Assurance Activities Report

for

ATEN Secure KVM Switch (CAC Models)

(Non-Proprietary)

Version 1.2

2022-03-08

Prepared by:

Leidos Inc.
https://www.leidos.com/CC-FIPS140
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:

ATEN
3F, No. 125, Section 2, Datung Road,
Sijhih District,
New Taipei City, 221
Taiwan

The TOE Evaluation was Sponsored by:

ATEN
3F, No. 125, Section 2, Datung Road,
Sijhih District,
New Taipei City, 221
Taiwan

Evaluation Personnel:

Justin Fisher
Greg Beaver
Allen Sant
Sindhu Veerabhadru
Madhav Nakar

Contents

1 Introduction

This document presents results from performing Evaluation Activities (EAs) associated with the evaluation of the ATEN Secure KVM Switch Series (CAC Models). This report contains sections documenting the performance of EAs associated with each of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) as specified in EAs for the individual components of the PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, including the following optional and selection-based SFRs:

Protection Profile for Peripheral Sharing Device [PSD PP]:

- FAU_GEN.1
- FDP_RIP_EXT.2
- FDP_SWI_EXT.2
- FIA_UAU.2
- FIA_UID.2
- FMT_MOF.1
- FMT_SMF.1
- FMT_SMR.1
- FPT_PHP.3
- FPT_STM.1
- FTA_CIN_EXT.1

PP-Module for Analog Audio Output Devices [AO Module]:

- None

PP-Module for Keyboard/Mouse Devices [KM Module]:

- FDP_FIL_EXT.1/KM
- FDP_RIP.1/KM
- FDP_SWI_EXT.3

PP-Module for User Authentication Devices [UA Module]:

- FDP_TER_EXT.2
- FDP_TER_EXT.3

PP-Module for Video/Display Devices [VI Module]:

- FDP_CDS_EXT.1
- FDP_IPC_EXT.1
- FDP_SPR_EXT.1/DP
- FDP_SPR_EXT.1/DVI-I
- FDP_SPR_EXT.1/HDMI

1.1 Applicable Technical Decisions

The NIAP Technical Decisions referenced below apply to [PSD PP] and the claimed PP-Modules. Rationale is included for those Technical Decisions that do not apply to this evaluation.

TD0506: Missing Steps to disconnect and reconnect display

This TD is applicable to the TOE.

TD0507: Clarification on USB plug type

This TD is applicable to the TOE.

TD0514: Correction to MOD_VI FDP_APC_EXT.1 Test 3 Step 6

This TD is applicable to the TOE.

TD0518: Typographical error in Dependency Table

This TD is applicable to the TOE.

TD0539: Incorrect selection trigger in FTA_CIN_EXT.1 in MOD_VI_V1.0

The TOE does not fit the Combiner Use Case and so the specific assignment required by the VI Module does not apply.

TD0557: Correction to Audio Filtration Specification Table in FDP_AFL_EXT.1.

This TD is applicable to the TOE.

TD0583: FPT_PHP.3 modified for PSD remote controllers

This TD is applicable to the TOE.

TD0584: Update to FDP APC_EXT.1 Video Tests

This TD is applicable to the TOE.

TD0585: Update to FDP_APC_EXT.1 Audio Output Tests

This TD is applicable to the TOE.

TD0586: DisplayPort and HDMI Interfaces in FDP_IPC_EXT.1

This TD is applicable to the TOE.

TD0593: Equivalency Arguments for PSD

This TD is applicable to the TOE.

1.2 Evidence

[PSD PP] Protection Profile for Peripheral Sharing Device, Version 4.0, July 19, 2019

[AO Module] PP-Module for Analog Audio Output Devices, Version 1.0, July 19, 2019

[AO-SD] Supporting Document for PP-Module for Analog Audio Output Devices, Version 1.0, July 19, 2019

[KM Module] PP-Module for Keyboard/Mouse Devices, Version 1.0, July 19, 2019

[KM-SD] Supporting Document for PP-Module for Keyboard/Mouse Devices, Version 1.0, July 19, 2019

[UA Module] PP-Module for User Authentication Devices, Version 1.0, July 19, 2019

[UA-SD]	Supporting Document for PP-Module for Keyboard/Mouse Devices, Version 1.0, July 19, 2019
[VI Module]	PP-Module for Video/Display Devices, Version 1.0, July 19, 2019
[VI-SD]	Supporting Document for PP-Module for Keyboard/Mouse Devices, Version 1.0, July 19, 2019
[Admin]	ATEN 2/4/8-Port USB DVI/HDMI/DisplayPort Single/Dual Display PPv4.0 Secure KVM Switch Administrator Guide, v1.03, 2021-1-25
[PAU]	ATEN 2/4/8-Port USB DVI/HDMI/DisplayPort Single/Dual Display PPv4.0 Secure KVM Switch Port Authentication Utility Guide, v1.03, 2021-1-25
[User]	ATEN 2/4/8-Port USB DVI/HDMI/DisplayPort Single/Dual Display PPv4.0 Secure KVM Switch User Manual, v1.03, 2021-1-25
[Audit]	ATEN 2/4/8-Port USB DVI/HDMI/DisplayPort Single/Dual Display PPv4.0 Secure KVM Switch Admin Log Audit Code, v1.03, 2021-1-25 (ATEN Proprietary)
[Isolation]	ATEN PP4.0 Secure KVM Isolation Document, v1.1 (ATEN Proprietary)
[Test]	ATEN Secure KVM PSD PP 4.0 Common Criteria Test Report and Procedures, Version 1.2, March 8, 2022
[ST]	ATEN Secure KVM Switch Series (CAC Models) Security Target, Version 1.1, 2022-03-08

1.3 Conformance Claims

Common Criteria Versions

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

Common Evaluation Methodology Versions

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

Protection Profiles

- [PSD PP] Protection Profile for Peripheral Sharing Device, Version 4.0, July 19, 2019
- [AO Module] PP-Module for Analog Audio Output Devices, Version 1.0, July 19, 2019
- [KM Module] PP-Module for Keyboard/Mouse Devices, Version 1.0, July 19, 2019
- [UA Module] PP-Module for User Authentication Devices, Version 1.0, July 19, 2019
- [VI Module] PP-Module for Video/Display Devices, Version 1.0, July 19, 2019

1.4 SAR Evaluation

The following Security Assurance Requirements (SARs) were evaluated during the evaluation of the TOE:

SAR	Verdict
ASE_CCL.1	Pass
ASE_ECD.1	Pass
ASE_INT.1	Pass
ASE_OBJ.2	Pass
ASE_REQ.2	Pass
ASE_TSS.1	Pass
ADV_FSP.1	Pass
AGD_OPE.1	Pass
AGD_PRE.1	Pass
ALC_CMC.1	Pass
ALC_CMS.1	Pass
ATE_IND.1	Pass
AVA_VAN.1	Pass

The evaluation work units are listed in the proprietary ETR. The evaluators note per the PP evaluation activities that many of the SARs were successfully evaluated through completion of the associated evaluation activities present in the claimed PP and PP-Modules.

2 Security Functional Requirement Evaluation Activities (PSD PP)

This section describes the evaluation activities associated with the SFRs defined in the ST and the results of those activities as performed by the evaluation team. The evaluation activities are derived from [PSD PP] and modified by applicable NIAP Technical Decisions. Evaluation activities for SFRs not claimed by the TOE have been omitted.

Evaluator notes, such as changes made as a result of NIAP Technical Decisions, are highlighted in **bold text**, as are changes made as a result of NIAP Technical Decisions. Bold text is also used within evaluation activities to identify when they are mapped to individual SFR elements rather than the component level.

When the evaluator references a random port; the port is chosen at random for that individual test in such a manner that the vendor supplying the device cannot predict which port will be selected. However, due to the nature of picking a random port there may be cases where the same port is chosen for multiple individual tests this case will be attempted to be avoided though will not exclusively be avoided.

2.1 Mandatory SFRs

2.1.1 User Data Protection (FDP)

2.1.1.1 FDP_APC_EXT.1 Active PSD Connections

2.1.1.1.1 TSS Evaluation Activities

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

Section 6.5.1 of [ST] states that the TOE enters a failure state if there is a self-test failure and that this happens if the power-on self-test or anti-tamper function fails.

Section 6.2.2 of [ST] states that no data transits the TOE when the TOE is powered off or when the TOE is in a failure state.

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

N/A

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

N/A

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

N/A

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

N/A

2.1.1.1.2 Guidance Activities

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

[Admin] **Chapter 2 Precautions and Preparation, Section Self-test failure** describes the indicators of a failure.

In the case of a self-test failure, the Secure KVM Switch becomes inoperable, with front panel LED combinations (on the Secure KVM) indicating the potential cause of the failure (such as button jam or KVM integrity compromise)

- A pre-defined combination of port and CAC LEDs indicate the cause of the failure.
- If all front panel LEDs on the Secure KVM (except the Power LED) flash continuously, it means KVM tampering is detected or a self-test failure has occurred (except for Pushbutton jam; see below).
- If Pushbutton jam is detected, both the port's LEDs (Port LED and CAC LED) will flash.

PSD:AO
If the ability of the TOE to grant or deny authorization to audio communications is configurable, the evaluator shall verify that the operational guidance describes how to configure the TSF to behave in the manner specified by the SFR. This includes the possibility of both administratively configured TOE settings and any peripherals/connectors that are included with the TOE that cause data flows to behave differently if peripherals are connected through them.

[User] **Chapter 2 Hardware Setup, Section Always use qualified and authorized peripheral devices** states that the ATEN Secure KVM Switch does not support an analogue microphone or line-in audio input. Never connect a microphone or headset microphone to the audio output port. Standard analogue speakers and headsets are supported.

Port selection via pushbutton / Remote Port Selector (RPS) only is used to enhance security. Keyboard, Mouse, Video, Audio and CAC reader switch together for secure switching.

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

N/A

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

N/A

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

N/A

2.1.1.1.3 Test Activities

There are no test Evaluation Activities for this component.

N/A

PSD:AO

Test Setup

The evaluator shall perform the following setup steps:

- Configure the TOE and the operational environment in accordance with the operational guidance.
- Play a different audio file on a number of computers for each TOE computer analog audio interface.
- Connect each computer to a TOE computer analog audio interface.
- Turn on the TOE.

Note that for a TOE that provides audio mixing function the evaluator shall maximize the volume on a specific channel where instructed in the following text to assign that specific computer.

Note: Electrical signals are considered not to flow between connected computers and data is considered not to transit the TOE if no signal greater than 45 dB of attenuation at the specific audio frequency is received

PSD:AO

Test 1-AO – Analog Audio Output Data Routing Methods.

This test verifies the functionality of the TOE routing methods while powered on, powered off, and in failure state.

Step 1: Connect amplified speakers to the TOE audio output device interface. Set the speakers to approximately 25% volume.

Step 2: [Conditional: if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP, then] perform step 3 for each switching method selected in FDP_SWI_EXT.2.2 in accordance with the operational user guidance.

Step 3: For each connected computer, ensure it is selected, listen to the amplified speakers, and verify that the audio is coming from the selected computer(s). Adjust the volume if necessary.

Step 4: Replace the speakers with a computer connected to the TOE analog audio output device interface and run audio spectrum analyzer software on it. Run tone generator software on all connected computers.

Step 5: Turn off the TOE, and for each connected computer, use the tone generator program to generate a sine wave audio tone for each of the designated frequencies and verify that no audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface.

Step 6: Power on the TOE, cause the TOE to enter a failure state, and verify that the TOE provides the user with an indication of failure. For each connected computer use the tone generator program to generate a sine wave audio tone for each of the designated frequencies and verify that no audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface.

The evaluator connected computers to the TOE, with each computer playing a different video. The evaluator verified that when switching between the different computers connected to the TOE, only the video playing on the currently selected computer could be heard through the connected speakers. This is because FDP_APC_EXT.1 Test 2-AO also requires playing audio on each selected port and verifying that the audio signal is received on the peripheral port, and that was done for all eight ports.

The evaluator replaced the TOE audio output with an oscilloscope and replaced the peer computer with an external signal generator. The evaluator turned the TOE off and verified that the TSF did not permit any of the designated frequencies to be carried through the TOE. The evaluator then placed the TOE into a failure state by deliberately inducing a push-button jam and verified that the TSF still did not permit any of the designated frequencies to be carried through the TOE. This was iterated for all ports.

Modified Per TD0585

PSD:AO

Test 2-AO – Analog Audio Output Interface Isolation

[Conditional: perform this test if "switching through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.]

This test verifies that no data or electrical signals flow between connected computers while the TOE is powered on or off.

Step 1. Continue with the setup from Test 1.

Step 2: Connect a computer to the TOE analog audio output device interface. Run audio spectrum analyzer software on all computers.

Step 3: Perform steps 4-13 for each TOE analog audio computer interface.

Step 4: Turn on the TOE and ensure the first computer is selected.

Step 5: Use the tone generator program on the first computer to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface and is not present in the audio spectrum analyzer software on any of the non-selected computers. This step does not fail if frequencies above 20 kHz are not present in the software on the connected computer due to attenuation as per FDP_AFL_EXT.1.

Step 6: For each other TOE analog audio computer interface, select that computer and use the tone generator program on the first computer (now no longer selected) to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is not present in the audio spectrum analyzer software on the selected computer, the other non-selected computers, or the computer connected to the TOE analog audio output device interface.

Step 7: Power off the TOE and use the tone generator program on the first computer to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is not present in the audio spectrum analyzer software on any of the other connected computers.

Step 8: Restart the TOE, select the first computer, and replace it with an external audio signal generator.

Step 9: For each non-selected computer connected to the TOE analog audio output computer interface, replace it with an oscilloscope set to measure the peak-to-peak voltage and perform steps 10-14.

Step 10: Perform steps 11-13 with the signal generator set to the following settings:

Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed

Signal average to 0v (negative swing).

Step 11: Set the signal generator to generate the designated frequencies and verify the signal on the oscilloscopes is 11.2 mV or less. This level of signal ensures signal attenuation of 45 dB in the extended audio frequency range.

Step 12: For each other TOE analog audio computer interface, select it, set the signal generator to generate the designated frequencies, and verify the signal on the oscilloscopes is 11.2 mV or less.

Step 13: Power off the TOE and set the signal generator to generate the designated frequencies and verify the signal on the oscilloscopes is 11.2 mV or less.

The following test was performed for each port.

The evaluator used an external signal generator to generate each of the designated frequencies on the port. An external signal generator was used rather than a software tone generator because commercial sound cards do not commonly support signal generation above 20 KHz, so a signal generator was used to reduce the risk of false negative results. The evaluator observed that no signal was detected on any of the non-selected ports, regardless of whether the TOE channel selection was set to the port that was currently generating audio or whether it was set to a different port. The evaluator also observed that the only time audio was received by the peripheral port was when the port that was currently generating audio was selected.

The evaluator then used the external signal generator to generate each of the designated frequencies at the two designated swing averages. The evaluator verified in each case that when the signal generator port is selected, the connected oscilloscope registered less than 11.2 mV on all non-selected ports, which passes the acceptable threshold for signal detection. The evaluator turned the TOE off and verified that the signal is also unable to traverse the TOE in this scenario.

PSD:AO

Test 3-AO – No Flow between Computers with Other Peripheral Device Types

[Conditional: Perform this test only if a PP-Module aside from the Analog Audio Output PP-Module is part of the PP-Configuration being claimed AND if "switching through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.]

This test verifies that power events at one TOE USB computer interface do not affect the analog audio output computer interface of another computer.

Note: "No sound appears" is defined as a temporary jump of at least 4 dB from the existing ambient noise floor.

Step 1: Connect a computer to the TOE analog audio output peripheral interface and run audio spectrum analyzer software on it and each connected computer.

Step 2: Perform steps 3-9 for each connected computer.

Step 3: Ensure the first computer is selected and perform steps 4-8 while the TOE is powered on and powered off.

[Conditional: Perform steps 4 and 5 only if the PP-Module for Video/Display Devices is part of the PP-Configuration being claimed.]

Step 4: For each other connected computer, disconnect and reconnect the video cables from the TOE computer interface several times. Verify that no sound appears on the audio analyzer software on the first computer.

Step 5: Disconnect and reconnect the first computer's video cables from the TOE computer interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers.

Step 6: [Conditional: If the PP-Module for Keyboard/Mouse Devices or PP-Module for User Authentication Devices is part of the PP-Configuration being claimed, then:] for each other connected computer, disconnect and reconnect the USB cable from the TOE USB computer interface several times. Verify that no sound appears on the audio analyzer software on the computer connected to the TOE analog audio output peripheral interface or any connected computers.

Step 7: [Conditional: If the PSD PP-Module for Keyboard/Mouse Devices is part of the PP-Configuration being claimed, then:] disconnect and reconnect the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM from the TOE KM peripheral device interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers.

Step 8: [Conditional: If the PP-Module for User Authentication Devices is part of the PP-Configuration being claimed and "external" is selected in FDP_PDC_EXT.4.1, then:] disconnect and reconnect the UA peripheral device from the TOE UA peripheral device interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers.

Step 9: [Conditional: If the PP-Module for User Authentication Devices is part of the PP-Configuration being claimed, then:] connect an authentication session to the first computer and verify that no sounds appears on the audio analyzer software on the other connected computers.

The evaluator set up the test environment per the evaluation activity and performed the following steps:

- Verification that video connect/disconnect events on the selected port do not bleed over as audio signals to any non-selected port (step 4)
- Verification that video connect/disconnect events on each non-selected port do not bleed over as audio signals to the selected port (step 5)
- Verification that CAC and HID connect/disconnect events on each non-selected port do not bleed over as audio signals to the selected port (step 6)
- Verification that HID connect/disconnect events on the peripheral keyboard/mouse ports do not bleed over as audio signals to any non-selected port (step 7)
- Verification that CAC peripheral connect/disconnect events on the peripheral CAC port do not bleed over as audio signals to any non-selected port (step 8)

With the TOE on, this testing was done over multiple iterations with each port functioning as the selected port, per step 2. Step 9 (verification that a CAC authentication event on the selected port does not bleed

over as audio signals to any non-selected port) was also performed with each port functioning as the selected port.

With the TOE off, steps 4-8 were repeated with port 1 as the selected port and all other ports as the non-selected ports. This is because the test requires the examination of each selected port and the TOE defaults to port 1 when it is not in an operational state; it is not possible for any other port to function as the selected port in this case.

PSD:AO

Test 4-AO – No Flow between Connected Computers over Time

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

Step 1: Ensure only one computer is connected and it is selected. Run a tone generator program on the connected computer and the audio analyzer software on a non-connected computer.

Step 2: Perform steps 3-11 while the TOE is powered on and powered off.

Step 3: Perform steps 4-5 for each of the designated frequencies.

Step 4: Use the tone generator program on the connected computer to generate a sine wave audio tone.

Step 5: Disconnect the connected computer, wait two minutes, connect the other computer, and verify that the generated audio frequency is not present in the audio spectrum analyzer software.

Step 6: Replace the connected computer with an external audio signal generator.

Step 7: Perform steps 8-11 with the signal generator set to the following settings:

Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed

Signal average to 0v (negative swing)

Step 8: Perform steps 9-11 for each of the designated frequencies.

Step 9: Use the signal generator to generate the signal.

Step 10: Disconnect the signal generator, wait two minutes, and replace it with an oscilloscope set to measure the peak-to-peak voltage.

Step 11: Verify the signal on the oscilloscope is 11.2 mV or less at the generated frequency.

This test was performed for each TOE analog audio output port. Additionally, the test collectively demonstrates behavior that would be a failure of FDP_UDF_EXT.1/AO (because a failure of this test would also mean that data output on one computer would subsequently reverberate back to the same port as an audio input), so the behavior described here was addressed by that testing as well.

The evaluator deviated from the listed test steps in the following manner to reduce the risk of false negatives:

- All testing that required tones to be generated/tested using connected computers were instead tested at the hardware level with oscilloscopes. The reason for this is because commercial PC sound cards commonly attenuate audio signals above 20 KHz. Therefore, if a connected computer fails to detect a signal, there is not sufficient assurance that the test actually passes, because it is possible that the TOE is incorrectly transmitting an audio signal to a computer on a non-selected port that is subsequently filtered out at the hardware level, giving the false appearance of a passing test.
- The purpose of the two minute wait in step 10 is to give the TOE adequate time to discharge any audio signal. The evaluator waited less than two minutes and verified the passing result in step 11. Based on this, there is sufficient assurance that the test would also pass if the full two minute wait had been performed.

The evaluator connected an external signal generator to the selected port and generated a signal at each of the designated frequencies. The evaluator disconnected the external generator, connected an oscilloscope

to the same port, and observed the port to see if a signal could be detected. The evaluator observed that the connected oscilloscope detected a value less than 11.2 mV, which passes acceptable threshold for signal detection. The evaluator repeated the steps with the TOE turned off and observed the results were similarly acceptable.

PSD:KM

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

The evaluator shall perform the following tests.

PSD:KM

Test 1-KM – KM Switching methods

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

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

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

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

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

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

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

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

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

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

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

For this test, the evaluator employed a sampling strategy per TD0593. Specifically, the tested TOE model was an 8-port model and four computers were connected to four arbitrarily-chosen ports for steps 1-4. As

this behavior demonstrates fundamental quality control of the product and not necessarily security functionality, any port on which keyboard/mouse inputs were not registered when selected would be indicative of a defective product. Steps 5-7 are not dependent on the number of connected computers or which ports they are connected to; the evaluator is simply attempting to cause a channel switch from whatever port is currently selected to any other port. This is also not dependent on the initial state (e.g., a switch from channel 1 to channel 2 and a switch from channel 2 to channel 3 could theoretically be triggered in the same manner).

The evaluator connected four computers to the TOE and connected a direct monitor to each of the computers to view the computer video feeds independent of the TOE. The evaluator then verified that the mouse and keyboard actions performed on the connected peripherals are only registered on the selected computer. The evaluator attempted to change the selected computer with each of the specified command sets and verified that the TOE rejected all keyboard-based attempts to change the selected computer. The evaluator also verified that the mouse was unable to change the selected computer. Specifically, the evaluator attempted to use the same function that KM devices from the same manufacturer have as a guard mechanism. The evaluator took the actions that would disengage the guard on KM devices and allow for a mouse cursor-initiated channel switch and observed that on KVM devices, this operation has no effect.

PSD:KM

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The evaluator used the keyboard and mouse to send traffic to the selected port to observe that it was registered on the first computer, as expected, while the second computer did not register any USB traffic on the sniffer. The evaluator iterated this test through all seven non-selected ports, moving the second computer to a different non-selected port each time. This process was repeated for each available port.

Steps 11 and 12 require the TOE to be in a powered off or failure state and to exercise behavior against "the selected computer"; since the TOE does not maintain the concept of a selected computer when in an unpowered or error state, a single port was chosen to demonstrate this. Specifically, the evaluator chose port 1 as this is the default selected computer when the TOE initially boots.

The conclusion of this testing was that the following behavior was observed in all tested cases:

- TOE powered on: USB traffic was only detected on the selected channel
- TOE powered off: no USB traffic was detected on any channel
- TOE in failure state: no USB traffic was detected on any channel

PSD:KM

Test 3-KM – Flow Isolation and Unidirectional Rule

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

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

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

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

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

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

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

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

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

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

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

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

momentarily and then stay off (indicating that the keyboard is powered on, although the selected computer is not connected).

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

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

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

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

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

For this test, the evaluator employed a sampling strategy per TD0593. The unidirectional functionality is implemented central to the TOE at the peripheral interface level and is not associated with any individual computer port interfaces. Therefore, there is not a case where any attempts to force a violation of unidirectional data flow would be successful on one port and unsuccessful on another port, because the enforcement happens prior to the data being routed to a port.

The evaluator connected a gaming mouse directly to one of the computers and verified that the computer recognized the gaming mouse and allowed for configuration of the gaming mouse. The evaluator connected the mouse through the TOE and verified that the computer no longer recognized the gaming mouse and did not permit configuration of the mouse.

The evaluator connected a keyboard directly to one of the computers and demonstrated that caps/num/scroll lock functionality worked and that the keyboard lights were responsive to their respective states. The evaluator then connected the keyboard through the TOE and verified that the caps/num/scroll lock keys continued to change the state of that configuration in the on-screen keyboard when toggled by the user, but that the lights on the keyboard were no longer responsive to changes in their state.

The evaluator verified that the TOE emulated the keyboard and mouse devices to all connected computers all the time. Step 12 was not applicable to the TOE because it is only performed if keyboard/mouse devices are not emulated.

PSD:KM

[TD0507]: Clarification on USB plug type

Test 4-KM – No Flow between Computer Interfaces

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

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

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

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

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

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

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

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

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

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

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

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

For this test of the ports selectable, the port was selected and all seven non-selected ports were observed. This was done by using two computers: one computer was connected to the selected port, and a second computer was connected to a non-selected port through a USB sniffer. Once the behavior of the non-selected port was observed, the evaluator moved the second computer to a different non-selected port and repeated the test. This was done until all non-selected ports were observed, after which the first computer was moved to a different sampled port as the selected port and the process was repeated.

The sampling was only performed for video interfaces on the same board; in the case of a multi-board device (i.e., a dual-head model), each video board is a distinct physical component so it is assumed that a digital signal cannot traverse from one board to another.

The evaluator verified that when the TOE is rebooted and intensive USB HID traffic is generated, the only communication to each of the other connected computers is the device enumeration communication from the TOE that emulates the connection to each of the connected computers. Validation that HID traffic does not traverse to non-selected ports is covered by FDP_APC_EXT.1 Test 2-KM, Step 6.

The evaluator connected a dummy USB device and verified that no new data packets are transferred across to other computers. The evaluator connected 5 V power unit capable of modulation to the TOE via USB Type-B and verified that no data is transferred to the other computers while it is being modulated.

PSD:KM

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

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

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

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

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

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

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

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

Step 7: Reboot the TOE and repeat step 6.

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

Step 9: Restart the TOE and repeat step 6.

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

For one arbitrary port, the evaluator set up two computers per the evaluation activity setup and verified only one computer was connected to the TOE. The evaluator then generated intensive mouse/keyboard data and verified that it was recorded by the connected computer's text editor and USB analyzer. The evaluator then disconnected the first computer and generated HID traffic with no computers connected. The evaluator then connected the second computer in place of the first and observed that no USB activity was captured (i.e., no buffer was emptied), consistent with the TOE properly not retaining and replaying the previous USB traffic. The evaluator repeated the observation after multiple reboots and the TOE being turned off.

PSD:UA

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

PSD:UA

Test Setup

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

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

PSD:UA

Test 1-UA: UA Switching methods

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

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

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

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

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

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

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

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

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

For this test, the evaluator employed a sampling strategy per TD0593. Specifically, the tested TOE model was an 8-port model and four computers were connected to four arbitrarily-chosen ports for. As this behavior demonstrates fundamental quality control of the product and not necessarily security functionality, any port on which CAC inputs were not registered when selected would be indicative of a defective product.

The evaluator measured the power for the LED on an open cable connected to the TOE's CAC port and verified the value is between 4.75 and 5.25 VDC. The evaluator verified that the selected computer could observe the CAC reader in its device manager. The evaluator also verified that when a switch operation occurs, the observed behavior was a temporary drop in voltage, a corresponding turn off of the external authentication device's power LED, and a restoration in voltage followed by the newly-selected computer detecting the presence of the device.

PSD:UA

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

For this test, the evaluator employed a sampling strategy per TD0593. Specifically, the tested TOE model was an 8-port model and two ports were chosen arbitrarily to function as the selected ports for the automatic session termination as the session termination is not dependent on the selected port, for the observation of directional of the selected port's traffic all ports were tested.

For each of these ports, all seven non-selected ports were observed. This was done by using two computers: one computer was connected to the selected port, and a second computer was connected to a non-selected port through a USB sniffer. Once the behavior of the non-selected port was observed, the evaluator moved the second computer to a different non-selected port and repeated the test. This was done until all non-selected ports were observed, after which the first computer was moved to a different sampled port as the selected port and the process was repeated.

The evaluator verified only the selected computer could see the authentication device in its device manager. The evaluator verified that an active authentication session on the selected computer is terminated either when the authentication element is removed or when the selected channel is changed. The evaluator also verified that no USB traffic is detected on any of the non-selected computers while the authentication device is being used or while the selected computer has its state changed (e.g., physically disconnected from/reconnected to the TOE, rebooted, placed in sleep mode, restored from sleep mode). The evaluator also verified that no CAC traffic was detected when the TOE is off or in a failure state.

PSD:UA

Test 3-UA: No Electrical Flow between Computer Interfaces.

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

This test verifies no electrical signals flow between connected computers when the TOE is powered on or off.

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

Step 1: Disconnect the first computer and replace it with a switchable 5 volt power supply with a USB Type-B plug. Modulate the 5 volt supply manually at various speeds from approximately one cycle per five seconds to one cycle per second. Verify that no new USB traffic is captured on the non-selected USB analyzers.

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

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

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

Step 4: Disconnect the USB dummy load and replace it with a switchable 5 volt power supply with a USB Type-B plug. Modulate the 5 volt supply manually at various speeds from approximately one cycle per five seconds to one cycle per second. Verify that no new USB traffic is captured on the non-selected USB analyzers.

For this test, the evaluator tested all ports.

The evaluator verified that replacing a computer on the selected port with a USB power supply and modulating the voltage on that power supply did not cause any USB signals to be detected on any other computer ports.

The evaluator also connected first a dummy USB device and then a USB power supply to the peripheral CAC port and verified that no data was detected on any of the computer USB ports while these devices were used.

PSD:UA

Test 4-UA: No Flow between Connected Computers over Time

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

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

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

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

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

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

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

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

For this test, the evaluator employed a sampling strategy per TD0593. Specifically, the tested TOE model was an 8-port model and one port was chosen arbitrarily as the selected port. Each port uses the same USB driver and memory components, so there is no design element that would cause different ports to behave differently. Additionally, since this test is for the functionality of a single port rather than non-interaction between multiple ports, there are no design considerations that would cause which port is chosen for testing to potentially have a different result from any other ports.

The evaluator used a USB capture device to observe communications between the CAC peripheral and the TOE and observed communications between the peripheral CAC reader and the connected computer (through the TOE) after both a successful and an unsuccessful authentication attempt. This was done to identify the type and amount of data that the CAC reader sends to the connected computer in both cases.

The evaluator successfully authenticated to the computer connected to port 1. The evaluator then disconnected this computer from its CAC port and connected a second computer to the same port in its place. Once this occurred, the evaluator waited a brief period to ensure that any short periodic data retransmission would be considered (and not just data transmission that occurred when the connection was initially made). The evaluator observed, both visually on the computer and through the USB traffic capture, that the only data transmitted from the CAC reader to this computer was the enumeration of the CAC reader subsequently followed by NAK packets; no data that relates to authentication was replayed to the second computer and the computer gave no indication that any authentication attempt or assertion of an active session was transmitted to it.

PSD:VI

The evaluation shall perform the following tests:

PSD:VI

[TD0539]: Incorrect selection trigger in FTA_CIN_EXT.1.1 in MOD_VI_V1.0

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

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

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

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

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

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

Step 5: Turn on the TOE.

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

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

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

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

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

For this test, the evaluator employed a sampling strategy per TD0593. Specifically, the tested TOE model was an 8-port model and four computers were connected to four arbitrarily-chosen ports. As this behavior demonstrates fundamental quality control of the product and not necessarily security functionality, any port on which a video signal was not detected when selected would be indicative of a defective product.

Additionally, FDP_APC_EXT.1 Test 3-VI tests other permutations of the video output because step 5 of that test requires the TSF to block MCCS signals. The only way to demonstrate this is to have a display connected to the TOE and have a visible picture of the selected channel. Therefore, the current test (FDP_APC_EXT.1 Test 1-VI) is not the only place where the evaluator demonstrates that a selected channel will appropriately display a video signal to a connected monitor.

The evaluator played a different video on each of the connected computers. The evaluator verified that the monitor connected to the TOE only displayed the currently selected computer's video. The evaluator verified that the TOE did not display any video when the TOE was turned off or in a failure state.

The evaluator verified that the active computer display on a connected TOE monitor is clearly indicated.

PSD:VI

Test 2-VI: Computer Video Interface Isolation

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

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

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

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

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

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

1. Video Graphics Array (VGA) – single ended probe on pins 13 and then 14;
2. High-Definition Multimedia Interface (HDMI) – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide Hot Plug Detect (HPD) signal; Check for signals - differential probe between pins 10 (+) and 12 (-);
3. Digital Visual Interface (DVI)-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-);
4. DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 23 (+) and 24 (-);

5. DisplayPort - connect pin 18 to a 3.3V power supply via 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+);
6. USB Type-C with DisplayPort as Alternate Function – connect pin A8 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals – Differential probe between pins A2 and A3, A10 and A11; B2 and B3, and B10 and B11.

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

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

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

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

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

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

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

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

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

For this test in steps 3 and 4 all permutations were tested, in steps 7-10, the evaluator employed a sampling strategy per TD0593. Specifically, the tested TOE models included several 4-port and 8-port models (with multiple tested models to ensure coverage of all claimed video protocols) and two or four ports were chosen arbitrarily for each to function as the selected ports; two ports for 4-port devices and four ports for 8-port devices. For each of these ports, all seven non-selected ports (or three non-selected ports, in the case of 4-port models) were observed. In each case, a computer was connected to the selected port, while an open video connecter was connected to a non-selected port so that the pins could be read using an oscilloscope probe. The video ports of a given type for each TOE model that supports that type are identical, so there is no expectation that any individual ports will behave any differently with regards to isolation.

For each supported video protocol, the evaluator connected a special video connector to the TOE with power to the designated pins and observed the specified pins for each video type. The evaluator then measured the differential between the designated pins, dependent on the supported video protocol, to demonstrate that no SYNC signal is transmitted to a non-selected video port.

For each supported video protocol, the evaluator then connected the same connector to the TOE without power and observed all pins. The evaluator performed some actions on the selected computer and verified that the observed pins showed no signals being transmitted to the sampled non-selected channels.

This test was repeated on devices that have multi-head displays where each head is on a separate board, only one board was sampled as they are physically isolated from one other and it is not possible for a signal on one board to travel to another board (between the two boards).

PSD:VI

[TD0514]: Correction to MOD_VI FDP_APC_EXT.1 Test 3 Step 6

[TD0584]: Correction to MOD_VI FDP_APC_EXT.1 Test 3 Step 8, Test 5 Step 11

Test 3-VI - Unauthorized Sub-protocols

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

This test verifies that unauthorized sub-protocols are blocked.

Perform this test for each of the selections in FDP_PDC_EXT.3.1/VI and FDP_IPC_EXT.1.1.

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 11: Collect all 20 EDID file captures, compare them bit-by-bit, and verify that they are all identical excluding null captures recorded in Step 7.

Step 12: [Conditional, if DisplayPort, DVI-D, DVI-I, HDMI, or USB Type-C is the selected protocol being tested at the computer video interface, then] run Consumer Electronics Control (CEC) and High-bandwidth Digital Content Protection (HDCP) tests or commands at the generator and verify in the testing device that no CEC or HDCP traffic is captured.

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

Step 14: [Conditional: If *"[HDMI] protocol*" is selected in FDP_IPC_EXT.1.2, then] perform steps 15 and 16 for both pin 13 (CEC) and 14 (UTILITY).

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

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

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

1. HDMI – connect scope to pin 19 and verify no HPD signal is detected;
2. DVI-D/DVI-I – connect scope to pin 16 and verify no HPD signal is detected;

3. DisplayPort - connect scope to pin 18 and verify no HPD signal is detected;
4. USB Type-C with DisplayPort as Alternate Function – connect scope to pin A8 and B8 and verify no HPD signal is detected.

Step 18: Repeat this test for each of the selections in FDP_PDC_EXT.3.1/VI and FDP_IPC_EXT.1.2.

The evaluator executed this testing multiple times as needed to ensure that each claimed video protocol was tested. Each iteration of testing was done on a single port. The video protocol filtering happens central to the TOE per its design, rather than on a per-port level. Therefore, the choice of port will not affect how the TSF implements this particular function.

The evaluator verified that the TOE blocked the MCCS commands by connecting a computer directly and verifying that the computer could control the MCCS commands, then connecting the monitor through the TOE and verifying the TOE blocked the MCCS commands.

The evaluator used the designated device types and verified that the protocol-specific sub-protocols were appropriately blocked for each protocol.

The evaluator verified that the HPD signal was not detected for each of the device video types.

PSD:VI

[TD0506]: Missing Steps to disconnect and reconnect display

Test 4-VI - Video and EDID Channel Unidirectional Rule

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

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

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

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

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

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

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

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

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

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

Step 8: Power up the TOE again.

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

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

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

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

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

For this test, the evaluator employed a sampling strategy per TD0593. Each distinct video protocol was tested, but a sampling of one of the device's video ports was tested. This was tested with a single open video cable that was connected to a tested port and probed; once the reading was collected. As the design and implementation of each video port is identical, there is not a feasible scenario in which unidirectionality would only be violated for some ports and not others;

The evaluator verified the TOE could read the EDID from the connected monitor during power-up and only on power-up. The evaluator connected a different monitor and verified that the EDID value did not change until the TOE was power cycled.

The evaluator attempted to send video data through the TOE in the reverse direction and verified the TOE blocked the video. The evaluator also verified that the SYNC signal is not present on the designated pin on the computer port for each of the supported display types when video data is attempted to be forced through the peripheral video port.

PSD:VI

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

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

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

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

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

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

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

Step 6: Reboot the TOE and repeat step 3.

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

Step 8. Restart the TOE and repeat step 3.

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

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

Step 11: Collect all 20 captured EDID files, compare them bit-by-bit, and verify that they are identical.

For this test, the evaluator employed a sampling strategy per TD0593. Each distinct video protocol was tested, but only a single port was tested per device. This is because the test in question is meant to demonstrate that arbitrary data cannot be written to the TOE's EDID memory (and by extension, a connected peripheral monitor) in such a way that it could be retransmitted back to a different computer that is subsequently connected to the same port. This is therefore an example of where sub-protocol

filtering rules would be violated, so this functionality is partially addressed by FDP_APC_EXT.1 Test 3-VI already.

The evaluator connected the TOE to a computer with the ability to write I2C data to the EDID range. The evaluator then verified that the TOE prevented the monitor's EDID data from being changed when the computer and monitor were connected to the TOE and various EDID manipulation operations were attempted. The evaluator connected a second computer to the same port and observed that the same EDID data was written to the computer, therefore showing that the attempts to modify the stored EDID data were unsuccessful.

2.1.1.2 FDP_PDC_EXT.1 Peripheral Device Connection

2.1.1.2.1 TSS Evaluation Activities

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

[ST] Section 6.2.6 defines the supported peripheral types as follows:

- Audio: analog audio output devices, per section 6.2.6 of [ST] (the ST introduction makes it clear that this refers to 3.5mm analog audio).
- Keyboard/Mouse: USB keyboard and mouse (standard 108-key US keyboard and 2-button, 3-button, and 5-button wired mouse or trackball), per section 6.2.6 of [ST].
- User Authentication Devices: USB smart card or CAC reader, per section 6.2.6 of [ST].
- Video/Display Devices: DisplayPort, DVI-I, or HDMI monitor, per section 6.2.6 of [ST]. It is clear from the TOE overview that that the supported video type(s) and number of console video ports (e.g., single/dual head) depend on TOE model.

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

Section 6.2.6 of [ST] summarizes the TOE external interfaces. This includes peripheral interfaces for analog audio, keyboard/mouse, user authentication, and video/display devices. The various tables in the introductory materials map these interfaces to console and peripheral ports of the TOE. The TOE's console (peripheral) ports are identical to the corresponding computer ports.

Section 6.2.6 of [ST] states that wireless keyboard/mouse devices are not supported by the TOE. Wireless transmission of all other peripheral types is assumed to be prevented by A.NO_WIRELESS_DEVICES because such devices would not present themselves to the TOE differently from wired devices of the same type and therefore the TSF has no innate capability to prevent their usage.

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

Appendix E of [PSD PP] defines the following unauthorized devices and protocols:

- USB Mass Storage Device
- Any unauthorized device connected to the PSD through a USB hub
- PS/2

Section 6.2.6 of [ST] states that only USB host peripheral devices are accepted on the keyboard/mouse ports via firmware so there is no mechanism for any unauthorized device types (including USB mass storage devices) to be accepted by this interface. Section 6.2 of [ST] indicates that the TOE supports the following types of devices: USB Keyboard and Mouse, analog audio speakers, USB smart card / CAC readers, and depending on model, DisplayPort, HDMI or DVI-I display. All other devices are rejected.

Section 6.2.6 of [ST] states that non-HID functions of a composite device, internal hub, and USB CAC hub are not supported by the TOE. It is implicit from this statement that USB mass storage devices are not supported, nor can USB hubs be used as a vehicle for the TSF to recognize a peripheral that would normally not be authorized.

[ST] does not reference PS/2 in its explicit enumeration of supported ports and interfaces and so is assumed not to be supported by the TOE. This is further supported by a port diagram of a representative TOE model (Figure 1) that does not show any PS/2 ports on the device.

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

The evaluator reviewed [ST] and identified that it describes peripheral interfaces for analog audio out, video, USB keyboard/mouse, and USB CAC devices. There is no reference to other security-relevant peripheral interface types. The evaluator separately reviewed product documentation (e.g., operational guidance and marketing materials on vendor website). In no cases were separate physical interfaces observed to have been omitted from [ST].

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

N/A

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

N/A

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

N/A

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

N/A

2.1.1.2.2 Guidance Activities

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

[User] **Chapter 1, Introduction, Overview** provides images of the ATEN Secure KVM Switches. Each connection and port type. Tables below the images provide an explanation of the numbered connections with a matching description.

[User] **Chapter 2 Hardware Setup, Section Installation Diagram** provides a diagram that illustrates how to connect the peripheral components to the KVM switch and the KVM switch to the computers.

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

[User] **Chapter 1, Introduction, Overview, Requirements** describes the required peripheral components:

- Console: describes the required peripheral components.
- Computers: describes the required ports on the computers.
- Cables: The KVM cable sets, which are specifically designed to work with this switch, are not supplied in the package and require a separate purchase.

[User] **Chapter 1, Introduction, Overview, Features** provides a description of the features and usage provided by KVMs.

[User] **Chapter 1, Introduction, Overview, Components** provides images of the ATEN Secure KVM Switches and provides a description of each connection and port type. Tables below the images provide an explanation of the numbered connections with a matching description providing.

[User] **Chapter 1, Introduction, Overview, Operating Systems** suggests the computer operating systems consisting of: Windows, Linux, UNIX, Novell, Mac, and DOS.

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

[User] **Chapter 1, Introduction, Overview, Features** provides a warning that the KVM switch supports analog audio (speaker only). Only unidirectional speaker data is allowed preventing the passage of the analogue audio by microphone input or line input. The ATEN Secure KVM Switch does not convert digital audio to analogue audio.

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

[User] **Chapter 2 Hardware Setup, Always use qualified and authorized peripheral devices** describes the visual or auditory indications provided to a user when the TOE rejects the connection of a device:

- ATEN Secure KVM Switch supports only standard USB devices (or pointing device). Do not connect a wireless keyboard/mouse, or any keyboard/mouse with an internal USB hub or composite device with Non-HID functions to the switch.
- If a non-qualified keyboard is connected, the keyboard will not function. No keystrokes will be seen on the screen.
- If a non-qualified mouse is connected, the mouse will not function. No cursor movement will be seen on the screen.
- The USB CAC port by default only supports authorized user authentication devices such as USB Smartcard or CAC readers. Do not connect other USB devices to the USB CAC port. Non-qualified or non-authorized USB devices will be rejected. Only appropriate qualified USB authentication devices (e.g., Smart Card and CAC readers by default) can be plugged into this port. During KVM operation, non-qualified or non-authorized USB devices will be filtered and rejected (the CAC LED that has port focus will flash).
- Always use a qualified monitor. Non-qualified monitors will be rejected (Video LED flashes).

[USER] **Chapter 3 Operation, LED Display** describes the visual or auditory indications provided to a user when the TOE rejects the connection of a device as shown in the table below:

LED	Indication
Video LED (on the Secure KVM switch)	The LED flashes when a non-qualified monitor is connected.
CAC LED (on the Secure KVM switch and the RPS) CAC models only	Flashes to indicate that a non-qualified USB Smart card / CAC reader is connected when the corresponding port has the focus.

Flashes to indicate that a non-qualified USB HID device is connected to console USB keyboard port or mouse port when the corresponding port has the focus.

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

N/A

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

[User] Chapter 2 Hardware Setup, Section Always **use qualified and authorized peripheral devices** describes the authorized devices for use and description of the non-authorized devices.

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

[User] **Chapter 2 Hardware Setup, Section Always use qualified and authorized peripheral devices** describes the authorized devices for use and description of the non-authorized devices.

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

[User] **Chapter 2 Hardware Setup, Section Always use qualified and authorized peripheral devices** describes the authorized devices for use and description of the non-authorized devices.

2.1.1.2.3 Test Activities

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

The evaluator observed the TOE and verified that the TOE only supported acceptable external wired interfaces, USB, Power, and video (DVI-I, HDMI, DisplayPort).

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

The evaluator examined the TOE design materials and observed no wireless interfaces. The evaluator checked for wireless certifications and found none.

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

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

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

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

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

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

Step 5: Verify the device is rejected.

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

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

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

Step 9: Verify the device is rejected.

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

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

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

Step 13: Verify the device is rejected.

The evaluator connected a USB mass storage device to the TOE and verified that the TOE rejected the device. The evaluator connected the USB mass storage device to the TOE through a USB hub and verified the TOE rejected the device. This was done for both the keyboard/mouse peripheral ports and the CAC peripheral port. The evaluator verified there are no PS/2 ports on the TOE to connect a PS/2 device to.

PSD:AO

Test 1-AO

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

For this test, verify device rejection through TOE user indication in accordance with the operational user guidance or an immediate cessation of traffic following device detection or enumeration, or incompatibility of the device interface with the peripheral interface.

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

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

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

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

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

The evaluator connected a microphone to the TOE and attempted to send audio data through the TOE. The evaluator verified the TOE did not permit any audio data from a microphone to traverse the TOE.

PSD:KM

Test 1-KM:

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

For this test, verify device rejection through TOE user indication in accordance with the operational user guidance, an immediate cessation of traffic following device detection or enumeration, no traffic captured on the USB sniffer or analyzer software other than NAK transactions or system messages, or incompatibility of the device interface with the peripheral interface. Also verify device rejection through examination of the USB sniffer or analyzer software for no traffic captured other than NAK transactions or system messages and through examination of the real-time hardware console for no display of new USB devices (recognized or not recognized).

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

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

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

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

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

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

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

Step 5: Verify the device is rejected.

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

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

The evaluator verified the TOE rejected each of the specified USB devices with and without a USB hub device present.

PSD:KM

Test 2-KM:

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

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

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

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

Step 2: Ensure the TOE is powered off.

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

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

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

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

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

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

The evaluator verified the TOE accepted each of the specified devices and each of the devices performed their designated purpose.

PSD:UA

Test 1-UA: Unauthorized Device Rejection

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

This test verifies that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections.

For this test, verify device rejection through TOE user indication in accordance with the operational user guidance, an immediate cessation of traffic following device detection or enumeration, no traffic captured on the USB sniffer or analyzer software other than NAK transactions or system messages, or incompatibility of the device interface with the peripheral interface. Also verify device rejection through examination of the USB sniffer or analyzer software for no traffic captured other than NAK transactions or system messages and through examination of the real-time hardware console for no display of new USB devices (recognized or not recognized).

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

Repeat this for each user authentication TOE peripheral interface.

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

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

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

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

Step 5: Verify the device is rejected.

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

The evaluator verified that the TOE rejected each of the unauthorized devices specified after device enumeration. The evaluator verified that when a USB hub is present, the device is still rejected.

PSD:UA

Test 2-UA: Authorized Device Acceptance

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

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

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

Step 1: Ensure the TOE is powered off.

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

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

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

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

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

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

The evaluator verified that the TOE accepted the authorized devices and that each of the authorized devices actually worked as intended.

PSD:VI

Test 1-VI: The evaluator shall verify that the TOE ports do not reject authorized devices and devices with authorized protocols as per the Peripheral Device Connections appendix in MOD_VI_V1.0.

Repeat this test for each of the selected protocols in FDP_PDC_EXT.3.1/VI:

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

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

Step 3: Ensure the TOE is powered off.

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

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

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

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

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

Step 9: Verify that the device displays the same image as in step 1 and 6.

The evaluator verified that the TOE was able to transmit the video data for each supported video type. The evaluator repeated this test for different video protocols as needed to show that all supported video types work as intended, based on the individual protocols that are supported by each of the tested TOE models.

2.1.1.3 FDP_RIP_EXT.1 Residual Information Protection

2.1.1.3.1 TSS Evaluation Activity

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

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

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

[ST] Appendix A contains the required letter of volatility. The letter covers the system controller, host controller, system EEPROM, system Flash, EDID emulator, and DP video controller. For each component, the manufacturer, part number, memory type, and memory size is specified.

Of the listed components, only the embedded RAM of the system controller and the embedded RAM of the Host Controller may contain user data, defined by [ST] as user keyboard/mouse inputs. This RAM is cleared when the TOE is unpowered or reset, when the tamper detection mechanism is triggered, or when a port is switched.

This section also states that all components are powered only by the TOE.

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

In addition to the materials above, Appendix A of [ST] identifies the system EEPROM, system Flash, EDID emulator, and DP video controller as being the TOE's only non-volatile storage. These are understood not to contain user data, both because of [ST]'s assertion that they do not, and because the actual data stored in these locations are identified as follows:

- System EEPROM – stores user configuration, TOE settings, and audit data (not considered to be user data per the claimed PP). The EEPROM does not contain user data.
- System Flash – stores unmodifiable firmware code. The Flash does not contain user data.
- EDID emulator – stores qualified EDID data. The EDID ROM does not contain user data.
- DP video controller – stores DP video controller code (as noted in [ST], this component is only present on TOE models with a DP interface). The Flash does not contain user data.
- Internal EDID RAM – The switch's internal EDID RAM does not contain user data.

2.1.1.3.2 Guidance Activities

There are no guidance Evaluation Activities for this component.

2.1.1.3.3 Test Activities

There are no test Evaluation Activities for this component.

2.1.1.4 FDP_SWI_EXT.1 PSD Switching

2.1.1.4.1 TSS Evaluation Activity

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

This activity is N/A; [ST] does not include this selection.

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

Section 6.2.10 of [ST] states that the TOE is switched through either a push button on the TOE device itself or through a channel selection on the wired remote control. Both of these are deliberately actuated selection mechanisms that would not accidentally be triggered through normal usage of connected peripherals.

2.1.1.4.2 Guidance Activities

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

[User] **Chapter 3 Section Operation, Manual Switching** states that the ATEN Secure KVM Switch offers manual port switching only. Press and release a port selection pushbutton (on the switch, or on the Remote Port Selector (RPS) if connected and aligned) to bring the KVM focus to the computer attached

to its corresponding port. To meet maximum security and channel isolation requirements, the keyboard, mouse, video, audio, and USB CAC reader ports will be switched together.

The term “aligned” defined in the ST states that aligned is defined as detected and accepted the connection by the KVM.

2.1.1.4.3 Test Activities

There are no test Evaluation Activities for this component.

N/A

2.1.2 Protection of the TSF (FPT)

2.1.2.1 FPT_FLS_EXT.1 Failure with Preservation of Secure State

This SFR is evaluated in conjunction with FPT_TST.1.

2.1.2.2 FPT_NTA_EXT.1 No Access to TOE

2.1.2.2.1 TSS Evaluation Activity

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

Section 6.5.2 of [ST] asserts that the TOE is designed in such a manner that physical and logical access to its internal memory is prevented from unauthorized access, except that connected computers may read video EDID memory, and authorized administrators may read configuration and audit data.

2.1.2.2.2 Guidance Activities

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

[Admin] **Chapter 3 Operation, Section Administrator Functions** states that Administrator functions of the ATEN Secure KVM Switch enable authorized administrators to configure the switch, configure the user authenticated devices or HID device filters, and audit log data generated by the Secure KVM Switch. An administrator must first log in and be authenticated to use the Secure KVM Switch administrator functions.

- Log Data Audit: This function enables authorized administrators to view log data and events generated by the Secure KVM Switch. The Log Data Audit function is enabled as soon as the Secure KVM Switch is manufactured. This capability cannot be terminated; it is not affected by KVM power-cycle, KVM Reset, or Reset KVM to Default.
- User Authentication Device and HID Device filtering configuration: This function enables authorized administrators to assign a whitelist and blacklist for the user authenticated devices, and a blacklist for HID devices.
- Secure KVM Configuration: This function enables authorized administrators to perform functions such as reset to factory default.

An administrator must first log in and be authenticated to use the Secure KVM Switch administrator functions.

2.1.2.2.3 Test Activities

There are no test Evaluation Activities for this component.

2.1.2.3 FPT_PHP.1 Passive Detection of Physical Attack

2.1.2.3.1 TSS Evaluation Activity

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

Section 6.5 of [ST] states that the TOE chassis has two tamper-evident labels protecting against opening the enclosure and that the wired remote control also has a label of its own. Removal of the tamper seals will indicate potential tampering from the visible reside left by the removed seals. [ST] does not explicitly state this but it is implicit in the definition of tamper labels.

Section 6.5.3 of [ST] states that if a mechanical intrusion is detected on the switch, the switch (without RPS connected) will be permanently disabled and all the front panel LEDs (except the Power LED) will flash continuously. A mechanical intrusion is detected by a pressure switch that trips when the enclosure is opened. If a mechanical intrusion is detected by the RPS (connected with the switch and aligned), this will permanently disable both the RPS itself and the switch, and all LEDs (on RPS) and the front panel LEDs except the Power LED (on switch) will flash continuously. To disable the KVM in the event of an aligned RPS, the RPS will send a "tampering command" to the KVM.

2.1.2.3.2 Guidance Activities

The evaluator shall verify that the operational user guidance describes the mechanism by which the TOE provides unambiguous detection of physical tampering and provides the user with instructions for verifying that the TOE has not been tampered with.

[User] **Chapter 2 Hardware Setup, Section Tampering prevention and detection** 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 following are identified:

- The ATEN Secure KVM Switch and the optional Remote Port Selector (RPS) include tamper-evident tape to provide visual indications of intrusion to the switch/ RPS enclosure. If the tamper-evident seal is missing, peeled, or looks as if it has been adjusted, avoid using the product and contact an ATEN dealer.
- The ATEN Secure KVM Switch and ATEN RPS are equipped with active always-on chassis intrusion detection:
    - If a mechanical intrusion is detected on the switch, the switch (without RPS connected) will be permanently disabled and all the front panel LEDs (except the Power LED) will flash continuously.
    - If a mechanical intrusion is detected by the RPS (connected with the switch and aligned), this will permanently disable both the RPS itself and the switch, and all LEDs (on RPS) and the front panel LEDs except the Power LED (on switch) will flash continuously.

If the switch or RPS enclosure appears breeched or all the LEDs are flashing continuously, the administrator is advised to stop using it, remove it from service immediately and contact your ATEN dealer.

2.1.2.3.3 Test Activities

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

The evaluator verified that the TOE possessed tamper evident seals and the labels could not be removed without providing any indication that the seal has been tampered. The evaluator verified that when the TOE's housing was tampered with, the TOE provided a visual that the device had been tampered.

Active anti-tamper testing is covered in FTP_PHP.3 testing.

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

The evaluator verified that the visual warnings of the housing tamper detection could not be disabled.

2.1.2.4 FPT_TST.1 TSF Testing

2.1.2.4.1 TSS Evaluation Activity

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

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

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

[ST] section 6.5.5 states that the TSF performs the following self-tests upon power on, reboot, or execution of a factory reset:

- Firmware integrity: the TOE validates the integrity of firmware by calculating the checksum of the firmware binary file and comparing to a pre-calculated value that is stored in the TOE.
- Accessibility of internal memory of the micro-controller: the TOE writes a block of predefined data to SRAM and then reads the block out to compare if it is identical.
- Computer interfaces isolation functionality: the TOE validates correct functionality of isolation by generating data flow on one port and checking that it is not received on another port.
- Key stuck test (KVM front panel Push button jam test): the TOE will check that the status of all button values in the micro-controller to ensure the push buttons are operational.
- Anti-tampering mechanism test: the TOE will verify if the tamper detection switch is triggered (includes KVM and RPS battery is damaged or exhausted tests).
- RPS (wired remote) connection self-tests.

It is clear from this list that the self-tests required by the claimed PP are performed.

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

[ST] section 6.5.5 identifies all of the TOE self-tests. Every self-test results in a visual indicator on the TOE or its remote control, depending on the component that experiences a self-test failure. All self-tests result in a shutdown of the TSF (the TOE itself remains on in a failure state but does not allow any security-relevant functionality) except for the following:

- If a wired remote control that is already experiencing a failure state is connected to the TOE chassis, the TOE chassis will remain functional but the remote control will remain inoperable. This does not affect the TSF because the TOE can function normally without a remote control connected and the TSF does not interface with the remote control while it is in a failure state, which means that a compromised remote control cannot be used as a vector to operate the TOE maliciously.
- A stuck button self-test failure may be a temporary state that is induced by the position of the button. This situation may be resolved by following troubleshooting guidance and restarting the TOE. The TOE does not perform any security-relevant functionality while the push button self-test fails, but will resume functionality upon successful clearing of the self-test failure state if the failure was due to a temporary issue and not a mechanical failure of the button itself.

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

Section 6.5.5 of [ST] indicates that when a key stuck self-test failure occurs, the port LED and CAC LED of the stuck port will both flash. For all other self-test failures on the TOE chassis, all front panel LEDs except for the power indicator will flash repeatedly. If a self-test failure of the wired remote control occurs, all LEDs on the remote will flash.

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

Section 6.5.5 of [ST] states that users can verify the integrity of the TOE by triggering a self-test (e.g., by powering on or rebooting the TOE) and examining the front panel LEDs for self-test failures.

2.1.2.4.2 Guidance Activities

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

[User] **Chapter 3 Operation, Section Powering On** and [Admin] **Chapter 3 Operation, Section Powering On** describes when a KVM switch performs self-tests, how the switch behaves during the self-tests, and what happens when a self-test fails. Section *Powering On* describes two indications of self-test failures:

a. Pushbutton jam: The jammed port's LEDs will flash.

b. All other self-test failures: All front panel LEDs (except the Power LED) flash continuously;

A KVM switch becomes inoperable if a self-test fails. The section includes instructions to attempt recovery from a self-test failure. [Admin] **Chapter 3 *Operation* section Log Data Audit** identifies self-test failures as critical audit data.

[Audit] The vendor provides guidance on audit records. This guidance identifies audit logs that are relevant to self-test functionality.

2.1.2.4.3 Test Activities

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

The evaluator jammed one of the buttons while powering on the TOE and verified that the TOE entered a failure state that lasted until the TOE was rebooted and the jammed button was resolved. The evaluator verified that the TOE did not perform any functionality until the failure state was left.

The self-test failure for tamper detection is tested as part of FPT_PHP.3 below. The other self-test failures (modified firmware and data flow violation) cannot be induced without some substitution or deliberate modification of a physical component that would trigger the tamper detection and render the TOE inoperable.

2.1.2.5 FPT_TST_EXT.1 TSF Testing

2.1.2.5.1 TSS Evaluation Activity

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

Section 6.5.5 of [ST] indicates that when a key stuck self-test failure occurs, the port LED and CAC LED of the stuck port will both flash. For all other self-test failures on the TOE chassis, all front panel LEDs except for the power indicator will flash repeatedly. If a self-test failure of the wired remote control occurs, all LEDs on the remote will flash.

2.1.2.5.2 Guidance Activities

The evaluator shall verify that the operational user guidance:

a) describes how the results of self-tests are indicated to the user
b) provides the user with a clear indication of how to recognize a failed self-test; and
c) details the appropriate actions to be completed in the event of a failed self-test.

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

Section **Powering On** in [User] **Chapter 3 Operation** and [Admin] **Chapter 3 Operation** describes when a KVM switch performs self-tests, how the switch behaves during the self-tests, and what happens when a self-test fails. Section **Powering On** provides the following indicators of a self-test failure.

In the case of a self-test failure, the Secure KVM Switch becomes inoperable, with front panel LED combinations (on the Secure KVM) indicating the potential cause of the failure (such as button jam or KVM integrity compromise)

- A pre-defined combination of port and CAC LEDs indicate the cause of the failure.
- If all front panel LEDs on the Secure KVM (except the Power LED) flash continuously, it means KVM tampering has been detected or a self-test failure has occurred (except for Pushbutton jam).
- If Pushbutton jam has been detected, both the port's LEDs (Port LED and CAC LED) will flash.

A KVM switch becomes inoperable if a self-test fails. The section includes instructions to attempt recovery from a self-test failure. [Admin] **chapter 3 Operation section Log Data Audit** identifies self-test failures as critical audit data.

[Audit] The vendor provides guidance on audit records. This guidance identifies audit logs that are relevant to self-test functionality.

2.1.2.5.3 Test Activities

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

The evaluator jammed one of the buttons while powering on the TOE and verified that the TOE entered a failure state that lasted until the TOE was rebooted and the jammed button was resolved. The evaluator verified that the TOE did not perform any functionality until the failure state was left.

The self-test failure for tamper detection is tested as part of FPT_PHP.3 below. The other self-test failures (modified firmware and data flow violation) cannot be induced without some substitution or deliberate modification of a physical component that would trigger the tamper detection and render the TOE inoperable.

2.2 Optional SFRs

2.2.1 Security Audit (FAU)

2.2.1.1 FAU_GEN.1 Audit Data Generation

2.2.1.1.1 TSS Evaluation 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.

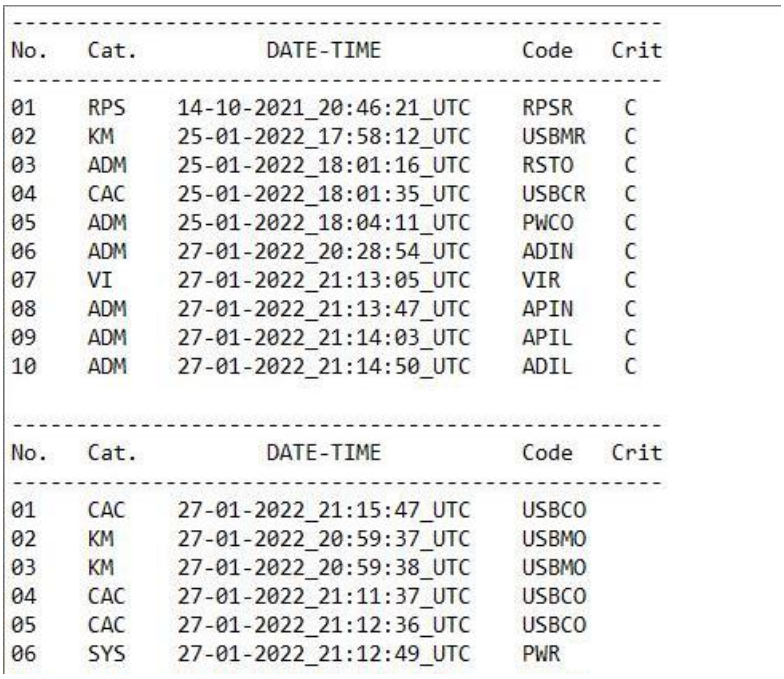
Section 6.1 of [ST] identifies the auditable events for the TOE and divides them into critical and non-critical types. For each audit record, this section also states that audit records include date, time, outcome of the event, and event type code. This section also describes how an administrator can read the stored audit logs and states that critical and non-critical event types are each stored in separate logs that store up to 32 events of that type; any additional events cause a FIFO rollover of the log entries.

2.2.1.1.2 Guidance Activities

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

[Admin] states in **Chapter 3 Operation, Section Administrator Functions** that the Log Data Audit function enables authorized administrators to view log data and events generated by the Secure KVM Switch. The Log Data Audit function is enabled as soon as the Secure KVM Switch is manufactured. This capability cannot be terminated; it is not affected by KVM power-cycle, KVM Reset, or Reset KVM to Default.

[Audit] The vendor provides guidance on audit records. The **Log/Event Audit code** table identifies the log codes and a description of each log code. The following is an example of the audit listing that can be generated by an administrator.



```
--------------------------------------------------
No.   Cat.          DATE-TIME           Code   Crit
--------------------------------------------------
01    RPS    14-10-2021_20:46:21_UTC    RPSR   C
02    KM     25-01-2022_17:58:12_UTC    USBMR  C
03    ADM    25-01-2022_18:01:16_UTC    RSTO   C
04    CAC    25-01-2022_18:01:35_UTC    USBCR  C
05    ADM    25-01-2022_18:04:11_UTC    PWCO   C
06    ADM    27-01-2022_20:28:54_UTC    ADIN   C
07    VI     27-01-2022_21:13:05_UTC    VIR    C
08    ADM    27-01-2022_21:13:47_UTC    APIN   C
09    ADM    27-01-2022_21:14:03_UTC    APIL   C
10    ADM    27-01-2022_21:14:50_UTC    ADIL   C

--------------------------------------------------
No.   Cat.          DATE-TIME           Code   Crit
--------------------------------------------------
01    CAC    27-01-2022_21:15:47_UTC    USBCO
02    KM     27-01-2022_20:59:37_UTC    USBMO
03    KM     27-01-2022_20:59:38_UTC    USBMO
04    CAC    27-01-2022_21:11:37_UTC    USBCO
05    CAC    27-01-2022_21:12:36_UTC    USBCO
06    SYS    27-01-2022_21:12:49_UTC    PWR
```

The interpretation of these audit codes must be referenced to [Audit] to determine their meaning.

[Audit] Section **About this Admin Log Audit Code** contains a note that identifies and explains what audit records that cannot be viewed by an administrator.

> **Note**: The following audit codes are generated which result in the Secure KVM Switch becoming inoperable. These Log/Event data logs can only be decoded by the Secure KVM Switch manufacturer.
>
> - ADML – KVM locked due to Administrators' failed login
> - IHWN – H/W integration test failed
> - SUMN – Checksum test failed
> - MEMN – Memory test failed
> - ISON – Self-test port data check failed (different from jammed button BTNJ)
> - TMPH – Anti-Tamper triggered
> - TMPR – Anti-Tamper triggered by RPS

2.2.1.1.3 Test 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 the TOE is capable of generating audit records for the identified functions and that they include the required details.

2.2.2 User Data Protection (FDP)

2.2.2.1 FDP_RIP_EXT.2 Purge of Residual Information

2.2.2.1.1 TSS Evaluation Activities

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

Section 6.2.9 of [ST] states that when Reset to Factory Default is engaged, the TOE terminates the active administrator session, restores all configuration settings and data to their original state (except for audit data, which is retained along with a log indicating the restore operation was performed), purges keyboard/mouse buffer data, and reboots the TOE.

This section also describes the TOE's reset button feature, which purges the keyboard/mouse buffer, sets the CAC interface to enabled, performs a self-test, and switches the input to port 1; this function acts as a volatile memory purge and does not affect other configuration settings or log data.

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

For each TOE component listed in Appendix A of [ST], a statement is included for the effect that the Restore Factory Default function has on it.

2.2.2.1.2 Guidance Activities

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

[User] **Chapter 1 Introduction, Section Components** states that pressing the *Reset Button* will reset the ATEN Secure KVM Switch. A reset is activated by pressing the *Reset Button* for more than 5 seconds, the keyboard/mouse buffer will be purged and the switch will reboot and perform a self-test. After a successful self-test, port focus will be switched to port 1, and the CAC function of each port will be set to factory default setting (enabled).

[Admin] **Chapter 3 Operation, Section Reset KVM to Default (Restore KVM to Factory Default)** that describes the administrator function which enables the authorized administrator to reset the Secure KVM Switch configuration to the factory default settings.

1. When the administrator performs Reset KVM to Default, settings previously configured by the administrator (such as USB device whitelist/blacklist and HID device blacklist) will be cleared and reset to the factory default settings.
2. Once Reset KVM to Default has been completed, the Secure KVM Switch will terminate the administrator logon mode, purge keyboard/mouse buffers, and power cycle the Secure KVM Switch automatically. After a successful self-test, the KVM port focus will be switched to Port 1, and the CAC function of each port will be set to the factory default (enabled).
3. Reset KVM to Default will not affect or erase the log data.
4. Reset KVM to Default will not affect the previously changed administrator password.
5. Reset KVM to Default will clear the whitelist/blacklist created by both the Secure KVM administrator functions and the ATEN Port Authentication Utility.

2.2.2.1.3 Test Activities

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

The evaluator verified that the TOE is able to perform a factory reset and remains in a secure state after the factory reset.

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

The evaluator verified that the factory reset did not clear the audit logs and that the logs were still present.

2.2.3 Identification and Authentication (FIA)

2.2.3.1 FIA_UAU.2 User Authentication Before Any Action

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

2.2.3.2 FIA_UID.2 User Identification Before Any Action

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

2.2.4 Security Management (FMT)

2.2.4.1 FMT_MOF.1 Management of Security Functions Behavior

2.2.4.1.1 TSS Evaluation Activities

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

Section 6.3 of [ST] states that management functions are accessed by an authorized administrator entering the Administrator Logon mode and entering a valid password.

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

This is N/A; the TSF only provides an administrator role.

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

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

Section 6.4.1 of [ST] addresses the points above as follows:

a) There is no login name for the login function; there is just a single administrator account

b) Passwords must contain at least one each of lowercase letter, uppercase letter, number, and special character, and be between 8-22 characters in length.

c) There is no mechanism to restore a lost or forgotten password.

d) The TOE has a default password that is changed after the first successful logon with the default password.

e) Three consecutive failed login attempts results in a 15 minute lockout; nine failed attempts result in the TOE being rendered inoperable.

f) The management functions assigned in FMT_MOF.1.1 are all described in this section.

2.2.4.1.2 Guidance Activities

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

In [Admin] **Chapter 3 Operation, section Administrator Functions** identifies functions that require a user to authenticate as the administrator. These functions are:

- User Authentication Device filtering configuration: enables an authorized administrator to assign whitelist and blacklist for user authentication devices.
- Secure KVM configuration: enables an authorized administrator to reset KVM to factory default and change administrator password.
- Log data audit: enables an authorized administrator to download, view, and audit log data.

[Audit] covers administrator functions for managing device blacklist/whitelist, reset to factory default, and change administrator password. [PAU] describes configuration of device blacklist/whitelist in detail under the **Port Authentication Utility Operation** heading.

2.2.4.1.3 Test Activities

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

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

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

Step 4: Log off from the TOE.

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

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

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

The evaluator logged on to the TOE using default credential data and verified that all management functions were available and had the intended effect when performed.

The evaluator verified that management functions were not accessible prior to authentication or when an invalid credential is entered.

2.2.4.2 FMT_SMF.1 Specification of Management Functions

2.2.4.2.1 TSS Evaluation Activities

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

[ST] section 6.4.2 identifies the management functions claimed in FMT_SMF.1 (modify TOE user authentication device filtering whitelist and blacklist, modify TOE keyboard and mouse filtering blacklist, reset to factory default, view audit logs, change password).

2.2.4.2.2 Guidance Activities

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

FMT_SMF.1 specifies the following management functions:

- Modify TOE user authentication device filtering whitelist and blacklist
- Modify TOE keyboard and mouse filtering blacklist
- Reset to Factory Default
- View audit logs
- Change password

In [Admin] **Chapter 3 Operation, Section Administrator Functions** identifies functions that require a user to authenticate as the administrator. These functions are:

- User Authentication Device filtering configuration: enables an authorized administrator to assign whitelist and blacklist for user authentication devices.
- Secure KVM configuration: enables an authorized administrator to reset KVM to factory default[1].
- Log data audit: enables an authorized administrator to download, view, and audit log data.

Section **Chapter 3 Operation, Section Administrator Functions** includes instructions to:

- Set up a computer for switch management,
- Put a switch into Administrator Logon mode,
- Logon as an administrator from the management computer, and
- Display a list of administrator functions.

[Audit] documents the available management functions in addition to describing audit events and audit record formats. [Audit] covers functions for managing device blacklist/whitelist, reset to factory default, and change administrator password. [PAU] describes the Port Authentication Utility, which provides

[1] Reset is an administrative interface in addition to the reset button on the KVM switch front panel.

administrators another method to configure user authentication device qualification lists. [PAU] includes instructions to:

- Set up a computer to run the utility,
- Logon to the utility,
- Use the utility to manage blacklist and whitelist rules,
- Prepare a switch to retrieve device information,
- Retrieve device information from a switch,
- Prepare a switch for upload,
- Upload blacklist and whitelist rules to the switch,
- Change the password for the utility, and
- Exit the utility.

Device information retrieval and blacklist/whitelist rule upload require authenticated, administrative logon to the KVM switch.

2.2.4.2.3 Test Activities

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

The evaluator verified that the TOE was capable of performing each of the claimed management functions.

2.2.4.3 FMT_SMR.1 Security Roles

Refer to the Evaluation Activities of FMT_MOF.1.1 above.

2.2.5 Protection of the TSF (FPT)

2.2.5.1 FPT_PHP.3 Resistance to Physical Attack

2.2.5.1.1 TSS Evaluation 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.

Section 6.5.3 of [ST] states that physical tampering is detected by the TSF if the enclosure of the TOE chassis or wired remote control is opened or if the battery is damaged or exhausted. This section also states that the device becomes permanently disabled when this occurs. When the wired remote control is connected to the TOE, tampering of the remote control will also disable the chassis to which it is connected. Additionally, this section states that the anti-tamper function is triggered when the battery is exhausted, and that the battery is rated for a minimum life of 5 years.

2.2.5.1.2 Guidance Activities

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

[User] **Chapter 3, Operation, Chassis Intrusion Detection** states:

To help prevent malicious tampering with the ATEN Secure KVM Switch, the switch (or the RPS) becomes inoperable and all front panel LEDs on the Secure KVM switch (except Power) or all Remote Port Selector (RPS) LEDs flash constantly when a chassis intrusion (such as the cover being removed) is detected (by the switch or by the RPS).

The intrusion detection protection is an always-on function. If all front panel LEDs on the Secure KVM Switch (except Power) flash continuously, all Remote Port Selector (RPS) LEDs flash, or either enclosure appears breached, avoid using the product and contact your ATEN dealer.

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

[User] and [Admin] repeatedly warn the user the KVM switch has active, always-on chassis intrusion detection security, which will permanently disable the switch in response to any attempt to open the enclosure.

2.2.5.1.3 Test Activities

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

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

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

The evaluator attempted to access the internal circuitry of the TOE and verified that the TOE tamper detection was triggered when the attempt was made. The evaluator verified that the tamper indication could not be disabled.

The evaluator observed that attempting to gain internal access to a Remote Port selector (RPS) accessory, while connected to the TOE resulted in both the RPS and the Physical device becoming tampered.

The evaluator shall perform the following steps:

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

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

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

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

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

The evaluator used a device provided by the vendor had disabled the housing tamper functionality so the evaluator could gain access to the internal circuitry but with all tamper functions still enabled. The evaluator attempted to remove the backup battery and verified that the TOE tamper response was triggered when the battery was removed and could not be reset.

2.2.5.2 FPT_STM.1 Reliable Time Stamps

2.2.5.2.1 TSS Evaluation Activities

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

Section 6.5.4 of [ST] states that the TOE provides its own internal clock.

The developer sets the time to UTC (Coordinated Universal Time) during manufacturing.

2.2.5.2.2 Guidance Activities

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

[Admin] **Chapter 3 Operation, Section Log Data Audit** states that the internal battery inside the KVM ensures that the clock is active at all times and allows for accurate time recordings for all events. The initial date is set in each KVM manually at the time of manufacturing.

2.2.5.2.3 Test Activities

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

The evaluator verified that the audit records in FAU_GEN.1 contained time stamps.

2.3 Selection-Based SFRs

2.3.1 User Data Protection (FDP)

2.3.1.1 FDP_SWI_EXT.2 PSD Switching Methods

2.3.1.1.1 TSS Evaluation Activities

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

[ST] section 6.2.10 states that switching is initiated through a push button on the TOE chassis or wired remote control.

None of the switching mechanisms involve any of the prohibited behavior (automatic port scanning, control through a connected computer, or control through keyboard shortcuts). Selection buttons are engaged through express user action.

PSD:KM

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

N/A; “peripheral devices using a guard” is not selected in FDP_SWI_EXT.2.2.

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

N/A

2.3.1.1.2 Guidance Activities

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

[User]**Chapter 3 Operation, Section Manual Switching** states that the ATEN Secure KVM Switch offers manual port switching only. Press and release a port selection pushbutton (on the switch, or on the Remote Port Selector (RPS) if connected and aligned) to bring the KVM focus to the computer attached to its corresponding port. To meet maximum security and channel isolation requirements, the keyboard, mouse, video, audio, and USB CAC reader ports will be switched together.

The operational user guidance does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms.

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

N/A; “peripheral devices using a guard” is not selected in FDP_SWI_EXT.2.2.

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

[AGD Notes]

2.3.1.1.3 Test Activities

There are no test Evaluation Activities for this component.

PSD:KM
The evaluator shall ensure that switching is always initiated through express user action using the selected mechanisms throughout testing for FDP_APC_EXT.1 above.
Additional tests for this SFR are performed in FDP_APC_EXT.1 test 1-KM above.

The evaluator verified that all switching of selected computers is the result of user action.

The evaluator verified that when the Remote Port Selector is connected to a 4 port device, the 5-8 buttons on the Remote port selector do not work.

PSD:UA

Test performed in FDP_APC_EXT.1 above.

2.3.2 TOE Access (FTA)

2.3.2.1 FTA_CIN_EXT.1 Continuous Indications

2.3.2.1.1 TSS Evaluation Activities

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

Section 6.6.1 of [ST] states that upon successful power on or reset, computer 1 is the selected computer by default.

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

Section 6.6.1 of [ST] documents that the TOE chassis and wired remote control both have LEDs accompanying each port selection button that indicate when a computer is connected (dim orange) and selected (bright orange). There are also green LEDs that perform a similar function for the CAC port; all interfaces are switched in tandem but the CAC port can be enabled/disabled separately from the other peripherals. This section also states that the indicators between the TOE chassis and the wired remote are synchronized.

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

N/A

2.3.2.1.2 Guidance Activities

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

[User] **Chapter 3 Operation, Section Powering On** and [Admin] **Chapter 3 Operation** indicates a KVM switch connects peripherals to computer port 1 after power on, power cycle, or reset.

Each KVM switch has a reset button. In [User] **Chapter 1 Introduction, Section Components** describes the reset function. In [Admin] **Chapter 3 Operation, Section Powering On** also describes the reset button feature.

Later in [Admin] **Chapter 3 Operation, Section Administrator Functions** identifies Reset KVM to Default as a Secure KVM Configuration administrator function. Section **Administrator Functions** describes what information Reset KVM to Default clears (such as USB device whitelist/blacklist) and what information reset does not clear (such as audit records and administrator password).

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

[User] **Chapter 3, Operation, Manual Switching** documents the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.

For increased security, the ATEN Secure KVM Switch offers manual port switching only. This is achieved by pressing the port selection pushbuttons located on the switch front panel or pressing the port selection pushbuttons located on the RPS' panel (if RPS is connected and aligned) Press and release a port selection pushbutton to bring the KVM focus to the computer attached to its corresponding port (see Port ID Numbering, below). To meet maximum security and channel isolation requirements, the keyboard, mouse, video, audio, and USB CAC reader ports will be switched together.

The Selected Port LED lights bright orange (on Switch and/or RPS) to indicate that the computer attached to its corresponding port has the KVM focus (keyboard, mouse, monitor, audio, and CAC reader).

PSD:VI

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

2.3.2.1.3 Test Activities

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

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

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

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

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

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

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

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

The evaluator verified that for TOE switch models, the default setting for the TOE upon power-on or reboot is that computer 1 is active. The evaluator observed that the port selection LED always indicates the selected computer for all tied peripherals.

The evaluator verified that the provided indication of the currently selected port that does not dim or disappear.

The evaluator observed that the user was able to enable and disable the CAC functionality for a particular port by holding the physical device button for 3 seconds and toggling the state.

PSD:VI

Additional testing for this component is performed in test 1-VI of FDP_APC_EXT.1 in section 2.1.1.1.3 above.

3 Security Functional Requirement Evaluation Activities (AO Module)

3.1 Mandatory SFRs

3.1.1 User Data Protection (FDP)

3.1.1.1 FDP_AFL_EXT.1 Audio Filtration

3.1.1.1.1 TSS Evaluation Activity

The evaluator shall check the TSS to verify that the TOE audio function implementation properly filters the audio passing through the TOE.

Section 6.2.1 of [ST] asserts that the TOE's audio function performs the required frequency filtration.

3.1.1.1.2 Guidance Activities

There are no guidance EAs for this component.

3.1.1.1.3 Test Activities

Step 1: Connect a computer to the TOE analog audio output peripheral interface and run audio analyzer software on it.

Step 2: For each connected computer, ensure it is selected, use its tone generator software to generate a sine wave audio tone for each of the frequencies in the Audio Filtration Specifications table and verify in the audio analyzer software that they are attenuated by at least the amount specified in the Audio Filtration Specifications table.

Step 3: Connect an oscilloscope to the TOE analog audio output peripheral interface and set it to measure the peak-to-peak voltage.

Step 4: For each connected computer, perform step 5 with the signal generator set to the following settings:

- Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed
- Signal average to 0V (negative swing)

Step 5: Set the signal generator to generate the frequencies in Audio Filtration Specifications table and verify the signal on the oscilloscope does not exceed the corresponding maximum voltage after attenuation.

The following test was done for a randomly selected computer port. The audio attenuation happens central to the TOE per its design, rather than having separate attenuators for each port. Therefore, the choice of port will not affect how the TSF implements this particular function.

The evaluator verified that the TOE attenuated the signals specified in the audio filtration specification table appropriately and the attenuated value was lower than specified in the table for all frequencies.

3.1.1.2 FDP_PDC_EXT.2/AO Authorized Devices (Audio Output)

3.1.1.2.1 TSS Evaluation Activity

There are no TSS EAs for this component.

3.1.1.2.2 Guidance Activities

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

[User] **Chapter 2 Hardware Setup, Section Always use qualified and authorized peripheral devices** describes the authorized devices for use and description of the non-authorized devices.

3.1.1.2.3 Test Activities

The evaluator shall verify that the TOE ports do not reject authorized devices and devices with authorized protocols as per the authorized peripheral device connections.
Repeat this test for each of the following devices: analog headphone, and analog speakers.
Step 1: Ensure the TOE is powered off.
Step 2: Connect the authorized device to the TOE peripheral interface.
Step 3: Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present.
Step 4: Play an audio file on the connected computer and verify the sound is heard through the authorized device.
Step 5: Disconnect the authorized device, then reconnect it to the TOE peripheral interface.
Step 6: Verify the TOE user indication described in the operational user guidance is not present.
Step 7: Play an audio file on the connected computer and verify the sound is heard through the authorized device.

This test was performed for a single randomly-selected computer port. This is because testing that comprehensively verifies that selected audio is properly transmitted to the peripheral audio interface when the proper channel is selected was performed in FDP_APC_EXT.1.

The evaluator verified that when an authorized device was connected to the TOE's peripheral audio port and a video with an audio component was playing on the connected and selected computer, the sound from the video was transmitted to the connected peripheral audio device.

3.1.1.3 FDP_PUD_EXT.1 Powering Unauthorized Devices

3.1.1.3.1 TSS Evaluation Activity

The evaluator shall verify the TSS states that the TOE does not supply power to an unauthorized device connected to the analog audio output interface.

Section 6.2.7 of [ST] states that the TOE does not supply power over the audio output interface.

The evaluator shall also verify that the TOE cannot be configured to supply power to a device connected to the analog audio output interface.

Section 6.2.7 of [ST] states that the TOE does not supply power over the audio output interface.

3.1.1.3.2 Guidance Activities

The evaluator shall verify that the guidance states that a microphone should never be connected to the TOE's analog audio output interface.

[User] **Chapter 2 Hardware Setup, Section Always use qualified and authorized peripheral devices** states that for security, the ATEN Secure KVM Switch does not support an analogue microphone or line-in audio input. Never connect a microphone or headset microphone to the audio output port. Standard analogue speakers and headsets are supported.

3.1.1.3.3 Test Activities

Step 1: Connect the amplified speakers directly to computer #1's analog audio output interface (typically green in color). Set the volume at the speakers to approximately 25%.

Step 2: Connect the computer interface audio cable to the TOE audio output computer interface and computer #1's analog audio microphone input interface (typically pink in color) instead of the computer analog audio output interface.

Step 4: Connect an open 3.5 millimeter stereo plug to the TOE analog audio peripheral interface.

Step 5: Power up the TOE and ensure computer #1 is selected.

Step 6: Measure the DC voltage of stereo plug from the TOE analog audio peripheral interface between the ground terminal and each one of the other two terminals (tip and ring) using a digital voltmeter.

Step 7: Verify the voltage is 0.2 volts or less, ensuring there is no DC bias voltage supplied to the microphone.

The evaluator connected an audio cable between one of the TOE's computer interfaces and a microphone jack on a computer and connected an open audio jack to the TOE peripheral audio out interface. The evaluator verified that the TOE supplied no DC bias voltage to the microphone and that no power was transmitted to the peripheral audio port.

3.1.1.4 FDP_UDF_EXT.1/AO Unidirectional Data Flow (Audio Output)

3.1.1.4.1 TSS Evaluation Activity

There are no TSS EAs for this component.

3.1.1.4.2 Guidance Activities

There are no guidance EAs for this component.

3.1.1.4.3 Test Activities

Note: Data is considered not to transit the TOE if no signal greater than 45 dB of attenuation at the specific audio frequency is received.

The evaluator shall perform the following test:

Step 1: Connect a computer to the TOE analog audio output peripheral interface, run its tone generator software, and run audio analyzer software on the connected computer.

Step 2: Perform steps 3-6 for each TOE analog audio output peripheral interface.

Step 3: For each connected computer, ensure it is selected, use the tone generator on the computer connected to the TOE analog audio output peripheral interface to generate the designated frequencies, and verify that the audio is not present on the selected computer's audio analyzer software.

Step 4: Replace the selected computer with an oscilloscope and connect an external audio signal generator to the TOE analog audio output peripheral interface. Perform step 5 with the signal generator set to the following settings:

- Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed;
- Signal average to 0V (negative swing)

Step 5: Set the signal generator to generate the designated frequencies, and verify the signal on the oscilloscope is 11.2 mV or less.

The following test was performed by connecting an oscilloscope to all computer ports to determine simultaneously that a generated signal on the peripheral port is not received by any computer ports, regardless of whether that port is the selected channel or not.

For step 3, the evaluator used an external signal generator and an oscilloscope to verify that the TSF does not permit any of the designated frequencies to traverse the TOE in the reverse direction (i.e., the TSF does not allow its audio output port to be misused as a microphone). This testing also demonstrated that whether or not the observed port was selected has no effect on this behavior.

For step 5, the evaluator re-transmitted the designated frequencies as only the positive voltage and negative voltage components of the signal. In this case, the sampled port did not show any voltage readings above the maximum threshold. This is sufficient to show that the voltage of the frequency does not affect whether any part of the signal is transmitted; therefore, the blocking of the frequency on the other ports is sufficient evidence that no component of the signal is transmitted over those ports under any circumstances

3.2 Optional SFRs

The AO Module does not define any optional SFRs.

3.3 Selection-Based SFRs

The AO Module does not define any selection-based SFRs.

4 Security Functional Requirement Evaluation Activities (KM Module)

4.1 Mandatory SFRs

4.1.1 User Data Protection (FDP)

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

4.1.1.1.1 TSS Evaluation Activity

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

Refer to section 2.1.1.2.1 above.

4.1.1.1.2 Guidance Activities

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

4.1.1.1.3 Test Activities

Testing of this component is performed through evaluation of FDP_PDC_EXT.1 Test 2 as specified in section 2.1.1.2.3 above.

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

4.1.1.2.1 TSS Evaluation Activity

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

Section 6.2.6 of [ST] states that USB 1.1/2.0 devices are supported for keyboard and mouse, specifically wired keyboard/keypad and wired mouse/trackball. Wireless devices are not supported, nor are non-HID functions of composite devices, USB hubs, or non-standard input devices with integrated USB hubs or other USB devices.

Section 6.2.4 of [ST] states that the keyboard/mouse USB ports have a default whitelist for allowed devices and that the TOE has a configurable blacklist to disallow a subset of the whitelisted devices; there is no separately configurable whitelist for these ports.

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

Section 6.2.4 of [ST] states that keyboard and mouse peripherals are emulated from the TOE to connected computers.

4.1.1.2.2 Guidance Activities

There are no guidance EAs for this component.

4.1.1.2.3 Test Activities

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

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

4.1.1.3.1 TSS Evaluation Activity

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

Section 6.2.6 of [ST] indicates that the TOE has embedded Caps/Num/Scroll Lock indicators and does not pass these back to the keyboard as part of enforcing unidirectional data flow.

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

Section 6.2.2 of [ST] asserts that the TOE routes keyboard/mouse data unidirectionally from the attached peripherals to the selected computer.

4.1.1.3.2 Guidance Activities

There are no guidance EAs for this component.

4.1.1.3.3 Test Activities

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

4.2 Optional SFRs

4.2.1 User Data Protection (FDP)

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

4.2.1.1.1 TSS Evaluation Activity

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

Section 6.2.4 of [ST] states that the TOE has configurable device filtration for keyboard and mouse devices.

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

Section 6.2.4 of [ST] states that the TOE has a default non-configurable whitelist of allowed HID devices such that all non-whitelisted devices are rejected by the TOE. Administrators may choose to further restrict the set of allowed devices through the configurable blacklist. If a device is present on both the blacklist and the whitelist, the blacklist takes priority.

4.2.1.1.2 Guidance Activities

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

The configurable HID device function enables authorized administrators to assign a blacklist for HID (keyboard/mouse) devices.

[Admin] **Chapter 3 Operation, Section User Authentication Device and HID Device Filtering Configuration** states that the user can only blacklist an HID device within the default HID devices* for the Keyboard/ Mouse Ports. Please connect the HID device (you would like to blacklist) directly to the Mouse Port (do not connect it to the KVM via a USB hub), and perform the configuration via administrator functions. After configuration, the blacklisted HID device will be rejected by both Keyboard/ Mouse Ports. A USB hub cannot be added to blacklist via administrator functions.

* The default HID devices for Keyboard/ Mouse Ports consist of the USB console keyboard/mouse ports by default only support the following – standard USB keyboards/mice, standard USB keyboards/mice via a USB hub, and the HID functions of a composite device. Do not connect other USB devices to the USB console keyboard/mouse ports. Non-qualified or non-authorized USB devices will be rejected.

4.2.1.1.3 Test Activities

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

The evaluator connected each of the devices on the PSD KM blacklist to the TOE one at a time and verified that the TOE rejected each of the devices.

Test 2
[Conditional: Perform this only if "configurable" is selected in FDP_FIL_EXT.1.1/KM] In the following steps the evaluator shall verify that whitelisted and blacklisted devices are treated correctly.
Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance.
Step 2: Connect to the TOE KM peripheral device interface a composite device which contains a HID class and a non-HID class.
Step 3: Configure the TOE KM CDF to whitelist the composite device.
Step 4: Verify that the HID-class part is accepted and that the non-HID class part is rejected through real-time device console and USB sniffer capture, or that the entire device is rejected.
Step 5: Configure the TOE KM CDF to blacklist the device.
Step 6: Verify that both the HID-class part and the non-HID class part is rejected through real-time device console and USB sniffer capture.

The evaluator verified that the TOE's blacklist was correctly enforced, since the TOE does not implement a whitelist and only a blacklist this was done by blacklisting a device and verifying it was rejected.

4.3 Selection Based SFRs

4.3.1 User Data Protection (FDP)

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

4.3.1.1.1 TSS Evaluation Activity

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

[ST] section 6.2.9 implies that the TOE has user data buffers for keyboard input because the described reset behavior includes purging keyboard/mouse buffers.

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

[ST] section 6.2.9 states that user keyboard data is purged when the TOE is switched to a different computer.

Additional details about this mechanism are included in the proprietary isolation document.

4.3.1.1.2 Guidance Activities

There are no guidance EAs for this component.

4.3.1.1.3 Test Activities

There are no test EAs for this component.

4.3.1.2 FDP_SWI_EXT.3 Tied Switching

4.3.1.2.1 TSS Evaluation Activity

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

Section 6.2.10 of [ST] states that all peripherals are tied to the same switch operation such that it is not possible to have different peripherals switched to different computers.

4.3.1.2.2 Guidance Activities

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

[User] **Chapter 3 Operation, Section Manual Switching** states that in order to meet maximum security and channel isolation requirements, the keyboard, mouse, video, audio, and USB CAC reader ports will be switched together.

4.3.1.2.3 Test Activities

The evaluator shall verify that the keyboard and mouse devices are always switched together to the same connected computer throughout testing in FDP_APC_EXT.1 in section 2.1.1.1.3 above.
Tests for this SFR are performed in FDP_APC_EXT.1 test 1-KM in section 2.1.1.1.3 above.

5 Security Functional Requirement Evaluation Activities (UA Module)

5.1 Mandatory SFRs

5.1.1 User Data Protection (FDP)

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

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

5.1.1.1.1 TSS Evaluation Activity

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

Section 6.2.5 of [ST] states that the CAC interface has a fixed whitelist of allowed devices that cannot be modified. This whitelist is used to restrict the port from being used by non-CAC devices. It goes on to say that the TOE also has a configurable whitelist and blacklist that supersedes the default list.

[Conditional – If "configurable" is selected in FDP_FIL_EXT.1.1/UA, then:] The evaluator shall examine the TSS and verify that it describes the process of configuring the TOE for whitelisting and blacklisting UA peripheral devices, including information on how this function is restricted to administrators.

Section 6.2.5 of [ST] states that administrators can configure whitelist/blacklist items by USB Class ID, Sub-Class, Protocol, Vendor ID, and Product ID of a USB device, and that wildcards are supported in the Product ID field.

This section defines the order of precedence for the filtration rules as follows:

1. Presence on administrator-defined blacklist (device is rejected)
2. Presence on administrator-defined whitelist (device is allowed)
3. Absence from both administrator defined lists, presence on default whitelist (device is allowed)
4. Absence from all lists (device is rejected)

The configurable device filtration function is restricted to administrators by requiring successful password authentication to the TOE's administrator account prior to its use.

5.1.1.1.2 Guidance Activities

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

[PAU] **Chapter 3 Operation** describes configuration of CAC authentication device blacklist/whitelist in detail under the **Port Authentication Utility Operation** heading.

5.1.1.1.3 Test Activities

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

The evaluator connected each of the devices on the PSD UA blacklist one at a time and verified that the TOE rejected each of the devices.

The Evaluator then cleared the white and blacklists on the device and configured the white and blacklists through the PAU. The evaluator verified whitelisted and blacklisted devices by the PAU were obeyed. The evaluator verified that the internal device white and blacklists `overrode the PAU configured values.

Test 2
[Conditional: Perform this only if "configurable" is selected in FDP_FIL_EXT.1.1/UA]
In the following steps the evaluator shall verify that whitelisted and blacklisted devices are treated correctly.
Step 1: Configure the TOE UA CDF to whitelist an authorized user authentication device, connect it to the TOE UA peripheral device interface, and verify that the device is accepted through real-time device console and USB sniffer capture.
Step 2: Configure the TOE UA CDF to blacklist the device and verify that the device is rejected through real-time device console and USB sniffer capture.
Step 3: Attempt to configure the TOE UA CDF to both whitelist and blacklist the device and verify that the device is rejected through real-time device console and USB sniffer capture.

The evaluator added an authentication device to the whitelist and verified the TOE allowed the device to be connected. The evaluator then added the device to the blacklist, without removing it from the whitelist, and verified the device was rejected. The evaluator then removed the device from the whitelist and verified that the device was rejected.

Test 3
[Conditional – Perform this only if "fixed" is selected in FDP_FIL_EXT.1.1/UA]
The evaluator shall examine the PSD UA whitelist and verify that all devices are authorized devices.

N/A; the TOE does not select "fixed" in FDP_FIL_EXT.1.1/UA.

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

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

5.1.1.3 FDP_PDC_EXT.4 Supported Authentication Device

5.1.1.3.1 TSS Evaluation Activity

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

[ST] section 6.2.6 states that the TOE uses an external authentication device.

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

Refer to section 2.1.1.2.1.

5.1.1.3.2 Guidance Activities

There are no guidance evaluation activities for this component.

5.1.1.3.3 Test Activities

There are no test evaluation activities for this component.

5.1.1.4 FDP_PWR_EXT.1 Powered by Computer

5.1.1.4.1 TSS Evaluation Activity

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

Section 6.2.8 of [ST] states that no external power source is allowed by the CAC interface.

5.1.1.4.2 Guidance Activities

There are no guidance EAs for this component.

5.1.1.4.3 Test Activities

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

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

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

For this test, the evaluator employed a sampling strategy per TD0593. Specifically, since the physical design of all computer ports is identical, there is no situation where one port may transmit power to the TOE while others do not. Therefore, sampling one port is sufficient to demonstrate that the TOE's design does not allow a computer port to supply power to the TOE.

The evaluator verified that when the TOE is disconnected from its power source, a powered-on computer that is connected to the TOE via the CAC port is unable to power on the TOE.

5.1.1.5 FDP_TER_EXT.1 Session Termination

5.1.1.5.1 TSS Evaluation Activity

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

Section 6.2.11 of [ST] states that the CAC interface is switched from its computer channel back to its micro-controller channel (i.e., the closed state) upon physical removal of the authentication element, terminating any active session; it does not persist the authentication data and allow the session to remain open.

5.1.1.5.2 Guidance Activities

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

[User] **Chapter 2 Hardware Setup, Section Installation** states that an active session on the selected computer is immediately terminated upon removal of the CAC card.

5.1.1.5.3 Test Activities

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

5.1.1.6 FDP_UAI_EXT.1 User Authentication Isolation

5.1.1.6.1 TSS Evaluation Activity

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

[ST] section 6.2.2 states that the authentication device connection is on a separate physical circuit that is isolated from all other peripherals. The keyboard/mouse ports cannot be used interchangeably with the CAC port as they each have their own separate filtration rules and data paths.

5.1.1.6.2 Guidance Activities

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

[PAU] **Chapter 2 Precautions and Preparations, Section Always use qualified and authorized peripheral devices** states that the USB CAC port by default only supports authorized user authentication devices such as USB Smartcard or CAC readers. Do not connect other USB devices to the USB CAC port. Non-qualified or non-authorized USB devices will be rejected.

5.1.1.6.3 Test Activities

Test 1

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

Perform this test for each computer interface.

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

Connect a display directly to each connected computer. Run USB protocol analyzer software and open a real-time hardware information console and a text editor on each connected computer. Ensure an authorized user authentication device is connected.

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

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

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

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

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

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

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

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

Step 8: Power down the TOE.

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

For this test, the evaluator used a connected CAC device to send CAC traffic to a connected computer. The evaluator verified, for each non-CAC USB port on the TOE (i.e., peripheral and computer keyboard/mouse USB ports), no USB traffic was detected while the CAC port was in use. The evaluator observed this by connecting a second computer to a non-selected port though a USB analyzer device and iterating which non-selected port the second computer was connected to while repeatedly sending traffic to the first computer. Only two computers are necessary because isolation with each non-selected port is tested sequentially.

The evaluator verified that the TOE did not transmit authentication data to the non-selected computer and that the authentication device was not present on the non-selected computers.

Test 2
[Conditional: Perform this test only if the TOE supports KM functionality.]
This test verifies that KM functionality is not sent to UA interfaces.
Perform this test while the TOE is powered on and powered off.
Step 1: Connect a KM device to the TOE KM peripheral interface.
Perform steps 2-3 for each TOE UA computer interface.
Step 2: Connect a USB sniffer to the TOE UA computer interface.
Step 3: Exercise the functions of the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM in MOD_KM_V1.0 and verify that no traffic is sent and captured on the USB sniffer.
[Conditional: Perform steps 4-5 only if "external" is selected in FDP_PDC_EXT.4.1]
Step 4: Disconnect the USB sniffer and connect it to the TOE UA peripheral device interface.
Step 5: Exercise the functions of the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM in MOD_KM_V1.0 and verify that no traffic is sent and captured on the USB sniffer.

For this test, the evaluator used a connected HID device to send HID traffic to a connected computer. The evaluator verified, for each CAC USB port on the TOE (i.e., peripheral and computer CAC USB ports), no USB traffic was detected while the HID port was in use. The evaluator observed this by connecting a second computer to a non-selected port though a USB analyzer device and iterating which non-selected port the second computer was connected to while repeatedly sending traffic to the first computer. Only two computers are necessary because isolation with each non-selected port is tested sequentially. This was observed when the TOE was on and when it was off.

Test 3
[Conditional: Perform this test only if the TOE supports video functionality and "USB Type-C with DisplayPort as alternate function" is selected in FDP_PDC_EXT.3.1/VI in MOD_VI_V1.0.]
This test verifies that USB video functionality is not sent to UA interfaces.
Perform this test while the TOE is powered on and powered off.
Perform steps 1-3 for each TOE UA computer interface and TOE USB type-C video peripheral interface.
Step 1: Connect a USB sniffer to the TOE UA computer interface.
Step 2: Connect a monitor to the TOE USB type-C video peripheral interface and verify that no traffic is sent and captured on the USB sniffer.
Step 3: Play a video on the selected computer and verify that no traffic is sent and captured on the USB sniffer.
[Conditional: Perform steps 4-7 only if "external" is selected in FDP_PDC_EXT.4.1]
Step 4: Disconnect the monitor.
Step 5: Disconnect the USB sniffer and connect it to the TOE UA peripheral device interface.
Step 6: Reconnect the monitor to the TOE USB type-C video peripheral interface and verify that no traffic is sent and captured on the USB sniffer.
Step 7: Play a video on the selected computer and verify that no traffic is sent and captured on the USB sniffer.

N/A, the TOE does not support USB Type-C video.

5.2 Optional SFRs

The UA Module does not define any optional SFRs.

5.3 Selection-Based SFRs

5.3.1 User Data Protection (FDP)

5.3.1.1 FDP_TER_EXT.2 Session Termination of Removed Devices

5.3.1.1.1 TSS Evaluation Activity

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

Section 6.2.11 of [ST] states that the CAC interface is switched from its computer channel back to its micro-controller channel (i.e., the closed state) upon physical removal of the authentication element, terminating any active session; it does not persist the authentication data and allow the session to remain open.

5.3.1.1.2 Guidance Activities

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

[User] Chapter 2 Hardware Setup, Section Installation states that an active session on the selected computer is immediately terminated upon removal of the CAC card.

5.3.1.1.3 Test Activities

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

5.3.1.2 FDP_TER_EXT.3 Session Termination upon Switching

5.3.1.2.1 TSS Evaluation Activity

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

Section 6.2.11 of [ST] states that when a channel switch occurs, the TSF resets the power supplied to the user authentication device for at least one second. This is sufficient to discharge the voltage to under 2V within 0.2 seconds, with the remainder of the second used to provide an additional safety margin. This is sufficient to ensure that activity for the connected authentication device is suspended with a switch occurs for long enough that re-authentication is necessary.

5.3.1.2.2 Guidance Activities

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

[Admin] **Chapter 3 Operation, Section Manual Switching** states that in order to meet maximum security and channel isolation requirements, the keyboard, mouse, video monitor, audio, and USB CAC reader ports will be switched together.

5.3.1.2.3 Test Activities

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

6 Security Functional Requirement Evaluation Activities (VI Module)

6.1 Mandatory SFRs

6.1.1 User Data Protection (FDP)

6.1.1.1 FDP_PDC_EXT.2/VI Authorized Devices (Video Output)

6.1.1.1.1 TSS Evaluation Activity

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

Refer to section 2.1.1.2.1.

6.1.1.1.2 Guidance Activities

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

6.1.1.1.3 Test Activities

Testing of this component is performed through evaluation of FDP_PDC_EXT.1 as specified in section 2.1.1.2.3 above.

6.1.1.2 FDP_PDC_EXT.3/VI Authorized Connection Protocols (Video Output)

6.1.1.2.1 TSS Evaluation Activity

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

Refer to section 2.1.1.2.1. Note that [ST] iterates this SFR as FDP_PDC_EXT.3/VI(DP), FDP_PDC_EXT.3/VI(H), and FDP_PDC_EXT.3/VI(D). This is because all TOE models support exactly one of DisplayPort, HDMI, or DVI. Each iteration of the SFR is intended to refer to the TOE models that implement the particular protocol identified by the iteration.

6.1.1.2.2 Guidance Activities

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

6.1.1.2.3 Test Activities

Testing of this component is performed through evaluation of FDP_APC_EXT.1 as specified in section 2.1.1.1.3 above.

6.1.1.3 FDP_UDF_EXT.1/VI Unidirectional Data Flow (Video Output)

6.1.1.3.1 TSS Evaluation Activity

There are no TSS EAs for this component.

N/A – no TSS EAs for this component.

6.1.1.3.2 Guidance Activities

There are no guidance EAs for this component.

N/A – no AGD EAs for this component.

6.1.1.3.3 Test Activities

This component is evaluated through evaluation of FDP_APC_EXT.1 as specified in section 2.1.1.1.3 above.

6.2 Optional SFRs

The VI Module does not define and optional SFRs.

6.3 Selection-Based SFRs

6.3.1 User Data Protection (FDP)

6.3.1.1 FDP_CDS_EXT.1 Connected Displays Supported

6.3.1.1.1 TSS Evaluation Activity

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

[ST] section 6.2.3 states that some models support one connected display while other models support two connected displays. The specific models that each selection applies to are identified in this section. Regardless of how many displays a specific TOE model supports, all TOE models support a single source video feed; models that support two connected displays support are multi-head devices; there are no combiner or multi-viewer TOE models.

6.3.1.1.2 Guidance Activities

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

[User] Section **About This Manual** identifies the different TOE versions and the number of displays supported by each.

6.3.1.1.3 Test Activities

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

6.3.1.2 FDP_IPC_EXT.1 Internal Protocol Conversion

6.3.1.2.1 TSS Evaluation Activity

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

The TOE includes some models with DisplayPort video support and some models that do not support DisplayPort (i.e., they support DVI or HDMI instead). This SFR only applies to DisplayPort models of the TOE and has therefore been identified as FDP_IPC_EXT.1(DP).

[ST] section 6.2.12.1 states that all TOE models that support DisplayPort video will convert the DisplayPort signal to HDMI before re-converting it and outputting it as Display Port Signal.

6.3.1.2.2 Guidance Activities

There are no guidance EAs for this component.

N/A – no AGD EAs for this component.

6.3.1.2.3 Test Activities

Testing for this SFR is covered under FDP_APC_EXT.1 Test 3-VI.

6.3.1.3 FDP_SPR_EXT.1/DP Sub-Protocol Rules (DisplayPort Protocol)

6.3.1.3.1 TSS Evaluation Activity

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

The TOE includes some models with DisplayPort video support and some models that do not support DisplayPort (i.e., they support DVI or HDMI instead). This SFR only applies to DisplayPort models of the TOE and has therefore been identified as FDP_SPR_EXT.1/DP(DP).

Section 6.2.12.1 of [ST] states that the TOE rejects communication of EDID information from computer to display as well as CEC, HDCP, and MCCS communications. This section also states that the TOE allows communication of EDID and HPD from display to computer as well as Link Training.

6.3.1.3.2 Guidance Activities

There are no guidance EAs for this component.

N/A – no AGD EAs for this component.

6.3.1.3.3 Test Activities

Testing for this SFR is covered under FDP_APC_EXT.1 Test 3-VI and Test 4-VI.

6.3.1.4 FDP_SPR_EXT.1/DVI-I Sub-Protocol Rules (DVI-I Protocol)

6.3.1.4.1 TSS Evaluation Activity

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

The TOE includes some models with DVI video support and some models that do not support DVI (i.e., they support DisplayPort or HDMI instead). This SFR only applies to DVI models of the TOE and has therefore been identified as FDP_SPR_EXT.1/DVI-I(D).

Section 6.2.12.3 of [ST] states that the TOE rejects communication of EDID information from computer to display as well as ARC, CEC, HDCP, HEAC, HEC, and MCCS communications. This section also states that the TOE allows communication of EDID and HPD from display to computer.

6.3.1.4.2 Guidance Activities

There are no guidance EAs for this component.

N/A – no AGD EAs for this component.

6.3.1.4.3 Test Activities

Testing for this SFR is covered under FDP_APC_EXT.1 Test 3-VI and Test 4-VI.

6.3.1.5 FDP_SPR_EXT.1/HDMI Sub-Protocol Rules (HDMI Protocol)

6.3.1.5.1 TSS Evaluation Activity

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

The TOE includes some models with HDMI video support and some models that do not support HDMI (i.e., they support DisplayPort or DVI instead). This SFR only applies to HDMI models of the TOE and has therefore been identified as FDP_SPR_EXT.1/HDMI(H).

Section 6.2.12.2 of [ST] states that the TOE rejects communication of EDID information from computer to display as well as ARC, CEC, HDCP, HEAC, HEC, and MCCS communications. This section also states that the TOE allows communication of EDID and HPD from display to computer.

6.3.1.5.2 Guidance Activities

There are no guidance EAs for this component.

N/A – no AGD EAs for this component.

6.3.1.5.3 Test Activities

Testing for this SFR is covered under FDP_APC_EXT.1 Test 3-VI and Test 4-VI.

7 Security Assurance Requirements

7.1 Isolation Document

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

Isolation details are proprietary to the vendor. The evaluator reviewed the isolation documentation and determined that it adequately described the process by which information flows for various peripheral types do not have physical or logical overlaps as well as the process by which disallowed information flows (e.g., user peripheral to non-selected computer, selected computer to non-selected computer, audio data flow from peripheral to computer, etc.) are prohibited.

Section 2 provides design information for the various interfaces, data flows, and operational states in support of how isolation is maintained through these interfaces, for these data flows, and when the TOE is in these states, specifically:

- Section 2.1 identifies the design of the TOE from an external interface standpoint.
- Section 2.2 identifies the isolation of keyboard and mouse data flow.
- Section 2.3 identifies the isolation of user authentication data flow.
- Section 2.4 identifies the isolation of video data flow.
- Section 2.5 identifies the isolation of audio data flow.

- Section 2.6 identifies how isolation is maintained when the tamper detection/response functionality is triggered.
- Section 2.7 identifies the self-test functionality and accompanying log data that can be used as evidence that the TOE is in a known operational state.

7.2 Class ASE: Security Targeted Evaluation

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

No additional evaluation activities are performed for this; refer to sections 2-6 above.

7.3 Class ADV: Development

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

7.3.1 ADV_FSP.1 Basic Functional Specification

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

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

No additional evaluation activities are performed for this; refer to sections 2-6. In particular, the Evaluation Activities for FDP_PDC_EXT.1 and the Isolation Document are sufficient to identify the security-relevant external interfaces for the TOE.

7.3.1.1 ADV_FSP.1 Evaluation Activity

There are no specific Evaluation Activities associated with these SARs. The Evaluation Activities listed in this PP are associated with the applicable SFRs; since these are directly associated with the SFRs, the tracing element ADV_FSP.1.2D is implicitly already done, and no additional documentation is necessary. The functional specification documentation is provided to support the evaluation activities described in Sections 2-6 and other activities described for AGD, and ATE SARs. The requirements on the content of the functional specification information are implicitly assessed by virtue of the other Evaluation Activities being performed. If the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided.

No additional evaluation activities are performed for this; refer to sections 2-6 above.

7.4 Class AGD: Guidance Documents

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

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

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

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

The evaluators observed that the administrative guidance for the TOE is broken up into [Admin] for the administrative interface and other documentation for the deployment and usage of the TOE. [Admin] includes "instructions to provide a protected administrative capability" per the evaluation activity. Specifically, discussion on all user roles and management functions claimed in each ST is present in this document. The other documentation includes "instructions to successfully and securely install the TSF" by showing schematic diagrams of the specific types of cables and peripherals that should be connected to the various TOE ports. It also includes "instructions to manage the security of the TSF…" by having various warnings on potentially insecure usage scattered throughout the documentation at various points. For example, the documentation includes warnings against the use of microphone devices, wireless devices, and CAC devices with external power sources. It also includes guidance on how to detect when the TOE is no longer operating in a secure state (e.g., in the event a self-test failure has occurred or the tamper response has been triggered).

7.4.1 AGD_OPE.1 Operational User Guidance

The operational user guidance does not have to be contained in a single document. Guidance to users and Administrators can be spread among documents or web pages. The developer should review the Evaluation Activities contained in Sections 2-6 of this PP to ascertain the specifics of the guidance for which the evaluator will be checking. This will provide the necessary information for the preparation of acceptable guidance.

The evaluators observed that user guidance for setup and operation of the TOE are presented as PDF documents and administrative guidance for the use of the TOE's management interface is presented as a separate document. Different user guidance is provided in different documents because the guidance is broken up by model type with respect to the supported peripheral interfaces.

7.4.1.1 AGD_PRE.1 Preparative Procedures

As with the operational user guidance, the developer should look to the Evaluation Activities contained in Sections 2-6 of this PP to determine the required content with respect to preparative procedures.

This is addressed through the completion of the various guidance evaluation activities in the previous sections.

7.5 Class ALC: Life-Cycle Support

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

7.5.1 ALC_CMC.1 Labeling of the TOE

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

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

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

The ST identifies every TOE component and the firmware version number. Each TOE device is labelled uniquely identifies the TOE model 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.

The following image shows a representative TOE model with the product vendor and model name on the faceplate:

Self-Test Results

The Self-Test verifies TOE Firmware version number.

```
DATE-TIME = 14-10-2021_12:17:43_UTC

MFG_DATE = 13-01-2021

TAMP_TEST = PASS

HW_TEST = PASS

FW_TEST = PASS

KVM_BATT_TEST = 3.0V

RPS_BATT_TEST = NA

RPS_TEST = NA

FW_CHECKSUM = 00D0C450

AUDT_ST = 13-01-2021_13:15:15_UTC

AUDT_SP = NA

FW_VER = v1.1.101

TTL_LOGS = 36
```

7.5.1.1 ALC_CMC.1 Evaluation Activity

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

Throughout the various documentation references, the evaluators observed that the device models referenced in the operational guidance are consistent with the TOE models identified in each ST, and that the models used for testing are a subset of the models identified in each ST, with physical labeling that correctly identifies the model.

7.5.2 ALC_CMS.1 TOE CM Coverage

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

7.6 Class ATE: Tests

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

7.7 ATE_IND Independent Testing – Conformance

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

The evaluator created [Test] to document the test requirements of [PSD PP] and the claimed PP-Modules. This report references external test evidence such as photographs, video recordings, and screen captures that were used to demonstrate that the required testing was performed. Section 4 of [Test] defines the equivalency arguments that were used and the specific TOE devices that were selected as being representative of the TOE. Independent testing took place at the Leidos AT&E lab in Columbia, Maryland from August 9, 2021 to February 8, 2022.

As part of testing, the evaluators used equivalency arguments in cases where design information and functional claims provided sufficient evidence that test results would be identical across multiple models. In some cases, only a portion of testing was repeated because product functionality was otherwise identical across the models.

The following non-TOE components were also used as part of the environment were:

- 5 Desktop Computers
    - 4 Identical Custom builds: Win 10 Pro 20H2, 64 Bit
        - CPU: Intel I3 10100
        - RAM: 8 GB Patriot PS001216
        - SSD: 500 GB NVMe Samsung EVO 970
        - GPU NVIDIA Quadro K420
        - PSU: Corsair CX 450M 450W 80+ Bronze
        - MOBO: MSI H410M Pro
        - Supported Video Types: VGA, DVI x2, HDMI, DP
    - 1 Dell XPS 8500: Ubuntu 20.04 LTS
        - CPU: Intel I5-3350P
        - RAM: 8GB
        - Programs: I2C v4.1
        - Supported Video Types: VGA, DVI, HDMI, DP
- 12 Total Monitors
    - HDMI
        - Samsung S24E10HL (Quantity:2)
        - LG 24MK430H-B (Quantity: 2)
    - DVI/VGA
        - Dell E246H0 (Quantity:1)
    - DVI/VGA
        - ASUS VW226 (Quantity: 3)
        - Dell P2210 (Quantity:1)
    - 4K Capable (DP/HDMI)
        - LG 27UL500 (Quantity:1)

        - Z-Edge U27P4K (Quantity:1)
    - DP/HDMI/DVI
        - Dell U2413F (Quantity:1)
- Amplified speakers – Altec Lansing VS2621
- USB Keyboards – Dell L100
- USB Mouse – Amazon Basics MSU0939
- CAC/Smartcard reader – GemPC Twin HWP108760

Additional non-TOE components were used throughout the course of the evaluation. The individual test case will have more information on how each of the testing components were used:

- Lab power supply – Mastech HY3010E S/N 001001010
- Oscilloscope – Agilent Infiniium DSO81004A
- USB Mouse – Patriot PP000199-PV560LULPWK S/N 20160103302
- USB Mouse – Dell Mouse P/N: 0C8639
- USB keyboard – Dell RT7D60
- USB keyboard – Dell L100 S/N: CN0RH6597357172200EJR
- Signal Generator – Tektronix AFG1062 S/N 1650219
- USB Protocol Analyzer – ITIC 1480A USB 2.0 LS/FS/HS
- Mass storage Device – SanDisk 16GB USB 2.0GB
- USB HUB – Sabrent USB Hub
- USB Printer – Canon Prixma IP2820 SN: KKCF48699
- USB Headset – JABRA UC VOICE 550MS S/N 12GA2CO65FC
- USB Headset – Plantronics DSP55 Adapter
- USB Smart-card reader – GemPC Twin P/N HWP108760 C
- Microphone – Singing Machine SMM-205
- Analog Headset—Audio-Technica ATH-M50x
- MCCS Console – SoftMCCS v.2.5.0.1084
- Keyboard emulator software – Microsoft Windows 10 virtual keyboard
- Audio analyzer software – Audacity v3.0.2
- Fluke 179 TRUE RMS Multimeter – S/N: 38820131

As can be seen above, the configuration used during testing of the TOE matches that which was defined in the Security Target. The following equivalency arguments were applied:

Device Groups

Device in this group are part of the VID: 11221

The below tables contain the full list of products covered by this device group.

#	Model Name	Description and NIAP Certification Version	Eval. Version
1	CS1182DP4C	2 Port DP Single Head with CAC	1.1.101
2	CS1142DP4C	2 Port DP Dual Head with CAC	1.1.101
3	CS1182H4C	2 Port HDMI Single Head with CAC	1.1.101
4	CS1142H4C	2 Port HDMI Dual Head with CAC	1.1.101
5	CS1182D4C	2 Port DVI Single Head with CAC	1.1.101
6	CS1142D4C	2 Port DVI Dual Head with CAC	1.1.101

Table 1: 2 Port Secure TOE Identifications

#	Model Name	Description and NIAP Certification Version	Eval. Version
1	CS1184DP4C	4 Port DP Single Head with CAC	1.1.101
2	CS1144DP4C	4 Port DP Dual Head with CAC	1.1.101
3	CS1184H4C	4 Port HDMI Single Head with CAC	1.1.101
4	CS1144H4C	4 Port HDMI Dual Head with CAC	1.1.101
5	CS1184D4C	4 Port DVI Single Head with CAC	1.1.101
6	CS1144D4C	4 Port DVI Dual Head with CAC	1.1.101

Table 2: 4 Port Secure TOE Identifications

#	Model Name	Description and NIAP Certification Version	Eval. Version
1	CS1188DP4C	8 Port DP Single Head with CAC	1.1.101
2	CS1148DP4C	8 Port DP Dual Head with CAC	1.1.101
3	CS1188D4C	8 Port DVI Single Head with CAC	1.1.101
4	CS1148D4C	8 Port DVI Dual Head with CAC	1.1.101

The following differences exist between the products in this group:

- The number of ports supported by the KVM: 2, 4 or 8
- The number of display boards present
- The type of video cable that is used for the Video Display

In order to limit the amount of time and effort to complete the evaluation, a well thought out sub group of products was selected that best address all of the possible differences. The following products were fully tested:

- CS1188DP4C

Partial testing was conducted on the following devices for the specified functionality.

- CS1184H4C – HDMI testing
- CS1148D4C – DVI Testing

Rationale: product functionality that is unrelated to the video peripheral type is not dependent on the specific video protocol that is supported (i.e., audio/HID/CAC peripheral support, administration, self-testing, etc.). Therefore, full testing on a model with one video protocol type is assumed to cover other models. Video protocol behavior is different for each supported protocol, so an iteration of video testing is needed for each specific protocol type.

Ports Available

The number of ports/channels a device supports/possess, does not affect the ability of the TOE to enforce the security constraints required on any specific channel. Thus, devices that have: 2, 4, 8 ports have all been considered equivalent and testing on one would suffice to prove that the TOE is capable of enforcing the requirements on other models with different supported port counts. This applies to items like the Audio functionality, the USB functionality, the CAC functionality and the Video functionality. Though each distinct video type was tested (DisplayPort, HDMI, DVI-I/D. Testing was executed on the TOE model which possessed the maximum number of Ports (4 port for HDMI models or 8 ports for DP/DVI models) with any device supported a fewer number of ports being considered equivalent.

All peripheral types have test requirements where it is necessary to show isolation between computer ports of the same peripheral type. In general, the sampling approach listed below was taken in these cases in accordance with TD0593, per peripheral type. All peripheral types have test requirements where it is necessary to show isolation between computer ports of the same peripheral type. In all cases, each permutation of port pairs (port where signal is being transmitted, and port being sampled where no signal is expected) were tested, and no equivalency is relied upon for this. For testing where the TOE's behavior is implemented by a central component and would not differ from a design perspective based on the selected port (e.g., unidirectional data flow testing), a single port sample was determined to be sufficient. Per section 3, when fewer computers or peripherals were available than ports that needed to be tested, the evaluators either used specialized hardware that could be used in place of a general-purpose computer (e.g., a multi-headed oscilloscope) or the testing was conducted over multiple iterations where the ports that had devices connected to them were swapped in successive iterations.

USB Functionality

The USB controller on the devices are all the same and thus the functionality of the USB peripheral transfer device channels is the same for each device in this set. Thus, testing of the USB peripherals on one device in each device group is sufficient for all of the devices in the device group.

Single vs Dual

Devices support one of two output types for video signal, single head, with only one display output, or multi-head, which has multiple display boards such as dual head (2 displays). The only differences between these devices is the number of display boards the device has, as in this case the TOE has a dedicated board for each of the display outputs. The display signal does not cross over between the boards, thus if the video in is connected on board 1 and the video out is connected on board 2 there will be no video displayed. Testing for the single head or dual head is considered equivalent, as the only difference is number of display boards present. Proof of non-transfer testing will be performed with the greatest number boards present to show that the signal will never traverse between the display boards even in the best case scenario for it to traverse. Since it is shown that video will never traverse between the boards the video tests performed on one board are considered equivalent to all other devices with the video board present regardless of the number of boards that are present. Since the functionality of the

multiple boards is independent of the video type this does not need to be tested for each individual video type and the specific video type independent testing is sufficient.

7.7.1 ATE_IND.1 Evaluation Activity

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

The evaluators created [Test] to address all test cases in [PSD PP] and the claimed PP-Modules. The testing is grouped by SFR to show direct correspondence with the required evaluation activities.

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.

Section 4 of [Test] defines the equivalency arguments used for the TOE testing. Specifically, not all testing was performed on all TOE models within the scope of the evaluation. Some models are fully tested, some models are partially tested, and some models are not tested because other test evidence coupled with the design information included in the STs provides sufficient assurance that the results would be the same if re-executed on those models.

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 evaluator observed that no special tools or configuration instructions are needed to place the TOE into its tested configuration. To the extent that specific tools are required for testing, these tools are the same as those that are specified in [PSD PP] and the claimed PP-Modules (e.g., oscilloscope, tone generator, specific types of allowed and disallowed USB devices, etc.) and therefore no argument is needed that their presence adversely affects the behavior of the TOE.

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.

[Test] reproduces the evaluation activities from [PSD PP] and the claimed PP-Modules, each of which include the test objectives, procedures, and expected results in sufficient detail for testing to be reproducible. These activities are written in an implementation-generic manner, but are sufficiently detailed for the evaluator to understand the expected steps. For example, the test procedures do not specify a particular method of switching selected channels, but this information was easily discernable to the evaluator through examination of the operational guidance.

7.8 Class AVA: Vulnerability Assessment

7.8.1 AVA_VAN.1 Vulnerability Survey

For the current generation of this PP, the evaluation lab is expected to survey open sources to discover what vulnerabilities have been discovered in these types of products and in the connected peripherals. In addition, the evaluation lab is expected to survey open sources to discover new vulnerabilities and weaknesses discovered in microcontrollers, ASICs, FPGAs, and microprocessors used in the TOE. In some cases, these vulnerabilities will require sophistication beyond that of a basic attacker. The labs will be expected to comment on the likelihood of these vulnerabilities given the documentation provided by the vendor. This information will be used for the development of future PPs.

The evaluators conducted vulnerability research on the TOE as part of the execution of the AVA_VAN.1 work units. The evaluators did not observe the existence of any general or specialized tools or techniques that are unique to the potential exploitation of peripheral switching functionality. Specifically, no attack techniques related to the following attempted exploits were found, beyond the behavior that is already addressed by the evaluation activities in [PSD PP] and the claimed PP-Modules:

- Attempting to violate security domains by transmitting data from one computer to another.
- Attempting to reverse unidirectional data flow by transmitting data through the TOE in the opposite direction of its intended usage (e.g., using the TOE audio output port as a microphone port).
- Attempting to exfiltrate data using an unintended mechanism, such as using the TOE's EDID memory to transmit non-EDID data or by using some other TOE interface or variable physical property as a side channel.
- Attempting to use a peripheral to interact with the TOE itself in an unauthorized manner (such as using a USB mass storage device to load modified firmware onto the TOE).
- Attempting to violate device filtration to allow an unauthorized peripheral type to interface with a connected computer through the TOE.

7.8.1.1 AVA_VAN.1 Evaluation Activity

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

The evaluators created [VA] to document the public vulnerability survey that was conducted for the TOE. As part of this activity, the evaluators looked for vulnerabilities not just in the TOE itself but also in OEM rebrands of the same physical devices and other peripheral sharing devices manufactured by competing vendors, in case that successful exploits have been developed against PSD technology in general. The evaluators did not identify any publicly disclosed vulnerability research that shows examples of successful attacks on the TOE or potentially exploitable flaws.

Searches of public domain sources for potential vulnerabilities in the TOE were conducted periodically throughout the evaluation, most recently on March 8, 2022. During each search, no known vulnerabilities were revealed.

Vulnerability searches were performed using the terms listed below for the rationale listed below:

Search Term	Search Type	Rationale
aten	Advanced: Vendor	TOE vendor
belkin	Advanced: Vendor	Comparable vendor
black box	Advanced: Vendor	Comparable vendor
blackbox	Advanced: Vendor	Comparable vendor
iogear	Advanced: Vendor	Comparable vendor
ipgard	Advanced: Vendor	Comparable vendor
kvm	Basic: Keyword	General type
kvm switch	Basic: Keyword	TOE type
peripheral switch	Basic: Keyword	TOE type
raritan	Advanced: Vendor	Comparable vendor
smartavi	Advanced: Vendor	Comparable vendor
tripplite	Advanced: Vendor	Comparable vendor
sekuryx	Advanced: Vendor	Comparable vendor

While some results were returned, no results applied to the specific TOE models or to the technology used by the TOE (for example, “kvm” returns results for the Linux Kernel-based Virtual Machine technology which is not applicable to the TOE). 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.