeat Steps 9 to 12 for all other TOE computer video interfaces.*
50. *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. Power up the TOE again.*
51. *Check that the video is not visible in the display.*
52. *Remove the display cable from the TOE and connect the oscilloscope to verify that no SYNC signal is passed through the TOE:*
    - *a. VGA – single ended probe on pins 13 and 14;*
    - *b. HDMI – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide HOT PLUG DETECT signal; Check for signals - differential probe between pins 10 (+) and 12 (-);*
    - *c. DVI-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HOT PLUG DETECT signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-);*
    - *d. DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HOT PLUG DETECT signal; Check for signals - Differential probe between pins 23 (+) and 24 (-);*
    - *e. DisplayPort - connect pin 18 to a 3.3V power supply via a 100 Ohm resistor to provide HOT PLUG DETECT signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+).*
53. *Repeat steps 50 to 52 with the display and oscilloscope connected to each of the TOE computer interfaces with that computer channel selected on the TOE.*
54. *Repeat steps 50 to 53 with the TOE powered off (no channel selected).*

The first device tested was the B002-DV1AC8. The evaluator began by connecting computer 1 directly to its display. The evaluator opened up an instance of MCCS and verified that the brightness of the display could be modified as a test control. The evaluator then connected the computer and display to the TOE. The evaluator verified that the brightness of the display could not be modified when connected through the TOE. The evaluator turned off the TOE and verified that the brightness could not be changed through MCCS. The TOE had no functionality and nothing was displayed on the monitor.

The evaluator unplugged the display from the TOE. The evaluator powered on the TOE and waited for the self-test to pass. Upon power up the evaluator plugged a new display into the TOE. The evaluator viewed that the computer did not learn the new EDID as the TOE provided a generic EDID. The evaluator powered off the TOE and swapped the display and the computer 1 video cable, reversing the direction of

the video. The evaluator powered the TOE back on and viewed that nothing was display on the monitor. The evaluator replaced the display with an open DVI cable measured with the oscilloscope. The evaluator probed pin 23 and 24 of the open cable and viewed no difference in signal. The TOE was powered off and the same pins were probed. The evaluator again viewed no difference in signal.

The evaluator also tested the B002-DP2AC4 and the B002-HD2AC4 for the EDID with DisplayPort and HDMI. All tests resulted in similar results.

The overall result of Test 4.4 Part 3 is a pass.

Part 4 – Authorized Video Interfaces

In the following steps the evaluator shall validate that the TOE video interfaces support only authorized video protocols.

SFRs mapped to the following test steps:

- *Authorized interfaces: FDP_IFF.1.5(2) Rule 13*

55. *Review TOE specification and check that the only video interfaces natively supported are one or more of the following: VGA, DVI, HDMI, and DisplayPort. Note that other protocols may be supported only through the use of special cables, adaptors, docking stations and dongles.*
56. *Check the TOE external interfaces to verify that the only video interfaces natively supported are one or more of the following: VGA, DVI, HDMI, and DisplayPort.*

The evaluator viewed that all devices tested only support the allowed video interfaces as defined in the Security Target. The verification was performed in conjunction with Test 4.7.

The overall result of Test 4.4 Part 4 is a pass.

4.2.14. Test 4.5 –User Authentication Device Switching and Isolation Rules

[Conditional] *The following test shall be performed only on a TOE that supports a user authentication device.*

Test Setup

The evaluator shall:

1. *Configure the TOE and the operational environment in accordance with the operational guidance.*
2. *Run USB protocol analyzer software on all connected computers to enable the capture of data on the TOE user authentication device USB interface.*
3. *Install the user authentication application and driver for the qualified user authentication device being used for testing (for example for the smart card reader and card).*
4. *Connect a qualified user authentication device to the TOE. Note that the user authentication device shall have a power LED or a DVM connected to its USB power lines (USB contacts #1 and #4).*
5. *Each connected computer must have its own directly connected display (although the display may be moved during testing to accomplish this). Open a real-time hardware information console window on each computer.*

Part 1 - Non- Emulated User Authentication Device Function switching and isolation

[Selection] *The following test shall be performed only on TOE devices with user authentication functionality that is not emulated. For TOE devices with emulated user authentication device functionality, skip to step 16 below.*

The following steps evaluate the TOE compliance with the allowed data flow as it is applied to the non-emulated user authentication device data. In the following test steps, the approved user authentication device is switched to one selected computer, and the evaluator verifies that all other computers are unable to see any USB traffic. The evaluator shall also turn the TOE power off and verify that the connected user authentication device is inaccessible.

SFRs mapped to the following test steps:

- *Switching rules: FDP_IFF.1.2(1) Rule 2*
- *Positive switching (allow data flow) – not emulated : FDP_IFF.1.3(1) Rule 1*
- *Negative switching: FDP_IFF.1.5(1) Rule 1*
- *Multiple instances: FDP_IFF.1.2(1) Rule 4*
- *Powered off isolation: FDP_IFF.1.5(2) Rule 2*

6. *Turn on the TOE.*
7. *Switch the TOE (or the TOE user authentication device, if different) to computer #1. Verify that the user authentication device power LED is illuminated / that the DVM reads 5 VDC. Note: If the DVM or power LED is not fast enough to detect the power dip –an oscilloscope may be used for this test instead.*
8. *Verify that the real-time hardware information console on computer #1 indicates the presence of the user authentication device.*
9. *View the display on each of the other computers to verify that the real-time hardware information consoles on these computers do not show the user authentication device.*
10. *Verify that the USB protocol analyzer software running at all non-selected computers does not detect any USB transaction from the TOE (i.e. the link is off or only NAK transactions are detected).*
11. *Disconnect and reconnect the selected computer TOE interface cables and attempt to detect USB traffic on any non-selected computer USB protocol analyzer (i.e. the link is off or only NAK transactions are detected).*
12. *Switch the TOE to computer #2 while observing the authentication device power LED / DVM. Power to the authentication device must be interrupted momentarily immediately after the channel is switched.*
13. *Repeat Steps 7 to 12 with the authentication device connected to each one of the remaining computers.*
14. *Switch to the computer with the connected authentication device. Turn the TOE off by removing power. Verify that the user authentication device is no longer visible on any of the connected computers.*
15. *Check that no USB transactions may be detected on the USB protocol analyzer for each connected computer.*

The evaluator began by configuring the environment in a manner appropriate for the test. An USB type B cable was run from each of the computers to the corresponding CAC device output interface found on the

TOE. The evaluator attached an open USB port to the CAC input and verified it measured 5 VDC. Next an authentication device was plugged into the TOE's CAC device input interface.

After the initial configuration the evaluator powered on the TOE and verified that the authentication device's power LED was illuminated. The evaluator switched to computer 1 and viewed the authentication device successfully in computer 1's device manager. The authentication device was not viewed in the device managers of the unselected computers. The evaluator also verified via USB packet captures that no USB data from the authentication device was transmitted to the unselected computers. The evaluator repeated the USB capture process while unplugging computer 1's USB cables from the TOE. The resulting captures showed no USB data was transmitted to the unselected computers.

The next step was to verify that power to the authentication device was cut briefly when switching computer channels on the TOE. The evaluator viewed the CAC power indicator light on the TOE and the power LED of the authentication device turned off briefly after switching to computer 2. Finally the evaluator powered off the TOE completely and viewed that the authentication device was not registered in the device manager of any of the computers. USB packet captures run on all of the computers showed no data being transmitted.

The overall result of Test 4.5 Part 1 is a pass.

Part 2 - Emulated User Authentication Device

[Selection] *The following test shall be performed only on a TOE with user authentication functionality that is emulated.*

In the following steps the evaluator shall verify that user authentication on one selected channel does not generate USB transactions on the non-selected connected computers. Also, the evaluator shall establish authentication sessions simultaneously with all connected computers and then terminate the session in one selected computer to verify that all other sessions terminate immediately.

Lastly, the evaluator shall establish an authentication session simultaneously with all connected computers and then power off the TOE to assure that all sessions are terminated immediately.

SFRs mapped to the following test steps:

- *Switching rules: FDP_IFF.1.2(1) Rule 2*
- *Positive switching (allow data flow) – emulated : FDP_IFF.1.3(1) Rule 2*
- *Negative switching: FDP_IFF.1.5(1) Rule 1*
- *Multiple instances: FDP_IFF.1.2(1) Rule 4*
- *Session termination: FTA_ATH_EXT.2*

16. *Configure the TOE and the operational environment in accordance with the operational guidance.*
17. *Connect a qualified user authentication device to the TOE / use internal (built-in) authentication device.*
18. *Each connected computer must have its own directly connected display. Open a real-time hardware information console window on each computer.*
19. *Run USB protocol analyzer software on each connected computer to enable the capturing of the TOE user authentication device USB interface.*
20. *Turn on the TOE. Switch the TOE (or the TOE user authentication device, if different) to computer #1. Authenticate using computer #1. At the same time, check that the connected*

computer USB protocol analyzers, except for selected computer, do not show transactions other than USB keep-alive traffic (NAK transactions).

21. *Switch the TOE (or the TOE user authentication device, if different) to computer #2.*
22. *Authenticate using computer #2. At the same time check that the connected computer USB protocol analyzers, except for selected computer, do not show transactions other than USB keep-alive traffic (NAK transactions).*
23. *Switch the TOE (or the TOE user authentication device, if different) to computer #3.*
24. *Authenticate using computer #3. At the same time check that the connected computer USB protocol analyzers except for selected computer do not show any transactions other than USB keep-alive traffic (NAK transactions).*
25. *Switch the TOE (or the TOE user authentication device, if different) to computer #4.*
26. *Authenticate using #4. At the same time check that the connected computer USB protocol analyzers except for selected computer do not show any transactions other than USB keep-alive traffic (NAK transactions).*
27. *Verify that all connected computers are logged-on (user authenticated).*
28. *Terminate the authentication session (for example – pull out the token or smart-card).*
29. *Verify that all session at each connected computer terminates immediately.*
30. *Repeat Steps 20 to 26 (skip steps 28 and 29) then power off the TOE.*
31. *Verify that the session at each connected computer terminates immediately.*

The user authentication functionality of the TOE is not emulated. Therefore this test is not applicable.

Part 3 - User Authentication Data Isolation Rule

[Conditional] *The following test steps shall be performed only on a TOE that does not have a built-in user authentication device. This test is not applicable to a TOE with built-in user authentication functionality (parts 3 and 4 are not applicable).*

In the following steps, the evaluator shall verify that the process of user authentication for one selected computer does not generate USB traffic on the other USB interfaces of the same computer. Additionally, the evaluator shall check that the same isolation is maintained when the TOE is powered off.

SFRs mapped to the following test steps:

- *Interface isolation: FDP_IFF.1.5(2) Rule 5*
- *Interface not shared: FDP_IFF.1.5(2) Rule 6*
- *Powered off isolation: FDP_IFF.1.5(2) Rule 14*

32. *Disconnect the user authentication device.*
33. *Verify that the TOE computer interfaces used for the user authentication device are different from the TOE computer interfaces used for keyboard and mouse (i.e., the interfaces shall be isolated, but may use a common ground).*
34. *Connect a USB protocol analyzer device (sniffer) between the keyboard and mouse computer interface for computer #1 on the TOE and the USB port on computer #1.*
35. *Run USB protocol analyzer software on each of the remaining computers. The USB protocol analyzer shall monitor the USB port connected to the TOE keyboard and mouse interface and the USB port connected to the TOE user authentication device port.*
36. *Connect and use a qualified USB user authentication device to authenticate to computer #1.*
37. *Verify that during this connection, enumeration and authentication processes show no USB*

traffic other than keep-alive traffic (NAK transactions). Verify that, upon completion of the authentication, the USB sniffer and the USB protocol analyzer software instances show no USB traffic other than keep-alive traffic (NAK transactions) on all other USB interfaces.

38. *Repeat steps 34 to 37 for each TOE computer interface.*
39. *Repeat steps 34 to 38 with the TOE powered off.*

The evaluator began by configuring the environment in a manner appropriate for the test. An USB analyzer device was used to sniff between the computer 1 keyboard and mouse interface on the TOE and a USB port on computer 1. An USB type B cable was run from each of the other computers to the corresponding keyboard/mouse and CAC device output interface found on the TOE. An authentication device was plugged into the TOE's CAC device input interface.

The evaluator ran USB packet capture software on an unselected computer along with the USB analyzer device. The evaluator attempted to authenticate with a smart card and viewed that no data was sent through the keyboard and mouse ports. The evaluator then powered off the TOE and repeated the authentication attempt and once again saw no data transferred through the keyboard/mouse ports.

The overall result of Test 4.5 Part 3 is a pass.

Part 4 - User Authentication Device Qualification - FDF

[Conditional] *The following test steps shall be performed only on a TOE that supports Fixed Device Filtration (FDF) functionality and does not have a built-in user authentication device. For all other TOE devices, skip to step 42 below.*

In the following steps the evaluator shall verify that the TOE properly handles qualified and non-qualified devices connected to the user authentication device port.

SFRs mapped to the following test steps:

- *Authorized device: FDP_IFF.1.5(2) Rule 13*

40. *Power up the TOE.*
41. *Connect the following unauthorized devices to the TOE user authentication device interface via a USB protocol analyzer device (sniffer) to verify that the devices are rejected:*

    a. USB audio device;

    b. USB storage device;

    c. USB camera;

    d. USB keyboard;

    e. USB printer; and

    f. USB Composite Device evaluation board with HID keyboard, Communication Device Class (CDC), and Mass Storage Class (MSC) devices. CDC and MSC shall be rejected.

Device Rejection shall be verified through:

I. TOE user indication in accordance with the user guidance; and

II. An immediate cessation of captured USB traffic following device enumeration.

The evaluator began by configuring the environment in a manner appropriate for the test. An USB type B cable was run from each of the computers to the corresponding CAC device output interface found on the TOE. The TOE by default accepts any CAC device and denies any non CAC device.

The evaluator viewed the device manager and USB protocol analyzer on the selected computer on the TOE for each device listed below. The device manager demonstrated that the device was not accepted by the TOE and the USB protocol analyzer showed no USB traffic to the computer.

a. USB audio device;

b. USB storage device;

c. USB camera;

d. USB keyboard;

e. USB printer; and

f. USB Composite Device evaluation board with HID keyboard, Communication Device Class (CDC), and Mass Storage Class (MSC) devices. CDC and MSC shall be rejected.

The overall result of Test 4.5 Part 4 is a pass. Evidence for this test can be found in Section 7.5.4 of the Test Report.

Part 5 - User Authentication Device Qualification - CDF

[Conditional] *The following test steps shall be performed only on a TOE that supports Configurable Device Filtration (CDF) function, and does not include a built-in user authentication.*

In the following steps the evaluator shall verify that the TOE properly handles qualified and non-qualified devices connected to the user authentication device port after proper configuration.

SFRs mapped to the following test steps:

- *Authorized device: FDP_IFF.1.5(2) Rule 13*
- [TD0251] *CDF management: FMT_SMF.1.1 a and FMT_SMF.1.1 b*
- *Restrict to admin: FMT_MOF.1.1*
- *Admin authentication: FIA_UAU.2*
- *Auditable log: FIA_UID.2.1*

42. Power up the TOE.

43. Following the administrative guidance, configure the TOE CDF to accept (white-list) or reject (black-list) USB authentication devices only. Verify that the CDF definitions are only available for logged-on and authenticated administrators.

44. Connect the following devices to the TOE user authentication device interface via a USB protocol analyzer device (sniffer) to verify that the devices are rejected or accepted based on the TOE configuration:

a. USB user authentication device;

b. USB audio device;

c. USB storage device;

d. USB camera;

e. USB keyboard; and

f. USB printer.

Device Rejection shall be verified through:

I. TOE user indication per user guidance; and

II. An immediate cessation of captured USB traffic following device enumeration.

45. Repeat steps 43 to 44 with the USB audio device white-listed.
46. Repeat steps 43 to 44 with the USB storage device white-listed.
47. Repeat steps 43 to 44 with the USB camera device white-listed.

48. Repeat steps 43 to 44 with the USB keyboard device white-listed.
49. Repeat steps 43 to 44 with the USB keyboard device white-listed and the USB camera black-listed.
50. Repeat steps 43 to 44 with the USB printer device white-listed and the USB storage device black-listed.
51. If the TOE CDF supports filtering criteria other than USB device class (for example: sub-class, protocol, vendor ID, device ID) then repeat steps 43 to 44 using at least 4 other criteria. 65
52. Download or otherwise access the TOE administrative log and verify that the processes performed in steps 42 to 51 are properly recorded.

The evaluator began by configuring the environment in a manner appropriate for the test. An USB type B cable was run from each of the computers to the corresponding CAC device output interface found on the TOE. The evaluator connected a smart card reader to the TOE's CAC device input interface. The evaluator authenticated to the TOE through the provided Administration software and selected the register CAC device option from the menu, thus registering the specific smart card reader connected to the TOE. Only one device can be registered at a time.

The evaluator viewed the device manager on the selected computer on the TOE. The device manager demonstrated that the device was accepted by the TOE. The authentication device was replaced with each of the following devices and the device manager demonstrated that the TOE rejected the devices:

a. USB user authentication device;

b. USB audio device;

c. USB storage device;

d. USB camera;

e. USB keyboard; and

f. USB printer.

The log was checked via the administration program after and it was verified that the registration of CAC devices were properly recorded. The same steps were performed to test the registering of the following non-authentication devices:

- USB audio device
- USB storage device

- USB camera
- USB keyboard.

The TOE only allows the registering of one device so by whitelisting one type of device, all others are automatically blacklisted, so no specific blacklist testing is applicable. There is also no means to register a device by sub class.

The overall result of Test 4.5 Part 5 is a pass.

4.2.15. Test 4.6 – Analog Audio Output Switching, Isolation and data-flow Rule

[Conditional] *This test is not required if the device does not support analog audio switching.*

The following steps evaluate TOE compliance with the allowed data flow as it is applied to the analog audio output.

Test Setup

The evaluator shall:

1. *Configure the TOE and the operational environment in accordance with the operational guidance.*
2. *Run media player with different audio files on each of the connected computers.*

Part 1 - Positive and Negative Analog Audio Output Switching Rule

In the following steps the evaluator shall confirm that an analog audio signal traversing the TOE from one user-selected connected computer does not leak to the non-selected computers' analog audio interfaces. Similarly, the evaluator shall verify that there is no significant leakage across the non-selected computers.

SFRs mapped to the following test steps:

- *Switching rules: FDP_IFF.1.2(1) Rule 2*
- *Positive switching (allow data flow): FDP_IFF.1.2(1) Rule 1d*
- *Negative switching: FDP_IFF.1.5(1) Rule 1*
- *Multiple instances: FDP_IFF.1.2(1) Rule 4*

3. *Connect amplified speakers to the TOE audio peripheral interface. Set the speakers to approximately 25% volume.*
4. *Turn on the TOE.*
5. *On each of the connected computers, play a video movie with a distinctive sound track. A different movie must be used for each connected computer.*
6. *Switch the TOE (or TOE audio) to computer #1.*
7. *Listen to the amplified speakers to verify that the movie on computer #1 is the one being played.*
8. *Repeat Steps 6 to 7 for each connected computer.*
9. *Turn the TOE off by disconnecting the power. Verify that no audio is heard.*
10. *Set the speaker volume output on computer #1 to approximately 25% volume level.*
11. *Connect the amplified speakers to the TOE audio output interface.*
12. *Run a tone generator program on computer #1. The generator shall be set to the maximum*

sound level (i.e., volume).

13. *Turn on the TOE.*
14. *Select computer #1.*
15. *Test the sound controls on computer #1. The following steps may be followed for Windows. Similar steps may be used for Linux based computers:*
    a. *Open the Windows Control Panel*
    b. *Select Sound, then the Sounds tab*
    c. *Select the system sound "Asterisk" and press Test. The Asterisk sound should be heard through the speakers [Allowed Data Flow].*
16. *Generate an audio tone of 100 hertz (Sine wave) on computer #1. A loud sound should be heard.*
17. *Connect the amplified speakers plug to the TOE computer interface #2 audio input jack and set the amplified speakers to full volume (100%).*
18. *Test the sound (e.g., press the Asterisk sound test button) on computer #1 again several times and verify that no sound can be heard through the speakers.*
19. *Use the sound generator software on computer #1 to generate test tones of 250 and 500 hertz and 1, 2, 4, 8, 10, 12, 14, and 15 kilohertz for a few seconds at each frequency step. Verify that no sound can be heard through the amplified speakers.*
20. *Repeat Steps 17 to 19 for all other TOE non-selected computer interface audio input ports.*
21. *Replace the amplified speakers with an oscilloscope and set to measure the peak-to-peak voltage.*
22. *Replace computer #1 with an external audio signal generator and set to pure sine wave around the average voltage of half output (positive signal only). Set the output signal to 2.00V peak-to-peak. (The oscilloscope may be used to calibrate the signal.)*
23. *Set the signal generator to generate 1Hz, 1KHz, 4KHz, 8KHz, 12KHz, 20KHz, 30KHz, 40KHz and 60KHz and use the oscilloscope to detect the leaked signal. The detected signal shall be 63.2mV (or well below noise level). This level of signal assures signal attenuation of 30 dBv in the extended audio frequency range.*
24. *Repeat step 23 with the audio generator set to signal average to 0V (negative swing). The detected signal shall be 63.2mV (or well below noise level). This level of signal assures signal attenuation of 30 dBv in the extended audio frequency range.*
25. *Repeat step 23 with the output signal set to 200mV peak-to-peak. The detected signal shall be 6.3mV (or well below noise level). This level of signal assures signal attenuation of 30 dBv in the extended audio frequency range.*
26. *Disconnect the power to the TOE and repeat Steps 15 to 25. The results shall be the same as for the powered on TOE.*
27. *Power up the TOE again. Select computer #1.*
28. *To test for audio leakages between two non-selected audio interfaces, plug the computer #1 audio output cable plug into the TOE computer interface #2 audio input jack. Connect the amplified speakers to each of the other TOE audio input jacks. Test the sound (e.g., press the Asterisk sound test button) again several times and verify that no sound can be heard at the amplified speakers.*
29. *Repeat Step 28 for each one of the remaining non-selected computer interfaces.*

The evaluator began by configuring the testing environment so that speakers set to about 25% volume were connected to the TOE's audio input. An audio cable was connected from each computer audio

interface on the TOE to the corresponding computer. The evaluator made sure each connected computer had a distinct video with audio that could be played. To test the audio switching of the TOE the evaluator played the videos on the connected computers and switched through the channels, verifying that the audio heard from the speakers was coming from the video of the selected computer. The evaluator powered off the TOE and verified that no more audio was heard coming from the speakers.

The next step was to test that no audio leakage occurred to an unselected interface. The evaluator switched to computer 1 and opened up tone generator software to produce a 100 Hz signal. The sound was heard, demonstrating that the tone generator software was working. The evaluator then unplugged the speakers from the TOE output and plugged them into the computer 2 audio input interface. The evaluator attempted to produce tones on computer 1 ranging from 250 Hz to 15 kHz and heard no sound coming from the speakers as expected. The speakers were then replaced with an oscilloscope to measure audio leakage. The computer 1 audio cable was replaced with a signal generator set to generate a pure sine wave of 2V peak to peak. The evaluator produced a series of audio frequencies ranging from 1 Hz to 60 kHz and verified via the oscilloscope that the audio leakage was less than noise level.

The process of verifying that audio leakage was less than noise level was repeated with a 2V signal with a 0V peak and with a signal of 200mV peak to peak. The audio leakage captured by the oscilloscope was less than noise level for all frequencies produced. All of the signals were then tested again with the TOE powered off and no audio leakage was measured by the oscilloscope.

The final step was to test for audio leakage between unselected channels on the TOE. The evaluator plugged the audio cable coming from computer 1 into computer 2's audio input interface on the TOE. The speakers were plugged into the computer 3 audio input interface. The evaluator switched to computer 1 and played a video with audio. No audio was heard coming from the speakers as expected.

The overall result of Test 4.6 Part 1 is a pass.

Part 2 - Analog Audio Data Flow Rules

In the following steps the evaluator shall verify that the TOE analog audio functions:

a. Are unidirectional (computer interface to peripheral device data flow only);

b. Will reject a microphone if connected to the audio peripheral interface port; and

c. Will attenuate the audio signal from a connected headset to a level that would not enable audio eavesdropping.

Note: For additional information on the required test equipment refer to Annex I of this document.

SFRs mapped to the following test steps:

- *Unidir audio: FDP_IFF.1.5(2) Rule 9*
- *Mic rejection: FDP_IFF.1.5(2) Rule 8*
- *Enable authorized: FDP_IFF.1.5(2) Rule 13*
- *Power off isolation: FDP_IFF.1.5(2) Rule 14*

30. *Connect the amplified speakers to the analog audio output jack on computer #1. (The audio output jack is typically lime green in color.) Set the volume at the speakers to approximately 25%.*
31. *Connect the TOE interface cable audio plug on computer #1 (i.e., the computer side) to the computer microphone input jack (typically pink in color) instead of the audio output jack.*
32. *Connect an open 3.5 millimeter stereo plug or jumper cable to the TOE audio peripheral*

interface jack (see details in Annex I).

33. *Power up the TOE and select computer #1.*
34. *Measure the DC voltage between the ground terminal and each one of the other two terminals (tip and ring) using a digital voltmeter.*
35. *Verify the voltage is lower than 0.2 volts, assuring that there is no direct current (DC) bias voltage supplied to a microphone.*
36. *Connect a standard analog PC microphone instead of the open plug to the TOE audio peripheral interface jack.*
37. *Open the Audio Sound Recorder application on computer #1 and start recording. Speak loudly into the microphone at approximately 1" [25 millimeter] distance.*
38. *Play the recorded audio track and verify that the sound cannot be heard (i.e., cannot be recognized over background noise). Attempt to hear the right side and left side separately.*
39. *Connect dynamic headphones (32 ohm typical impedance) instead of the microphone to the TOE audio peripheral interface jack.*
40. *Repeat Steps 37 to 39 using the standard headphones as a low-gain microphone.*
41. *Run an audio tone generator program on computer #1 (i.e., sine wave at maximum volume level).*
42. *Connect the audio output jack computer #1 to the TOE audio peripheral interface jack. This will inject a strong audio signal from computer #1 to the TOE output.*
43. *Connect the amplified speaker's audio input plug to the TOE audio interface jack on computer #1 and check that the amplified speaker's volume is set to approximately 25%.*
44. *Generate test tones of 250 and 500 hertz and 1, 2, 4, 8, 10, 12, 14, and 15 kilohertz for a few seconds at each frequency step.*
45. *Verify that the test sound cannot be heard through the amplified speakers.*
46. *Replace the amplified speakers with an oscilloscope and set to measure peak-to-peak voltage.*
47. *Replace computer #1 with an external audio signal generator and set to pure sine wave around average voltage 0V (negative swing). Set output signal to 2.00V peak to peak (oscilloscope may be used to calibrate the signal).*
48. *Set the signal generator to generate 1Hz, 1KHz, 4KHz, 8KHz, 12KHz, 20KHz, 30KHz, 40KHz and 50KHz and use the oscilloscope to detect the leaked signal. The detected signal shall be 11.2mV (or well below noise level). This level of signal assures signal attenuation of 45 dBv in the extended audio frequency range.*
49. *Turn the TOE off and repeat Steps 41 to 48.*

The evaluator began by configuring the environment for the test. The speakers were plugged directly into computer 1's audio output port. An audio cable was run from computer 1's microphone input port to the corresponding computer 1 audio input port on the TOE. An open audio cable was connected to the TOE's audio output port. The evaluator used a multimeter to measure the DC voltage of the open cable between the ground and the other terminals (tip and ring). The evaluator verified that the measure was less than 0.2V.

The open cable was replaced by a microphone and the evaluator used recording software to attempt to record audio on computer 1. Playback of the recording verified that no audio was actually recorded. The microphone was then replaced by a headset which was again used to attempt to record audio. The evaluator again verified that no audio was actually recorded.

To test against reverse audio the evaluator plugged a cable from computer 1's audio output to the TOE's audio output. The speakers were plugged into the TOE's computer 1 audio input interface. Audio generator software was used on computer 1 to generate sounds of different frequencies ranging from 250 Hz to 15 kHz. No audio was heard from the connected speakers as expected. The amplified speakers were then replaced by an oscilloscope to measure the reverse audio. An external audio generator was connected to the TOE's audio output port and a 2V peak to peak signal was generated. The evaluator created a series of frequencies between 1 Hz and 50 kHz and measured that the signal captured by the oscilloscope was below noise level. The evaluator then powered off the TOE and performed all reverse audio tests again and heard no audio or saw no signal captured by the oscilloscope.

The overall result of Test 4.6 Part 2 is a pass.

4.2.16. Test 4.7 – No Other External Interfaces

In the following test, the evaluator shall examine the TOE external interfaces to assure that only the interfaces (connectors) allowed by this PP are available.

SFRs mapped to the following test steps:

- *No other external devices: FDP_IFF.1.5(1) Rules 2, 3*

The evaluator shall:

1. *Check the TOE and its supplied cables, and accessories to assure that there are no external wired interfaces other than:*
    a. *Computer interfaces;*
    b. *Peripheral device interfaces; and*
    c. *Power interfaces.*
2. *Check TSS to verify that the TOE does not support wireless interfaces. Check for radiated emissions data and Radio Frequency certification information.*

The evaluator verified that no external interface existed on each of the tested devices other than the computer interfaces, peripheral device interfaces, and the power interface. The TOE does not support wireless interfaces. The overall result of Test 4.7 is a pass.

4.2.17. Test 4.8 – No Flow between Computer Interfaces (USB-to-USB, Power-to-USB)

In this test, the evaluator shall confirm that the following types of events in one TOE computer interface do not have any effect on any other TOE computer interface:

- *Computer reboot or power off;*
- *Normal USB traffic flowing to the selected computer;*
- *Enumeration of various USB devices on non-selected computer interfaces;*
- *Peripheral device over-current event effect on non-selected computers; and*
- *USB power signaling effect between computer interfaces.*

SFRs mapped to the following test steps:

- *User authentication isolation: FDP_IFF.1.5(1) Rule 1*

- *General isolation: FDP_IFF.1.5(2) Rule 1*
- *User authentication isolation: FDP_IFF.1.5(2) Rule 5*

The evaluator shall:

1. *Configure the TOE and the operational environment in accordance with the operational guidance.*
2. *Connect a USB protocol analyzer device (sniffer) between the TOE USB computer interface #2 and computer #2 (i.e., the first non-selected computer).*
3. *Run USB protocol analyzer software on all remaining computers.*
4. *Turn on the TOE and observe the TOE enumeration data flow on all USB protocol analyzers.*
5. *Ensure the TOE is switched to computer #1.*
6. *Reboot computer #1. Check for any new USB traffic on all non-connected computer USB analyzers. No packets should be captured other than USB keep-alive traffic (NAK transactions).*
7. *Generate a high level of USB HID traffic by moving the mouse at high speed and holding down the keyboard space key at the same time. Check for any new USB traffic on all non-connected computer USB analyzers. No packets should be captured other than USB keep-alive traffic (NAK transactions).*
8. *Connect and disconnect the following additional USB devices to the keyboard, mouse and user authentication device ports (if applicable): USB keyboard, USB mouse, USB storage device, USB Audio device and USB user authentication device. Check for any new USB traffic on all non-connected computer USB analyzers. No packets should be captured other than USB keep-alive traffic (NAK transactions).*
9. *Plug a USB overload plug (USB Type-A plug with a 2.5 ohm / 10 watt resistor connected between position 1 and 4) into the keyboard, mouse and user authentication device ports. The evaluator shall check for any new USB traffic on all non-connected computer USB analyzers. No packets should be captured other than USB keep-alive traffic (NAK transactions). Remove the plug after the test is completed.*
10. *Connect a switchable 5 volt power supply with a USB Type-B plug into the TOE USB keyboard, mouse and user authentication device computer interfaces. 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. Check for any new USB traffic on all non-connected computer USB analyzers. No packets should be captured other than periodic USB keep-alive traffic (NAK transactions).*
11. *Repeat Steps 9 to 10 with each one of the other TOE USB ports.*

The initial required steps for rebooting the computer and checking that no mouse and keyboard data was sent to the unselected computers were already demonstrated in Test 4.2 Part 1 and Test 4.3 Part 1. Verifying no data is sent to the connected computers when an unauthorized device is plugged into the TOE was demonstrated in Test 4.2 Part 1 and Test 4.3 Part 1 for keyboard and mouse ports and Test 4.5 Part 1 for the user authentication port.

The remaining test steps involved the use of an USB overload plug. The evaluator configured the environment so that each of the computers were connected to their corresponding TOE interfaces, for keyboard/ mouse and CAC devices. The evaluator switched to computer 1 and ran USB capture software on the unselected computers. The evaluator plugged an USB overload plug (USB Type-A plug with a 2.5 ohm / 10 watt resistor connected between position 1 and 4) into the keyboard/mouse TOE input interface.

The evaluator then plugged the USB overload plug into the CAC device TOE input interface. The evaluator verified that no USB traffic was captured on the unselected computers during the process. A power supply was then used to send a modulating 5V signal through the USB plug. The powered USB was plugged into the keyboard/mouse input interface of the TOE and then the CAC device input interface of the TOE. The evaluator verified via USB capture that no USB data was sent to the unselected computers.

The overall result of Test 4.8 is a pass.

4.2.18. Test 4.9 – No Flow between Computer Interfaces with TOE Powered Off (USB-to-USB, Power-to-USB)

In this test, the evaluator shall confirm that the following types of events in one computer interface do not have any effect on any other computer interface while the TOE is powered off:

- *Computer reboot or power off; and*
- *USB power signaling effect between computer interfaces.*

It should be noted that although the TOE is powered off, some components of the TOE may still be powered from the connected computers.

SFRs mapped to the following test steps:

- *General isolation: FDP_IFF.1.5(2) Rule 1*
- *Unpowered isolation: FDP_IFF.1.5(2) Rule 14*

The evaluator shall:

1. *Configure the TOE and the operational environment in accordance with the operational guidance.*
2. *Connect a USB protocol analyzer device (sniffer) between the TOE USB computer interface #2 and computer #2 (i.e., the first non-selected computer).*
3. *Run USB protocol analyzer software on each of the remaining computers.*
4. *Turn on the TOE and observe TOE enumeration data flow on all connected computers.*
5. *Disconnect the power source to the TOE.*
6. *Check that the TOE USB computer interfaces are alive by observing the presence of periodic keep-alive traffic (NAK transactions) on all connected computers through the USB protocol analyzer. If the USB interface is alive, continue testing steps 7 and 8 below; if not, no further testing is required.*
7. *Reboot computer #1. Check for any new USB traffic on all non-connected computer USB analyzers. No packets should be captured other than USB keep-alive traffic (NAK transactions).*
8. *The evaluator shall connect a switchable 5 volt power supply with a USB Type-B plug (see Annex I of this PP for details) to the TOE USB keyboard, mouse and user authentication device computer interfaces. The 5 volt supply shall be modulated (i.e., cycle on and off) manually at various speeds from approximately one cycle per five seconds to one cycle per second. Check for any new USB traffic on the USB protocol analyzer connected to each non-selected computer. No packets should be captured other than USB keep-alive traffic (NAK transactions).*

The testing of the keyboard and mouse in Test 4.2 Part 3 and Test 4.3 Part 3 already demonstrates that the keyboard and mouse are emulated by the TOE to the connected computer. If the TOE is powered off the keyboard/mouse can no longer be emulated and there is not an alive USB connection. The testing seen in Test 4.5 Part 3 demonstrates that no USB data from the CAC device port is sent to the computers after the TOE is powered off, including NAK transactions.

4.2.19. Test 4.10 – No Flow between Computer Interfaces (Power-/ USB-to-Audio)

[Conditional] This test is not required if the TOE device does not support analog audio switching.

In this test, the evaluator shall verify that power events at one TOE USB computer interface do not

SFRs mapped to the following test steps:

- *General isolation: FDP_IFF.1.5(2) Rule 1*
- *Unpowered isolation: FDP_IFF.1.5(2) Rule 14*

The evaluator shall:

1. *Configure the TOE and the operational environment in accordance with the operational guidance.*
2. *Set the speaker volume output on computer #1 to maximum (100%).*
3. *Connect amplified speakers to the TOE peripheral interface audio output and set to maximum volume.*
4. *Power up the TOE. Select computer #1.*
5. *Disconnect and reconnect the USB interface cable on computer #2 several times. Verify that no sound (i.e., clicking or digital noise) can be heard through the amplified speakers. [No USB to audio leakage.]*
6. *Connect the amplified speakers audio input plug to the computer #2 audio input computer interface.*
7. *Connect a user authentication device to the TOE (e.g., a smart-card reader). Perform authentication to connected computer #1.*
8. *Verify that no sound can be heard through the amplified speakers.*
9. *Repeat Steps 4 to 8 for all other computer interface combinations.*
10. *Repeat steps 5 to 9 with the TOE powered off.*

The evaluator began by configuring the environment so that all of the computers were connected to their corresponding interface on the TOE for keyboard/mouse and CAC devices. An amplified speaker was connected to the TOE audio output. The evaluator performed several actions, including unplugging/replugging the USB cables from some of the unselected computer interfaces on the TOE, unplugging/replugging the connected keyboard/mouse, and unplugging/plugging a CAC device from the TOE. The evaluator heard no audio coming from the speakers during this process. The evaluator repeated the actions with the TOE off and again heard no audio coming from the speakers.

The overall result of Test 4.10 is a pass.

4.2.20. Test 4.11 – Peripheral to Peripheral Interface Rule

[Conditional] *The evaluator shall run this test for any TOE implementation in which the peripheral device interfaces may be switched independently (i.e., the user authentication is switched separately from mouse and keyboard). This test is not required if separate switching is not supported.*

[Conditional] *This test is only required if the two independently switched peripherals have the same protocol (for example both are USB).*

In this test, the evaluator shall verify that the TOE implementation properly isolates the peripheral device interfaces that are not switched together.

Note that the following test assumes that the USB keyboard and mouse combination and the USB user authentication device are independently switched. The test may be modified to support different combinations of peripheral devices with minor changes.

SFRs mapped to the following test steps:

- *General isolation: FDP_IFF.1.5(2) Rule 1*

The evaluator shall:

1. *Configure the TOE and the operational environment in accordance with the operational guidance.*
2. *Connect one computer (A) with USB protocol analyzer software to channel #1 of the TOE.*
3. *Connect another computer (B) with USB protocol analyzer software to channel #2 of the TOE.*
4. *Connect a qualified USB Authentication device to the TOE.*
5. *Connect a USB keyboard to the TOE through a USB protocol analyzer device (sniffer).*
6. *Power up the TOE. Switch the keyboard and mouse to computer A and the user authentication device to computer B.*
7. *Authenticate to computer B and verify that the USB protocol analyzer running on computer A does not detect any USB transactions other than keep-alive traffic (NAK transactions). Verify that the USB protocol analyzer device (sniffer) does not detect any USB transactions other than keep-alive (NAK transactions).*
8. *Repeat steps 5 to 7 with a USB mouse instead of a keyboard.*
9. *Power off the TOE.*
10. *Remove the USB protocol analyzer device (sniffer) and connect the keyboard and the mouse directly to the TOE.*
11. *Connect the USB protocol analyzer device (sniffer) between the user authentication device and the TOE.*
12. *Power up the TOE.*
13. *Type on the keyboard and move the mouse. At the same time check that the USB protocol analyzer running on computer B does not detect any USB transactions other than keep-alive traffic (NAK transactions). Verify that the USB protocol analyzer device (sniffer) does not detect any USB transactions other than keep-alive traffic (NAK transactions).*

The TOE does not support independent switching of peripheral devices. Therefore this test is not applicable to the TOE.

2.1.5 FDP_ACC.1 Subset Control

2.1.5.1 TSS Assurance Activities

Assurance Activities for this SFR are covered by the next SFR FDP_ACF.1.1 below.

See section 2.1.6.1 below in section 2.1.6 FDP_ACF.1 Security Attribute Based Access Control.

2.1.5.2 Guidance Assurance Activities

Assurance Activities for this SFR are covered by the next SFR FDP_ACF.1.1 below.

See section 2.1.6.2 below in section 2.1.6 FDP_ACF.1 Security Attribute Based Access Control.

2.1.5.3 Test Assurance Activities

Assurance Activities for this SFR are covered by the next SFR FDP_ACF.1.1 below.

See section 2.1.6.3 below in section 2.1.6 FDP_ACF.1 Security Attribute Based Access Control.

2.1.6 FDP_ACF.1 Security Attribute Based Access Control

2.1.6.1 TSS Assurance Activities

The evaluator shall verify that the TSS describes the allowed devices for each peripheral port type. The description does not need to include brand or model information, but must provide the following information:

a. Whether or not the USB keyboard and USB mouse console ports are interchangeable or may be combined into one port (composite USB device);

b. Whether or not PS/2 keyboard and mouse console ports are supported.

c. What types of authentication devices (e.g., smart card, CAC, token, biometric reader) are supported, how they are identified, and whether or not the TOE enables configurable user authentication device profiling (filtering);

d. What audio out devices types are supported; and

e. What user display interface protocols are supported by the TOE.

If hub and composite devices are permitted, the TSS must describe how the TOE filters endpoints.

Table 8 Peripheral Devices supported by the KVM TOE in section 1.6.2.3 Peripheral Devices Supported by the TOE provides details of the types of peripheral devices the TOE supports. In section 1.6.2.1 Evaluated Products, Tables 5, 6, and 7 identify interfaces for each model of the TOE. In section 1.6.2.4 Protocols Supported by the KVM TOE, Tables 9, 10, and 11 identify protocols for each console peripheral port.

ST section 7.2 TOE External Interfaces Security Functions lists the types of external interfaces.

a. "Whether or not the USB keyboard and USB mouse console ports are interchangeable or may be combined into one port (composite USB device)"

Paragraph "[O.PERIPHERAL_PORTS_ISOLATION]: FDP_IFC.1(1) and FDP_IFF.1(1)" in section 7.1 TOE Keyboard and Mouse Functionality states keyboard and mouse TOE ports are interchangeable.

Also in section 7.1, paragraph "[O.DISABLE_UNAUTHORIZED_PERIPHERAL]: FDP_ACC.1 and FDP_ACF.1 / [O.DISABLE_UNAUTHORIZED_ENDPOINTS]: FDP_ACC.1 and FDP_ACF.1" covers hubs and composite USB devices including how the TOE rejects non-keyboard and non-mouse input. A composite device must have at least one endpoint which is a keyboard or mouse HID class.

b. "Whether or not PS/2 keyboard and mouse console ports are supported"

The ST only references USB for keyboard and mouse console ports; PS/2 is not supported.

c. "What types of authentication devices (e.g., smart card, CAC, token, biometric reader) are supported, how they are identified, and whether or not the TOE enables configurable user authentication device profiling (filtering)"

ST section 7.6 TOE User Authentication Device Subsystem Security Functions indicates a user authentication device is switched not emulated. The TOE supports USB 1.1/2.0 user authentication devices including CAC. The section indicates the default filter allows standard smartcard readers, PIV/CAC USB 1.1/2.0 readers, tokens, and biometric readers. In section 7.6, subsection CDF (Configurable Device Filtration) describes device filtering, which is configurable for the TOE. The TOE can identify user authentication devices by USB Product ID, Vendor ID, class, and serial number.

d. "What audio out devices types are supported"

Table 8 lists the audio output device types the TOE supports. ST section 7.3 TOE Audio Subsystem Security Functions states "All TOE devices support analog audio out switching." Paragraph "TOE External Interfaces Security Functions – KVM" in section 1.6.2.7 KVM TOE Security Functions Overview does not list a digital audio output interface. Digital audio is only passed through video for KVM devices.

e. "What user display interface protocols are supported by the TOE"

In section 1.6.2.4 Protocols Supported by the KVM TOE, Tables 9, 10, and 11 identify display interface protocols for each model's console peripheral ports. Protocol support varies by model but includes DVI-I, DisplayPort, and HDMI as well as VGA through a DVI-to-VGA adapter. Tables 12, 13, and 14 identify display interface protocols for each model's computer ports. Protocol support varies by model but includes DVI-I and DisplayPort as well as VGA through a DVI-to-VGA adapter. Paragraph "TOE External Interfaces Security Functions – KVM" in section 1.6.2.7 KVM TOE Security Functions Overview summarizes display interface support combinations by model type.

[Conditional] If the TOE supports fixed user authentication device filtering (FDF) *- then the evaluator shall also verify that the TSS includes a statement indicating that the peripheral device qualification profiles cannot be changed after production.*

Section 7.6 of the ST states that the TOE is shipped with fixed device filtration for the CAC (user authentication device) port. By default, this filter will only permit connectivity of USB devices that match the supported device types.

[Conditional] If the TOE supports configurable user authentication device filtering (CDF) *- Verify that the TSS provides information on how the whitelist and blacklist are loaded into the TOE and which users are authorized to load / change these parameters. (Only privileged administrators shall be authorized to perform this activity.)*

Subsection CDF (Configurable Device Filtration) in section 7.6 TOE User Authentication Device Subsystem Security Functions describes filter configuration. The subsection covers registration by an authorized administrator. Section 7.5 TOE Administration and Security Management Tool identifies the tool provided for device management. All devices not whitelisted by the CDF function are considered to be blacklisted.

2.1.6.2 Guidance Assurance Activities

The evaluator shall verify that the user guidance provides instructions for the implementation and use of all implemented connection types, and their limitations. The guidance must describe the visual indications provided to a user when a connected device is rejected.

The [Owner] documentation describes the supported interfaces and authorized peripheral types in the "Installation" section. This section also describes the limitations placed by the TSF on each of the peripheral port interfaces. For example, immediately following the steps to connect a keyboard/mouse to the TOE, it states that keyboard and mouse devices with internal USB hub/composite device functions are not supported, nor are wireless keyboard and mouse devices.

The [Owner] documentation indicates the following visual indications when a connected device is rejected in the "KVM LEDs" section:

- Monitor: console video port LED flashing
- Keyboard/mouse: all port selection and push-button LEDs flashing simultaneously
- USB authentication device: console CAC port LED flashing

2.1.6.3 Test Assurance Activities

Tests covering this SFR are tests 4.2 and 4.3 above.

See section 2.1.4.1 above in section 2.1.4 FDP_IFF.1(2) Simple Security Attributes.

2.1.7 FDP_RIP.1 Subset Residual Information Protection

[TD0136] applies to FDP_RIP.1.

2.1.7.1 TSS Assurance Activities

The TSS shall include a detailed Letter of Volatility. The evaluator shall verify that the TSS Letter of Volatility provides at least the following information:

a. It indicates which TOE components have a non-volatile memory, the non-volatile memory technology, manufacturer and part number and memory size.

b. The type of data that the TOE may store on each one of these components.

c. 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.

d. If the specific component may be independently powered by something other than the TOE (for example – by a connected computer).

The TSS must indicate whether or not the TOE has user data buffers and how these buffers are deleted when the user switches to another computer.

Note that user configuration and TOE settings are not user data and therefore may be stored in the TOE on non-volatile memory components.

ST appendix B contains the required letter of volatility. The letter covers the main PCBA and front panel PCBA as well as the video PCBA for KVM devices. The letter describes Emulation MCU, Keyboard and Mouse USB Host Controller, CAC USB Host Controller devices on the main PCBA. It describes the EDID Emulator device on the video PCBA. The front panel PCBA has no non-volatile or volatile memory.

The description of each PCBA and device includes the manufacturer, part number, device type, function, and memory. For each component, the description of memory covers the type of memory (flash, EEPROM flash, EEPROM, or SRAM), size of non-volatile memory, type of data stored, clearing of memory at power down, and clearing of memory when anti-tampering is triggered.

Appendix B indicates only EDID Emulator may be independently powered by a connected computer (search "All the EDID emulators are powered by their respective computers or the TOE"). ST section 7.4 TOE Video Subsystem Security Functions contains details of EDID Emulator isolation.

Appendix B explains the TOE erases SRAM in the Keyboard and Mouse USB Host Controller when switching between connected computers. Paragraph "[O.PURGE_TOE KB_DATA_WHILE_SWITCHING]: FDP_RIP.1" provides details in section 7.1 TOE Keyboard and Mouse Functionality.

Appendix B covers user data stored in SRAM when power is disconnected from the device. No data is stored in main PCBA, the emulation MCU, the Keyboard and Mouse USB Host Controller, and video PCBA when power is disconnected. The CAC USB Host Controller does not store user data in SRAM.

Paragraph [O.USER_AUTHENTICATION_RESET]: FDP_IFF.1(1) and FTA_ATH_EXT.1" in section 7.6 TOE User Authentication Device Subsystem Security Functions describes how the TEO resets the user authentication device when switching connected computers.

2.1.7.2 Guidance Assurance Activities

Check the user or administrative guidance for any limitations regarding transfer of the TOE between different security levels / roles in the organization. Ensure this guidance is consistent with the claims in the Security Target.

The user guidance does not provide specific limitations regarding transfer of the TOE between different security levels/roles in the organization.

2.1.7.3 Test Assurance Activities

The evaluator shall:

1. *Verify that the TSS Letter of Volatility provides assurance that no user data remains in the TOE after power down.*
2. *Perform the TOE memory purge or Restore Factory Defaults according to the guidance and verify that the TOE enters a desirable secure state.*

The following test provides some basic indications that the TOE keyboard stack and buffer are properly deleted upon TOE switching to a different computer:

3. *Configure the TOE and the operational environment in accordance with the operational guidance.*
4. *Run a text editor on computers #1 and #2.*
5. *Set both computers to the highest keyboard repeat rate.*
6. *Power up the TOE and select computer #1.*
7. *Type the letter "A" continuously on the user keyboard (i.e., hold down the "A" button). After a few seconds, release the "A" button and switch to computer #2.*
8. *Hold down the "B" button.*
9. *Repeat this process several times and verify that only the letter "A" appears on computer #1 and only the letter "B" appears on computer #2.*

The evaluator began by authenticating to the Administration software provided with the TOE. The evaluator selected the Restore Factory Defaults option from the menu. The evaluator viewed that the current CAC device was unregistered and default settings were restored.

The evaluator then tested that the TOE keyboard stack and buffer are properly deleted upon TOE switching to a different computer. The evaluator configured the environment so that a keyboard was connected to one of the TOE's keyboard/mouse input ports. The computers were connected to their corresponding keyboard/mouse output interface on the TOE via USB. The evaluator configured the maximum keyboard repeat rate on computers 1 and 2 via the keyboard settings. The evaluator open an instance of notepad on both computers and switched between computer 1 and 2, holding the 'a' key when switched to computer 1 and the 'b' key when switched to computer 2. The evaluator viewed that only 'a' was seen typed on computer 1 and only 'b' was seen typed on computer 2. This verified that the buffer did not carry over when switching channels on the TOE.

The overall result of Test 4.12 is a pass.

2.2 Class FPT: Protection of the TSF

2.2.1 FPT_PHP.1 Passive Detection of a Physical Attack

2.2.1.1 TSS Assurance Activities

The evaluator shall verify that the TSS indicates that the TOE provides unambiguous detection of physical tampering. The evaluator shall verify that the TSS provides information that describes how the

TOE indicates that it has been tampered with and how these indications cannot be turned on by the TOE user.

ST section 7.8 TOE Tampering Protection describes how the TOE indicates tampering in paragraph "[O.ANTI_TAMPERING_INDICATION]: FPT_PHP.1." Section 7.4 TOE Video Subsystem Security Functions describes how EDID programming also causes LED to flash. However, the tamper indication and EDID programming LED flashing are distinct.

2.2.1.2 Guidance Assurance Activities

The evaluator shall verify that the 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.

The [Owner] documentation contains a section called "Features" which describes the anti-tamper switches and tamper-evident seal as the mechanisms by which the TOE provides unambiguous detection of tampering attempts. This section states that if the anti-tampering protection is triggered the front panel LEDs will flash repeatedly and if the tamper-evident seals are removed, it will be obvious by visual inspection.

2.2.1.3 Test Assurance Activities

The test for this SFR combined with the ant-tampering function testing. See test 4.13 below.

Please see section 2.2.2.3 below in section 2.2.2 FPT_PHP.3 Resistance to Physical Attack.

2.2.2 FPT_PHP.3 Resistance to Physical Attack

2.2.2.1 TSS Assurance Activities

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

In ST section 7.8 TOE Tampering Protection, paragraph "[O.ANTI_TAMPERING]: FPT_PHP.3" describes the TOE's reaction to opening the device enclosure. Paragraphs "[O.ANTI_TAMPERING_BACKUP_POWER]: FPT_PHP.3" and "[O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER]: FPT_PHP.3" cover protection of the anti-tampering battery.

2.2.2.2 Guidance Assurance Activities

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

The [Owner] documentation states that the anti-tampering functionality is triggered by any attempts to open the physical enclosure of the TOE and that the triggering of the anti-tamper switches will disable the device.

Guidance shall also include a clear description of the anti-tampering triggering user indications.

The [Owner] documentation states in the "Features" section that the user indication for a tampered device is that all LEDs will flash repeatedly. If the anti-tampering switches have not been triggered but the tamper-evident seal has been removed, it will be obvious to the user by visual inspection that this has occurred.

2.2.2.3 Test Assurance Activities

Test 4.13 Tampered TOE is permanently disabled and properly isolated

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

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

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

Part 1 – Anti-tampering triggering

In the following steps the evaluator shall trigger the anti-tampering function.

SFRs mapped to the following test:

- *Passive detection of physical attack: FPT_PHP.1*
- *Anti-tampering triggering: FPT_PHP.3.1*

The evaluator shall:

1. *Attempt to open the PSS enclosure enough to gain access to its internal circuitry. The evaluator shall then verify that the TOE becomes permanently disabled and that the TOE provides the proper indication that it has been tampered with, in accordance with the user guidance.*
2. *Verify that at least one tamper evident label was damaged in accordance with the user guidance information.*
3. *Attempt to turn off the tampering indications through user configuration, panel dimming etc. Verify that the tampering indications are persistent.*

The evaluator tested the tampering mechanism of the TOE by attempting to unscrew the top enclosure. Unscrewing the top enclosure is the only way to gain access to the internal components of the TOE. After about a full turn of the screw the TOE began to flash and beep indicating the tampered state. The evaluator verified that the TOE had no functionality, including displaying video or allowing input from the keyboard and mouse. The evaluator rebooted the TOE and viewed that the TOE remained in the tampered state with the indication and no functionality. There exists no interface to disable the tamper state. Additionally the evaluator attempted to get passed the tamper label and viewed that the tamper attempt was visible after via the label.

The overall result of Test 4.13 is a pass.

Part 2 – Anti-tampering is permanent

In the following test steps the evaluator shall attempt to restore normal TOE operation after TOE anti-tampering has been triggered.

SFRs mapped to the following test:

- *Anti-tampering is permanent: FPT_PHP.3.2*

4. *The evaluator shall perform the memory purge or Restore Factory Defaults procedure in accordance with the user guidance and verify that the TOE remains in a disabled state.*
5. *The evaluator shall attempt to access the TOE settings to reset the tampering state. The configuration functionality shall be inaccessible, or attempts to recover from the tampered state fail.*

The TOE is completely disabled when in its tampered state. Therefore it is not possible to authenticate to the TOE to perform the Restore Factory Defaults procedure once tampering has occurred.

Part 3 – Anti-tampering isolation

In the following test steps the evaluator shall validate that the TOE behavior conforms to the data isolation requirements when the device has been tampered with (i.e. the TOE anti-tampering function has been triggered).

SFRs mapped to the following test:

- *Anti-tampering isolation: FPT_PHP.3.2*

6. *Use a TOE sample that was previously tampered with (i.e. the TOE anti-tampering function was triggered).*
7. *Connect the TOE to computers and peripherals as required and power it up. Verify that the TOE indicates the tampered state in accordance with user guidance.*
8. *Verify that the following data flows are blocked:*

    a. [Conditional] If the TOE supports keyboard switching - verify that the keyboard does not function;

    b. [Conditional] If the TOE supports mouse switching - verify that the mouse does not function;

c. [Conditional] If the TOE supports display switching - verify that no video is shown on the user display;

d. [Conditional] If the TOE supports user authentication device switching - verify that the authentication device is not shown on any computer; and

e. [Conditional] If the TOE support analog audio device switching - verify that no audio can be heard;

9. Power off the TOE and repeat step 9.

The evaluators attempted to interact with the keyboard, mouse, CAC, and audio interfaces (both computer interfaces and console interfaces) after the tamper detection was triggered. The TOE has no functionality when in a tampered state.

2.2.3 FPT_FLS.1 Failure with Preservation of Secure State

2.2.3.1 TSS Assurance Activities

Assurance Activities for this SFR were integrated with the TSF Testing Assurance Activities below.

Please see section 2.2.4.1 below in section 2.2.4 FPT_TST.1 TSF Testing.

2.2.3.2 Guidance Assurance Activities

Assurance Activities for this SFR were integrated with the TSF Testing Assurance Activities below.

Please see section 2.2.4.2 below in section 2.2.4 FPT_TST.1 TSF Testing.

2.2.3.3 Test Assurance Activities

Assurance Activities for this SFR were integrated with the TSF Testing Assurance Activities below.

Please see section 2.2.4.3 below in section 2.2.4 FPT_TST.1 TSF Testing.

2.2.4 FPT_TST.1 TSF Testing

2.2.4.1 TSS Assurance Activities

The evaluator shall verify that the TSS describes the self- tests that are performed on start up or on reset (if a reset function is available). The evaluator shall verify that the self-test covers at least the following:

a. a basic integrity test of the TOE hardware and firmware (for example, memory testing and firmware checksum compare);
b. a test of the computer interfaces' isolation functionality (for example, generating data flow on one port and checking that it is not received on another port);
c. a test of the user interface – in particular tests of the user control mechanism (for example checking that the front panel push-buttons are not jammed); and

d. a test of the anti-tampering mechanism (for example checking that the backup battery is functional).

ST section 7.9 TOE Self-Testing and Security Audit lists states the TOE makes integrity tests of its hardware, firmware, anti-tampering system, and control functions as well as testing data traffic isolation. Sections 7.1, 7.3, 7.4, 7.6, and 7.9 each describe how the TOE behaves when a self-test fails. Section 7.9 indicates the TOE executes self-tests immediately after power up, which includes start up and reset.

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 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.

ST section 7.8 TOE Tampering Protection, paragraph "[O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE]: FPT_PHP.3 and FPT_FLS.1" describes how the TOE permanently disables operation when it detects tampering. In section 7.9 TOE Self-Testing and Security Audit paragraph "[O.SELF_TEST_FAIL_TOE_DISABLE]: FPT_TST.1 and FPT_FLS.1" describes temporarily disabling the TOE when a self-test fails. The TSS does not identify any instances where disabling does not occur after a self-test failure.

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 PSS functionality once the failure is detected.

ST section 7.9 TOE Self-Testing and Security Audit paragraphs "[O.SELF_TEST_FAIL_TOE_DISABLE]: FPT_TST.1 and FPT_FLS.1" and "[O.SELF_TEST_FAIL_INDICATION]: FPT_TST.1" describe TOE behavior when a self-test fails. The paragraphs cover temporarily disabling the TOE and turning on all front panel LEDs, respectively.

2.2.4.2 Guidance Assurance Activities

The evaluator shall verify that the 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 response to a failed self-test.

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

Under the "Miscellaneous KVM Functionality" section in [Owner], the "Power Up Self-Test" heading states that if all front panel LEDs are illuminated and not flashing, the self-tests have failed. In the event that this has occurred, the only remedies are to check for a jammed port selection button and power cycle the TOE or to contact the manufacturer. If any other behavior is observed upon start-up of the TOE, the self-tests can be assumed to have passed.

2.2.4.3 Test Assurance Activities

Test 4.14 Self-Test Pass and Fail

In this test the evaluator shall cause a TOE self-test failure to verify that the TOE responds by disabling normal functions and providing proper user indications.
The evaluator shall also attempt to remove / disconnect the anti-tampering battery to check that the TOE indicates that it has been tampered with.

SFRs mapped to the following test:

- *Self-test failure: FPT_FLS.1*
- *Self-testing: FPT_TST.1*

The evaluator shall:

1. *Receive from the vendor a specially made TOE sample that was assembled and armed without the top part of the enclosure being assembled or secured. (For example, the TOE may have anti-tampering switches secured in the close position with adhesive tape.)*
2. *Setup and power up the TOE sample and check that it is operating normally (specifically that it does not indicate that it has been tampered with). The evaluator shall verify that the TOE provides the appropriate indication of a passed self-test in accordance with the user guidance.*
3. *Power off the TOE.*
4. *The evaluator shall hold the computer #2 channel select push-button while powering up the TOE. The TOE self-test must recognized a jammed button error and enter a failed TOE state in accordance with the user guidance.*
5. *Verify that the TOE is disabled and that proper user indications are provided.*
6. *Power off the TOE and power it on again (this time without the #2 button pressed). The TOE should operate normally after passing the self-test.*
7. *The evaluator shall temporarily remove or disconnect the TOE anti-tampering battery and return it back / connect it back after a short time (few seconds).*
8. *Power up the TOE and verify that it indicates that it has been tampered with through the proper tampering state indications.*
9. *Confirm that the TOE normal functionality is disabled – no keyboard, mouse, display, audio switching etc.*
10. *Turn the TOE on and off several times and confirm that the results are consistent.*

The vendor provided a special version of the TOE with the top of the enclosure removed and the anti-tampering switches forced in the closed position. The evaluator verified that this modified TOE still functioned correctly. The first step was to test the TOE recognizing a possible jammed switch. The evaluator powered on the TOE while holding down one of the channel switches. The TOE recognized a possible jammed button and entered a failed state where all the channel lights remained on and no functionality existed. The evaluator rebooted the TOE and verified on power up that the TOE's functionality returned.

The next step was to test removal of the anti-tampering battery. The anti-tampering battery was removed from the TOE and the evaluator viewed that the TOE indicated a tampered state by flashing and beeping. All functionality was verified to no longer exist. The evaluator plugged the anti-tampering battery back in the TOE and rebooted the TOE several times. The evaluator viewed that the tampering state was permanent along with the flashing and beeping indications.

The overall result of Test 4.14 is a pass.

2.3 Class FTA: TOE Access

2.3.1 FTA_CIN_EXT.1 Extended: Continuous Indications

2.3.1.1 TSS Assurance Activities

The evaluator shall verify that the TSS describes how the switch behaves on power up. The TSS must indicate whether or not the TOE has a reset option and, if so, the TSS shall describe how the switch behaves when this option is exercised.

ST section 7.7 TOE User Control and Monitoring Security Functions describe power-up behavior of the TOE in paragraph "[O.SELF_TEST]: FPT_TST.1". In section 7.7, paragraph "[O.CONTINUOUS_INDICATION]: FTA_CIN_EXT.1" describes how the TOE displays state to a user during operation. In section 7.9 TOE Self-Testing and Security Audit, paragraph "[O.SELF_TEST_FAIL_INDICATION]: FPT_TST.1" describes the state the TOE displays when a self-test fails. Section 7.7 refers the reader to section 1.6.2.6.6 for a description of Restore Factory Default (reset) behaviors.

2.3.1.2 Guidance Assurance Activities

The evaluator shall verify that the user guidance notes which computer port group will be connected on TOE power up or recovery from reset, if this is an option. Where a reset option is available, use of this feature must be described in the user guidance.

The "Installation" section of the [Owner] documentation notes that by default, the computer connected to port 1 will always be selected after power up.

The "RESET: Restore Factory Defaults" section in this guide as well as section 7.8 in [Admin] provide guidance on how to reset the device to factory defaults.

2.3.1.3 Test Assurance Activities

Test 4.15 – Power Up Defaults, Continuous Indications and Single Control

In this test the evaluator shall verify that the TOE power up default settings are consistent with the user guidance. If the TOE defaults are affected by the TOE configuration, then each available configuration shall be tested.

The evaluator shall also check that the TOE provides proper consistent indication of each peripheral device group selected. Indications shall be always on.

SFRs mapped to the following test:

- *Continuous indications: FTA_CIN_EXT.1.1*
- *Power up defaults: FTA_CIN_EXT.1.1*

The evaluator shall:

1. *Configure the TOE and the operational environment in accordance with the operational guidance.*
2. *Select a connected computer port group and power down the TOE.*
3. *Power up the TOE and verify that the expected selected computer is indicated, and that this is the computer that is connected.*
4. *Repeat steps 2 to 3 for several selected configurations, covering at least each one of the available TOE configurations.*
5. *Verify that the TOE selected computer indications are always on (i.e., continuous) and fully visible to the TOE user.*
6. *[**Conditional**] If the TOE allows peripherals to be connected to different computers (i.e., different SPF) - then verify that each selection has its own selection indication.*
7. *[**Conditional**] If TOE panel is equipped with a dimming function – verify that in standard room illumination conditions, indications are visible at minimum brightness settings.*

The evaluator selected each channel then rebooted the TOE. As expected the TOE also switches to channel 1 after startup. The selected channel indications are always on and easily visible. The TOE does not allow independent switching of peripherals or a dimming function. The overall result of Test 4.15 is a pass.

3 Optional Security Functional Requirement Assurance Activities

3.1 Class FAU: Security Audit

3.1.1 FAU_GEN.1 Audit Data Generation

3.1.1.1 TSS Assurance Activities

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

ST section 7.9 TOE Self-Testing and Security Audit describes the audit event log in paragraph "[O.ANTI_TAMPERING]: FAU_GEN.1.1 and FAU_GEN.1.2." The paragraph lists the event types, which include administrator and user log on/off. The audit records include event type, date/time stamp, and pass/fall status. The paragraph covers audit record storage. The TOE can store up to 100 records in non-volatile memory with new events overwriting the oldest events.

3.1.1.2 Guidance Assurance Activities

None defined.

3.1.1.3 Test Assurance Activities

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

The evaluator verified that each of the audit records described in the TSS were produced when the specified event occurred. The evaluator was able to view the event log by authenticating to the TOE via authenticating to the Administration software provided and selecting the Dump Log option from the menu. The evaluator viewed that log dump table contained the proper header information as described in guidance.

All of the collected audits along with the collected header information and the actions taken to generate the audits are located in section 6.1 of the Test Report.

3.2 Class FDP: User Data Protection

3.2.1 FDP_RIP.1(2) Residual Information Protection (Memory)

Moved to optional requirements as per [TD0144].

3.2.1.1 TSS Assurance Activities

The evaluator shall verify that the TSS describes the TOE's reaction to memory purge or Restore Factory Defaults.

ST sections 7.1 and 7.7 describes the behavior of the TOE when a Restore Factory Default (reset) action is performed. Section 7.7 also references section 1.6.2.6.6 which states that this operation is initiated by an Administrator and describes the behavior that occurs when the operation is performed.

3.2.1.2 Guidance Assurance Activities

Check that the user guidance provides a method to purge TOE memory or to Restore Factory Default settings.

The “RESET: Restore Factory Defaults” sections in the [Owner] documentation as well as section 7.8 in [Admin] provide guidance on how to reset the device to factory defaults.

3.2.1.3 Test Assurance Activities

Perform the TOE memory purge or Restore Factory Defaults according to the guidance and verify that the TOE enters a desirable secure state.

The evaluator performed the Restore Factory Defaults function on the TOE in conjunction with Test 4.12. The result of this test is a pass.

3.3 Class FIA: Identification and Authentication

3.3.1 FIA_UAU.2 User Authentication Before Any Action

3.3.1.1 TSS Assurance Activities

Refer to the assurance activities of FMT_MOF.1.1

Please see section 3.4.1.1 below in section 3.4.1 FMT_MOF.1 Management of Security Functions Behavior.

3.3.1.2 Guidance Assurance Activities

Refer to the assurance activities of FMT_MOF.1.1

Please see section 3.4.1.2 below in section 3.4.1 FMT_MOF.1 Management of Security Functions Behavior.

3.3.1.3 Test Assurance Activities

Refer to the assurance activities of FMT_MOF.1.1

Please see section 3.4.1.3 below in section 3.4.1 FMT_MOF.1 Management of Security Functions Behavior.

3.3.2 FIA_UID.2 User Identification Before Any Action

3.3.2.1 TSS Assurance Activities

Refer to the assurance activities of FMT_MOF.1.1

Please see section 3.4.1.1 below in section 3.4.1 FMT_MOF.1 Management of Security Functions Behavior.

3.3.2.2 Guidance Assurance Activities

Refer to the assurance activities of FMT_MOF.1.1

Please see section 3.4.1.2 below in section 3.4.1 FMT_MOF.1 Management of Security Functions Behavior.

3.3.2.3 Test Assurance Activities

Refer to the assurance activities of FMT_MOF.1.1

Please see section 3.4.1.3 below in section 3.4.1 FMT_MOF.1 Management of Security Functions Behavior.

3.4 Class FMT: Security Management

3.4.1 FMT_MOF.1 Management of Security Functions Behavior

3.4.1.1 TSS Assurance Activities

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

ST section 7.5 TOE Administration and Security Management Tool describes the management interface for the TOE. The interface requires user name and password for identification and authentication before granting access for the management functions listed in Table 16 – KVM TOE User/Administrator Services and Accessibility in section 1.6.2.6 Administrative and User configuration of the KVM TOE. The TOE restricts access by role. Administrative actions include the ability to change the user and administrator credentials, so a previous administrator can have logical access to the TOE revoked.

3.4.1.2 Guidance Assurance Activities

The evaluator shall check the user and administrative guidance to verify that the administrative functions defined above are only available to identified administrators.

[Admin] Section 7 *Administrator Functions*, provides the guidance and identifies the functions limited to administrators as the following:

- Change User Access Credentials
- Change Admin Access Credentials
- Event Log (auditing)
- Select Mode - KVM/KM
- Restore Factory Default (reset)

Other administrative functions are provided by the TOE but they are available to both users and administrators so they are not listed here.

3.4.1.3 Test Assurance Activities

[TD0251] *The testing for this SFR is covered in Test 4.5, Part 5.*

The ST claims the following management functions:

- assign whitelist and blacklist definitions for the TOE user authentication device qualification

function
- Restore Factory Default
- Dump Log
- Select Mode
- change Access Credential

In each case, the management interface is not accessible until the user is identified and authenticates. The testing of each of these functions has been demonstrated in section 7.15 of the Test Report.

3.4.2 FMT_SMF.1 Specification of Management Functions

3.4.2.1 TSS Assurance Activities

The evaluator shall check to ensure the TSS describes the various administrator and user TOE configurations and how they are used by the TOE.

FMT_SMF.1 specifies user authentication device qualification, Restore Factory Default, Dump Log, Select Mode, and Change Access Credentials. Table 16 – KVM TOE User/Administrator Services and Accessibility in section 1.6.2.6 Administrative and User configuration of the KVM TOE identifies these management functions. Section 7.5 TOE Administration and Security Management Tool identifies the management interface for configuring the TOE. Section 7.6 TOE User Authentication Device Subsystem Security Functions covers configuration for user authentication device qualification. Section 1.6.2.6.6 covers Restore Factory Default. Paragraph "[O.ANTI_TAMPERING]: FAU_GEN.1.1 and FAU_GEN.1.2" in section 7.9 TOE Self-Testing and Security Audit includes detail for Dump Log. Section 1.6.2.6.5 covers Select Mode. Section 7.5 TOE Administration and Security Management Tool covers Change Access Credentials identifies user name and password as access credentials.

3.4.2.2 Guidance Assurance Activities

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

[Admin] Section 6 *User Functions* identifies the functions and provides the guidance to perform the following functions:

- User – Log-in
- User – CAC Port Configuration (for models with CAC support)
- User – View Registered CAC Peripheral (for models with CAC support)
- User – Terminate Session

[Admin] Section *7 Administrator Functions* identifies the functions and provides the guidance to perform the following functions:

- Administrator – Log-in
- Administrator – CAC Port Configuration (for models with CAC support)
- Administrator – View Registered CAC Peripheral (for models with CAC support)
- Administrator – Change User Credentials

- Administrator – Change Administrator Credentials
- Administrator – Event Log (auditing)
- Administrator – Select Mode (KVM/KM)
- Administrator – Restore Factory Defaults
- Administrator – Terminate Session

3.4.2.3 Test Assurance Activities

[TD0251] *The testing for this SFR is covered in:*

- *FMT_SMF.1.1 a – Test 4.5, Part 5.*

The testing of the claimed management functions is described in FMT_MOF.1.

3.4.3 FMT_SMR.1 Security Roles

3.4.3.1 TSS Assurance Activities

Refer to the assurance activities of FMT_MOF.1.1 above.

Please see section 3.4.1.1 above in section 3.4.1 FMT_MOF.1 Management of Security Functions Behavior.

3.4.3.2 Guidance Assurance Activities

Refer to the assurance activities of FMT_MOF.1.1 above.

Please see section 3.4.1.2 above in section 3.4.1 FMT_MOF.1 Management of Security Functions Behavior.

3.4.3.3 Test Assurance Activities

Refer to the assurance activities of FMT_MOF.1.1 above.

Please see section 3.4.1.3 above in section 3.4.1 FMT_MOF.1 Management of Security Functions Behavior.

4 Selection-Based Security Functional Requirement Assurance Activities

4.1 Class FTA: TOE Access

4.1.1 FTA_ATH_EXT.1 User Authentication Device Reset

4.1.1.1 TSS Assurance Activities

The evaluator shall verify that the TSS describes how the TOE resets the power to the user authentication device. The TSS shall also describe the amount of capacitance in the TOE and how it will affect the voltage decrease on an average user authentication device. Capacitance shall be small enough to assure that low-power devices would reach less than 2.0 V during that one second power reset.

ST section 7.6 TOE User Authentication Device Subsystem Security Functions describes power reset when switching connected computer in paragraph "[O.USER_AUTHENTICATION_RESET]: FDP_IFF.1(1) and FTA_ATH_EXT.1." The description covers the drop in voltage.

4.1.1.2 Guidance Assurance Activities

The evaluator shall verify that the user guidance provides information about the prohibited use of user authentication devices with external power sources.

The [Owner] documentation states that connection of authentication devices with external power sources is prohibited in the "Installation" section.

4.1.1.3 Test Assurance Activities

Testing for this SFR is covered by Test 4.5 Part 1 above.

Please see section 2.1.4.3 above in section 2.1.4 FDP_IFF.1(2) Simple Security Attributes.

5 Security Assurance Activities

5.1 Class ADV: Development

5.1.1 ADV_FSP.1 Basic Functional Specification

There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described in Section 4.2 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 assurance activities being performed; if the evaluator is unable to perform an activity because the there is insufficient interface information, then an adequate functional specification has not been provided.

There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described for each SFR, and for other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information are implicitly assessed by virtue of the other assurance activities being performed.

5.2 Class AGD: Guidance Documents

5.2.1 AGD_OPE.1 Operational User Guidance

Some of the contents of the operational guidance will be verified by the assurance activities in Section 4.2 and evaluation of the TOE according to the Common Evaluation Methodology (CEM). The following additional information is also required.

The operational guidance shall contain instructions for configuring the TOE environment to support the functions of the TOE. These instructions shall include configuration of the TOE as well as configuration of the connected computers and peripheral devices.

The [Owner] documentation provides instructions to configure the TOE as well as configuration of the connected computers and peripheral devices. See section “Installation”.

[Admin] provides the guidance for an administrator to use the Tripp Lite Secure KVM Administration and Security Management Tool to configure the TOE.

5.2.2 AGD_PRE.1 Preparative Procedures

The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses the computer platforms and peripheral devices claimed for the TOE in the ST.

The [Owner] documentation contains a section called “System Requirements”, which list the supported computer platforms and peripheral devices consistent with the claims made in the ST.

5.3 Class ATE: Tests

5.3.1 ATE_IND.1 Independent Testing – Conformance

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 Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance 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.

The Assurance Activities found in the PP were replicated to successfully test a sampling of the claimed platforms. A separate Test Report was produced with the summary of all the platforms tested. The Test Report devised an equivalency argument that considered the following factors when determining what specific tests should be performed on what specific models:

- Variable number of ports supported by the KVM
- Variable number of video outputs
- Different display interfaces (DVI, HDMI, DisplayPort)
- Common Access Card (CAC) support

The evaluators analyzed these factors using proprietary and non-proprietary design information and chose the following TOE models for conducting various testing subsets:

- B002-DP2AC4
- B002-DV1AC8
- B002-HD2AC4

Section 4 of the TR contains information on the default configurations of the test environment with each of the platforms. This section also provides additional information on the other testing equipment required to perform testing.

Each Assurance Activity was given its own test case in the Test Report. Each test case consists of the test steps from the PP along with the actual performed test steps and any corresponding evidence. Additional information on the set up of the test environment and use of the additional test equipment can also be found in each test case.

5.4 Class ALC: Life-cycle Support

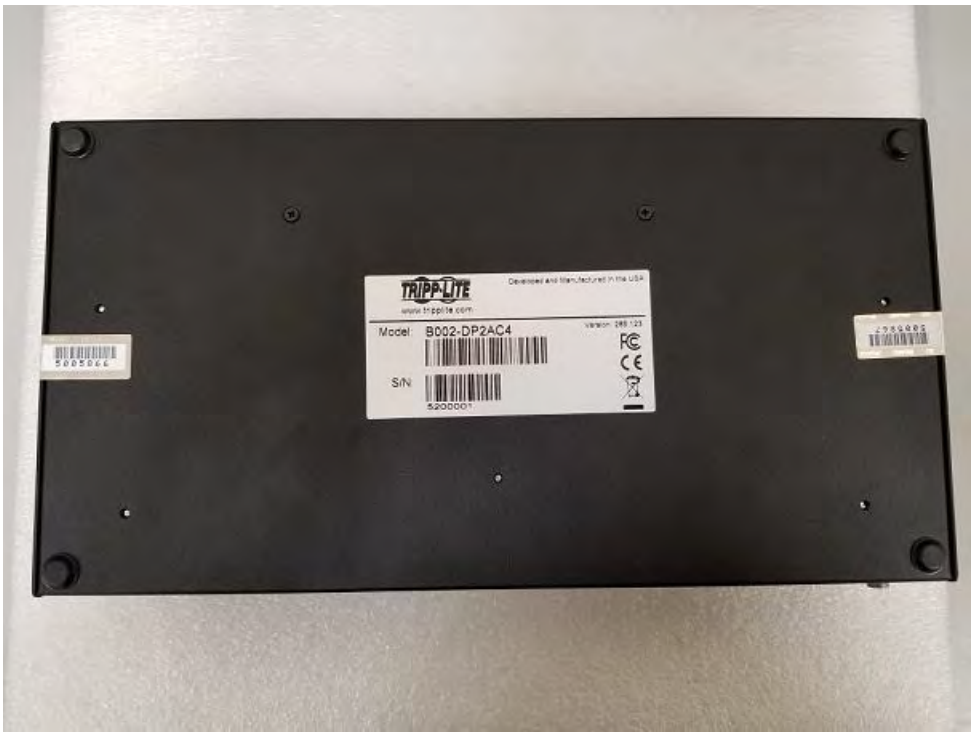
5.4.1 ALC_CMC.1 Labeling of the TOE

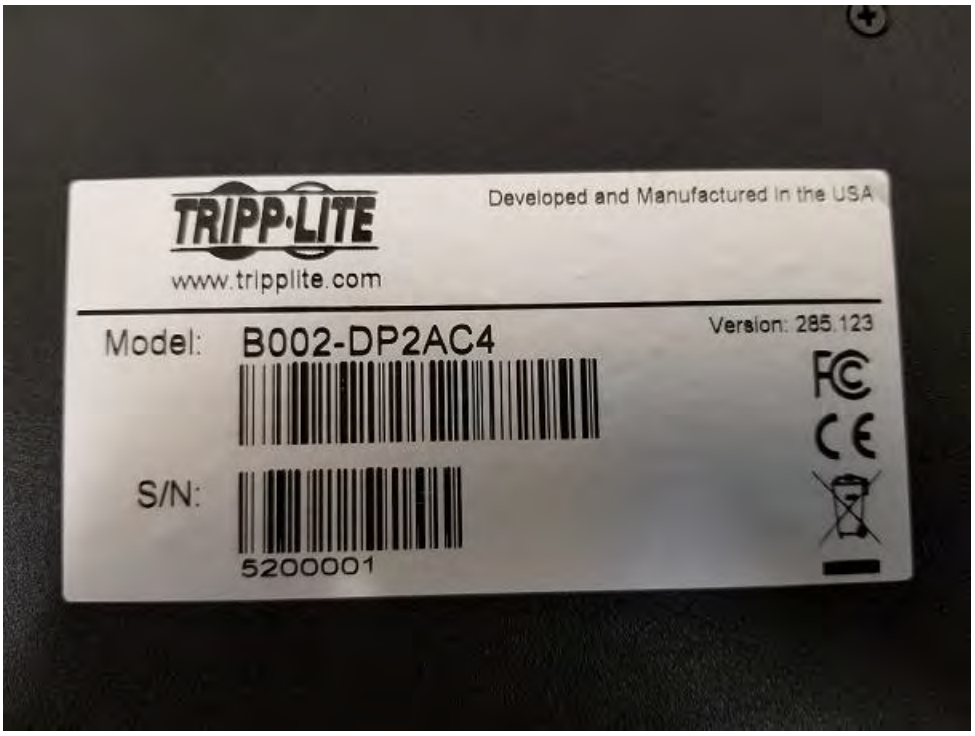
The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising

the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.
Additionally, the evaluator shall verify that the labels required by FPT_PHP.1 are present and intact, as follows:

- *The TOE is labeled with at least one unique identifying tamper-evident marking (such as unique serial number) that can be used to authenticate the device.*
- *Tamper evident labels have been placed in critical locations on the TOE enclosure to assure that any attempt to open the enclosure enough to gain access to its internal components will change at least one label to a tampered state.*
- *at least one tamper evident label is placed in a location that will be visible to the user operating the TOE.*

[ST] identifies every TOE component and the firmware version number. Each TOE device is labelled and each label uniquely identifies the TOE model number, version number, and serial number. Tamper evident labels have been placed in critical locations on the TOE enclosure to assure that any attempt to open the enclosure enough to gain access to its internal components will change at least one label to a tampered state. At least one tamper evident label is placed in a location that will be visible to the user operating the TOE. The following images show the underside of a chassis for one of the claimed models of the TOE. In the first image the tamper seals are clearly visible on the sides of the chassis. The second image is a zoomed-in version of the first image to show the product label in greater detail. Upon inspection it is evident that the TOE model and version are consistent with what is provided in [ST].





The TOE labels correspond to the model numbers and firmware version numbers identified in the ST.

Tripp Lite maintains a website advertising the TOE. The website www.tripplite.com includes a page for KVMs, which can be filtered down to Desktop KVM Switches (https://www.tripplite.com/products/rack-mount-desktop-kvm-switches~14?2027=Desktop). This website identifies the individual product models by name. These models can be compared to those in the ST to easily determine whether a given model was within the scope of the evaluated TOE. Therefore, there is a reasonable expectation that the vendor's website identifies the correct version of the TOE for purchase.

Tripp Lite also maintains a website at https://www.tripplite.com/pages/niap-secure-kvm at which the product documentation used in the evaluation can be obtained. The [Admin] Guide identifies the same link as the location where the administrator can download the Administration and Security Management Tool.

5.4.2 ALC_CMS.1 TOE CM Coverage

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 (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

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 (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

5.5 Class AVA: Vulnerability Assessment

[TD0083] Vulnerability Survey Assurance Component (AVA_VAN.1) in PSS PP v3.0

AVA_VAN.1 “Vulnerability Survey” assurance component is included in the PSS PP v3.0.

5.5.1 AVA_VAN.1 Vulnerability Survey

TD0083: Vulnerability Survey Assurance Component (AVA_VAN.1) in PSS PP v3.0

The Protection Profile for Peripheral Sharing Switch Version 3.0 omitted the AVA_VAN.1 “Vulnerability Survey” assurance component. However, this component is needed and being added with this technical decision.

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

Searches of public domain sources for potential vulnerabilities in the TOE were conducted periodically throughout the evaluation, most recently on August 20, 2018. During each search, no known vulnerabilities were revealed. In the absence of public vulnerabilities, the evaluation team determined that the test assurance activities prescribed by the claimed PP, specifically related to unintended switching, connectivity of unauthorized peripherals, attempts to reverse audio signal, and attempts to breach the physical boundary of the TOE demonstrate sufficient resilience of the TOE to an attacker of Basic attack potential.