

# Black Box Secure KM Switch Security Target (CAC Models)

Release Date: November 3, 2021

Revision: 1.07

Author: John Hickey, Black Box Corporation



# Table of Contents

- 1 Introduction.....6**
  - 1.1 ST and TOE Identification ..... 6
  - 1.2 PP Reference Identification ..... 6
  - 1.3 Organization ..... 7
  - 1.4 Conventions ..... 8
  - 1.5 Technical Definitions ..... 8
    - 1.5.1 ST Specific Terminology ..... 8
    - 1.5.2 Acronyms ..... 12
  - 1.6 TOE Overview ..... 12
    - 1.6.1 TOE Architecture (High Level) ..... 12
    - 1.6.2 TOE Details ..... 13
  - 1.7 TOE Scope and Boundary ..... 18
    - 1.7.1 Overview ..... 18
    - 1.7.2 Environment..... 19
  - 1.8 Guidance Documents ..... 20
  - 1.9 Features Outside of TOE Evaluation Scope ..... 20
- 2 Security Problem Description ..... 20**
  - 2.1 Assumptions ..... 21
  - 2.2 Organizational Security Policies ..... 22
  - 2.3 Threats ..... 22
- 3 Security Objectives ..... 24**
  - 3.1 Security Objectives for the TOE ..... 24
  - 3.2 Security Objectives for the Operational Environment ..... 26
- 4 Security Requirements..... 28**
  - 4.1 TOE Security Functional Requirements ..... 28
    - 4.1.1 Overview ..... 28
    - 4.1.2 Class FAU: Security Audit ..... 30
    - 4.1.3 Class FDP: User Data Protection ..... 31
    - 4.1.4 Class FIA: Identification and Authentication ..... 37
    - 4.1.5 Class FMT: Security Management..... 37
    - 4.1.6 Class FPT: Protection of the TSF ..... 38

Black Box Secure KM Switch Security Target (CAC Models)	Rev 1.07
4.2 Rationale for TOE Security Requirement Dependencies .....	39
4.3 TOE Security Assurance Requirements.....	39
<b>5 Conformance Claims .....</b>	<b>41</b>
5.1 CC Conformance Claims .....	41
5.2 PP Conformance Claims .....	41
5.3 ST Conformance Requirements .....	41
<b>6 TOE Summary Specification.....</b>	<b>43</b>
6.1 TOE External Interfaces Security Functions .....	43
6.2 TOE Administration, User Control, and Monitoring Security Functions .....	43
6.3 TOE Tampering Protection.....	45
6.4 TOE Self-Testing .....	47
6.5 TOE Audio Subsystem Security Functions .....	47
6.6 TOE Keyboard and Mouse Functionality.....	49
6.7 TOE User Authentication Device Subsystem Security Functions.....	51
<b>Appendix A – Product’s Model Name Structure.....</b>	<b>54</b>
<b>Appendix B – Letter of Volatility .....</b>	<b>55</b>
Main PCBA: USB .....	55
Front Panel PCBA .....	57

## Table of Figures

Figure 1: Standard Setup of 4-Port KM TOE Installation.....	19
---	----

# List of Tables

- Table 1 – ST Composition ..... 6
- Table 2 – ST Identification..... 6
- Table 3 – ST Technical Definitions ..... 12
- Table 4 – ST Acronyms ..... 12
- Table 5 – Black Box 4-Port Secure TOE Identification..... 13
- Table 6 – Black Box 8-Port Secure TOE Identification..... 13
- Table 7 – Peripheral Devices supported by the TOE ..... 14
- Table 8 – Console Port Protocols (4-Port TOE model) ..... 14
- Table 9 – Console Port Protocols (8-Port TOE model) ..... 14
- Table 10 – Computer Port Protocols (4-Port TOE model) ..... 15
- Table 11 – Computer Port Protocols (8-Port TOE model) ..... 15
- Table 12 – TOE Services ..... 15
- Table 13 – TOE User/Administrator Services and Accessibility..... 16
- Table 14 – TOE Physical Boundary Composition ..... 19
- Table 15 – TOE Components ..... 20
- Table 16 – Environment Components..... 20
- Table 17 – Assumptions ..... 22
- Table 18 – Threats ..... 23
- Table 19 – Security Objectives for the TOE..... 26
- Table 20 – Security Objectives for the Operational Environment ..... 27
- Table 21 – TOE SFR Overview ..... 30
- Table 22 – Audio Filtration Specifications..... 31
- Table 23 – TOE Security Assurance Requirements..... 40

## Document Revisions

Revision#	Date	By	Updates
1.00	June 1, 2020	John Hickey, Black Box	Initial Document Outline
1.01	July 7, 2020	John Hickey, Black Box	Formatting updates and adding NIAP TDs
1.02	July 21, 2020	John Hickey, Black Box	Responding to comments based on preliminary evaluation
1.03	December 30, 2020	John Hickey, Black Box	Updates based on validator feedback
1.04	May 21, 2021	John Hickey, Black Box	Incorporation of NIAP feedback and finalization
1.05	June 25, 2021	John Hickey, Black Box	Incorporation of additional NIAP feedback
1.06	October 1, 2021	John Hickey, Black Box	Incorporation of additional NIAP feedback
1.07	November 3, 2021	John Hickey, Black Box	Incorporation of additional NIAP feedback

# 1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

The composition of the ST is listed in the table below.

No.	Security Target Composition
1	A security problem described as a set of assumptions about the security aspects of the environment (see Chapter 2, Security Problem Description).
2	A set of threats which the product is proposed to identify and counter (see Chapter 2, Security Problem Description).
3	Known rules which the product must comply to (see Chapter 2, Security Problem Description and Chapter 5, Conformance Claims).
4	A set of security objectives to address the security problem (see Chapter 3, Security Objectives).
5	A set of security requirements to address the security problem (see Chapter 4, Security Requirements and Chapter 6, Extended Components Definition).
6	The IT security functions provided by the TOE that meet the set of requirements (see Chapter 7, TOE Summary Specification).

Table 1 – ST Composition

The structure and content of this ST complies with the requirements stated in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 11.

## 1.1 ST and TOE Identification

This section provides information needed to identify and control this ST and its Target of Evaluation (TOE).

<b>ST Title</b>	<b>Black Box Secure KM Switch Security Target (CAC Models)</b>
<b>Revision Number</b>	1.07
<b>ST Publish Date</b>	November 3, 2021
<b>ST Authors</b>	John Hickey, Black Box
<b>TOE Identification</b>	See Tables 5 and 6 below
<b>Keywords</b>	KM, Secure, Black Box, Protection Profile 4.0

Table 2 – ST Identification

## 1.2 PP Reference Identification

The TOE claims conformance to the following PP-Configuration:

PP-Configuration Reference: PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, and User Authentication Devices (CFG\_PSD-AO-KM-UA\_V1.0)

PP-Configuration Sponsor: National Information Assurance Partnership (NIAP)

PP-Configuration Version: 1.0

The claimed PP-Configuration consists of the Base-PP referenced below and PP-Modules that define required functionality and evaluation activities for the specific peripheral types supported by the TOE.

PP Reference: Protection Profile for Peripheral Sharing Device  
PP Sponsor: National Information Assurance Partnership (NIAP)  
PP Version: 4.0  
PP Date: July 19, 2019

PP-Module Reference: PP-Module for Analog Audio Output Devices  
PP-Module Sponsor: National Information Assurance Partnership (NIAP)  
PP-Module Version: 1.0  
PP-Module Date: July 19, 2019

PP-Module Reference: PP-Module for Keyboard/Mouse Devices  
PP-Module Sponsor: National Information Assurance Partnership (NIAP)  
PP-Module Version: 1.0  
PP-Module Date: July 19, 2019

PP-Module Reference: PP-Module for User Authentication Devices  
PP-Module Sponsor: National Information Assurance Partnership (NIAP)  
PP-Module Version: 1.0  
PP-Module Date: July 19, 2019

## 1.3 Organization

### Security Target Introduction (Section 1)

- Identification of the TOE and ST
- Overview of the TOE
- Overview of the content of the ST, document conventions, relevant terminology
- Description of the TOE security functions
- Physical and logical boundaries for the TOE
- Hardware and software that make up the TOE

### Security Problem Description (Section 2)

- Threat List
- Set of organizational security policies
- Set of TOE and TOE environment assumptions

### Security Objectives (Section 3)

- List of Security objectives for the TOE and TOE environment
- Description of how Security Objectives can be trusted to counter the threats identified for the TOE.

### Security Requirements (Section 4)

- List of Security Functional Requirements (SFRs) met by the TOE

- Security Functional Requirements exposition
- List of Security Assurance Requirements (SARs) met by the TOE
- Security Assurance Requirements (SARs) exposition

Conformance Claims (Section 5)

- Applicable Common Criteria (CC) conformance claims
- Protection Profile (PP) conformance claims
- Assurance Package conformance claims

Summary Specification (Section 6)

- List of Security functions provided by the TOE
- How the Security functions satisfy the SFRs.
- List of Security assurance measures for the TOE
- Security assurance measures exposition

## 1.4 Conventions

The Common Criteria (CC) defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement made by ST author (refinements reproduced as-is from the PP are not formatted as such): Indicated with added/substituted text in **bold** text and deletions with ~~strikethroughs~~, if necessary;
- Selection: Indicated with underlined text;
- Assignment within a Selection (or vice versa): Indicated with *italicized and underlined* text;
- Iteration: Indicated by appending the SFR name with a slash followed by text that uniquely references the iteration (e.g. FDP\_PDC\_EXT.2/KM for an iteration of the FDP\_PDC\_EXT.2 SFR that applies specifically to keyboard/mouse functionality)

Extended SFRs are identified with the label “\_EXT” after the requirement name.

In cases where the claimed PP or Module has already completed an operation, the formatting used by the PP or Module is preserved in the ST. Specifically, all completed operations are formatted as *italicized* text and with the original open/closing brackets preserved.

## 1.5 Technical Definitions

See CC Part 1 Section 4 for definitions of common CC terms.

### 1.5.1 ST Specific Terminology

Term	Description
Active Interface/Connection	An Interface between a PSD and Device that currently has user data flowing through it.



<b>Administrator</b>	A person who administers (e.g., installs, configures, updates, audits, maintains) a PSD, Connected Peripherals, and Connections.
<b>Analog Audio</b>	Data stream that uses voltage to describe a continuous sound wave.
<b>Analog Audio Output Computer Interface, or Computer Interface</b>	The Connector on a PSD through which analog audio data enters the PSD from a Connected Computer.
<b>Analog Audio Output Peripheral Interface, or Peripheral Interface</b>	The Connector on a PSD through which analog audio data exits the PSD bound for a peripheral device.
<b>Attenuation</b>	A reduction in signal strength commonly occurring while transmitting analog or digital signals over long distances.
<b>Audio codec</b>	PC subsystem capable of encoding and decoding a digital data stream of audio.
<b>Audio Output Peripheral Device</b>	Speakers, handset, and earphones.
<b>Authorized Peripheral</b>	A Peripheral Device that is both technically supported and administratively permitted to have an active interface with the PSD.
<b>Blacklist</b>	List containing one or more device attributes that will cause the PSD to reject the devices having that attribute.
<b>Configurable Device Filtration (CDF)</b>	A PSD function that filters traffic based on properties of a connected peripheral device and criteria that are configurable by an Administrator.
<b>Composite Device (USB)</b>	A peripheral device that supports more than one device class.
<b>Computer Interface</b>	The PSD's physical receptacle or port for connecting to a computer.
<b>Connected Computer</b>	A computing device connected to a PSD. May be a personal computer, server, tablet, or any other computing device.
<b>Connected Peripheral</b>	A Peripheral that is connected to a PSD.
<b>Connection</b>	A physical or logical conduit that enables Devices to interact through respective interfaces. May consist of one or more physical (e.g., a cable) or logical (e.g., a protocol) components.
<b>Connector</b>	The plug on a Connection that attaches to a Computer or Peripheral Interface.
<b>Device</b>	An information technology product. In the context of this PP, a Device is a PSD, a Connected Computer, or a Connected Peripheral.
<b>Digital Audio</b>	Data stream that uses digital values to describe a sound wave in sampled intervals.

<b>Disconnection of authentication element</b>	Removal of the authentication element, disconnection of a peripheral authentication device (if possible), or switching to a different connected computer (if possible).
<b>Display</b>	A device that visually outputs user data, such as a monitor.
<b>Emulate</b>	Imitate the behavior of a device or a function in a device.
<b>Endpoint (USB)</b>	A source or a sink of data. Universal Serial Bus (USB) host is centric; endpoints occur at the end of the communications channel at the USB function.
<b>Enumeration (USB)</b>	A process that starts as soon as a device connects to the USB host. In this process, the host and the device jointly define the communications and power settings.
<b>Extended Audio Frequency Range</b>	The range from 1Hz to 60 KHz
<b>External Authentication Device</b>	An authentication device that has an exposed USB interface.
<b>Fixed Device Filtration (FDF)</b>	PSD function that accepts or rejects peripheral devices based on fixed parameters loaded during production.
<b>Guard</b>	A PSD function that requires multiple express user actions in order to switch between Connected Computers using Connected Peripherals.
<b>Headphones</b>	Computer audio peripheral device with one or more small speakers
<b>HID</b>	A device that allows input from, or sends output to human users.
<b>Host (USB)</b>	Initiates all communication on the USB and numbers the connected devices.
<b>Interface</b>	A shared boundary across which two or more Devices exchange information through a Connection.
<b>Interface (USB)</b>	Groups of endpoints. Each interface relates with a single device function. An exception to this is endpoint zero, which is for device configuration and not associated with any interface.
<b>Internal Authentication Device</b>	An authentication device that has no exposed interface.
<b>Isolator or Filter</b>	A PSD with a single Connected Computer.
<b>KM</b>	A type of PSD that shares a keyboard and pointing device between Connected Computers. A KM may optionally include an analog audio device.
<b>Letter of Volatility</b>	A letter issued by the manufacturer outlining whether onboard memory can store data when the device is powered off (non-volatile) or not (volatile).
<b>Monitoring</b>	The ability of a User to receive an indicator of the current Active Interface.

<b>Non-Selected Computer</b>	A Connected Computer that has no Active Interfaces with the PSD.
<b>Peripheral/Peripheral Device</b>	A Device with access that can be Shared or Filtered by a PSD.
<b>Peripheral Interface</b>	The PSD's physical receptacle or port for connecting to a Peripheral Device.
<b>Protocol</b>	A set of rules or procedures for transmitting data between electronic devices.
<b>Remote Controller</b>	Remote component of the PSD that extends the controls and indications through a cable.
<b>Removal of authentication element</b>	Removal of smart-card, token, or proximity card from the authentication device reader.
<b>Secure State</b>	An operating condition in which the PSD disables all connected peripheral and connected computer interfaces when the correctness of its functions cannot be ensured.
<b>Selected Computer</b>	A Connected Computer that has Active Interfaces with the PSD.
<b>Sub-Protocol</b>	A set of common commands flowing within a protocol.
<b>Supported Peripheral</b>	A Peripheral Device that is technically supported by the PSD.
<b>Touch Screen</b>	A pointing device Peripheral Device that enable users to touch one or more objects on the screen or to point the cursor device to specific locations.
<b>USB Audio codec</b>	Computer audio peripheral device with USB digital input/output, one or more analog audio outputs and one or more analog audio inputs.
<b>USB Device</b>	USB devices are leafs in the USB tree that are connected to the host.
<b>USB Dummy Load</b>	A USB Type A plug with resistor connected between positions 1 and 4 and used to simulate overloading a TOE USB peripheral device interface.
<b>USB Hub</b>	A device that expands a single USB port into several so there are more ports available to connect devices to a host system.
<b>User</b>	A person that interacts with a PSD (or a process or mechanism acting on behalf of a person).
<b>User Authentication Device</b>	A Peripheral Device that is used to affirm the identity of a User attempting to authenticate to a computer (e.g., smart card reader, biometric authentication device, proximity card reader).
<b>User Authentication Session</b>	A peripheral device used to authenticate the identity of the user, such as a smart-card reader, biometric authentication device, or proximity card reader.
<b>User Authentication Session Information</b>	User data for user authentication devices.

<b>User Data</b>	Information that the User inputs to the Connected Computer or is output to the User from the Connected Computer (and including user authentication and credential information)
<b>Whitelist</b>	List containing one or more device attributes that will cause the TOE to accept the devices having that attribute.

Table 3 – ST Technical Definitions

### 1.5.2 Acronyms

Acronym	Full Definition
ARC	Audio Return Channel
CEC	Consumer Electronics Control
dB	Decibel
dBv	A measurement of voltage ratio to 1 volt
HID	Human Interface Device
HPD	Hot Plug Detect
KHz	Kilohertz
KM	Keyboard, Mouse
mV	Millivolt
PC	Personal Computer
PSD	Peripheral Sharing Device
PS/2	Personal System/2
OSP	Organizational Security Policies
PSD	Peripheral Sharing Device
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
USB	Universal Serial Bus

Table 4 – ST Acronyms

## 1.6 TOE Overview

### 1.6.1 TOE Architecture (High Level)

Black Box Secure Peripheral Sharing Switches (PSD) provide a secure medium to share a single set of peripheral components such as keyboard and mouse/pointing devices among one or multiple computers over USB.

The Black Box Secure PSD product utilizes multiple isolated microcontrollers to emulate the connected peripherals in order to prevent a multitude of threats. The TOE is also equipped with numerous uni-directional data flows forcing devices to guarantee isolation of connected computer data channels.

Black Box Secure KM port models:

- 4-Port
- 8-Port

The Black Box Secure PSD is compatible with standard personal/portable computers, servers or thin-clients. Connected computers are assumed to run off-the-shelf general-purpose operating systems such as Windows or Linux. The PSD includes ports for the following interfaces, depending on model:

- USB keyboard – the TOE does not allow USB traffic to flow from the TOE to a connected keyboard via the peripheral port
- USB mouse or other pointing device – the TOE does not allow USB traffic to flow from the TOE to a connected pointing device via the peripheral port
- 3.5mm Audio Input (computer ports) – the TOE does not allow audio output to flow from the TOE to a connected computer via the computer ports (i.e. the use of a microphone peripheral is not supported)
- 3.5mm Audio Output (peripheral port) – the TOE does not allow audio input to flow from a peripheral to the TOE via the peripheral port (i.e. the use of a microphone peripheral is not supported)
- USB authentication device (e.g. Smart-card reader, PIV/CAC reader, Token or Biometric reader)

Tables 5 and 6 below provide a summary of the Black Box Secure KM security features by supported interface types. A detailed description of the TOE security features and how they are mapped to the claimed SFRs can be found in Section 6 (TOE Summary Specification) below.

## 1.6.2 TOE Details

### 1.6.2.1 Evaluated Products

#	Model Name	Description	Eval. Version
1	KVS4-1004KX	4-Port Secure KM w/audio and CAC	4.11.000

Table 5 – Black Box 4-Port Secure TOE Identification

#	Model Name	Description	Eval. Version
1	KVS4-1008KX	8-Port Secure KM w/audio and CAC	4.11.000

Table 6 – Black Box 8-Port Secure TOE Identification

Notes:

- CAC = Common Access Card filtered USB port.
- Description - Includes text that is printed on a label attached to each device on the bottom.
- Eval. Version – Firmware and hardware revision per each device.
- Black Box’s model name logic can be found in Appendix A.

### 1.6.2.2 Common Criteria Product Type

The TOE is classified as a “Peripheral Sharing Device” (KM device) in the Common Criteria. Hardware and firmware components are included in the TOE.

### 1.6.2.3 Peripheral Devices Supported by the TOE

The peripheral devices that supported by the TOE are listed in the following table.

Console Port	Authorized Devices
--------------	--------------------

<b>Keyboard</b>	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.
<b>Audio out</b>	Analog amplified speakers, Analog headphones.
<b>Mouse / Pointing Device</b>	Any wired mouse or trackball without internal USB hub or composite device functions.
<b>User Authentication Device</b>	USB devices identified as user authentication (base class 0Bh, e.g. Smart-card reader, PIV/CAC reader, Token, or Biometric reader)

Table 7 – Peripheral Devices supported by the TOE

1.6.2.4 *Protocols Supported by the TOE*

Tables 8 and 9 below identify the console (peripheral) interface protocols supported by the TOE. Tables 10 and 11 below identify the host (computer) interface protocols supported by the TOE.

<b>Model</b>	<b>KVS4-1004KX</b>
Keyboard USB 1.1/2.0	✓
Mouse USB 1.1/2.0	✓
Audio Analog Stereo	✓
CAC USB 1.1/2.0	✓

Table 8 – Console Port Protocols (4-Port TOE model)

<b>Model</b>	<b>KVS4-1008KX</b>
Keyboard USB 1.1/2.0	✓
Mouse USB 1.1/2.0	✓
Audio Analog Stereo Output	✓
CAC USB 1.1/2.0	✓

Table 9 – Console Port Protocols (8-Port TOE model)

Model	KVS4-1004KX
Keyboard and Mouse USB 1.1/2.0	✓
Audio - Analog Stereo Input	✓
CAC USB 1.1/2.0	✓

Table 10 – Computer Port Protocols (4-Port TOE model)

Model	KVS4-1008KX
Keyboard and Mouse USB 1.1/2.0	✓
Audio - Analog Stereo Input	✓
CAC USB 1.1/2.0	✓

Table 11 – Computer Port Protocols (8-Port TOE model)

1.6.2.5 *Logical Scope of the TOE*

1.6.2.5.1 Basic KM TOE Function Overview

Secure KM devices allow an individual user to utilize a set of peripherals to operate in an environment with one or several isolated computers. KM devices allow switching keyboard, mouse, audio, and USB/CAC from one isolated computer to another.

Table 12 below shows the various TOE services that were verified in the current evaluation.

TOE Service	Verification
User peripheral isolation from source computer	✓
Enable/Disable user USB device to each channel	✓
Admin access to management and log functions	✓
Restore factory defaults function	✓
Mapping user keyboard and mouse to chosen computer	✓
Cursor control of selection channels	✓
Mapping user audio device to chosen computer	✓
Mapping user USB CAC peripheral device to selected computer	✓

Table 12 – TOE Services

## 1.6.2.6 Administrative and User configuration of the TOE

Table 13 below shows a summary of user/administrator administrative and security management features. An authenticated User and authenticated Administrator are both considered types of administrators for the PSD PP. See section 6.2 for detailed description of the administration tool architecture.

Menu Option	User	Administrator
Change User Access Credentials		✓
Change Admin Access Credentials		✓
View Registered CAC Device	✓	✓
Register New CAC Device	✓	✓
Dump Log		✓
Restore Factory Default (reset)		✓
Terminate Session	✓	✓

Table 13 – TOE User/Administrator Services and Accessibility

- 1.6.2.6.1 Change User and Admin Credentials option is available for Administrator only, allows updating both the username and password.
- 1.6.2.6.2 View Registered CAC Device option is available for Administrator and User, allows checking what peripheral USB device was registered if any.
- 1.6.2.6.3 Register New CAC Device option is available for Administrator and User, allows registration of a new peripheral USB device to the CAC port.
- 1.6.2.6.4 Dump Log (auditing) option is available for Administrator only, allows generating a detailed report of security functions such as self test, rejected peripheral USB device connection, restore factory default (reset) and failure to log in.
- 1.6.2.6.5 Restore Factory Default (reset) option is available for Administrator only. The following events will occur when selecting this option:
1. 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.
  2. User and Administrator log-in credential will be reset back to default.
  3. The TOE will perform power down for 1,000ms followed by power up.
  4. During power down, all connected devices will be disconnected from the computers and all internal cache other than auditing log will be wiped.
  5. After power up the TOE buzzer will buzz twice to indicate completion of power reset and successful self test results.



### 1.6.2.6.6 Terminate Session logs out the authenticated User or Administrator.

### 1.6.2.7 TOE Security Functions Overview

The following list is an overview of the security features supported by the TOE.

#### TOE Keyboard and Mouse Security Functions

1. No data is stored in non-volatile memory (SRAM only).
2. USB Keyboard and mouse data flows are converted to a serial data flow channel which is isolated from each connected computer and all TOE internal circuitry.
3. Keyboard and mouse channels are isolated electrically and logically from each connected computer and all TOE internal circuitry.
4. Uni-directional data flow enforced by using uni-directional optical data diodes.
5. Temporary power shut down during channel switching to eliminate previous cached keyboard/mouse commands.
6. Device/Host emulators used to prevent connected computer and peripheral device direct communication/data leakage.
7. Device/Host emulators used to maintain KM emulation system on all channels during TOE operation (enabling non-selected connected computers to have emulation even when the user uses another PC).
8. The TOE rejects all unauthorized peripheral devices.
9. Keyboard LEDs will not turn on despite valid keyboard commands being executed (ex: Caps Lock LED will not turn on) to enforce unidirectional communication.
10. The TOE only allows valid and simple keyboard and mouse commands. All other USB traffic is rejected. All advanced keyboard and mouse devices will have their non-basic features disabled by the TOE.
11. Keyboard and mouse channels remain isolated when the TOE is not powered.

#### TOE External Interfaces Security Functions

1. No docking protocols supported by the TOE.
2. No analog audio input allowed by peripherals connected to the TOE.
3. Devices allowed by the TOE:
  - Wired USB 1.1/2.0 keyboard and mouse
  - 3.5mm Analog audio output jack
  - Administrator controlled configurable USB 1.1/2.0 user authentication port that can authorize specific USB devices (default allows only CAC/biometric reader)

#### TOE Audio Subsystem Security Functions

1. Stereo audio channel for each connected computer that is isolated electronically/logically from all TOE internal circuitry.
2. No analog microphones allowed by the TOE.
3. LM4880 Boomer audio power amplifier designed specifically to provide high quality output power with a minimal amount of external components using surface mount packaging.
4. LM4880 Boomer analog output amplifier enforces uni-directional data flow from computer to TOE on both left and right stereo audio with internal transistors to prevent microphone access to the computer.
5. Audio data flow is not converted, stored, or used by the TOE to prevent data leakage.
6. Audio channels remain isolated when the TOE is not powered.

#### TOE User Authentication Device Subsystem Security Functions

1. Electrically/logically isolated USB/CAC port for each connected computer.

2. Administrator controlled configurable USB/CAC ports that can authorize specific USB devices.
3. During USB/CAC channel switching, temporary power dip resets authentication to prevent data leakage.
4. The TOE rejects all unauthorized USB/CAC devices in default settings.
5. USB/CAC LED indication when port being used by an authorized device (solid light), unauthorized device (flashing light), or unused (off).
6. USB/CAC channels remain isolated when the TOE is not powered.

**TOE User Control and Monitoring Security Functions**

1. Visual indications of current channel state via TOE push-button LEDs.
2. Connected computer channel can be changed by manual pressing of push-button on TOE.
3. Front panel LED indications cannot be dimmed or altered in any way during TOE operation.

**Self-Testing**

1. TOE self-testing function that forcibly executes prior to system power up.
2. Self-testing function failure temporarily disables normal TOE operation until system reboot and subsequent passing of all self-test functions.
3. Self-testing function failure has visual and audible indications (flashing push-button LEDs, pulsing relays).

**Anti-Tampering**

1. Permanently active anti-tampering system powered by external supply or internal backup battery (rated for 10 years of operation).
2. Anti-tampering system trigger forces isolation of all connected computers and peripheral devices.
3. Visible and audible indications occur after anti-tampering system trigger (flashing push-button LEDs, pulsing relays, internal alarm beeping).
4. Generated log function to provide an auditable trail for TOE security events.
5. All TOE microcontrollers are protected against firmware read/write from external tools.
6. Uniquely numbered holographic tamper evident label (TEL) placed on TOE to indicate any physical attempt to access TOE internal circuitry.

A more detailed version of this overview is provided in Section 6 below.

## 1.7 TOE Scope and Boundary

### 1.7.1 Overview

The TOE is a Peripheral Sharing Device that supports the following types of peripherals:

- Analog audio output
- Keyboard/Mouse input
- User authentication device input

The TOE models also include an isolator that lacks switching capability.

The physical boundary of the TOE consists of (refer to Figure 1 and Table 14 below):

No.	Physical Boundary of TOE
1	One Black Box Secure KM Switch

2	The TOE computer interface cables that are shipped with the product
3	The permanently programmed embedded firmware inside the TOE on each microcontroller and processor
4	Log data, settings data, state data stored in the TOE
5	The TOE power supply that is shipped with the product
6	User Guidance Manual. Current version available for download at: <a href="https://www.blackbox.com/NIAP4/documentation">https://www.blackbox.com/NIAP4/documentation</a>
7	Administrator Guidance. Current version available for download at: <a href="https://www.blackbox.com/NIAP4/documentation">https://www.blackbox.com/NIAP4/documentation</a>

Table 14 – TOE Physical Boundary Composition

The evaluated TOE configuration only includes supplied computer interface cables attached to the TOE (no peripherals are supplied by Black Box). The following figures represent the TOE and its environment.

The figures below show representative examples of supported TOE models and their connections to peripherals and computers. This includes a 4-port single-head model. The 8-port model behaves the same way as 4-port models except that additional connected computers are supported.

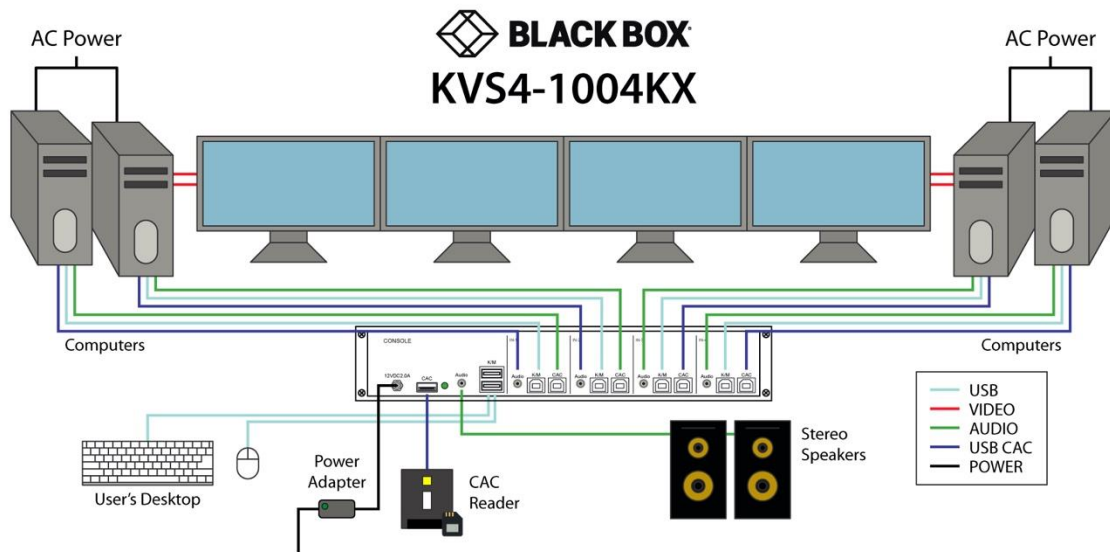


Figure 1: Standard Setup of 4-Port KM TOE Installation

### 1.7.2 Environment

The following tables identify hardware components and indicate whether or not each component is in the TOE or Environment.

Component	Part Number (P/N)	Description
Each device listed in Tables 5 and 6 above.	Same as model number	TOE Hardware

<b>Black Box KM Cables</b>	USB005-0006	USB Cable – Type A Male to Type B Male, Black, 6-ft. (1.8-m)*
	EJ110-0005	3.5-mm Stereo Audio Cable, 24 AWG, Male/Male, 5-ft. (1.5-m)*

Table 15 – TOE Components

\*These cables are used for connecting the TOE to peripheral devices/connected computers.

<b>Component</b>	<b>Description</b>
<b>Standard USB Mouse</b>	Shared Peripheral Hardware
<b>Standard USB Keyboard</b>	Shared Peripheral Hardware
<b>Audio Device (Speakers: supports 3.5mm connector)</b>	Shared Peripheral Hardware
<b>USB User Authentication Device or any other USB device which was configured to work with the TOE in advance.</b>	Console user authentication device interface
<b>Standard PC, Server, portable computer or thin client running any operating system</b>	Connected Computer(s)

Table 16 – Environment Components

## 1.8 Guidance Documents

User manuals for each TOE model and an administrative guide are available for download via the following link: <https://www.blackbox.com/NIAP4/documentation>. The following links on the page are relevant to the TOE:

- Advanced 4/8-Port Secure KM Switch
- Secure KVM Administration and Security Management Tool Guide (CAC)

Note that the Administration and Security Management Tool Guide applies to both KVM and KM product models; none of the management functionality relates to video interfaces so this guide applies fully to the TOE even though it has “KVM” in the title.

## 1.9 Features Outside of TOE Evaluation Scope

This section identifies any items that are specifically excluded from the TOE.

- **Cursor Control Topology:** the default behavior of the product is that cursor control can be used to decrement the selected channel by swiping left after disengaging the guard, and to increment the selected channel by swiping right after disengaging the guard. The product can be configured into alternate topologies that change the relationship between the mouse swipe direction and the channel switching behavior. In the evaluated configuration, the default configuration is used.

## 2 Security Problem Description

This section lists the assumptions pertaining to the environment in which the TOE is to be used in and describes the conditions for the secure operation of the TOE.

Note: The following content in this section has been taken from the Security Problem Description of the claimed PSD PP and the other PP-Modules in the claimed PP-Configuration and are replicated here for clarity.

### 2.1 Assumptions

The following table defines the assumptions regarding the deployment and use of the TOE. These assumptions are defined in the PSD PP and the PP-Modules that comprise the PP-Configuration that the TOE claims conformance to.

Assumption	Definition
<b>Protection Profile for Peripheral Sharing Device</b>	
<b>A.NO_TEMPEST</b>	Computers and peripheral devices connected to the PSD are not TEMPEST approved.  (Added from PP-Module for Keyboard/Mouse Devices) The TSF may or may not isolate the ground of the keyboard and mouse computer interfaces (the USB ground). The Operational Environment is assumed not to support TEMPEST red-black ground isolation.
<b>A.PHYSICAL</b>	The environment provides physical security commensurate with the value of the TOE and the data it processes and contains.
<b>A.NO_WIRELESS_DEVICES</b>	The environment includes no wireless peripheral devices.
<b>A.TRUSTED_ADMIN</b>	PSD Administrators and users are trusted to follow and apply all guidance in a trusted manner.
<b>A.TRUSTED_CONFIG</b>	Personnel configuring the PSD and its operational environment will follow the applicable security configuration guidance.
<b>A.USER_ALLOWED_ACCESS</b>	All PSD users are allowed to interact with all connected computers. It is not the role of the PSD to prevent or otherwise control user access to connected computers. Computers or their connected network shall have the required means to authenticate the user and to control access to their various resources.
<b>PP-Module for Analog Audio Output Devices</b>	
<b>A.NO_MICROPHONES</b>	Users are trained not to connect a microphone to the TOE audio output interface.
<b>PP-Module for Keyboard/Mouse Devices</b>	

N/A – this PP-Module does not define any assumptions beyond those defined in the PSD PP.
<b>PP-Module for User Authentication Devices</b>
N/A – this PP-Module does not define any assumptions beyond those defined in the PSD PP.

Table 17 – Assumptions

## 2.2 Organizational Security Policies

No Organizational Security Policies (OSPs) are listed in the claimed PP that needs to be addressed by the TOE.

## 2.3 Threats

The following table defines the threats expected to be mitigated by the TOE. These threats are defined in the PSD PP and the PP-Modules that comprise the PP-Configuration that the TOE claims conformance to.

Threat	Definition
<b>Protection Profile for Peripheral Sharing Device</b>	
<b>T.DATA_LEAK</b>	A connection via the PSD between one or more computers may allow unauthorized data flow through the PSD or its connected peripherals.
<b>T.SIGNAL_LEAK</b>	A connection via the PSD between one or more computers may allow unauthorized data flow through bit-by-bit signaling.
<b>T.RESIDUAL_LEAK</b>	A PSD may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer.
<b>T.UNINTENDED_USE</b>	A PSD may connect the user to a computer other than the one to which the user intended to connect.
<b>T.UNAUTHORIZED_DEVICES</b>	The use of an unauthorized peripheral device with a specific PSD peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSD or its connected computers.
<b>T.LOGICAL_TAMPER</b>	An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code or data stored in the PSD's volatile or non-volatile memory to allow unauthorized information flows.
<b>T.PHYSICAL_TAMPER</b>	A malicious user or human agent could physically modify the PSD to allow unauthorized information flows.
<b>T.REPLACEMENT</b>	A malicious human agent could replace the PSD during shipping, storage, or use with an alternate device that does not enforce the PSD security policies.

<b>T.FAILED</b>	Detectable failure of a PSD may cause an unauthorized information flow or weakening of PSD security functions.
<b>PP-Module for Analog Audio Output Devices</b>	
<b>T.MICROPHONE_USE</b>	A malicious agent could use an unauthorized peripheral device such as a microphone, connected to the TOE audio out peripheral device interface to eavesdrop or transfer data across an air-gap through audio signaling.
<b>T.AUDIO_REVERSED</b>	A malicious agent could repurpose an authorized audio output peripheral device by converting it to a low-gain microphone to eavesdrop on the surrounding audio or transfer data across an air-gap through audio signaling.
<b>PP-Module for Keyboard/Mouse Devices</b>	
N/A – this PP-Module does not define any threats beyond those defined in the PSD PP.	
<b>PP-Module for User Authentication Devices</b>	
N/A – this PP-Module does not define any threats beyond those defined in the PSD PP.	

Table 18 – Threats

### 3 Security Objectives

This chapter defines the security objectives for the TOE and the Operational Environment.

- Security Objectives for TOE are directly addressed by TOE
- Security Objectives for Operational environment are not addressed directly by TOE. These security objectives are addressed by non-technical methods, such as through the IT domain.

#### 3.1 Security Objectives for the TOE

The following table defines the security objectives that must be satisfied by the TOE. These objectives are defined in the PSD PP and the PP-Modules that comprise the PP-Configuration that the TOE claims conformance to.

Security Objective	Definition
<b>Protection Profile for Peripheral Sharing Device</b>	
<b>O.COMPUTER_INTERFACE_ISOLATION</b>	The PSD shall prevent unauthorized data flow to ensure that the PSD and its connected peripheral devices cannot be exploited in an attempt to leak data. The TOE-Computer interface shall be isolated from all other PSD-Computer interfaces while TOE is powered.
<b>O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED</b>	The PSD shall not allow data to transit a PSD-Computer interface while the PSD is unpowered.
<b>O.USER_DATA_ISOLATION</b>	The PSD shall route user data, such as keyboard entries, only to the computer selected by the user. The PSD shall provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
<b>O.NO_USER_DATA_RETENTION</b>	The PSD shall not retain user data in non-volatile memory after power up or, if supported, factory reset.
<b>O.NO_OTHER_EXTERNAL_INTERFACES</b>	The PSD shall not have any external interfaces other than those implemented by the TSF.
<b>O.LEAK_PREVENTION_SWITCHING</b>	The PSD shall ensure that there are no switching mechanisms that allow signal data leakage between connected computers.
<b>O.AUTHORIZED_USAGE</b>	The TOE shall explicitly prohibit or ignore unauthorized switching mechanisms, either because it supports only one connected computer or because it allows only authorized mechanisms to switch between connected computers. Authorized switching mechanisms shall require express user action restricted to console buttons, console switches, console touch screen, wired remote control, and peripheral devices using a guard. Unauthorized switching mechanisms include keyboard shortcuts, also known as "hotkeys," automatic port scanning, control through a connected computer, and control through keyboard shortcuts. Where applicable, the results of the switching activity shall be indicated by the TSF so that it is clear to the user that the switching mechanism was engaged as intended.



	A conformant TOE may also provide a management function to configure some aspects of the TSF. If the TOE provides this functionality, it shall ensure that whatever management functions it provides can only be performed by authorized administrators and that an audit trail of management activities is generated.
<b>O.PERIPHERAL_PORTS_ISOLATION</b>	The PSD shall ensure that data does not flow between peripheral devices connected to different PSD interfaces.
<b>O.REJECT_UNAUTHORIZED_PERIPHERAL</b>	The PSD shall reject unauthorized peripheral device types and protocols.
<b>O.REJECT_UNAUTHORIZED_ENDPOINTS</b>	The PSD shall reject unauthorized peripheral devices connected via a Universal Serial Bus (USB) hub.
<b>O.NO_TOE_ACCESS</b>	The PSD firmware, software, and memory shall not be accessible via its external ports.
<b>O.TAMPER_EVIDENT_LABEL</b>	The PSD shall be identifiable as authentic by the user and the user must be made aware of any procedures or other such information to accomplish authentication. This feature must be available upon receipt of the PSD and continue to be available during the PSD deployment. The PSD shall be labeled with at least one visible unique identifying tamper-evident marking that can be used to authenticate the device. The PSD manufacturer must maintain a complete list of manufactured PSD articles and their respective identification markings' unique identifiers.
<b>O.ANTI_TAMPERING</b>	The PSD shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the PSD would be evident, and optionally thwarted through disablement of the TOE. Note: This applies to a wired remote control as well as the main chassis of the PSD.
<b>O.SELF_TEST</b>	The PSD shall perform self-tests following power up or powered reset.
<b>O.SELF_TEST_FAIL_TOE_DISABLE</b>	The PSD shall enter a secure state upon detection of a critical failure.
<b>O.SELF_TEST_FAIL_INDICATION</b>	The PSD shall provide clear and visible user indications in the case of a self-test failure.
<b>PP-Module for Analog Audio Output Devices</b>	
<b>O.UNIDIRECTIONAL_AUDIO_OUT</b>	The PSD shall enforce the unidirectional flow of audio data from the analog audio computer interface to the analog audio peripheral interface.
<b>O.COMPUTER_TO_AUDIO_ISOLATION</b>	The PSD shall isolate the analog audio output function from all other TOE functions.
<b>PP-Module for Keyboard/Mouse Devices</b>	
<b>O.EMULATED_INPUT</b>	The TOE shall emulate the keyboard and/or mouse functions from the TOE to the connected computer.

<b>O.UNIDIRECTIONAL_INPUT</b>	The TOE shall enforce unidirectional keyboard and/or mouse device's data flow from the peripheral device to only the selected computer.
<b>PP-Module for User Authentication Devices</b>	
<b>O.USER_AUTHENTICATION_ISOLATION</b>	The TOE shall isolate the user authentication function from all other TOE functions.
<b>O.SESSION_TERMINATION</b>	The TOE shall immediately terminate an open session with the selected computer upon disconnection of the authentication element.

Table 19 – Security Objectives for the TOE

### 3.2 Security Objectives for the Operational Environment

The following table defines the security objectives that must be satisfied by the TOE's operational environment to ensure that the TOE's functions will be sufficient to mitigate the defined threats. These objectives are defined in the PSD PP and the PP-Modules that comprise the PP-Configuration that the TOE claims conformance to.

Security Objective	Definition
<b>Protection Profile for Peripheral Sharing Device</b>	
<b>OE.NO_TEMPEST</b>	The operational environment will not use TEMPEST approved equipment.
<b>OE.PHYSICAL</b>	The operational environment will provide physical security, commensurate with the value of the PSD and the data that transits it.
<b>OE.NO_WIRELESS_DEVICES</b>	The operational environment will not include wireless keyboards, mice, audio or user authentication.
<b>OE.TRUSTED_ADMIN</b>	The operational environment will ensure that trusted PSD Administrators and users are appropriately trained.
<b>OE.TRUSTED_CONFIG</b>	The operational environment will ensure that administrators configuring the PSD and its operational environment follow the applicable security configuration guidance.
<b>PP-Module for Analog Audio Output Devices</b>	
<b>OE.NO_MICROPHONES</b>	The operational environment is expected to ensure that microphones are not plugged into the TOE audio output interfaces.
<b>PP-Module for Keyboard/Mouse Devices</b>	
N/A – this PP-Module does not define any environmental security objectives beyond those defined in the PSD PP.	
<b>PP-Module for User Authentication Devices</b>	

N/A – this PP-Module does not define any environmental security objectives beyond those defined in the PSD PP.

Table 20 – Security Objectives for the Operational Environment

## 4 Security Requirements

The following section describes the IT security requirements of the TOE and its operational environment. The Common Criteria separates the TOE security requirements into two distinct categories:

1. Security functional requirements (SFRs) the TOE needs to satisfy to pass the security objectives (examples are listed below).
  - Identification/Authentication
  - Security management
  - User information protection
2. Security assurance requirements (SARs) specify evidence that provides grounds for confidence the TOE in its operational environment can satisfy the security objectives (examples are listed below).
  - Testing
  - Configuration Management
  - Vulnerability Assessment

The SFRs and SARs are discussed in more detail in the following subsections.

### 4.1 TOE Security Functional Requirements

The SFRs the TOE must satisfy are listed below in this section.

#### 4.1.1 Overview

The TOE claims all of the mandatory SFRs defined in the PP and PP-Modules that belong to the claimed PP-Configuration. The TOE also meets some of the optional and selection-based SFRs in the PP and PP-Modules. For Base-PP SFRs that are modified by one or more of the claimed PP-Modules, the modifications as required by those PP-Modules have been made.

The SFRs have been replicated below for clarity. Table 21 below displays the SFR IDs, their names, and where they originate from.

SFR ID	Name	Source
FAU_GEN.1	Audit Data Generation	PSD PP (optional)
FDP_AFL_EXT.1	Audio Filtration	Audio Output Module (mandatory)
	Active PSD Connections	PSD PP (mandatory)
FDP_APC_EXT.1	Note that the ST iterates this SFR for each of the claimed PP-Modules, per the instructions found in section 5.1.2 of each PP-Module.	
FDP_FIL_EXT.1/KM	Device Filtering (Keyboard/Mouse)	Keyboard/Mouse Module (optional)
FDP_FIL_EXT.1/UA	Device Filtering (User Authentication Devices)	User Authentication Module (mandatory)

<b>FDP_PDC_EXT.1</b>	Peripheral Device Connection	PSD PP (mandatory)
<b>FDP_PDC_EXT.2/AO</b>	Peripheral Device Connection (Audio Output)	Audio Output Module (mandatory)
<b>FDP_PDC_EXT.2/KM</b>	Authorized Devices (Keyboard/Mouse)	Keyboard/Mouse Module (mandatory)
<b>FDP_PDC_EXT.2/UA</b>	Authorized Devices (User Authentication Devices)	User Authentication Module (mandatory)
<b>FDP_PDC_EXT.3/KM</b>	Authorized Connection Protocols (Keyboard/Mouse)	Keyboard/Mouse Module (mandatory)
<b>FDP_PDC_EXT.4</b>	Supported Authentication Device	User Authentication Module (mandatory)
<b>FDP_PUD_EXT.1</b>	Powering Unauthorized Devices	Audio Output Module (mandatory)
<b>FDP_PWR_EXT.1</b>	Powered By Computer	User Authentication Module (mandatory)
<b>FDP_RIP.1/KM</b>	Residual Information Protection (Keyboard Data)	Keyboard/Mouse Module (selection-based)
<b>FDP_RIP_EXT.1</b>	Residual Information Protection	PSD PP (mandatory)
<b>FDP_RIP_EXT.2</b>	Purge of Residual Information	PSD PP (optional)
<b>FDP_SWI_EXT.1</b>	PSD Switching	PSD PP (mandatory)
<b>FDP_SWI_EXT.2</b>	PSD Switching Methods	PSD PP (selection-based)
<b>FDP_SWI_EXT.3</b>	Tied Switching	Keyboard/Mouse Module (selection-based)
<b>FDP_TER_EXT.1</b>	Session Termination	User Authentication Module (mandatory)
<b>FDP_TER_EXT.2</b>	Session Termination of Removed Devices	User Authentication Module (selection-based)
<b>FDP_TER_EXT.3</b>	Session Termination upon Switching	User Authentication Module (selection-based)
<b>FDP_UAI_EXT.1</b>	User Authentication Isolation	User Authentication Module (mandatory)
<b>FDP_UDF_EXT.1/AO</b>	Unidirectional Data Flow (Audio Output)	Audio Output Module (mandatory)

<b>FDP_UDF_EXT.1/KM</b>	Unidirectional Data Flow (Keyboard/Mouse)	Keyboard/Mouse Module (mandatory)
<b>FIA_UAU.2</b>	User Authentication Before Any Action	PSD PP (optional)
<b>FIA_UID.2</b>	User Identification Before Any Action	PSD PP (optional)
<b>FMT_MOF.1</b>	Management of Security Functions Behavior	PSD PP (optional)
<b>FMT_SMF.1</b>	Specification of Management Functions	PSD PP (optional)
<b>FMT_SMR.1</b>	Security Roles	PSD PP (optional)
<b>FPT_FLS_EXT.1</b>	Failure with Preservation of Secure State	PSD PP (mandatory)
<b>FPT_NTA_EXT.1</b>	No Access to TOE	PSD PP (mandatory)
<b>FPT_PHP.1</b>	Passive Detection of Physical Attack	PSD PP (mandatory)
<b>FPT_PHP.3</b>	Resistance to Physical Attack	PSD PP (optional)
<b>FPT_STM.1</b>	Reliable Time Stamps	PSD PP (optional)
<b>FPT_TST.1</b>	TSF Testing	PSD PP (mandatory)
<b>FPT_TST_EXT.1</b>	TSF Testing	PSD PP (mandatory)

Table 21 – TOE SFR Overview

#### 4.1.2 Class FAU: Security Audit

##### FAU\_GEN.1 Audit Data Generation

- FAU\_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:
- a. Start-up and shutdown of the audit functions;
  - b. All auditable events for the [*not specified*] level of audit; and
  - c. [*administrator login, administrator logout, self-test failures, peripheral device acceptance and rejections, [all administrative functions claimed in FMT\_MOF.1 and FMT\_SMF.1]*].
- FAU\_GEN.1.2** The TSF shall record within each audit record at least the following information:
- a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

- b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other information*].

#### 4.1.3 Class FDP: User Data Protection

##### FDP\_AFL\_EXT.1 Audio Filtration<sup>1</sup>

**FDP\_AFL\_EXT.1.1** The TSF shall ensure outgoing audio signals are filtered as per [*Audio Filtration Specifications table*].

Frequency (kHz)	Minimum Attenuation (dB)	Maximum Voltage After Attenuation
14	23.9	127.65 mV
15	26.4	95.73 mV
16	30.8	57.68 mV
17	35.0	35.57 mV
18	38.8	22.96 mV
19	43.0	14.15 mV
20	46.0	10.02 mV
30	71.4	0.53 mV
40	71.4	0.53 mV
50	71.4	0.53 mV
60	71.4	0.53 mV

Table 22 – Audio Filtration Specifications

##### FDP\_APC\_EXT.1/AO Active PSD Connections (Audio Output)

**FDP\_APC\_EXT.1.1/AO** The TSF shall route user data only from the interfaces selected by the user.

**FDP\_APC\_EXT.1.2/AO** The TSF shall ensure that no data **or electrical signals** flow between connected computers whether the TOE is powered on or powered off.

**FDP\_APC\_EXT.1.3/AO** The TSF shall ensure that no data transits the TOE when the TOE is powered off.

**FDP\_APC\_EXT.1.4/AO** The TSF shall ensure that no data transits the TOE when the TOE is in a failure state.

**Application Note:** This *SFR* is originally defined in the Base-PP but is refined and iterated to apply to the audio output interface per section 5.1.2 of the Audio Output PP-Module.

<sup>1</sup> As modified by NIAP TD0557

**FDP\_APC\_EXT.1/KM Active PSD Connections (Keyboard/Mouse)**

**FDP\_APC\_EXT.1.1/KM** The TSF shall route user data only to the interfaces selected by the user.

**FDP\_APC\_EXT.1.2/KM** The TSF shall ensure that no data **or electrical signals** flow between connected computers whether the TOE is powered on or powered off.

**FDP\_APC\_EXT.1.3/KM** The TSF shall ensure that no data transits the TOE when the TOE is powered off.

**FDP\_APC\_EXT.1.4/KM** The TSF shall ensure that no data transits the TOE when the TOE is in a failure state.

**Application Note:** *This SFR is originally defined in the Base-PP but is refined and iterated to apply to the audio output interface per section 5.1.2 of the Keyboard/Mouse PP-Module.*

**FDP\_APC\_EXT.1/UA Active PSD Connections (User Authentication)**

**FDP\_APC\_EXT.1.1/UA** The TSF shall route user data only to or from the interfaces selected by the user.

**FDP\_APC\_EXT.1.2/UA** The TSF shall ensure that no data **or electrical signals** flow between connected computers whether the TOE is powered on or powered off.

**FDP\_APC\_EXT.1.3/UA** The TSF shall ensure that no data transits the TOE when the TOE is powered off.

**FDP\_APC\_EXT.1.4/UA** The TSF shall ensure that no data transits the TOE when the TOE is in a failure state.

**Application Note:** *This SFR is originally defined in the Base-PP but is refined and iterated to apply to the audio output interface per section 5.1.2 of the User Authentication PP-Module.*

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

**FDP\_FIL\_EXT.1.1/KM** The TSF shall have [fixed] device filtering for [keyboard, mouse] interfaces.

**FDP\_FIL\_EXT.1.2/KM** The TSF shall consider all [*PSD KM*] blacklisted devices as unauthorized devices for [keyboard, mouse] interfaces in peripheral device connections.

**FDP\_FIL\_EXT.1.3/KM** The TSF shall consider all [*PSD KM*] whitelisted devices as authorized devices for [keyboard, mouse] interfaces in peripheral device connections only if they are not on the [*PSD KM*] blacklist or otherwise unauthorized.

**Application Note:** *The TSF enforces fixed device filtration on the keyboard/mouse interface by implicitly blacklisting all USB devices that are not keyboard or mouse devices.*

**FDP\_FIL\_EXT.1/UA Device Filtering (User Authentication Devices)**



**FDP\_FIL\_EXT.1.1/UA** The TSF shall have [configurable] device filtering for [*user authentication device*] interfaces.

**FDP\_FIL\_EXT.1.2/UA** The TSF shall consider all [*PSD UA*] blacklisted devices as unauthorized devices for [*user authentication device*] interfaces in peripheral device connections.

**FDP\_FIL\_EXT.1.3/UA** The TSF shall consider all [*PSD UA*] whitelisted devices as authorized devices for [*user authentication device*] interfaces in peripheral device connections only if they are not on the [*PSD UA*] blacklist or otherwise unauthorized.

***Application Note:*** *By default, the TSF will implicitly blacklist all devices that are not standard smart card readers, PIV/CAC USB tokens, or biometric readers. When configurable device filtration is used, any device that is not explicitly allowed is implicitly blacklisted.*

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

**FDP\_PDC\_EXT.1.1** The TSF shall reject connections with unauthorized devices upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

**FDP\_PDC\_EXT.1.2** The TSF shall reject connections with devices presenting unauthorized interface protocols upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

**FDP\_PDC\_EXT.1.3** The TOE shall have no external interfaces other than those claimed by the TSF.

**FDP\_PDC\_EXT.1.4** The TOE shall not have wireless interfaces.

**FDP\_PDC\_EXT.1.5** The TOE shall provide a visual or auditory indication to the User when a peripheral is rejected.

### **FDP\_PDC\_EXT.2/AO Peripheral Device Connection (Audio Output)**

**FDP\_PDC\_EXT.2.1/AO** The TSF shall allow connections with authorized devices as defined in [*Appendix E of the Analog Audio Output Devices Module*] and [

- authorized devices and functions as defined in the PP-Module for Keyboard/Mouse Devices.
- authorized devices as defined in the PP-Module for User Authentication Devices

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

**FDP\_PDC\_EXT.2.2/AO** The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*Appendix E of the Analog Audio Output Devices Module*] and [

- authorized devices presenting authorized interface protocols as defined in the PP-Module for Keyboard/Mouse Devices,
- authorized devices presenting authorized interface protocols as defined in the PP-Module for User Authentication Devices

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

### **FDP\_PDC\_EXT.2/KM Peripheral Device Connection (Keyboard/Mouse)**

**FDP\_PDC\_EXT.2.1/KM** The TSF shall allow connections with authorized devices **and functions** as defined in [*Appendix E of the Keyboard/Mouse Devices Module*] and [

- authorized devices as defined in the PP-Module for Audio Output Devices,
- authorized devices as defined in the PP-Module for User Authentication Devices,

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

**FDP\_PDC\_EXT.2.2/KM** The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*Appendix E of the Keyboard/Mouse Devices Module*] and [

- authorized devices presenting authorized interface protocols as defined in the PP-Module for Audio Output Devices,
- authorized devices presenting authorized interface protocols as defined in the PP-Module for User Authentication Devices,

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

### **FDP\_PDC\_EXT.2/UA Peripheral Device Connection (User Authentication Devices)**

**FDP\_PDC\_EXT.2.1/UA** The TSF shall allow connections with authorized devices as defined in [*Appendix E of the User Authentication Devices Module*] and [

- authorized devices as defined in the PP-Module for Audio Output Devices,
- authorized devices and functions as defined in the PP-Module for Keyboard/Mouse Devices,

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

**FDP\_PDC\_EXT.2.2/UA** The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*Appendix E of the User Authentication Devices Module*] and [

- authorized devices presenting authorized interface protocols as defined in the PP-Module for Audio Output Devices,
- authorized devices presenting authorized interface protocols as defined in the PP-Module for Keyboard/Mouse Devices,

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

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

**FDP\_PDC\_EXT.3.1/KM** The TSF shall have interfaces for the [USB (keyboard), USB (mouse)] protocols.

**FDP\_PDC\_EXT.3.2/KM** The TSF shall apply the following rules to the supported protocols: [*the TSF shall emulate any keyboard or mouse device functions from the TOE to the connected computer*].

### **FDP\_PDC\_EXT.4 Supported Authentication Device**

**FDP\_PDC\_EXT.4.1** The TSF shall have an [external] user authentication device.

### **FDP\_PUD\_EXT.1 Powering Unauthorized Devices**

**FDP\_PUD\_EXT.1.1** The TSF shall not provide power to any unauthorized device connected to the analog audio peripheral interface.

### **FDP\_PWR\_EXT.1 Powered By Computer**

**FDP\_PWR\_EXT.1.1** The TSF shall not be powered by a connected computer.

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

**FDP\_RIP.1.1/KM** The TSF shall ensure that any keyboard data in volatile memory is purged upon switching computers.

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

**FDP\_RIP\_EXT.1.1** The TSF shall ensure that no user data is written to TOE non-volatile memory or storage.

### **FDP\_RIP\_EXT.2 Purge of Residual Information**

**FDP\_RIP\_EXT.2.1** The TOE shall have a purge memory or restore factory defaults function accessible to the administrator to delete all TOE stored configuration and settings except for logging.

**FDP\_SWI\_EXT.1 PSD Switching**

**FDP\_SWI\_EXT.1.1** The TSF shall ensure that switching can be initiated only through express user action.

**FDP\_SWI\_EXT.2 PSD Switching Methods**

**FDP\_SWI\_EXT.2.1** The TSF shall ensure that no switching can be initiated through automatic port scanning, control through a connected computer, or control through keyboard shortcuts.

**FDP\_SWI\_EXT.2.2** The TSF shall ensure that switching can be initiated only through express user action using [console buttons, peripheral devices using a guard].

***Application Note:** Switching may only be performed by peripheral devices using a guard. The mouse peripheral may be used to perform switching. The switching is accomplished using mouse movements and the guard is to press the middle mouse button (scroll wheel button) twice prior to performing the switching operation.*

**FDP\_SWI\_EXT.3 Tied Switching**

**FDP\_SWI\_EXT.3.1** The TSF shall ensure that [*connected keyboard and mouse peripheral devices*] are always switched together to the same connected computer.

**FDP\_TER\_EXT.1 Session Termination**

**FDP\_TER\_EXT.1.1** The TSF shall terminate an open session upon removal of the authentication element.

**FDP\_TER\_EXT.2 Session Termination of Removed Devices**

**FDP\_TER\_EXT.2.1** The TSF shall terminate an open session upon removal of the user authentication device.

**FDP\_TER\_EXT.3 Session Termination upon Switching**

**FDP\_TER\_EXT.3.1** The TSF shall terminate an open session upon switching to a different computer.

**FDP\_TER\_EXT.3.2** The TSF shall reset the power to the user authentication device for at least one second upon switching to a different computer.

**FDP\_UAI\_EXT.1 User Authentication Isolation**

**FDP\_UAI\_EXT.1.1** The TSF shall isolate the user authentication function from all other TOE USB functions.

#### **FDP\_UDF\_EXT.1/AO Unidirectional Data Flow (Audio Output)**

**FDP\_UDF\_EXT.1.1/AO** The TSF shall ensure [*analog audio output data*] transits the TOE unidirectionally from [*the TOE analog audio output computer*] interface to [*the TOE analog audio output peripheral*] interface.

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

**FDP\_UDF\_EXT.1.1/KM** The TSF shall ensure [*keyboard, mouse*] data transits the TOE unidirectionally from the [*TOE [keyboard, mouse]*] peripheral interface(s) to the [*TOE [keyboard, mouse]*] interface.

### **4.1.4 Class FIA: Identification and Authentication**

#### **FIA\_UAU.2 User Identification before Any Action**

**FIA\_UAU.2.1** The TSF shall require each administrator to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that administrator.

#### **FIA\_UID.2 User Identification before Any Action**

**FIA\_UID.2.1** The TSF shall require each administrator to be successfully identified before allowing any other TSF-mediated actions on behalf of that administrator.

### **4.1.5 Class FMT: Security Management**

#### **FMT\_MOF.1 Management of Security Functions Behavior**

**FMT\_MOF.1.1** The TSF shall restrict the ability to [*modify the behavior of*] the functions [*user/administrator authentication, configurable CAC device filtering, dump log, restore factory default, terminate session*] to [*the authorized administrators*].

***Application Note:*** *The TSF defines a lesser-privileged user role in addition to the administrator role mandated by the claimed PP. Refer to Table 13 for the functions available to each role.*

#### **FMT\_SMF.1 Specification of Management Functions**

**FMT\_SMF.1.1** The TOE shall be capable of performing the following management functions: [*change user access credential, change administrator access credential, view registered CAC device, register new CAC device, dump log, restore factory default, terminate session*].

#### **FMT\_SMR.1 Security Roles**

**FMT\_SMR.1.1** The TSF shall maintain the roles [*administrators, users*].

*Application Note:* *The TSF defines a lesser-privileged user role in addition to the administrator role mandated by the claimed PP. Refer to Table 13 for the functions available to each role.*

**FMT\_SMR.1.2** The TSF shall be able to associate users with roles.

### **4.1.6 Class FPT: Protection of the TSF**

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

**FPT\_FLS\_EXT.1.1** The TSF shall preserve a secure state when the following types of failures occur: failure of the power-on self-test and [failure of the anti-tamper function].

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

**FPT\_NTA\_EXT.1.1** TOE firmware, software, and memory shall not be accessible via the TOE's external ports, with the following exceptions: [the configuration data, settings, and logging data that may be accessible by authorized administrators].

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

**FPT\_PHP.1.1** The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

**FPT\_PHP.1.2** The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

#### **FPT\_PHP.3 Resistance to Physical Attack<sup>2</sup>**

**FPT\_PHP.3.1** The TSF shall resist [*a physical attack for the purpose of gaining access to the internal components, to damage the anti-tamper battery, to drain or exhaust the anti-tamper battery*] to the [*TOE enclosure and any remote controllers*] by the attacked component becoming permanently disabled.

---

<sup>2</sup> As modified by NIAP TD0583

**Application Note:** *This SFR is modified per NIAP TD0583 to include reference to remote controllers. This modification is not applicable to the TOE because it does not have any remote controllers.*

### FPT\_STM.1 Reliable Time Stamps

**FPT\_STM.1.1** The TSF shall be able to provide reliable time stamps.

### FPT\_TST.1 TSF Testing

**FPT\_TST.1.1** The TSF shall run a suite of self-tests [*during initial start-up and at the conditions [upon reset button activation]*] to demonstrate the correct operation of [*user control functions and [active anti-tamper functionality]*].

**FPT\_TST.1.2** The TSF shall provide authorized users with the capability to verify the integrity of [TSF data].

**FPT\_TST.1.3** The TSF shall provide authorized users with the capability to verify the integrity of **the** [TSF].

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

**FPT\_TST\_EXT.1.1** The TSF shall respond to a self-test failure by providing users with a [visual] indication of failure and by shutdown of normal TSF functions.

## 4.2 Rationale for TOE Security Requirement Dependencies

The TOE claims all SFRs from the claimed PP and all claimed PP-Modules with the following exceptions:

- FDP\_RDR\_EXT.1 (from Keyboard/Mouse Module) – this is an optional SFR that the TSF does not claim to address.

In all cases, the omitted SFRs have been excluded from the TSF because they refer to optional functionality that may be excluded at the TOE developer's discretion.

## 4.3 TOE Security Assurance Requirements

The table below defines the SARs claimed by the TOE. These are the same SARs that are required by the claimed PP-Configuration.

Assurance Class	Assurance Component ID	Assurance Components Description
Development	ADV_FSP.1	Basic Functional Specification

<b>Guidance Documents</b>	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
<b>Life Cycle Support</b>	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
<b>Tests</b>	ATE_IND.1	Independent Testing – Conformance
<b>Vulnerability Assessment</b>	AVA_VAN.1	Vulnerability Survey

Table 23 – TOE Security Assurance Requirements



## 5 Conformance Claims

The following section describes the ST Conformance Claims.

### 5.1 CC Conformance Claims

This ST is compliant with the following CC documents:

- [CC1] - Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 5, April 2017.
- [CC2] - Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 5, April 2017.
- [CC3] - Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 5, April 2017.
- [CEM] - Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 5, April 2017.
- [Addenda] - CC and CEM addenda – Exact Conformance, Selection-Based SFRs, Optional SFRs, Version 0.5, May 2017.

This ST is CC Part 2 extended and CC Part 3 conformant.

### 5.2 PP Conformance Claims

This ST claims exact conformance to the PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, and User Authentication Devices, Version 1.0 and the following technical decisions:

1. TD0507 - Clarification on USB plug type, published date 03/03/2020
2. TD0518 - Typographical error in Dependency Table, published date 06/15/2020
3. TD0557 - Correction to Audio Filtration Specification Table in FDP\_AFL\_EXT.1, published date 12/08/2020
4. TD0583 – FPT\_PHP.3 modified for PSD remote controllers, published date 05/12/2021
5. TD0585 - Update to FDP\_APC\_EXT.1 Audio Output Tests, published date 04/29/2021
6. TD0593 - Equivalency Arguments for PSD, published date 06/03/2021

### 5.3 ST Conformance Requirements

This Security Target is in exact conformance with the PP. That is, the ST meets all the assurance requirements as defined by section D.2 of CC Part 1.

The mandatory requirements of the PP and all PP-Modules contained within the PP-Configuration are met. The ST is an instantiation of the claimed PP-Configuration. Additionally, optional requirements from these materials are claimed as needed and selection-based requirements are claimed where required. The ST does not omit any mandatory requirements, nor does it define or claim any requirements that are not defined in any of the components of the claimed PP-Configuration.

This ST meets all assurance requirements defined in the PP-Configuration.



## 6 TOE Summary Specification

This section summarizes the security functions of the TOE and the subsequent Assurance Measures taken to ensure their proper implementation. See Table 21 in Section 4 for the entire list of SFRs that address the security objectives for this TOE. These objectives will be broken down in the subsequent sections for further detail.

### 6.1 TOE External Interfaces Security Functions

[O.NO\_OTHER\_EXTERNAL\_INTERFACES]: FDP\_PDC\_EXT.1

[O.REJECT\_UNAUTHORIZED\_PERIPHERAL]: FDP\_PDC\_EXT.1

[O.REJECT\_UNAUTHORIZED\_ENDPOINTS]: FDP\_PDC\_EXT.1

The TOE only supports AC/DC power, USB keyboard and mouse, analog audio output, and user authentication devices. The filter is set at default to allow only standard smart-card reader USB 1.1/2.0 token or biometric reader but when user or administrator registers new CAC devices, the TOE will start to support these registered devices. All other peripheral types are rejected, either physically (because the TOE does not support the required physical interface) or logically (because the TOE does not recognize the connected peripheral as authorized).

### 6.2 TOE Administration, User Control, and Monitoring Security Functions

[O.AUTHORIZED\_USAGE]: FAU\_GEN.1, FDP\_SWI\_EXT.1, FDP\_SWI\_EXT.2, FIA\_UAU.2, FIA\_UID.2, FMT\_MOF.1, FMT\_SMF.1, FMT\_SMR.1, FPT\_STM.1

Each TOE is equipped with Administration and Security Management Tool that can be initiated by running an executable file on a computer with keyboard connected to the same computer via the TOE. The tool requires administrator or a user to be successfully identified and authenticated by name and password in order to gain access to any supported feature. The TOE has a menu-driven interface in which the user or administrator can initiate the supported functions. See below for descriptions of the supported features, Table 13 above will note differences of access by administrator and user accounts.

- Change User Access Credentials
  - Updates the username and password for the “user” account
- Change Admin Access Credentials
  - Updates the username and password for the “admin” account
- View Registered CAC Device
  - Displays the name, manufacturer, Product ID, and Vendor ID of current registered CAC device
- Register New CAC Device
  - Updates the currently registered CAC device
- Dump Log
  - Prints out the last 100 logs the TOE recorded
- Restore Factory Default
  - Resets the user credentials, administrator credentials, and registered CAC device to default settings
- Terminate Session
  - Ends the current administrative tool session

The TOE is shipped with default credentials for the administrator and user account; these should be changed on first use as part of the initial setup process. Successful and failed authentication attempts are logged, as are logouts. The TOE does not enforce any failure limitations (e.g. lockout after a certain number of successive failures). If an administrator has lost their username and/or password, they must contact the manufacturer for assistance.

The administrator/user account passwords as well as the names of the accounts themselves can both be changed. The restrictions for each are as follows:

- Minimum 4 characters
- Maximum 8 characters
- All Letters (Upper and Lower case), Numbers, and the following special characters are allowed ! @ # \$ % ^ & \* ( ) \_ + - = " ? /
- The following special characters are not allowed ~ ` { } | [ ] \ ; ' < > , .
- Any other character not specified above is not allowed.
- Space and Tab are not allowed

All usage of the TOE requires authentication to the Administration and Security Management Tool except for switching. All TOE models can be switched using push-buttons on the TOE chassis.

Additionally, switching the selected computer is also possible using cursor control with a guard. Specifically, if the user wants to switch the active computer, they can press the middle mouse button (scroll wheel button) twice and then 'swipe' in a given direction to change the channel. In addition to requiring the use of a guard, cursor control switching is unambiguous because the TOE will emit an audible signal when the selected computer has changed. By default, swiping left will cycle the channel down and swiping right will cycle the channel up. This does not roll over; i.e. swiping left on channel 1 or swiping right while on the highest channel will have no effect. There are no switching mechanisms that can be engaged using automatic port scanning, control through a connected computer, or control through keyboard shortcuts. The console buttons and mouse peripheral (using a guard) are the only available switching mechanisms.

The TOE has a non-volatile memory event log which records all abnormal security events that occur within TOE operation. This log can be accessed by the identified and authorized administrator and dumped into a .txt file using a connected computer and a program. If the TOE anti-tampering state has been triggered, the access log can only be accessed by de-soldering the memory IC from the internal circuitry and extracted using low-level factory tools (TOE is permanently disabled).

The following events are logged in sequential order with time/date stamp and Pass/Fail status:

APU	Administrator Credential Update
ALO	Administrator Log On
ALF	Administrator Log Off
ARM	Arming A/T System
CAC	CAC Configuration
LGD	LOG Dump
PWU	Power Up
PWD	Power Down
RCA	Rejected CAC Device

AFD	Restore Factory Default
RKM	Rejected Keyboard or Mouse
STS	Self-Test
TMP	Device Tampered, Review by MFR only
ULO	User Log On
ULF	User Log Off
UPU	User Credential Update

The TOE can store up to 100 events. When the allocated memory is fully used, new events will be recorded over the oldest events (first in first out mode).

The TOE includes an internal system clock function that is used for time stamps of audit records. The TOE's clock is set at manufacture time and is set to Pacific Standard Time (GMT -8) by default.

The TOE indicates the selected channel using a panel of LEDs that are located directly above the channel selection buttons for the connected computer. When the user presses a channel selection button, the corresponding LED will light up to indicate the selected computer. The channel selection buttons are also backlit. When the backlight is on, the CAC port is active. The user may disable the CAC port for a particular channel by pressing and holding the channel selection button until the backlight has turned off. This can only be used to enable/disable the CAC port for the active computer; it is not possible for one computer to be active (as indicated by the LED panel) while the CAC port is active on a different computer (as indicated by the backlight of a different channel selection button). During operation, all front panel LED indications cannot be turned off or dimmed by the user in any way including after Restore Factory Default (reset). This prevents user confusion of current TOE state.<sup>3</sup> When the TOE has booted successfully, it will default to computer 1 being the selected computer.

[O.LEAK\_PREVENTION\_SWITCHING]: FDP\_SWI\_EXT.1, FDP\_SWI\_EXT.2

All switching mechanisms must be deliberately engaged by the user. There are no mechanisms that allow data intended for the selected computer to be transmitted to a different computer, and there are no interfaces that allow data to be transmitted directly between computers.

### 6.3 TOE Tampering Protection

In order to mitigate potential tampering and replacement, the TOE is devised to ensure that any replacement may be detected, any physical modification is evident, and any logical modification may be prevented. The tamper protection mechanism is only triggered by tamper detection or failure of self-testing; there is no method by which a user can falsely or accidentally trigger the tamper protection indicator such that the TOE incorrectly indicates that it is operating in a tampered state.

The TOE is designed so that access to the TOE firmware, software, or its memory via its accessible ports is prevented. No access is available to modify the TOE or its memory. To mitigate the risk that a potential attacker will tamper with a TOE and then reprogram it with altered functionality, the compliant TOE external and internal interfaces are locked for code read and write. The programmable components of the TOE's programming ports are permanently disabled for both read

---

<sup>3</sup> See section 1.6.2.6.6 above for detailed information about Restore Factory Default (reset)

and write operations. The TOE's operational code may not be upgradeable through any of the TOE external or internal ports.

[O.NO\_TOE\_ACCESS]: FPT\_NTA\_EXT.1

The TOE is designed to prevent any physical or logical access its internal memory. All TOE microcontrollers run from internally protected flash memory. The TOE firmware is read/write protected, inaccessible by JTAG interfacing, and cannot be modified or updated by any external tools. All firmware is executed on SRAM and protected against external access/modification of code or stacks.

The only memory access that is granted to external entities are the following:

- Connected computers may read the EDID memory
- Authorized administrators may read memory related to the TOE's configuration data, settings, and logging data.
- Authorized users may read memory related to configuration data for the current CDF configuration.

[O.TAMPER\_EVIDENT\_LABEL]: FPT\_PHP.1

Each TOE has one uniquely labeled front panel holographic tamper evident label (TEL) placed over the boundary between the upper and lower half of the TOE enclosure. The TEL has a recorded unique serial number that is monitored for TOE authentication purposes. Any attempt to access the internals of the TOE will cause permanent visible damage to the TEL.

[O.ANTI\_TAMPERING]: FPT\_PHP.1 FPT\_PHP.3

In addition to the TEL on the front panel, the TOE is physically designed to trigger the anti-tampering system once opened. The TOE enclosure is composed of all-around reinforced stainless steel construction, which shields it from outside intrusion through brute physical force. There is also a mechanical switch on the inside of the TOE that triggers the anti-tampering state when the enclosure is manually opened.

Once the anti-tampering state is triggered, the TOE is permanently disabled. There is no access available to reset the TOE to factory defaults once the anti-tampering state is active. All channels are electrically and logically isolated by setting all TOE multiplexers to isolation and opening all data relays. All stored information on the TOE is also erased.

When the anti-tampering system is triggered, the TOE shuts down all ports and functionality. The following user indications occur once the anti-tampering system is triggered:

1. All the push-button LEDs flash repeatedly
2. Alarm from internal speaker beeps repeatedly
3. Relays on the TOE pulse repeatedly

The TOE power supply controls the anti-tampering system during powered operation. When the TOE is not supplied with external power, a backup battery located on the TOE circuit board keeps the anti-tampering system powered. The battery is rated for an operational life of 10 years, but this is extended when the TOE is externally powered as the battery depletion rate is reduced in this case.

The TOE has a non-volatile battery controller that is powered by both the backup battery and the power supply of the TOE, depending on whether or not the TOE is externally powered. The data retention voltage of this controller is between 1V and 5V. If the voltage of the backup battery depletes below 1V, the anti-tampering function will be triggered, either immediately upon detection if the TOE

is powered on, or on the first boot after detection if the TOE is powered off when the depletion threshold is reached. This permanently disables the TOE.

## 6.4 TOE Self-Testing

[O.SELF\_TEST]: FPT\_TST.1

All TOEs have a self-testing function that executes immediately after power is supplied including Restore Factory Default (reset) and power reset, before normal operation access is granted to the user. Self Test function includes the following activities:

1. Basic integrity test of the TOE hardware (no front panel push buttons are jammed).
2. Basic integrity test of the TOE firmware.
3. Integrity test of the anti-tampering system and control function.
  - a. Ensure the calendar date had been set.
  - b. Ensure the anti-tamper switches had not been opened when powered off.
  - c. Ensure the anti-tamper switches are currently closed.
  - d. Ensure the anti-tamper battery had not been tampered with when powered off.
  - e. Ensure the anti-tamper battery is still intact.
4. Ensure the isolation between HID traffic and CAC traffic of each computer.
5. Ensure the isolation of HID and CAC traffic between different computers.

Users verify the integrity of the TSF and its data through these mechanisms. All features of the TOE front panel are tested during power up self-testing. From power up until the termination of the TOE self-test, no channel is selected. This ensures no TOE state is enabled to the user until all self tests have been passed. If all self tests are passed, normal operation is indicated audibly through one beep of the internal alarm followed by one pulse of an internal relay. If any self-tests fail, the TOE is temporarily disabled to the extent that all computer, peripheral, and CAC ports are deactivated, and the management interface cannot be accessed. The user can reboot the TOE (power off/power on) to attempt to clear the error state.

[O.SELF\_TEST\_FAIL\_TOE\_DISABLE]: FPT\_FLS\_EXT.1, FPT\_TST\_EXT.1

If a self-testing function does not meet normal operation requirements (failure), the TOE is temporarily disabled until the issue is resolved and the TOE is rebooted (power off/power on). If the unit is permanently defective, then it must be replaced.

[O.SELF\_TEST\_FAIL\_INDICATION]: FPT\_TST\_EXT.1

If self-testing fails, all front panel LEDs will turn on to indicate self test failure. TOE normal operation is disabled until the issue is resolved and the system is rebooted. When the system passes all self-testing functions, normal operation is indicated by one beep from the internal speaker and one pulse from an internal TOE relay.

## 6.5 TOE Audio Subsystem Security Functions

The TOE enforces requirements for data isolation and peripheral authorization for the analog audio output interface.

[O.COMPUTER\_INTERFACE\_ISOLATION,  
O.COMPUTER\_INTERFACE\_ISOLATION\_TOE\_UNPOWERED, O.USER\_DATA\_ISOLATION,  
O.PERIPHERAL\_PORTS\_ISOLATION, O.REJECT\_UNAUTHORIZED\_PERIPHERAL]:  
FDP\_APC\_EXT.1/AO, FDP\_PDC\_EXT.1, FDP\_PDC\_EXT.2/AO, FDP\_PUD\_EXT.1

When the TOE is not powered, an audio isolation relay is opened to isolate the audio input ports from all internal TOE circuitry. The TOE does not supply power to any device connected to the analog audio output interface. Each connected computer has its own isolated stereo audio channel that flows from the connected computer's audio input port to the analog stereo output port of the TOE. The analog audio output interface is the only physical interface for this function; unauthorized peripherals are either physically incompatible or logically incompatible (as is the case with audio input devices).

[O.UNIDIRECTIONAL\_AUDIO\_OUT]: FDP\_AFL\_EXT.1, FDP\_APC\_EXT.1/AO, FDP\_UDF\_EXT.1/AO

The use of microphones as input devices is prohibited. All TOE devices support analog audio out switching and all TOE devices will prevent microphone devices. These microphones are stopped through the use of uni-directional audio diodes on both left and right stereo channels (forces data flow from only the computer to the connected audio device) and the LM4880 Boomer analog output amplifier which enforces uni-directional audio data flow. All audio signals are filtered in accordance with the Audio Filtration Specifications table (Table 22) above.

The audio system is protected mechanically to provide physical isolation of the audio ports to all the remaining sources; at any given moment, only one source is connected to the audio multiplexer. This type of physical connection ensures the complete isolation between an input computer and limits any possible leakage. The multiplexer provides protection for channel to channel crosstalk as the off channel will not get any audio signal when the active channel is on a high frequency. The multiplexer is also able to control the OFF-Isolation at a level of 120 dB and channel separation at 116 dB.

Furthermore, uni-directional audio diodes are placed in parallel on both right and left stereo channels to ensure uni-directional data flow from the connected computer to the audio analog output port on the TOE which prevents any reverse audio from leaking. Audio data from the connected peripheral devices to the connected computer is blocked by the audio uni-directional electronic circuit. Only analog audio is supported, all digital audio will be blocked using a dedicated filter. The output signal is limited to range between 45dB and 75dB.

[O.COMPUTER\_TO\_AUDIO\_ISOLATION]: FDP\_APC\_EXT.1/AO, FDP\_UDF\_EXT.1/AO

The TOE system controls the audio switching between each connected computer channel using isolated unidirectional audio buses. The TOE audio interface uses a solid state multiplexer and mechanical relays to ensure audio/computer channel isolation.

[O.NO\_USER\_DATA\_RETENTION]: FDP\_RIP\_EXT.1, FDP\_RIP\_EXT.2

The TOE audio subsystem does not delay, store, or convert audio data flows. This prevents any audio overflow during switching between isolated audio channels. The Letter of Volatility in Appendix B identifies all non-volatile memory components of the TOE and the data that is stored on them; these components do not store audio data.

[O.SELF\_TEST]: FPT\_TST.1

[O.SELF\_TEST\_FAIL\_TOE\_DISABLE]: FPT\_FLS\_EXT.1, FPT\_TST\_EXT.1

[O.ANTI\_TAMPERING\_PERMANENTLY\_DISABLE\_TOE]: FPT\_PHP.3 and FPT\_FLS.1

If the TOE fails to pass the audio self test or anti-tampering is triggered, the same audio isolation relay is opened to isolate the audio inputs, preventing data leakage.



## 6.6 TOE Keyboard and Mouse Functionality

The TOE enforces requirements for data isolation and peripheral authorization for the keyboard/mouse interface.

[O.COMPUTER\_INTERFACE\_ISOLATION, O.COMPUTER\_INTERFACE\_ISOLATION\_TOE\_UNPOWERED, O.USER\_DATA\_ISOLATION, O.PERIPHERAL\_PORTS\_ISOLATION, O.REJECT\_UNAUTHORIZED\_ENDPOINTS, O.REJECT\_UNAUTHORIZED\_PERIPHERAL]: FDP\_APC\_EXT.1/KM, FDP\_FIL\_EXT.1/KM, FDP\_PDC\_EXT.1, FDP\_SWI\_EXT.3

In order to completely isolate the keyboard and mouse interfacing for all connected computers, host and device emulators are used to control these peripheral interfacings. The host emulator receives serial commands from the USB keyboard and mouse and stores them in SRAM. These commands are sent through the current channel to its respective isolated microcontroller (the device emulator). The TOE device emulator then interacts with its assigned isolated connected computer via USB. Having separate isolated device emulators assures that the connected computers do not have an electrical or logical information channel with the TOE or peripheral devices. External devices connected to the USB KM ports of the TOE cannot be used to supply power to the TOE.

When the TOE is in a failure state (either because it has experienced self-test failure or physical tampering), no data will be transmitted through the TOE.

Each isolated device emulator is powered by the TOE. Each isolated host emulator is powered in conjunction by its respective connected computer and the TOE. The host emulator is being reset whenever the computer or the TOE are powered on. Uni-directional diodes are used to isolate all power domains from each connected computer to each device emulator.

In addition to device emulators for interface isolation, computer/host emulators are used by the TOE to interact with the peripheral interfacing of connected keyboard and mouse devices. The host emulator further isolates these peripheral devices from connected computers and TOE circuitry. Any threat that attempts to access connected computers through peripheral keyboard and mouse devices must bypass both the host and the device emulator for each isolated channel. The data exchange between the host and device emulators is limited to basic keyboard and mouse commands.

A secure peripheral switch (multiplexer) is used to assure the selection of just one tied keyboard and mouse serial data stream during TOE operation. The secure multiplexer has a third position, isolation, which is activated when the TOE has been tampered with or self-test has failed to disable the keyboard and mouse stream.

The keyboard and mouse processor is programmed in firmware only to accept 108-key keyboard and 3-button mouse USB devices. Unauthorized peripheral devices will be rejected by the TOE's keyboard and mouse ports. Wireless keyboard and mouse are special USB composite devices; when this type of device is recognized by the TOE, all front LED's of the TOE will blink and the user will need to disconnect and reboot the TOE. The only USB host peripheral devices that are allowed by the TOE are keyboard and mouse host emulators. Basic USB 1.1/2.0 HID-class devices are authorized as valid endpoints by the TOE. Note that devices having integrated USB hub and composite devices will only be supported if the connected device has at least one endpoint which is a keyboard or mouse HID class. All other non-keyboard/mouse HID class endpoints will be disabled in this scenario. Both keyboard and mouse TOE ports are interchangeable. It is assumed based on the claimed PP that all standard peripheral devices are untrusted; therefore, the TOE protects the

system from attacks that may be executed to exploit such devices and enable unauthorized data flows. By creating uni-directional isolated keyboard and mouse TOE channels that are tied to the two USB 1.1/2.0 ports on the TOE, unauthorized data flows are eliminated.

Inside the TOE, the keyboard and mouse peripherals are switched together from one isolated connected computer to the next isolated connected computer. There is no user/administration configuration that allows keyboard and mouse functionality to split into separate serial data channels. Keyboard and mouse data flow is not connected to any other TOE data flow (audio, USB/CAC) or other external interfaces.

[O.NO\_USER\_DATA\_RETENTION]: FDP\_RIP\_EXT.1, FDP\_RIP\_EXT.2, FDP\_RIP.1/KM  
TOE Non-Volatile Memory is not used to store keyboard and mouse data. All keyboard and mouse commands are stored on Static Random Access Memory (SRAM). Since SRAM is volatile memory, all data is cleared off the stack when the TOE is powered down and during Restore Factory Default. The buffer for keyboard and mouse data is 128 bits and is continuously read and cleared during use.

During switching between one connected computers to another, the TOE system controller assures that the keyboard and mouse stacks are deleted. The switching process takes between 250 to 500 milliseconds (ms). Internal components of the TOE temporarily shut down power to the keyboard and mouse peripherals to ensure the elimination of any built-up of cached commands from the previous channel. This temporary power reset prevents data leakage. In addition, the TOE is deleting all keyboard and mouse stacks upon Restore Factory Default function.

More information about the keyboard/mouse buffer and its clearing, including the physical components responsible for doing this, can be found in Appendix B below. This Appendix also lists the non-volatile memory components of the TOE and the data that is stored on them to show that the TOE does not store user data in non-volatile memory.

[O.EMULATED\_INPUT]: FDP\_PDC\_EXT.2/KM, FDP\_PDC\_EXT.3/KM

Isolated host/device emulators are used to interact with the serial commands sent via keyboard and mouse over USB. The host emulator receives a serial data stream from the tied keyboard and mouse peripherals. This data is passed through a peripheral data diode, optical isolator, and a mechanical relay to the device emulator. This prevents any type of bi-directional communication between the keyboard/mouse and the connected computers.

[O.UNIDIRECTIONAL\_INPUT]: FDP\_UDF\_EXT.1/KM

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. This can be seen in the TOE by observing the embedded keyboard LEDs of CAPS, Num, and Scroll Lock. When connected to the computer through the TOE, these indicators are not functional as this data is not able to pass between the TOE and the computer and vice-versa. Thus, the use of these embedded keyboard LEDs is not supported by the TOE.

[O.SELF\_TEST]: FPT\_TST.1

[O.SELF\_TEST\_FAIL\_TOE\_DISABLE]: FPT\_FLS\_EXT.1, FPT\_TST\_EXT.1

[O.ANTI\_TAMPERING\_PERMANENTLY\_DISABLE\_TOE]: FPT\_PHP.3 and FPT\_FLS.1

When the TOE is not powered, an isolation relay is opened to isolate the KM input ports from all internal TOE circuitry. If the TOE fails to pass the KM self test or anti-tampering is triggered, the same

isolation relay is opened to isolate the KM inputs, preventing data leakage. All stored keyboard and mouse information is erased from the TOE.

## 6.7 TOE User Authentication Device Subsystem Security Functions

The TOE enforces requirements for data isolation and peripheral authorization for user authentication device interface.

The TOE has Configurable Device Filtration (CDF) for the USB CAC peripheral port. The default behavior is to allow a USB device with a “user authentication” base class (0Bf) to interface with this port, which includes devices such as smart card reader, PIV/CAC token, or biometric reader. All devices must be bus powered only (no external power source allowed). CDF can be used by the TOE to override the default FDF behavior. Whenever a USB device is plugged into the TOE CAC port, the connection detector verifies that a USB device is now connected to the TOE CAC port. The host USB sniffer then stores the connected USB Product ID (PID), Vendor ID (VID), class and serial number. If the connection detector verifies that a device is connected, a verification signal is sent to the MCU. The MCU then checks to see if the current USB device is currently registered by the TOE. If the PID, VID, class, and serial number do not match the registered TOE USB devices, the USB device is rejected by the TOE. Registered devices are whitelisted by the TOE; all other devices are implicitly blacklisted.

The TOE default settings accept standard smart-card reader, PIV/CAC USB 1.1/2.0 token or biometric reader. Only an Identified and authorized user/administrator can register other USB devices. Once a device has been registered on the TOE, no other USB peripheral device (including the default smart-card readers/biometric readers) will be allowed to operate on the TOE USB port. To re-enable default operations, an identified and authorized user/administrator must delete the registered device.

When a USB hub is connected to the TOE it will not recognize it as an accepted device even if a standard smart-card reader or similar approved device is connected to the hub. The TOE will recognize that a USB hub is connected and block all communications to this hub, regardless of what devices are connected to the hub. The USB hub cannot be registered to the TOE by an administrator to be used with approved devices.

[O.COMPUTER\_INTERFACE\_ISOLATION, O.COMPUTER\_INTERFACE\_ISOLATION\_TOE\_UNPOWERED, O.USER\_DATA\_ISOLATION, O.PERIPHERAL\_PORTS\_ISOLATION, O.REJECT\_UNAUTHORIZED\_ENDPOINTS, O.REJECT\_UNAUTHORIZED\_PERIPHERAL]: FDP\_APC\_EXT.1/UA, FDP\_FIL\_EXT.1/UA, FDP\_PDC\_EXT.1, FDP\_PDC\_EXT.2/UA, FDP\_PDC\_EXT.4, FDP\_PWR\_EXT.1, FDP\_SWI\_EXT.2

Each connected computer has an isolated computer interface with its individual CAC port. Each computer interface has isolated circuitry on the TOE and its own individual power plane. Each USB CAC must be powered by the TOE. All data channels are electrically and logically isolated to prevent data leakage.

When the TOE is in a failure state (either because it has experienced self-test failure or physical tampering), no data will be transmitted through the TOE.

The TOE uses an external authentication device.

The TOE is shipped with Fixed Device Filtration for the CAC port (and the Configurable Device Filtration provides further configurable filter options). The filter is set at default to allow only standard smart-card reader USB 1.1/2.0 token or biometric reader but when user registers new CAC devices, the TOE will start to support these registered devices. All user authentication ports are tied to their respective isolated channel to prevent data leakage. Any unauthorized user authentication device or unqualified USB device will be rejected by the TOE. When this occurs, the user is notified of the rejection as the LED indicator of the USB CAC device and the button backlight of the current channel will both blink repeatedly until that peripheral is removed.

[O.AUTHORIZED\_USAGE]: FAU\_GEN.1, FDP\_SWI\_EXT.1, FDP\_SWI\_EXT.2, FIA\_UAU.2, FIA\_UID.2, FMT\_MOF.1, FMT\_SMF.1, FMT\_SMR.1, FPT\_STM.1

Only an identified and authenticated user/administrator can register a USB CAC/peripheral device. The device enumeration details are monitored before and during operation with pre-stored values to determine if the device is qualified/unqualified for TOE interfacing. The CDF definitions may define one or more device characteristics such as: USB device class, sub-protocol, VID, PID and serial number.<sup>4</sup>

Details about the TOE's identification and authentication mechanism as well as its ability to generate audit records are presented in section 6.2 above.

[O.USER\_AUTHENTICATION\_ISOLATION]: FDP\_UAI\_EXT.1

The TOE's CAC ports (for both console and computer interfaces) are physically separate from the keyboard/mouse ports. Each connected computer has an isolated computer interface with its individual CAC port. Each computer interface has isolated circuitry on the TOE and its own individual power plane. All data channels are electrically and logically isolated to prevent data leakage.

[O.SESSION\_TERMINATION]: FDP\_TER\_EXT.1, FDP\_TER\_EXT.2, FDP\_TER\_EXT.3

When ports are switched, the power to the CAC port is reset for 1,000ms, using an integrated high-side power switch optimized for Universal Serial Bus (USB) applications. The USB power switch offers current and thermal limiting, short circuit protection, controlled rise time, and under-voltage lockout functionality using internal port USB Power Switch and Over-Current Protection. The USB internal power switch completely disconnects the power line (5VDC) from the connected CAC device. The turn off time tested under capacitance of 100 $\mu$ F requires 200 $\mu$ s to drop from 5V to 2V and 250 $\mu$ s to drop from 5V to under 1.8V. Since the power disconnect time has been set to 1,000ms, it allows the CAC device to be completely discharged and erase any internal information.

When a connected authentication device is disconnected from the TOE, either because it is physically disconnected or because the TOE is switched to a different channel, the previously-active session on the connected computer is disabled. Similarly, if an authentication device is connected to the TOE that uses removable authentication elements, removal of the authentication element causes a session to be terminated (e.g., removal of a smart card from a connected card reader).

[O.NO\_USER\_DATA\_RETENTION]: FDP\_RIP\_EXT.1, FDP\_RIP\_EXT.2

No data is stored by the TOE in regards to user authentication device data. User authentication device data is not processed or emulated on the TOE. The Letter of Volatility in Appendix B

---

<sup>4</sup> Registration of a USB CAC/peripheral device is part of Administration and Security Management Tool outlined in section 6.2 above

identifies all non-volatile memory components of the TOE and the data that is stored on them; these components do not store user authentication device data.

[O.SELF\_TEST]: FPT\_TST.1

[O.SELF\_TEST\_FAIL\_TOE\_DISABLE]: FPT\_FLS\_EXT.1, FPT\_TST\_EXT.1

[O.ANTI\_TAMPERING\_PERMANENTLY\_DISABLE\_TOE]: FPT\_PHP.3 and FPT\_FLS.1

While the TOE is not powered, all user authentication device channels are isolated through a peripheral multiplexer. If the TOE fails during self testing or TOE anti-tampering is triggered, the same multiplexer will isolate all channels as during non-powered operation to prevent data leakage. All open authentication sessions will be disconnected during channel isolation.

## Appendix A – Product’s Model Name Structure

### KM

XXXX-	XXX	X	XXX	X
KVS4 = Secure KVM NIAP 4.0	100=Single Head	4=4 Port	K=KM	X = CAC
		8=8 Port		

## Appendix B – Letter of Volatility

### Main PCBA: USB

Device: Controller Board Main MCU - ATxmega256A3U-AU

Manufacturer: Atmel

Type: Microcontroller

#### Functions:

The Controller Board Main MCU is responsible for controlling the operations of the USB, Keyboard and Mouse, CAC, and front panel board. No other source can independently power the Controller Board Main MCU other than the TOE.

#### Memory type:

1. Flash Firmware 4KB EEPROM, 256KB Programmable Flash (non-volatile):
  - All Main MCU firmware that controls its operation is saved in its own dedicated flash memory. This firmware cannot be changed by any user or programmer. All Main MCU firmware is erased if anti-tampering is triggered.
2. User 2KB EEPROM Flash (non-volatile):
  - The Main MCU has dedicated flash EEPROM to save all registration of USB devices, and a log of operations.
3. SRAM (volatile):
  - The Main MCU uses SRAM memory to run the entire TOE system. The SRAM is erased as soon as the external power supply is disconnected. All SRAM is erased if anti-tampering is triggered. No user data is stored inside the SRAM when the power is disconnected from the TOE, or if anti-tampering has been triggered.

The Controller Board Main MCU contains a 128-bit data buffer for keyboard and mouse input. The contents of this buffer are continuously read and cleared. When a switching operation is initiated, the buffer is immediately erased prior to the switch being performed. The erasure is performed by the triggering of an AP2146 power switch that supplies power to the buffer. When the switch operation is initiated the power is removed for 1ms, causing the data to be wiped.

When the Restore Factory Default operation is performed, all the user memory will be erased and brought back to its initial state.

Device: Emulation MCU - PIC18F25J50-I/SS

Manufacturer: Microchip

Type: Microcontroller

#### Functions:

The Emulation MCU controls all USB device emulation and communication between the Controller Board Main MCU and the USB connections of the TOE connected computers. No other source can independently power the Emulation MCU other than the TOE.

#### Memory type:

1. Flash Firmware 32KB Programmable Flash (non-volatile):

- All Emulation MCU firmware that controls its operation is saved in its own dedicated flash memory.
2. SRAM (volatile):
    - The Emulation MCU uses SRAM memory to run USB device emulation. The SRAM is erased as soon as the external power supply is disconnected. All SRAM is erased if anti-tampering is triggered. No user data is stored inside the SRAM when the power is disconnected from the TOE, or if anti-tampering has been triggered.

Note: No flash ROM is dedicated to the Emulation MCU to save any data or log.

When the Restore Factory Default operation is performed, or power reset is initiated, or USB cable is disconnected from the computer, all the working memory of Emulation MCU is reset to default. The main function of this device is the emulate keyboard and mouse only. All the memory/RAM needed is for internal operation and not related to any user data.

Device: Keyboard and Mouse USB Host Controller - SL811HS and **ARM Cortex**  
Manufacturer: Cypress, ST  
Type: USB Host processor

#### Functions:

The Keyboard and Mouse USB Host Controller is responsible for controlling the USB protocol, storing the device information of the connected keyboard and mouse, and communicating with the Controller Board Main MCU. The Keyboard and Mouse USB Host Controller ties both keyboard and mouse serial transmissions into one line and transfers them to the Main MCU before emulation. No other source can independently power the Keyboard and Mouse USB Host Controller other than the TOE.

#### Memory Type:

1. SRAM (volatile):
  - The Keyboard and Mouse USB Host Controller uses SRAM memory to store USB Keyboard and Mouse peripheral commands and USB keyboard and mouse device information. The SRAM is erased after each designated TOE channel switch to purge any stored keyboard and mouse commands. The SRAM is erased as soon as the external power supply is disconnected. All SRAM is erased if anti-tampering is triggered. No user data is stored inside the SRAM when the power is disconnected from the TOE, or if anti-tampering has been triggered.

Note: No flash ROM is dedicated to the KM USB Host Controller to save any data or log.

When the Restore Factory Default operation is performed, or power reset is initiated, or USB keyboard or mouse is disconnected from the TOE, all the working memory of KM USB Host Controller is reset to default. The main function of this device is to read the keyboard and mouse and convert to secure internal communication. All the memory/RAM needed is for internal operation and not related to any user data.

Device: CAC USB Host Controller - SL811HS and **ARM Cortex**  
M Manufacturer: Cypress, ST  
Type: USB Host Processor



**Functions:**

The CAC USB Host Controller is responsible for all the operations of the TOE CAC port, and communication with the Controller Board Main MCU. This includes USB user authentication device registration, validation, and communication with connected computers. No other source can independently power the CAC USB Host Controller other than the TOE.

**Memory type:**

1. SRAM (volatile):
  - The CAC USB Host Controller uses SRAM memory to store USB device information (PID/VID) during CAC device registration. After the MCU has read this information, the SRAM is erased. The SRAM is also erased if anti-tampering is triggered, or power is disconnected from the device.

Note: No flash ROM is dedicated to the CAC USB Host Controller to save any data or log.

When the Restore Factory Default operation is performed, or power reset is initiated, or USB CAC device is disconnected from the TOE, all the working memory of CAC USB Host Controller is reset to default. The main function of this device is to read the device ID to ensure it is a permitted device. All the memory/RAM needed is for internal operation and not related to any user data.

## **Front Panel PCBA**

The front panel board has no ROM or RAM functionality.