Assurance Activities Report

for

IPGARD Secure KM Switch (CAC Models)

Version 1.1

2021-06-25

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:

IPGARD, Inc.
2455 W Cheyenne Ave Ste 112
North Las Vegas, NV 89032

The TOE Evaluation was Sponsored by:

IPGARD, Inc.
2455 W Cheyenne Ave Ste 112
North Las Vegas, NV 89032

Evaluation Personnel:

Justin Fisher
Shreyansh Kansara
Madhav Nakar
Pascal Patin
Allen Sant
Furukh Siddique
Sindhu Veerabhadru

Contents

1 Introduction

This document presents results from performing Evaluation Activities (EAs) associated with the evaluation of the IPGARD Secure KM Switch. 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, and User Authentication Devices, including the following optional and selection-based SFRs:

Protection Profile for Peripheral Sharing Device [PSD PP]:

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

PP-Module for Analog Audio Output Devices [AO Module]: N/A, [AO Module] contains no optional or selection-based SFRs.

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

- Optional Requirements
  - FDP_FIL_EXT.1/KM
- Selection-Based Requirements
  - FDP_RIP.1/KM
  - FDP_SWI_EXT.3

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

- Optional Requirements
  - N/A – PP-Module defines no optional requirements
- Selection-Based Requirements
  - FDP_TER_EXT.2
  - FDP_TER_EXT.3

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.

TD0507: Clarification on USB plug type

This TD is applicable to the TOE.

TD0518: Typographical error in Dependency Table

This TD is not applicable to the TOE; the TD affects the content of the claimed PP but does not affect the claimed SFRs or how they are evaluated.

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 not applicable to the TOE. The TOE boundary does not include a remote controller.

TD0585: Update to FDP_APC_EXT.1 Audio Output Tests

This TD is applicable to the TOE.

TD0593: Equivalency Arguments for PSD

This TD is applicable to the TOE.

1.2 Evidence

[ST] IPGARD Secure KM Switch Security Target (CAC Models), Version 1.05, June 25, 2021

[Admin] IPGARD Secure KVM Administration and Security Management Tool Guide (CAC), Version 1.1, February 11, 2021

[KMN] IPGARD Advanced 4/8-Port Secure KM Switch User Manual, Revision 1.11, July 3, 2018

[Test] IPGARD PSD PP 4.0 Common Criteria Test Report and Procedures, Version 1.1, June 25, 2021

[VA] SmartAVI Vulnerability Survey, Version 1.2, June 25, 2021

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

2 Security Functional Requirement Evaluation Activities (PSD PP)

This section describes the evaluation activities associated with the SFRs defined in [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.

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 6.4 of [ST] indicates that the TOE enters a temporary failure state if there is a self-test failure. This section indicates that the following self-tests are performed:

- Basic integrity test of TOE hardware (no front panel buttons are jammed)
- Basic integrity test of TOE firmware
- Integrity test of anti-tampering system and control functions (calendar check, anti-tamper switch check, anti-tamper battery check)
- Data traffic isolation between ports

Section 6.4 of [ST] indicates that the TOE enters a permanent failure state if the tamper response mechanism is triggered through manual opening of the chassis enclosure.

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

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.

The [KMN] guidance document includes a section called “LED’s Behavior” that specifies the audio/visual indicators of the TOE entering a failure state, either through the tamper response mechanism or through failure of power-on self-tests.

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.

The TOE has no ability to grant or deny authorization to audio peripherals so this activity is not applicable.

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

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. 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.

PSD:AO

Step 5 modified by NIAP TD0585

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 evaluator 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 signal was detected on the connected oscilloscope, and when a different port is selected, the connected oscilloscope registered less than 11.2 mV, 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 connected external speakers to the TOE and then connected/disconnected the USB and CAC connections while listening for audio signals on the non-selected port. The evaluator verified that no audio was heard on the selected computer during this process.

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.

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 for a signal. 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.

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 taken on one computer are not bled across to another 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.

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 connected the peer computer through a USB analyzer and performed the specified actions. In each case, the evaluator verified that the TOE did not send any data to the peer computers and none of the actions are replicated to the other non-selected computers.

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.

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 verified that the TOE emulated the keyboard and mouse devices to all connected computers all the time.

PSD:KM

Step 9 modified by NIAP TD0507

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.

The evaluator verified that when the TOE is rebooted, 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.

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.

The evaluator connected a computer to the TOE through a USB analyzer and performed the specified steps. The evaluator verified that the TOE did not replay any of the USB traffic to the second computer.

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.

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 device manager of the connected computer. 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.

The evaluator verified only the selected computer could see the authentication device in the device manager. The evaluator verified that the connected computers automatically logged off after the authentication element was disconnected. The evaluator verified that the TOE only sent data to the selected computer.

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.

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: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.

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.

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] defines the supported peripheral types as follows:

- Audio: analog audio output devices, per section 6.5 of [ST] (the ST introductions make it clear that this refers to 3.5mm analog audio).
- Keyboard/Mouse: USB keyboard and mouse (standard 108-key US keyboard and three-button mouse), per section 6.6 of [ST].
- User Authentication Devices: USB smart-card reader, PIV/CAC USB token, or biometric reader, per section 6.7 of [ST].

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 6.1 of [ST] summarizes the TOE external interfaces. This includes peripheral interfaces for analog audio, keyboard/mouse, and user authentication devices, as well as AC/DC power which is not security-relevant. The various tables in the TOE Overview maps these interfaces to console and peripheral ports of the TOE. In general, the TOE's console (peripheral) ports are identical to the corresponding computer ports, with the following exception:

- To pass audio into the TOE from the connected computers, the computer side analog audio ports are input (red) ports while the console side is an output (green) port.

Section 6.6 of [ST] states that wireless keyboard/mouse devices are not supported by the TOE because these are enumerated as special composite device types. 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 6.6 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 6.7 of [ST] indicates that the CAC port enforces fixed device filtration by default to allow only smart-card readers, PIV/CAC tokens, and biometric readers. The fixed device filtration is therefore understood to prevent acceptance of USB mass storage devices on this interface.

Section 6.6 of [ST] states that any composite devices connected to the TOE or devices connected through a USB hub on the keyboard/mouse ports will be authorized if there is at least one HID class endpoint, with all other endpoints being disabled. Section 6.7 states that USB hubs are blocked by the TSF on CAC ports by default as part of fixed device filtration enforcement; CAC devices on a USB hub can be authorized only if configurable device filtration is used to whitelist the hub.

[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 2) 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 they each describe peripheral interfaces for analog audio out, 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 either 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

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.

The [KMN] guidance document includes a schematic of the rear panel of a representative model that clearly shows the physical ports that are available for a model of that type. The title page of each document identifies the models covered by the document so that it is clear to the reader what models the document applies to.

The “Installation” section of the guidance documents include a list of authorized devices for each of the TOE’s physical interfaces. This section also includes the steps for connecting all of the various computer and peripheral interfaces to the TOE and has a high-level diagram showing the connections between the TOE and the various computers and peripherals with color-coded lines. For those TOE model types that include multi-head units, this section also has a diagram showing how the various display cables are connected to the multiple computer and peripheral port interfaces.

Based on this information, sufficient guidance exists to show what physical interfaces are present on any given TOE model and how these are connected to computers and peripherals in order to use the TOE in the intended manner.

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

The “Installation” section of the various guidance documents include guidance for how to connect all external cables to the TOE regardless of function. Where necessary, these procedures alongside the physical schematic of the TOE rear panel identify the physical form factor of the connection that is used. For example, the guidance specifically states that USB Type-A to Type-B is needed for connectivity between the TOE and connected computers, and USB Type-A interfaces are visible on the rear panel schematic for the input interfaces.

The “Technical Specifications” section of the various guidance documents also identify the specific supported physical interfaces for each TOE model.

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

The table under “System Requirements” in the various guidance documents identify the authorized devices for the console. The document does not explicitly identify the risk of misuse; however, it is understood by the reader that any supported peripheral type can be used in the product’s evaluated configuration. There are no interfaces where the user is instructed to avoid their use for security purposes.

[Admin] describes the process for registering USB peripherals via whitelist. It includes a warning that only appropriate devices should be whitelisted so that arbitrary USB communications cannot be made through the TOE.

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.

The various guidance documents include a section called “LED’s Behavior” that identifies what the various LED indications represent. This section indicates that a flashing CAC LED indicates an unauthorized CAC peripheral is connected, and all port and CAC selection LEDs are flashing an unauthorized keyboard or mouse peripheral is connected.

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.

This activity applies to [KM Module] so the scope of this activity relates to keyboard and mouse devices.

The various guidance documents include a table under “System Requirements” to identify all authorized peripheral devices by type. It identifies the following as being supported:

- Keyboard: Wired keyboard and keypad without internal USB hub or composite device functions, unless the connected device has at least one endpoint which is a keyboard or mouse HID class, KVM/KM extender.
- Mouse/Pointing Device: Any wired mouse or trackball without internal USB hub or composite device functions.

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.

This activity applies to [UA Module] so the scope of this activity relates to user authentication devices.

The various guidance documents include a table under “System Requirements” to identify all authorized peripheral devices by type. It identifies the following as being supported: Smart-card reader, PIV/CAC reader, token, or Biometric reader.

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, and Power.

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. 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 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.

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.

Appendix B of [ST] contains the required letter of volatility. The letter covers the main PCBA and front panel PCBA. The letter describes Emulation MCU, Keyboard and Mouse USB Host Controller, CAC USB Host Controller devices on the main PCBA.

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

Appendix B explains the TOE erases SRAM in the Keyboard and Mouse USB Host Controller when switching between connected computers, as well as when power is disconnected from the TOE and when anti-tampering has been triggered. No data is stored in main PCBA, the emulation MCU, and the Keyboard and Mouse USB Host Controller when power is disconnected. The CAC USB Host Controller does not store user data in SRAM.

Section 6.7 of [ST] states that when ports are switched, the power to the CAC port is reset for 1,000ms and describes the mechanism for doing this in such a manner to provide assurance that the CAC device is reset.

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

Appendix B of [ST] identifies user data as being stored only in volatile SRAM. There is no non-volatile storage of 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.

Section 6.2 of [ST] states that the TOE supports switching between connected computers.

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 of [ST] states that the TOE supports switching between connected computers. The following are the supported switching mechanisms:

- The selected channel can be switched using push-button toggles on the TOE chassis.
- The selected channel can alternatively be switched using mouse cursor control using a guard. Specifically, the guard is to press the middle mouse button twice and the cursor control is to 'swipe' the mouse left to decrement the selected channel or right to increment it.

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.

The [KMN] guidance document includes a section called "Front Panel Control" that describes how to use the push buttons to change the selected computer.

2.1.1.4.3 Test Activities

There are no test Evaluation Activities for this component.

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 6.3 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. Additionally, it asserts that the TOE's firmware is read/write protected, inaccessible via JTAG, and cannot be externally modified or updated. This section states that authorized administrators may read memory related to the TOE's configuration and auditing, and users may read memory related to current CDF configuration, consistent with the claims made in FPT_NTA_EXT.1.1.

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.

The evaluator reviewed [Admin] and determined that the TOE satisfies this requirement by default and no configuration option exists to affect its behavior.

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 6.3 of [ST] states that the TOE has a front panel tamper evident label that is placed over the boundary between the upper and lower portion of the TOE chassis such that any attempt to open the physical enclosure would necessarily create tamper evidence.

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.

The [KMN] guidance document includes a section called “Security Features” that states that the unit is covered with a tamper-evident seal that will leave visual evidence of its removal. This section also states that the internal anti-tamper switch being triggered will render the device useless and repeatedly flash its front panel LEDs and sound a buzzer like audible indication. The “LED’s Behavior” section of these documents also states that if all front panel LEDs are flashing and the buzzer is beeping, the device has been tampered with.

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 and audible indication that the device had been tampered.

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 audible and 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).

Section 6.5 of [ST] indicates that the TOE enters a temporary failure state if there is a self-test failure. This section indicates that the following self-tests are performed:

- Basic integrity test of TOE hardware (no front panel buttons are jammed)
- Basic integrity test of TOE firmware
- Integrity test of anti-tampering system and control functions (calendar check, anti-tamper switch check, anti-tamper battery check)
- Data traffic isolation between ports

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.

Section 6.4 of [ST] indicates that a self-test failure temporarily deactivates the TOE by disabling all ports and turns on all front panel LEDs to indicate a failure. This is functionally identical to a shutdown because no TSF-mediated behavior can occur. Rebooting the TOE is the only method by which a self-test failure can be cleared.

Section 6.3 of [ST] indicates that a failure of the tamper response function (i.e. because the anti-tamper switch has been triggered or the backup battery has failed) will result in the permanent disabling of the TOE.

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 6.4 of [ST] indicates that the TSF will respond to a self-test failure by disabling all external ports and displaying all front panel LEDs until the user attempts to clear the failure state by rebooting the TOE. Section 6.3 indicates that the TSF will respond to a failure of the anti-tamper backup battery by becoming permanently disable. This battery is rated for an operational life of 10 years.

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 6.4 of [ST] indicates that self-tests to verify the integrity of the TSF and its data are automatically performed during power-on, and successful completion of the self-tests will result in an audible alert. A user receiving this alert is sufficient for them to have assurance that the integrity of the TSF and its data are verified.

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.

The "LED's Behavior" section of the various user guides identifies how the TOE communicates to the user the results of a successful or failed self-test. This section also states that the user can attempt to resolve a self-test error by restarting the TOE, and specifically refers to the self-test as a "power up self test." From this, there is sufficient information for the user to understand that a self-test may be manually executed by powering on or restarting the TOE. The TOE does not have a separate 'restart' button or option; a restart is achieved by unpowering and re-powering the TOE.

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.

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 6.4 of [ST] states that the TOE's response to a self-test failure includes shutting down all peripheral ports and access to the administrative interface, and that failure is indicated visually through turning on all front panel LEDs.

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 [KMN] guidance documents include a note in the "LED's Behavior" section flagged as "IMPORTANT!" This note describes how a failed self-test is communicated to the user (with separate indicators for anti-tamper failure vs user control failure), what checks can be done to attempt to correct the failure, and how to contact the manufacturer if these checks do not correct the failure.

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

The "LED's Behavior" section of the various guidance documents describes separate indications for anti-tamper and user control self-test failures.

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.

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 6.2 of [ST] states that the TOE has a non-volatile audit log that can store up to 100 events, where the oldest events are overwritten when the audit log is full and new events need to be generated. This section lists the individual audit record types and states that each audit record is logged with the event type (three-letter code, with all types and their corresponding codes listed in [ST]), time/date stamp, and pass/fail status. This section also states that the administrator can use a utility to download the audit log to their local computer as a text file.

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] describes how to use a connected computer to interface with the TOE using the admin tool. The "Event Log (auditing)" section describes how to view the audit logs. This also includes a sample output of audit data, a description of the columns, and a table that explains what events the three-letter 'event code' fields refer to for interpreting the logs.

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 of each references section 1.6.2.6.5 for a description of Restore Factory Default (reset) behavior. When this operation is initiated, the following steps are performed:

- If there was any registered USB peripheral device to the CAC port, it will be removed and the TOE will accept only standard smart-card reader USB 1.1/2.0 token or biometric reader.
- User and Administrator log-in credential will be reset back to default.
- The TOE will perform power down for 1,000ms followed by power up.
- During power down, all connected devices will be disconnected from the computers and all internal cache other than auditing log will be wiped.
- After power up the TOE buzzer will buzz twice to indicate completion of power reset and successful self test results.

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.

The Letter of Volatility in Appendix B of [ST] identifies the following effects on each component in response to the Restore Factory Default operation:

- Controller Board Main MCU: all user memory erased and returned to its initial state
- Emulation MCU: all working memory reset to default (no user data contained in this memory)
- KM USB Host Controller: USB keyboard/mouse are disconnected and working memory is reset to default (no user data contained in this memory)
- CAC USB Host Controller: working memory reset to default (this is used primarily to read the device ID of the connected device to determine if it is authorized, no user data contained in this memory)

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.

The “Restore Factory Defaults” section of [Admin] describes how to use the administration tool to factory reset the TOE.

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 6.2 of [ST] states that the TOE is managed through an Administration and Security Management Tool executable file, and that unauthorized access to the TOE's management interface through this tool is prevented by username/password authentication (credential data is stored on the TOE, not the tool). This section notes that the TOE has a default credential that should be changed on first use.

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

[ST] identifies a 'User' and 'Administrator' role on the management interface. According to Table 13 in [ST], the User role's sole authority to manage the TSF is to view/modify configurable device filtration for the CAC device and to terminate their own session. The Administrator role can perform all TOE management functions, including these.

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) f) All functions identified in the above assignment.

Section 6.2 of [ST] addresses the required items as follows:

- Administrator name limitations and syntax requirements: both the Administrator and User account names can be modified with the following constraints:
    - Minimum 4 characters
    - Maximum 8 characters
    - Allowed characters are uppercase and lowercase letters, numbers, and the following special characters: ! @ # $ % & * ( ) _ + - = " ? /
- Administrator password limitations and syntax requirements: both the User and Administrator password are subject to the same constraints as the username field.

- Restoring lost name or password: There is no user-facing mechanism to restore lost username or password. ST states that the owner must contact the manufacturer for assistance when this occurs. (Factory reset would restore the credentials to their default values but authentication is required to trigger a factory reset or else a user could initiate a factory reset to change the admin credential and effectively bypass the authentication mechanism).
- Initial setting of administrator credentials: the TSF does not enforce a password change on first use and only recommends this as part of the initial setup process. Changing a user or administrator credential on first use is changed in the same manner as changing it normally.
- Logon success, fail limitations, and logging: the TSF does not enforce any lockout of the management interface on excessive failed authentication attempts. All logon attempts (whether successful or failed) are logged. The TOE only has one User role account and one Administrator role account (regardless of what they are renamed to) so the Administrator Log On and User Log On audit events are sufficient to uniquely identify the role attempting to access the TSF.
- All functions identified in the assignment: [ST] identifies the following additional functions:
    - View registered CAC device: allows the User or Administrator to see the current whitelisted CAC device, if configured
    - Register new CAC device: allows the User or Administrator to modify the configurable device filtration behavior for the CAC interface to whitelist a particular device
    - Dump log: exports the TOE's audit log to a .txt file on the computer running the management tool
    - Restore factory default: the factory default process was discussed under FDP_RIP_EXT.2 above
    - Terminate session: this simply ends the active session on the management tool

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.

[Admin] separates the available functions into those that can be done by the 'User' role (section 6) and those that can be done by the 'Administrator' role (section 7). These functions by role correspond to what is specified in [ST].

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 verified that the TOE was capable of recording changes to the administrator password and required the updated password to be used for authentication after the password was changed.

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.

Refer to section 2.2.4.1.1 above.

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.

The evaluator identified the following management functions defined in [ST] are described in [Admin] as follows:

- Change user access credential – Referenced in “Change User Credentials” section
- Change administrator access credential – Referenced in “Change Administrator Credentials” section
- View registered CAC device – Referenced in “View Registered CAC Peripheral”
- Register new CAC device – Referenced in “CAC Port Configuration”
- Dump log – Referenced in “Event Log (auditing)”
- Restore factory default – Referenced in “Restore Factory Defaults”
- Terminate session – Referenced in “Terminate Session”

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 6.3 of [ST] states that the TOE's reaction to both opening the device enclosure and to exhaust the anti-tamper battery is to permanently disable the TOE. This section notes that the anti-tamper battery is rated for 10 years of use.

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.

The [KMN] guidance document includes a note under the "LED's Behavior" section that makes the reader aware that anti-tamper functionality is indicated by all front panel LEDs flashing and the buzzer beeping.

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.

The "LED's Behavior" section in the guidance referenced above states that tampering results in permanent disablement of the TOE.

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 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 that was already opened 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 6.2 of [ST] states that the TOE provides reliable timestamps through use of an internal system clock.

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.

Section 7.6 of [Admin] states that the system time is set during initial manufacturing, so there is no mechanism to configure the time.

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] indicates two methods of switching:

- Console buttons: push buttons on the TOE chassis that allow for the desired computer to be selected.
- Cursor control: the selected computer can be switched if the user 'swipes' the connected mouse to the side (left to decrement the selected channel, right to increment).

None of the switching mechanisms involve any of the prohibited behavior (automatic port scanning, control through a connected computer, control through keyboard shortcuts). Console buttons and preview screen control mechanisms are engaged through the express user action of button presses on the TOE

chassis, while cursor control uses mouse commands as a guard. Specifically, the cursor control is not activated unless the user first double-clicks the middle mouse button.

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.

Section 6.2 of [ST] describes the use of cursor control for channel selection. Specifically, it describes how the user can 'swipe' the mouse left or right to decrement or increment the selected channel. This section also states that having this enabled does not disable the use of console buttons as channel selection methods, but that the TOE enforces a two minute delay between engaging a new switching method (e.g. so that it is not possible to change the channel using a console button and then immediately change it back using cursor control).

Section 6.2 of [ST] also identifies the 'guard' on the cursor control mechanism as the user needing to double-click the middle mouse button before the mouse movement will be interpreted by the TOE as a command to switch the selected channel. This action requires multiple deliberate actions to be performed and creates a narrow time window during which the control mechanism is active, both of which ensure that the switching mechanism cannot be engaged accidentally.

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

N/A per PP-Module guidance.

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.

The [KMN] guidance document includes a section called "System Operation" that indicates that the input buttons on the front panel are used to switch the active channel.

The [KMN] guidance document includes a section called "CAC (Common Access Card, Smart Card Reader) Installation" that describes how to enable the CAC port for the active computer.

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.

The [KMN] guidance document includes a section called "Scroll Wheel KM Switching" that describes how to switch channels using the mouse peripheral, including how to engage the guard (click the mouse wheel twice). This document also includes a "Hotkey Commands" section that describes how to configure the topology for the screen layout (i.e. which direction does the user have to 'swipe' to change to a different port selection).

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

2.3.1.1.3 Test Activities

There are no test Evaluation Activities for this component.

N/A

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.

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 6.2 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 6.2 of [ST] indicates that the selected channel is indicated using an LED panel, where each LED is located above the selection button for that particular channel. It also states that the channel selection buttons themselves are backlit and pressing and holding the channel selection button to turn on/off the backlight indicates that the CAC port is active/inactive for the selected channel. [ST] notes that this cannot be used to enable CAC on one channel while another channel is selected; the CAC port is always tied to the other ports even if it is deactivated.

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.

The [KMN] guidance document notes under the “Installation” section that the computer connected to port 1 will always be selected by default after power up. It is also clear from reviewing this guidance that no reset option exists so the TOE is reset by unpowering it directly.

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.

The [KMN] guidance document includes a section called “Front Panel Control” that describes how to use the push buttons to change the selected computer. This section also states that the corresponding LED for the input port will light up when selected.

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 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.

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 6.5 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 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.

This evaluation activity is from the [AO Module] Supporting Document so it is assumed to apply specifically to audio output peripherals.

The [KMN] guidance document includes a note box labeled "IMPORTANT WARNINGS – For security reasons:" that states that the product does not support microphone audio input or line input. This is clearly

identified under the “Installation” section of the guidance. The “System Requirements” table under the “Installation” section clearly identifies the supported audio output peripherals. The “Technical Specifications” table in the guidance lists the audio output interface as “(1) Connector Stereo 3.5mm Female.” These pieces of information are sufficient for the reader to understand the supported peripherals and intended usage of the audio output interface.

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.

The evaluator verified that when an authorized device was connected to the TOE’s 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 speakers.

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 6.5 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 6.5 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.

The [KMN] guidance document includes a note box labeled “IMPORTANT WARNINGS – For security reasons:” that states that the product does not support microphone audio input or line input. This is clearly identified under the “Installation” section of the guidance.

3.1.1.3.3 Test Activities

Evaluator Note: the absence of a Step 3 is a direct reproduction from the test definition in [AO Module]

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 verified that the TOE showed no bias towards the computer's microphone port and that no power was transmitted to the microphone.

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 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).

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.

Refer to the guidance evaluation activities for FDP_PDC_EXT.1 (section 2.1.1.2.2).

4.1.1.1.3 Test Activities

Testing of this component is performed through evaluation of FDP_PDC_EXT.1 Test 2.

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 6.6 of [ST] states that basic USB 1.1/2.0 HID-class devices are authorized as valid endpoints. This section also states that devices with an integrated USB hub or composite devices will be recognized only if there is at least one HID-class endpoint, and in that case only that endpoint will be recognized.

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

Section 6.6 of [ST] states that keyboard and mouse functions are emulated by the TOE, and that the keyboard mouse processor is programmed in firmware specifically only to accept 108-key keyboard and 3-button mouse devices.

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 6.6 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 6.6 of [ST] asserts unidirectional functionality as follows: “To ensure uni-directional data flow, data diodes, optical isolators, and mechanical relays are placed in series between the TOE host emulators and device emulators. Each isolated device emulator has its own respective diode, optical isolator and relay to assure electrical/logical data isolation from other data channels and other TOE functions.”

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 6.5 of [ST] indicates that the keyboard/mouse interface automatically filters non-HID class devices. This is consistent with FDP_FIL_EXT.1/KM’s claim of fixed device filtration.

[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.

N/A – “configurable” is not selected in FDP_FIL_EXT.1.1/KM for either ST.

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.

FDP_FIL_EXT.1.1/KM does not select “configurable” so this activity does not apply to the TOE.

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.

N/A; the TOE does not support configurable device filtration for KM ports.

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.

Appendix B of [ST] states that the Controller Board MCU has a 128-bit buffer for keyboard and mouse data.

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

Appendix B of [ST] states that when switching computers, an AP2146 power switch is triggered for 1ms to remove power from the buffer, which is sufficient time for its contents to be cleared.

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.

The evaluators reviewed [ST] and observed that all switching mechanisms will simultaneously switch all peripherals to the targeted computer, so keyboard and mouse switching is tied.

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.

The evaluator reviewed the guidance documentation and observed that there are no buttons, configuration settings, or other mechanisms that could be used to independently control which input peripherals keyboard and mouse inputs are directed to. All switching of these peripherals are tied.

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.

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 6.7 of [ST] describes the TOE's filtration for CAC devices. Specifically, by default, fixed device filtration is enabled to allow only smart-card reader, PIV/CAC USB token, or biometric reader. If configurable device filtration is enabled, this supersedes the fixed device filtration; specifically, the configurable filtration allows for a single device to be whitelisted such that all other devices are rejected.

[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 6.7 of [ST] states that an authenticated user/administrator may configure device filtration. Section 6.2 describes the 'Register CAC Device' function that is used to do this. The TSF can be reverted to fixed device filtration through factory reset or by removal of the registered device from the whitelist.

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.

FDP_FIL_EXT.1.1/UA selects "configurable." The evaluator reviewed [Admin] and observed that it includes instructions on how to whitelist individual USB devices under the "CAC Port Configuration" sections. Specifically, it not only states how to whitelist an individual peripheral but also states that only a single peripheral can be whitelisted at a time. The "View Registered CAC Peripheral" section describes how to see the current whitelist. Consistent with [ST], the guide lists this behavior under both the 'User' and 'Administrator' sections as both roles can perform these functions.

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.

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 configured the TOE to accept a specific UA device and verified that the TOE rejected all other devices while accepting the configured device.

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.

Section 6.7 in [ST] 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 6.7 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.

The evaluator verified that the connected computer could not be used to power 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 6.7 of [ST] states that when ports are switched, the CAC port is unpowered for 1,000 ms using an integrated high-side power switch optimized for USB. This completely depowers the CAC device from the 5V DC feed for a sufficient amount of time to fully discharge the power.

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.

The “CAC (Common Access Card, Smart Card Reader) Installation” section of the various guidance documents states that an active session on a computer is terminated upon removal of the CAC device.

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.

The evaluator reviewed [ST] and determined that they each identify the CAC port as a distinct physical interface from the keyboard/mouse ports, e.g. by identifying unique sets of filtering rules for each.

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.

The [KMN] guidance document clearly shows separate ports labeled ‘CAC’ and ‘K/M’ for both computer and peripheral connections on the sample rear panel diagram.

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.

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.

The evaluator verified that the TOE did not transmit authentication data from the authentication device to the keyboard or mouse USB cables.

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 6.7 of [ST] states that disconnection of a CAC device from the TOE causes the previously-active session on the connected computer to be disabled. [ST] identifies both device removal and a channel switch as mechanisms that cause session termination.

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.

The “CAC (Common Access Card, Smart Card Reader) Installation” section of the various guidance documents states that an active session on a computer is terminated upon removal of the CAC device.

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.

Refer to section 5.1.1.5.1.

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.

The “System Operation” section of the various guidance documents state that an open session is terminated upon switching to a different computer.

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 Assurance Requirements

6.1 Isolation Document

Note this section refers to the non-proprietary version of [ST]. A proprietary ST was also submitted with the evaluation that included additional isolation materials that were not suitable for public disclosure.

6.1.1 FDP_APC_EXT.1 Active PSD Connections

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.

The vendor included isolation information and assessment in section 7 and Appendix B of [ST] rather than in a separate document. IPGARD organized section 7 by TOE function. Each TOE function subsection describes the implementation of the function and then explains how the implementation meets each applicable security objective along with the corresponding security functional requirements.

Section 6.5 of [ST] covers isolation of audio data flows. The descriptions address the following security objectives relevant to isolation: O.COMPUTER_INTERFACE_ISOLATION, O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED, O.PERIPHERAL_PORTS_ISOLATION, O.UNIDIRECTIONAL_AUDIO_OUT, and O.COMPUTER_TO_AUDIO_ISOLATION. The evaluation activities for the SFRs that are identified in [ST] as being mapped to these objectives confirm the objectives are met.

Section 6.6 of [ST] covers isolation of keyboard and mouse data flows. The proprietary copy of [ST] includes materials that show mechanical, optical, and electrical isolation for a representative TOE model. Because all TOE models claim a single input group, there is no risk of data transmission between multiple input groups. The description addresses a number of TOE objectives; those that are relevant specifically to isolation include O.COMPUTER_INTERFACE_ISOLATION, O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED, O.USER_DATA_ISOLATION, O.PERIPHERAL_PORTS_ISOLATION, and O.UNIDIRECTIONAL_INPUT. The evaluation activities for the SFRs that are identified in [ST] as being mapped to these objectives confirm the objectives are met.

Section 6.7 of [ST] covers isolation of user authentication device data flows. The proprietary copy of [ST] depicts the USB user authentication device subsystem. The description addresses the following security objectives relevant to isolation: O.COMPUTER_INTERFACE_ISOLATION, O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED, O.USER_DATA_ISOLATION, O.PERIPHERAL_PORTS_ISOLATION, and O.USER_AUTHENTICATION_ISOLATION. The evaluation activities for the SFRs that are identified in [ST] as being mapped to these objectives confirm the objectives are met.

Sections 6.3 (tampering protection), 6.4 (self-testing), and Appendix B (Letter of Volatility) of [ST] cover firmware dependencies. Section 6.3 addresses protection of TOE firmware. Section 6.4 describes integrity testing of TOE firmware along with the TOE's response to integrity failures. Appendix B covers storage of TOE firmware. The evaluation activities for the SFRs that are identified in [ST] as being mapped to these objectives confirm the objectives are met.

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

- D.1 General: simply summarizes the requirements of the following sections.
- D.2 Design Description: the overall presentation of the isolation documentation is separated by peripheral type. For each peripheral type, a block diagram (proprietary ST only) is provided along with a description of the diagrammed behavior. The logical and electrical isolation of each of the peripheral channels is described, and the diagrammed materials are sufficient to show the internal and external interfaces of the TOE. The TSS also describes how isolation is triggered in the event of a self-test failure.
- D.3 Isolation Means Justification: The following is a list of potential unauthorized data flows along with references in [ST] to where and how those unauthorized data flows are blocked:
    - **Selected computer to user input peripheral** – sections 6.5 and 6.7 of [ST] describe how data flows are unidirectional from user input peripherals to the selected computer. The proprietary copy of [ST] also includes design information that shows the data flows in a series of block diagrams.
    - **user peripheral output to user peripheral input** – sections 6.5, 6.6, and 6.7 describe how data flows between peripheral ports are prevented through satisfaction of O.PERIPHERAL_PORTS_ISOLATION.
    - **user peripheral input to user peripheral output** – same as 'user peripheral output to user peripheral input' above.
    - **user peripheral output to selected computer** – section 6.5 describes unidirectional data flows for the audio output behavior. The proprietary copy of [ST] also includes design information in both sections that shows the data flows in a series of block diagrams.
    - **user peripheral output to non-selected computer** – same as 'user peripheral output to selected computer' above.
    - **connected computers** – the isolation between connected computers is described in sections 6.5, 6.6, and 6.7, including information on how that isolation is maintained in the event of a self-test failure. Section 6.4 describes how the data isolation is self-tested.
    - **user peripheral input to non-selected computer** – sections 6.6 and 6.7 describe how this data flow is blocked through satisfaction of the O.USER_DATA_ISOLATION objective.
    - **selected computer to non-selected computer** – audio isolation between connected computers is the same as 'connected computers' above.
    - **any data to external entities** – section 6.1 lists the external interfaces to the TOE and shows that there are no additional external interfaces beyond those that are authorized to transmit data.
    - **external entities to any TSF data** – same as 'any data to external entities' above.
    - **user authentication device to non-selected computer** – section 6.7 describes how user authentication data only flows to the connected computer. The proprietary copy of [ST] also includes design information that shows the relevant data flow in a block diagram.
    - **user authentication device to other peripheral device** – section 6.7 describes how the CAC port is isolated from other peripheral interfaces. [ST] also includes design information that shows the relevant data flow in a block diagram.
    - **other peripheral device to user authentication device** – same as 'user authentication device to other peripheral device' above.
    - **user authentication device to other TSF data** – section 6.7 describes how the CAC interface is isolated from other TSF data. The proprietary copy of [ST] also includes design information that shows the relevant data flow in a block diagram.
- D.4 Firmware Dependencies: The Letter of Volatility (Appendix B) describes how all of the TOE firmware is handled. Specifically, the USB firmware exists separately from the display firmware.

The self-test functionality coupled with the immutability of the firmware storage is sufficient to demonstrate that any catastrophic failure of the firmware will cause the TSF to fail closed and continue to enforce isolation.

PSD:AO
The evaluator shall examine the Isolation Documentation to determine that it describes the logic under which the TSF permits audio flows from a connected computer to a connected audio output interface.

Section 6.5 of [ST] states that unidirectional data flow is enforced from the connected computer to audio output interface through the use of unidirectional audio diodes on both left and right stereo channels and unidirectional amplifier.

PSD:AO
The evaluator shall examine the Isolation Documentation to determine that it describes how the TOE enforces audio output data flow isolation from other TOE functions, such that it is not possible for two computers connected to the TOE to use the TOE to communicate with one another. The description shall ensure the signal attenuation in the extended audio frequency range between any computer audio output interfaces is at least 45 dB measured with a 2V input pure sine wave at the extended audio frequency range, including negative swing signal.

Section 6.5 of [ST] states that audio output is filtered in accordance with the Audio Filtration Specifications table specified in [AO Module]. In addition to this, this section states that the TOE's audio multiplexer can control OFF-isolation at a level of 120 dB and channel separation at 116 dB. This protects channel-to-channel crosstalk by ensuring that non-selected channels will not receive audio signal when the active channel is transmitting on a high frequency. Isolation is further enforced by limiting the analog output signal to a range between 45-75 dB and by blocking all digital audio signals.

As mentioned above, unidirectional audio diodes prevent audio transmission to a connected computer, and this is the case regardless of whether the audio signal originates from the console port or from a different connected computer.

PSD:AO
The evaluator shall examine the Isolation Documentation to determine that it describes how the TOE prevents the audio output signal from traversing the TOE while the TOE is powered off.

Section 6.5 of [ST] states that an audio isolation relay is opened when the TOE is unpowered, and that opening this relay isolates the audio input ports (for the computer interfaces) from all internal circuitry. This interface also cannot be used to supply power to the TOE.

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

Section 6.6 of [ST] states that user data is buffered in SRAM, which requires an active power source to operate. It also states that the KM ports cannot be used to supply power to the TOE. Therefore, it is not possible for user data to transit the TOE while it is unpowered because user input data cannot be buffered in SRAM. Additionally, when the TOE is unpowered, an isolation relay is opened to isolate the KM input ports from the rest of the TOE's internal circuitry.

When the TOE is powered on, isolation between connected computers is enforced through the fact that the TOE uses emulated keyboard and mouse input, and that each computer channel has its own microcontroller. Therefore, the emulation occurs after the input data has already been routed to the selected channel through a peripheral multiplexer.

6.1.2 FDP_TER_EXT.3 Session Termination upon Switching

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

Section 6.5 of [ST] describes the process by which power is reset to the CAC interface when a switch occurs. Specifically, power to the USB CAC port is cut for a period of 1,000 ms through the use of an integrated high-side power switch that is optimized for USB applications. This switch completely disconnects the 5V DC power to the connected CAC device. A power-down time of 250 microseconds is sufficient to drop power flow from 5V to under 1.8V which is theoretically a low enough voltage to power down the CAC interface. As 1,000 ms is 400x the duration of 250 microseconds, this adds considerable margin to ensure that power is reset under normal operating conditions, without being sufficiently long to disrupt the speed of switching functionality from a user perspective.

6.1.3 FDP_UAI_EXT.1 User Authentication Isolation

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

Section 6.7 of [ST] states that the TOE CAC ports are physically separate from the KM USB ports. Separation is enforced through separate external ports, isolated internal circuitry, and individual power planes. Logical isolation is also enforced through the use of filtration mechanisms to ensure that CAC devices are not recognized as valid on ports intended for HID devices, and vice versa.

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

PSD:AO
The evaluator shall examine the Isolation Documentation to determine that it describes how the TOE enforces audio output data flow isolation from other TOE functions, such that the audio output peripheral interface is unidirectional and no data can be routed from a connected peripheral back to a connected computer. The description shall ensure the signal attenuation between any TOE audio output peripheral device interface and any other TOE computer audio output interface is at least 45 dB measured with a 2V input pure sine wave at the extended audio frequency range, including negative swing signal.

Isolation of data flow between connected computers is described in section 7.1.1 above.

Enforcement of unidirectional data flow (such that data cannot be routed from a peripheral to a connected computer) is enforced through the use of unidirectional diodes on left and right stereo channels. The LM4880 Boomer analog output amplifier enforces unidirectional audio flow as well. In addition to this, this section states that the TOE's audio multiplexer can control OFF-isolation at a level of 120 dB and channel separation at 116 dB. This protects channel-to-channel crosstalk by ensuring that non-selected channels will not receive audio signal when the active channel is transmitting on a high frequency. Isolation is further enforced by limiting the analog output signal to a range between 45-75 dB and by blocking all digital audio signals.

6.2 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.

All ST evaluation has been performed in the proprietary Evaluation Technical Report and in the evaluation activities above.

6.3 Class ADV: Development

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 2-5 above and to the Isolation Document materials in section 6.1 above. 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.

6.3.1.1 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 2-5 above and to the Isolation Document materials in section 6.1 above.

6.4 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 [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).

6.4.1 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.

6.4.1.1 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.

6.5 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.

6.5.1 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).

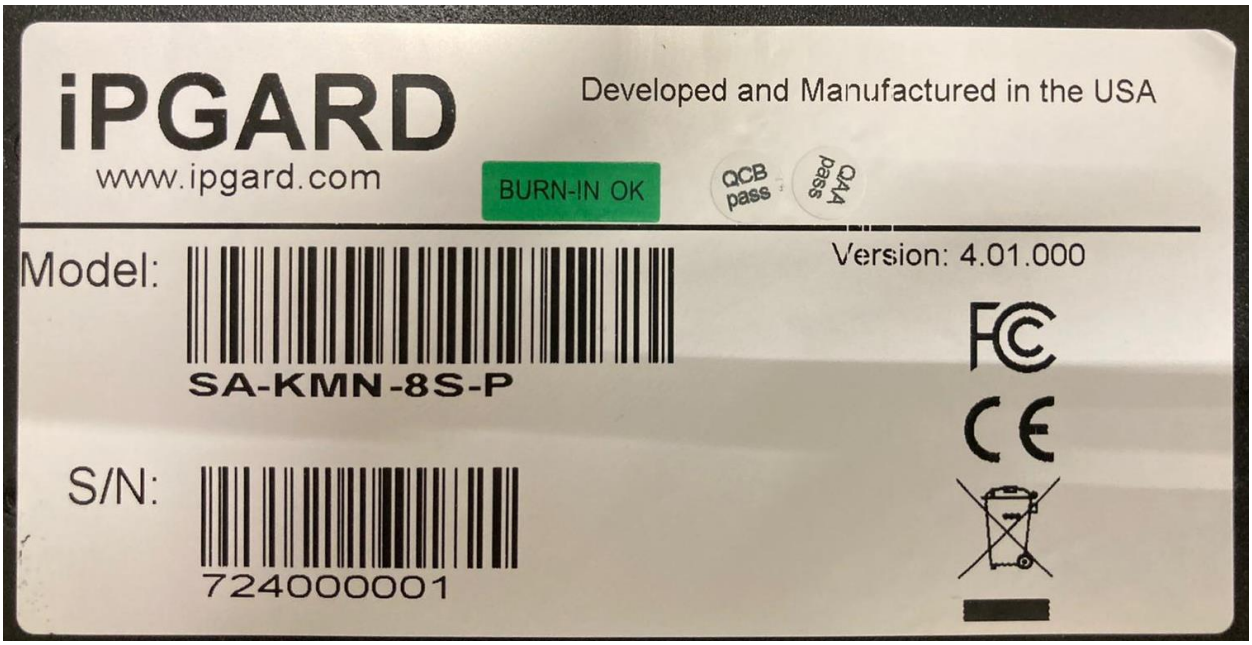
The evaluator performs the CEM work units associated with ALC_CMC.1, as well as the Evaluation Activity specified below.

[ST] identifies every TOE component and the firmware version number. Each TOE device is labelled and each label uniquely identifies the TOE model number, version number, and serial number. Tamper evident labels have been placed in critical locations on the TOE enclosure to assure that any attempt to open the enclosure enough to gain access to its internal components will change at least one label to a tampered state. At least one tamper evident label is placed in a location that will be visible to the user operating the TOE.

The following image shows a representative TOE model with the product vendor and model name on the faceplate:

The following image shows the underside of the same chassis. This image shows the product label which includes the model name and firmware version, as well as the applied tamper evident seals on the external housing.

The following image is a close-up of the label from the previous image.



6.5.1.1 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 [ST], and that the models used for testing are a subset of the models identified in [ST], with physical labeling that correctly identifies both the model and its associated firmware version.

6.5.2 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.

6.6 Class ATE: Life-Cycle Support

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.

6.7 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 was conducted between January 11 and May 26, 2021, with additional supplemental evidence collected as needed through June 30, 2021.

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 models were tested, with parentheses to indicate what subset of testing was performed on them, if any (no parenthetical statement indicates that full testing was done):

- SA-KMN-8S-P

The tested environment consisted of the following non-TOE components:

- 4x desktop computers
- 1x keyboard
- 1x mouse
- 1x external speakers
- 1x CAC smartcard reader
- 1x printer
- 1x USB thumb drive
- 1x audio headset
- 1x USB hub
- 1x microphone
- 1x multimeter
- 1x oscilloscope
- 1x external signal generator

The following equivalency arguments were applied:

- Ports available – The number of available ports on each device does not affect the device's ability to enforce the security controls on any given port or selected port combination. Design information and test sampling is used to demonstrate that no arbitrarily-chosen pair of ports is designed or implemented in a manner that would affect their isolation from one another when compared to any other pair. For audio isolation, equivalency was asserted through the following two test samples:
    - For one arbitrarily-chosen port, all fifteen designated frequencies were played on that port, and all other ports on the device were observed to ensure that no signal bleed was detected.
    - For each other port, at least one arbitrarily-chosen frequency was played on that port, and all other ports on the device were observed to ensure that no signal bleed was detected.

This was iterated enough times such that at least every port was sampled at least once and at least every frequency was sampled at least once.

- USB functionality – All devices use an identical USB controller; thus, testing on one device is sufficient to demonstrate equivalent behavior on other devices.
- USB device types – The TOE's USB fixed device filtration is implemented based on the enumerated device class. Arbitrary representative devices of HID and CAC classes were chosen; testing did not include an exhaustive sample of every type of peripheral that enumerates as one of those types. In particular, CAC testing only included a card reader and not a biometric reader.

6.7.1 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 ST 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.

6.8 Class AVA: Vulnerability Assessment

6.8.1 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 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

6.8.1.1 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 June 25, 2021. During each search, no known vulnerabilities were revealed.