IPGARD Secure KVM/Matrix Switch Security Target

Release Date: May 10, 2018
Document ID: SST-0S0-ALL
Revision: 5.03
Author: Albert Cohen, IPGARD Inc.

Table of Contents

Table of Figures

List of Tables

Document Revisions

Revision#	*Date*	*By*	*Updates*
5.00	December 27, 2017	Albert Cohen, IPGARD	Initial Document Outline
5.01	January 18, 2017	Albert Cohen, IPGARD	Updates and corrections per Leidos evaluation report, round 1
5.02	March 6, 2018	Albert Cohen, IPGARD	Updates and corrections per Leidos evaluation report, round 2
5.03	May 10, 2018	Albert Cohen, IPGARD	Updates and corrections per Leidos evaluation report, round 3; removed proprietary information

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.

An ST in the Peripheral Sharing Switch (PSS) Protection Profile (PP) is defined as the following:

Security Target - Implementation-dependent statement of security needs for a specific identified TOE.

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).

ST Title	IPGARD Secure KVM/Matrix Switch Security Target
Revision Number	5.03
ST Publish Date	May 10, 2018
ST Authors	Albert Cohen, IPGARD Inc.
TOE Identification	See Tables 5, 6 and 7 below
Keywords	KVM, Isolator, Matrix, Secure, IPGARD, Protection Profile 3.0

Table 2 – ST Identification

1.2 PP Reference Identification

PP Reference: Protection Profile for Peripheral Sharing Switch (PSS)
PP Sponsor: National Information Assurance Partnership (NIAP)
PP Version: 3.0

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

Extended Components Definition (Section 6)

- Components required for the ST but not listed in Part II or Part III of the CC.

Summary Specification (Section 7)

- 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: Indicated with *italicized and underlined* text;
- Iteration: Indicated by appending the iteration number in parenthesis (e.g., (1), (2), (3)).

Extended SFRs are identified with the label "_EXT" after the requirement name.

In cases where the claimed PP has already completed selections and/or assignments such that a conformant ST is required to reproduce these operations, the formatting conventions used in the original PP apply.

In cases where the claimed PP includes a statements in an SFR flagged with [Conditional], the statement itself is preserved if and only if it applies to the TOE. Regardless of whether the statement itself applies, the '[Conditional]' text is removed in all cases.

1.5 Technical Definitions

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

1.5.1 ST Specific Terminology

Terminology	Description
Administrator	A person who administers (e.g. installs, configures, updates, maintains) a system of device(s) and connections.
Configurable Device Filtration (CDF)	PSS function that qualifies (accepts or rejects) peripheral devices based on field configurable parameters.
Connected Computer	A computing device (platform) connected to the PSS. May be a personal computer, server, tablet or any other computing device with user interaction interfaces.
Connection	Enables devices to interact through respective interfaces. It may consist of one or more physical (e.g. a cable) and/or logical (e.g. a protocol) components.
Device	An information technology product with which actors (persons or devices) interact.
Display	A Human Interface Device (HID), such as a monitor or touch screen.
External Entity	An entity outside the TOE evaluated system, its connected computers and its connected peripheral devices.
Fixed Device Filtration (FDF)	PSS function that qualifies (accepts or rejects) peripheral devices based on fixed parameters.

Human Interface Device (HID)	A device that allows for user input. For example, keyboard and mouse.
Interface	Enables interactions between actors.
Isolator	A PSS with single connected computer.
Keyboard	A Human Interface Device (HID) such as a keyboard, keypad or other text entry device.
Non-Selected Computer	A connected computer not currently selected by the PSS user.
Peripheral	A device that exposes an actor's interface to another actor.
Peripheral Group	An ordered set of peripherals.
Pointing Device	A Human Interface Device (HID), such as a mouse, track ball or touch screen (including multi-touch).
Selected Computer	A connected computer currently selected by the PSS user.
User	A person or device that interacts with devices and connections.
User Authentication Device	A peripheral device used to authenticate the identity of the user, such as a smart-card reader, biometric authentication device or proximity card reader.

Table 3 – ST Technical Definitions

1.5.2 Acronyms

Acronym	Full Definition	KVM/Matrix Related
AUX	DisplayPort Auxiliary Channel	KVM/Matrix
CAC	Common Access Card	KVM/Matrix
CCTL	Common Criteria Test Lab	KVM/Matrix
CDC	Communication Device Class	KVM/Matrix
CODEC	Coder-Decoder	KVM/Matrix
dBv	A measurement of voltages ratio – decibel volt	KVM/Matrix
DC	Direct Current	KVM/Matrix
DP	DisplayPort	KVM/Matrix
DVI	Digital Visual Interface	KVM/Matrix
EDID	Extended Display Identification Data	KVM/Matrix
FDF	Fixed Device Filtration	KVM/Matrix
HD	High Definition	KVM/Matrix
HDMI	High Definition Multimedia Interface	KVM/Matrix
HEAC	HDMI Ethernet Audio Control	KVM/Matrix
HID	Human Interface Device	KVM/Matrix
IP	Internet Protocol	KVM/Matrix
USB Keep-Alive NAK transaction	USB 2.0 standard handshake PID (1010B) – Receiving device cannot accept data or transmitting device cannot send data.	KVM/Matrix
KM	Keyboard, Mouse	KVM
KVM	Keyboard, Video and Mouse	KVM/Matrix
LED	Light-Emitting Diode	KVM/Matrix
LoS	Line-of-Sight	KVM/Matrix

MCU	Microcontroller Unit	KVM/Matrix
MCCS	Monitor Control Command Set	KVM/Matrix
MHL	Mobile High-Definition Link	Not in use
MSC	Mass Storage Class	KVM/Matrix
mV	millivolt	KVM/Matrix
OSD	On-Screen Display	KVM/Matrix
PC	Personal Computer	KVM/Matrix
PIN	Personal Identification Number	KVM/Matrix
PSS	Peripheral Sharing Switch	KVM/Matrix
S/PDIF	Sony/Philips Digital Interface Format	KVM/Matrix
SP	Special Publication	KVM/Matrix
SPF	Shared Peripheral Functions	KVM/Matrix
TMDS	Transition-Minimized Differential Signalling	KVM/Matrix
UART	Universal Asynchronous Receiver / Transmitter	KVM/Matrix
USB	Universal Serial Bus	KVM/Matrix
V	Volt	KVM/Matrix
VESA	Video Electronics Standards Association	KVM/Matrix
VGA	Video Graphics Array	KVM/Matrix

Table 4 – ST Acronyms

1.6 TOE Overview

1.6.1 TOE Architecture (High Level)

IPGARD Secure Peripheral Sharing Switches (PSS) provide a secure medium to share a single set or more of peripheral components such as keyboard, video display and mouse/pointing devices among one or multiple computers over USB, DVI, HDMI, and DisplayPort for KVM/Matrix Switches. For KVM/Matrix models, the architecture is such that only one set of keyboard and mouse operation is permitted at a time, thereby enforcing a single user mode of operation even when multiple input port groups are present.

IPGARD Secure PSS 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 flow forcing devices to guarantee isolation of connected computer data channels.

IPGARD Secure KVM port models:

- 1-Port
- 2-Port
- 4-Port
- 8-Port

IPGARD Secure KVM video outputs (displays):

- Single head
- Dual-head
- Quad-head

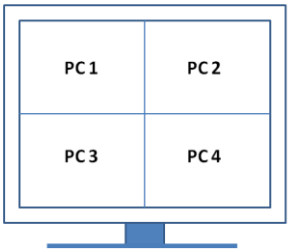
IPGARD Secure Matrix port models:

- 4-Port
- 8-Port

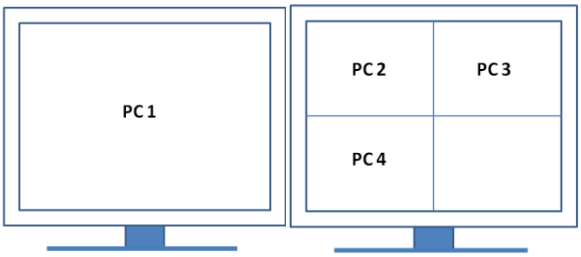
IPGARD Secure Matrix video outputs (displays):

- Single head – 2 or 4 displays

IPGARD KVM with Preview Screen provides the capability of presenting one or more video input over a single or two monitors. For instance -
Single monitor system:
All connected PC's to the TOE (PC 1, 2, 3 and 4) can output video into one monitor.



Two monitors system:
PC 1 outputs video to monitor 1 on the left and the rest (PC 2, 3 and 4) are outputting video to monitor 2.



The IPGARD Secure PSS 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 PSS includes ports for the following interfaces, depending on model:

- USB keyboard
- USB mouse
- DVI, HDMI 1.4 and DisplayPort 1.2 Video Input (computer ports)
- DVI, HDMI 1.4 and DisplayPort 1.2 Video Output (peripheral port)
- 3.5mm Audio Input (computer ports)
- 3.5mm Audio Output (peripheral port)
- USB Smart-card reader, PIV/CAC reader, Token or Biometric reader

Computers of varying sensitivities are connected to a single TOE that is intended to restrict peripherals connection to one computer at a time. Data leakage is prevented across the TOE to avoid severe compromise of the user's information.

Modern Secure KVM/Matrix security approaches address the risk of TOE local user data leakage through remote attacks to coupled networks in addition to protecting user information passing through the TOE.

Tables 5, 6, and 7 below provide a summary of the IPGARD Secure KVM/Matrix PSS security features. A detailed description of the TOE security features and how they are mapped to the claimed PP SFRs can be found in Section 7 (TOE Summary Specification) below.

1.6.2 TOE Details

1.6.2.1 *Evaluated Products*

#	Model Name	P/N	Description and NIAP Certification Version	Eval. Version
1	SDVN-1S-P	1872-IPG-1034	1-Port SH Secure DVI-I KVM w/audio and CAC, PP 3.0	255.101
2	SUHN-2S	1872-IPG-1035	2-Port SH Secure HDMI KVM w/audio, PP 3.0	255.212
3	SUHN-2S-P	1872-IPG-1036	2-Port SH Secure Pro HDMI KVM w/audio and CAC, PP 3.0	255.112
4	SUHN-2D	1872-IPG-1037	2-Port DH Secure HDMI KVM w/audio, PP 3.0	255.212
5	SUHN-2D-P	1872-IPG-1038	2-Port DH Secure Pro HDMI KVM w/audio and CAC, PP 3.0	255.112

Table 5 – IPGARD 2-Port and Isolator Secure TOE Identification

#	Model Name	P/N	Description and NIAP Certification Version	Eval. Version
1	SUHN-4S	1872-IPG-1039	4-Port SH Secure HDMI KVM w/audio, PP 3.0	255.222
2	SUHN-4S-P	1872-IPG-1040	4-Port SH Secure Pro HDMI KVM w/audio and CAC, PP 3.0	255.122
3	SUHN-4D	1872-IPG-1041	4-Port DH Secure HDMI KVM w/audio, PP 3.0	255.222
4	SUHN-4D-P	1872-IPG-1042	4-Port DH Secure Pro HDMI KVM w/audio and CAC, PP 3.0	255.122
5	SUHN-4Q-P	1872-IPG-1043	4-Port QH Secure Pro HDMI KVM w/audio and CAC, PP 3.0	255.122
6	SDVN-42-X	1872-IPG-1044	4-Port SH Secure DVI-I Matrix KVM w/audio and CAC, 2 Users, PP 3.0	255.121
7	SDVN-44-X	1872-IPG-1045	4-Port SH Secure DVI-I Matrix KVM w/audio and CAC, 4 Users, PP 3.0	255.121
8	SDMN-4S-P	1872-IPG-1046	4-Port SH Secure Pro DVI-I KVM w/audio, CAC and preview screen, PP 3.0	255.421

Table 6 – IPGARD 4-Port Secure TOE Identification

#	Model Name	P/N	Description and NIAP Certification Version	Eval. Version
1	SDPN-8S	1872-IPG-1047	8-Port SH Secure DP KVM w/audio, PP 3.0	255.233
2	SDPN-8S-P	1872-IPG-1048	8-Port SH Secure Pro DP KVM w/audio and CAC, PP 3.0	255.133
3	SDVN-82-X	1872-IPG-1049	8-Port SH Secure DVI-I Matrix KVM w/audio and CAC, 2 Users, PP 3.0	255.131
4	SDVN-84-X	1872-IPG-1050	8-Port SH Secure DVI-I Matrix KVM w/audio and CAC, 4 Users, PP 3.0	255.131

Table 7 – IPGARD 8-Port Secure TOE Identification

Notes:

- CAC = Common Access Card filtered USB port.
- DP = DisplayPort video.
- SH = Single head; DH = Dual head; QH = Quad head.

- P/N = Part Number of the device as specified by the manufacturer
- Description - Includes text that is printed on a label attached to each KVM/Matrix on the bottom.
- Eval. Version – Firmware and hardware revision per each device.
- IPGARD'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 Switch" (KVM/Matrix 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 KVM/Matrix TOE are listed in the following table.

Console Port	Authorized Devices
Keyboard	Wired keyboard and keypad without internal USB hub or composite device functions, unless the connected device has at least one endpoint which is a keyboard or mouse HID class, KVM/Matrix extender;
Display	Display, Projector, Video or KVM extender.
Audio out	Analog amplified speakers, Analog headphones, Digital audio appliance.
Mouse / Pointing Device	Any wired mouse or trackball without internal USB hub or composite device functions. Touch-screen, Multi-touch or digitizer, KVM/Matrix extender.
User Authentication Device	Smart-card reader, PIV/CAC reader, Token or Biometric reader*

Table 8 – Peripheral Devices supported by the KVM/Matrix TOE

*TOE – Models with –P or –X only

1.6.2.4 *Protocols Supported by the KVM/Matrix TOE*

Tables 9, 10 and 11 below identify the TOE console interface protocols supported. Tables 12, 13, and 14 below identify the TOE computer (host) interface protocols supported.

Model	SDVN-1S-P	SUHN-2S	SUHN-2S-P	SUHN-2D	SUHN-2D-P
Keyboard USB 1.1/2.0	✓	✓	✓	✓	✓
VGA	✓				
DVI-I	✓				
HDMI		✓	✓	✓	✓
Mouse USB 1.1/2.0	✓	✓	✓	✓	✓
Audio Analog Stereo	✓	✓	✓	✓	✓

CAC USB 1.1/2.0	✓		✓		✓

Table 9 – 2- Port and Isolator KVM TOE Console Port Protocols

Note: VGA video output is supported only with DVI to VGA adapter

Model	SUHN-4S	SUHN-4S-P	SUHN-4D	SUHN-4D-P	SUHN-4Q-P	SDVN-42-P	SDVN-44-P	SDMN-4S-P
Keyboard USB 1.1/2.0	✓	✓	✓	✓	✓	✓	✓	✓
DVI-I						✓	✓	✓
HDMI	✓	✓	✓	✓	✓			
Mouse USB 1.1/2.0	✓	✓	✓	✓	✓	✓	✓	✓
Audio Analog Stereo	✓	✓	✓	✓	✓	✓	✓	✓
CAC USB 1.1/2.0		✓		✓	✓	✓	✓	✓

Table 10 – 4-Port KVM/Matrix TOE Console Port Protocols

Note: VGA video output is supported only with DVI to VGA adapter

Model	SDPN-8S	SDPN-8S-P	SDVN-82-P	SDVN-84-P
Keyboard USB 1.1/2.0	✓	✓	✓	✓
DVI-I			✓	✓
DP	✓	✓		
Mouse USB 1.1/2.0	✓	✓	✓	✓
Audio Analog Stereo Output	✓	✓	✓	✓
CAC USB 1.1/2.0		✓	✓	✓

Table 11 – 8-Port KVM/Matrix TOE Console Port Protocols

Note: VGA video input is supported only with DVI to VGA adapter

Model	SDVN-1S-P	SUHN-2S	SUHN-2S-P	SUHN-2D	SUHN-2D-P
Keyboard and Mouse USB 1.1/2.0	✓	✓	✓	✓	✓
VGA	✓				
DVI-I	✓				
HDMI		✓	✓	✓	✓
Audio - Analog Stereo Input	✓	✓	✓	✓	✓

CAC USB 1.1/2.0	✓		✓		✓

Table 12 – 2-Port and isolator KVM TOE Computer Port Protocols

Note: VGA video input is supported only with DVI to VGA adapter

Model	SUHN-4S	SUHN-4S-P	SUHN-4D	SUHN-4D-P	SUHN-4Q-P	SDVN-42-P	SDVN-44-P	SDMN-4S-P
Keyboard and Mouse USB 1.1/2.0	✓	✓	✓	✓	✓	✓	✓	✓
DVI-I						✓	✓	✓
HDMI	✓	✓	✓	✓	✓			
DP								
Audio - Analog Stereo Input	✓	✓	✓	✓	✓	✓	✓	✓
CAC USB 1.1/2.0		✓		✓	✓	✓	✓	✓

Table 13 – 4-Port KVM/Matrix TOE Computer Port Protocols

Note: VGA video input is supported only with DVI to VGA adapter

Model	SDPN-8S	SDPN-8S-P	SDVN-82-P	SDVN-84-P
Keyboard and Mouse USB 1.1/2.0	✓	✓	✓	✓
DVI-I			✓	✓
HDMI				
DP	✓	✓		
Audio - Analog Stereo Input	✓	✓	✓	✓
CAC USB 1.1/2.0		✓	✓	✓

Table 14 –8-Port KVM/Matrix TOE Computer Port Protocols

Note: VGA video input is supported only with DVI to VGA adapter

1.6.2.5 *Logical Scope of the KVM/Matrix TOE*

1.6.2.5.1 Basic KVM TOE Function Overview

Secure KVM/Matrix devices allow an individual user to utilize a set of peripherals to operate in an environment with one or several isolated computers. These devices allow switching keyboard, mouse, display, audio, and USB/CAC (models with –P or –X in model name only) from one isolated computer to another, except that Matrix devices can support multiple peripheral groups.

Table 15 below shows the various KVM/Matrix TOE services that were verified in the current evaluation.

KVM/matrix 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 display to chosen computer	✓
Mapping user keyboard and mouse to chosen computer	✓
Cursor control of selection channels[1]	✓
Mapping user audio device to chosen computer	✓
Mapping user USB CAC peripheral device to selected computer	✓

Table 15 – KVM/Matrix TOE Services

1.6.2.6 Administrative and User configuration of the KVM/Matrix TOE

Table 16 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 PSS PP. See section 7.5 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		✓
Select Mode – KVM/KM (unavailable on Matrix or Preview Screen models)		✓
Restore Factory Default (reset)		✓
Terminate Session	✓	✓

Table 16 – KVM/Matrix TOE User/Administrator Services and Accessibility

*only for models with –P or –X

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] For any KVM device that is configured to be in KM mode. Matrix and Preview Screen models do not support KM mode.

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 Select Mode option is available for Administrator only, allows switching between KVM and KM operation mode. In KVM mode, switching channel is available by pressing the front panel buttons only. In KM mode, switching is available by either pressing the front panel buttons or moving the mouse cursor from one screen to another. In the evaluated configuration, the Administrator must specify the '2 minute delay' KM mode, which automatically makes one switching method unavailable for two minutes following the use of the other method. This is done to ensure ambiguous control of the switching function. Note that this functionality is not included on IPGARD Secure Matrix port models or Preview Screen models.

1.6.2.6.6 Restore Factory Default (reset) option is available for Administrator only. The following events will occur when selecting this option:

1. Device will be switched to KVM mode.
2. 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.
3. User and Administrator log-in credential will be reset back to default.
4. The TOE will perform power down for 1,000ms followed by power up.
5. During power down, all connected devices will be disconnected from the computers and all internal cache other than auditing log will be wiped.
6. After power up the TOE buzzer will buzz twice to indicate completion of power reset and successful self test results.

1.6.2.7 *KVM/Matrix TOE Security Functions Overview*

The following list is an overview of the security features supported by the KVM/Matrix 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 logical 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. 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. 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 TOE is not powered

TOE External Interfaces Security Functions

1. No docking protocols supported by TOE
2. No analog audio input allowed by TOE
3. Devices allowed by KVM TOE
    - Wired USB 1.1/2.0 keyboard and mouse
    - 3.5mm Analog audio output jack
    - TOE DVI models: DVI input/DVI output
    - TOE DP models: DP 1.2 input/DP 1.2 output
    - TOE HDMI models: HDMI 1.4 input/HDMI 1.4 output
    - 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 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 TOE is not powered

TOE Video Subsystem Security Functions

1. Video channels are isolated, disabling bidirectional communication with monitors/displays using dedicated EEPROMs for EDID emulation. The video output signal will be transmitted to the display using a single dedicated EDID address, preventing any unauthorized transactions between the display and the PC.
2. Video channels remain isolated when TOE is not powered
3. Uni-directional EDID read/write process prevents bi-directional communication
4. TOE rejects all non valid EDID devices
5. DVI, DP 1.2 and HDMI 1.4 video inputs supported by TOE

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. 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 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 only 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
4. Cursor control of selection channels – KVM device (non-Matrix or Preview Screen) configured in KM mode only. Note that in the evaluated configuration, the TOE is configured such that while both push button and cursor control switching are available, using one switching method disables the other method for a period of two minutes, preventing ambiguous control

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 7 below.

1.7 TOE Scope and Boundary

1.7.1 Overview

The TOE is a Peripheral Sharing Switch that is configured as KVM/Matrix.

The physical boundary of the TOE consists of (refer to Figure 1, Figure 2 and Table 17 below):

No.	Physical Boundary of TOE
1	One IPGARD Secure KVM/Matrix 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: https://www.ipgard.com/NIAP/documentation)

7	Administrator Guidance (current version available for download at: https://www.ipgard.com/NIAP/documentation)

Table 17 – TOE Physical Boundary Composition

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

Note: Some TOE models support the operation of multiple user displays.

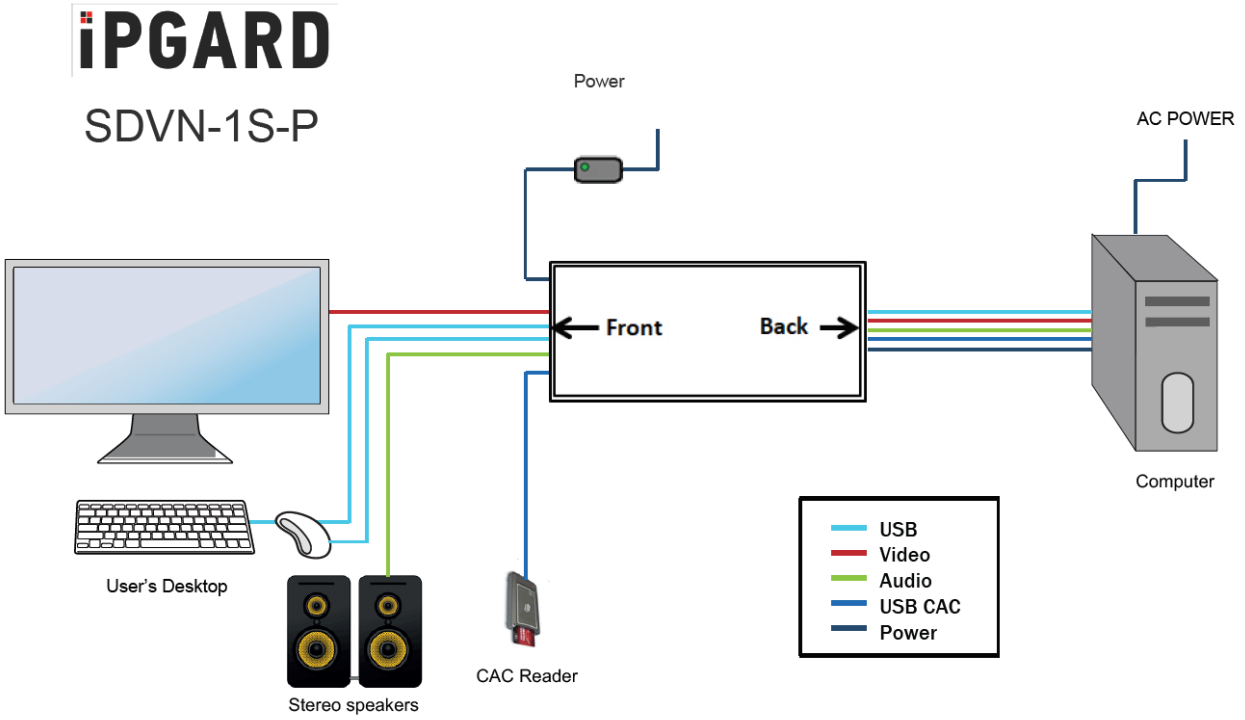


Figure 1: Standard Setup of 1-Port KVM TOE Installation

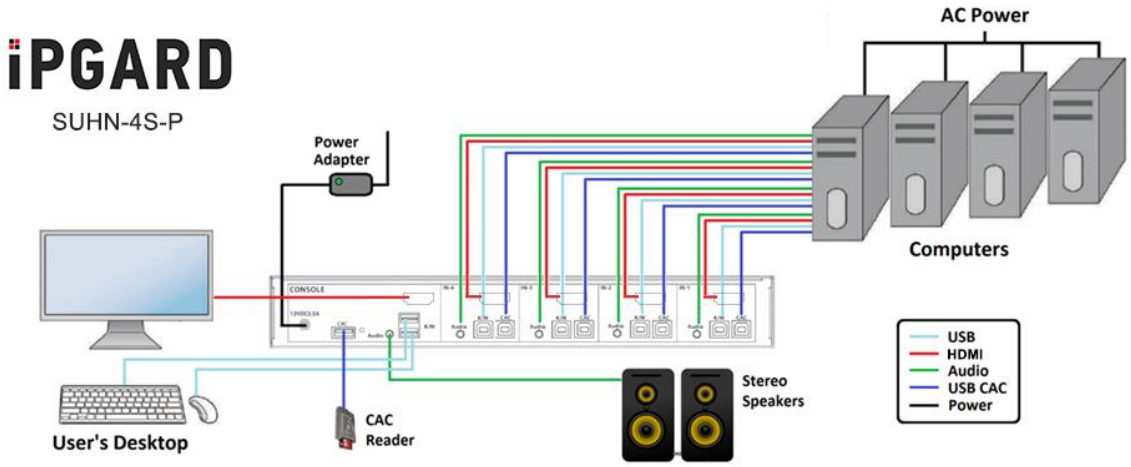


Figure 2: Standard Setup of 4-Port KVM TOE Installation

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, 6, and 7 above.	Specified in tables	TOE Hardware
IPGARD KVM Cables	CBL0055-18	KVM/KM Cable (1.8 m), USB Type-A to USB Type-B*
	CBL0017-18	KVM/KM Cable (1.8 m), Audio out, 3.5mm*
	CBL0048-18	KVM Cable (1.8 m), DVI-A to VGA, USB, Black*
	CBL0086-18	KVM Cable (1.8 m), DVI-D to DVI-D Single-Link, USB*
	CBL0087-18	KVM Cable (1.8 m), DVI-D to DVI-D Dual-Link, USB*
	CBL0091-18	KVM Cable (1.8m), HDMI to HDMI, USB*
	CBL0065-18	KVM Cable (1.8 m), DVI-D to DVI-D Single-Link, USB, Audio out, CAC, Black*
	CBL0069-18	KVM Cable (1.8 m), DP to DP, USB A to USB B*

Table 18 – TOE Components

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

Component	Description
Standard USB Mouse	Shared Peripheral Hardware
Standard USB Keyboard	Shared Peripheral Hardware
Standard Computer Display	Shared Peripheral Hardware
Audio Device (Speakers: supports 3.5mm connector)	Shared Peripheral Hardware
USB User Authentication Device or any other USB	Console user authentication

device which was configured to work with the TOE in advance.	device interface
Standard PC, Server, portable computer or thin client running any operating system	Connected Computers

Table 19 – Environment Components

1.8 Guidance Documents

A product user's manual and an Administrators guide are available for download via the following link: https://www.ipgard.com/NIAP/documentation. All documentation is relevant and within TOE scope.

1.9 Features Outside of TOE Evaluation Scope

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

There are no items excluded from the TOE.

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 PSS PP and is replicated here for clarity.

2.1 Security Assumptions

The Security Objectives and Security Functional Requirements (SFRs) described in the following sections of this ST are based on the condition that all of the assumptions have been met.

Assumption	Definition
A.NO_TEMPEST	It is assumed that the computers and peripheral devices connected to the TOE are not TEMPEST approved.
A.NO_SPECIAL_ANALOG_CAPABILITIES	It is assumed that the computers connected to the TOE are not equipped with special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators and users are trusted to follow and apply all guidance in a trusted manner.
A.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

Table 20 – Security 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 Listed Threats

- The following text was copied from PP for PSS Version 3.0 section 2.1:

Peripheral Sharing Switches (PSS) are at high risk of a targeted attack as they are often used to support users operating over wide security gaps. If a remote attacker can access a computer connected to a PSS, then a targeted attack may be launched in an attempt to access the other connected computer or network via the PSS.

PSS may also be deployed across networks with similar security levels, which must be isolated to maintain security and availability.

The most critical threat affecting a PSS is an intentional attack designed to leak data between two connected computers. A remote attacker may abuse one hacked computer connected to the PSS in an attempt to inject code or data onto the other connected computer or network. Alternatively, an attacker may attempt to leak data from the one side of the PSS to the hacked computer on the other side of the TSS (and from there to the remote attacker).

Shared peripheral devices may be exploited to temporarily store data while switched between computers. It is assumed that all standard connected peripheral devices are vulnerable to data retention through documented or undocumented memory space. For example, an attacker could exploit display Plug and Play signals (e.g., extended display identification data (EDID) or Video Electronics Standards Association (VESA) Monitor Control Command Set (MCCS)) to store target data payloads while the PSS is switched to the targeted computer or network, and then later download this data payload while the display is switched to the other computers or networks. The leaked data payload may be later collected, encrypted and sent to the remote attacker site through various channels such as web access, emails, or IP telephony.

Data may also be leaked between computers across the PSS via various signaling methods. Signaling methods refer to the use of simple bit-by-bit effects used to transfer data across the PSS while in use or while the PSS is being switched between computers. Signaling may use electrical leakages across computers or some other event that may be sensed at the other side of the PSS. For example, if one computer connected to the PSS is attempting to power cycle its USB (Universal Serial Bus) port power and another computer connected to the PSS senses these power changes through another port host interface, data may be leaked across these computers.

It should be noted that the data leaked from the PSS in these cases may be unrelated to the data entered or received by the specific user. Data may leak through the PSS without user awareness when the user is performing normal operational tasks or while the PSS is left powered on and unattended.

It should also be noted that the scope of threats in this PP are limited to threats that are reasonably within the physical and design limitations of standard computers. It is assumed that connected computers are standard personal computer (PC) platforms with no special analog, video, or data collection cards or peripherals. For example, in KVM, video signal leakage through the PSS between the user-selected computer and a non-selected computer is not considered as a reasonable threat as not all standard PCs are capable of analyzing and digitizing a weak cross-talk signal or a full strength signal.

This PP does not cover TEMPEST threats and it is assumed that the computers connected to the PSS as well as the peripheral devices are not TEMPEST approved. Also, it should be noted that the PSS applicable to this PP are expected to have a common ground plane / grounded enclosure that will short all connected computer ground planes.

A subset of the data leakage threat is the special case of user data (e.g., text entered via keyboard) or residual user data that is leaked to a computer connected to the PSS, but not selected.

- The following text was copied from PP for PSS Version 3.0 section 2.2:

Peripheral Sharing Switches allow the user to switch between connected computers. Unintended switching is a security threat in which data could be routed to the wrong connected computer without the user's knowledge. For example, keyboard shortcuts are often used in commercial

switches to switch to another channel. If a user inadvertently presses a keyboard shortcut combination, the user could be typing on a channel other than the one to which the user intended to connect. In an environment where the PSS is used to connect computers of differing classifications, the situation becomes a critical threat that must be mitigated. Therefore, the use of keyboard shortcuts, or "hotkeys" should be disallowed. Similarly, a scanning function is commonly used in commercial switches. This feature is also a security threat and should be disallowed.

To address the unintended switching threat, the PSS must:

1. Require a deliberate user action to switch between connected computers, and
2. Provide a continuous visual indication of the computer to which the user is connected.

Traditionally, the method of "deliberate action" from the user was push-button switching. While this method is still acceptable and the most widely used, other methods have gained popularity as technology has evolved. These methods include use of a touch screen, mouse or cursor control. It should be noted that the user must always have line-of-sight (LoS) to either the PSS itself or to the switching mechanism.

Visual indication has traditionally been handled by light-emitting diode (LED) indicators on the front panel of the PSS. Other acceptable indication methods include lighted push-buttons, graphic or text displays, and on-screen displays (OSDs). If a display is used, it must be "always on" to ensure that continuous indication is provided.

- The following text was copied from PP for PSS Version 3.0 section 2.3:

Peripheral device threats can be divided into two areas:

1. *Unauthorized peripheral device threats* – threats imposed by peripheral devices that should not be connected to the specific PSS port (e.g., a user might connect a mass storage device to the TOE console keyboard port).
2. *Authorized but untrusted peripheral device threats* – threats imposed by legitimate and authorized peripheral devices while being used with the TOE, as all standard authorized peripheral devices connected to the TOE may be untrusted (e.g., a standard USB keyboard with a firmware update endpoint may be used to leak data when switched by the PSS).

Unauthorized Peripheral Device Threats

Peripheral devices that are not authorized for use in a specific TOE port may cause security breaches such as data theft or data leakage. Also, each TOE peripheral port should have an approved list of authorized peripheral devices. Annex C of the referenced PP contains the PSS authorized peripheral devices list.

Authorized But Untrusted Peripheral Device Threats

For the purpose of the referenced PP, it may be assumed that all standard authorized peripheral devices are untrusted. The term "standard" in the context of the referenced PP means commercial off-the-shelf peripherals and does not cover special purpose high-security peripherals that may be used as well. The TOE must be designed to securely operate with all peripheral devices and therefore, the TOE must mitigate the potential threats of all authorized peripheral devices.

It should be noted that standard peripheral devices may be secure and trusted in operation with other types of equipment; however, the use of these devices with a TOE may exploit severe data leakage threats.

- The following text was copied from PP for PSS Version 3.0 section 2.4:

Audio threats in TOE may be resulted from the following:

1. *The user intentionally or unintentionally connects a microphone to the PSS*. A microphone may be misused by a hacked connected computer to leak data or voice (audio eavesdropping) to a remote site.
2. The user uses an audio output device (for example – headphones) that may be misused as a microphone, enabling a remote attacker to perform audio eavesdropping in the vicinity of the TOE.

The audio CODEC used in most PCs and portable devices is a highly flexible analog signal processor. It can amplify and filter a weak signal and, in many cases, it can be switched to multiple physical ports through software. If one computer connected to the TOE is hacked by a remote attacker, that computer may also be misused to provide audio eavesdropping in the vicinity of the TOE.

It is also possible to use that computer to "listen" to audio being played by another hacked computer on a different network, bridging the air-gap between the two networks and leaking data through audio signaling.

Another well-known threat is the misuse of audio output devices such as headphones to work as a low- gain dynamic microphone. All dynamic headphones are very similar to microphones (moving coil and static magnet). With proper amplification, the weak signal generated by these devices can be used for audio eavesdropping around the TOE.

It should be noted here that amplified speakers are not vulnerable to this type of threat as the amplifier serves to provide isolation for the weak reverse signal and attenuates it below usable levels.

It also should be noted that digital audio passed, in KVM, through the video (for example in HDMI) or passed through separate lines is not a concern, since it does not introduce analog signal leakage vulnerabilities.

- The following text was copied from PP for PSS Version 3.0 section 2.5:

Tampering (i.e., replacement or modification) of a TOE can be detrimental to the enforcement of the intended security policies. Unauthorized replacement of a TOE could occur during shipment, storage, or even when in use, depending upon the specific circumstances and degree to which attackers may have access. If the user cannot determine that the correct device has been received, or the user is unable to identify when a device in use may have been replaced, the user may inadvertently use a TOE that does not enforce the required or expected security policies.

PSS tampering could involve physical modifications to the TOE device or logical modifications accomplished via the various TOE connectors.

The physical tampering of a TOE is comparable to TOE replacement and could also occur at any time (e.g., shipping, storage and use). If physical TOE tampering is not identified, the entire TOE logic could be replaced and physical connections, controls, and indicators could be altered.

Ultimately, if physical tampering occurs and goes unidentified the TOE may no longer enforce the required or expected security policies.

Logical tampering of a TOE is effectively comparable to TOE replacement. If tampering occurs and goes undetected, the TOE security-enforcing functions may have been modified such that the TOE may no longer enforce the required or expected security policies. Logical tampering might involve modifying the TOE firmware (e.g., during the firmware update process) to effect a permanent change in the TOE. Alternately, logical tampering might involve modification (e.g., via a buffer overrun attack) of in-memory code or data structures to effect a temporary change in the TOE. Such attacks could be launched from an attached computer, peripheral, or via some other connection (e.g., debug ports) under the control of a malicious user. It should be noted that the malicious user may be the local TOE user or a remote user who attempts to attack the organization from a remote location.

- The following text was copied from PP for PSS Version 3.0 section 2.6:

A catastrophic TOE failure may cause data leakage across its connected computers; therefore, the TOE design must minimize the potential of an undetected catastrophic failure. Other less critical TOE failures may weaken or disable security mechanisms, leaving the TOE vulnerable to attacks or misuse that in turn may cause data leakages.

Data leakage through the TOE may cause significant damage to the operating organization as it may operate undetected for a long time. Damage potential may be higher if the security gap across the TOE is wide (e.g., National security to Internet), or if the security level of the computers connected is high. Even across the same security level (i.e., network segmentation), the damage potential is high as penetration into one network may assist the potential attacker in further penetrating another targeted network through a breached TOE connected between these networks.

Also, if the TOE switching mechanism fails, the TOE should prevent an unintended switching condition. For example, if a push-button is stuck, the TOE may behave as if it is in scanning mode and the user may be confused as to which computer is selected, resulting in a security threat similar to the keyboard shortcut example discussed previously.

2.3.1 Threats Addressed - Operating Environment

The claimed PP lists no threats against the user's assets which specify protection within the TOE environment.

2.3.2 Threats Addressed - TOEs

The claimed PP lists the subsequent threats to the user's/organization's assets that the ST claims to protect in Section 2. The following threats have been replicated below for clarity.

Threat	Definition
T.DATA_LEAK	A connection via the PSS between computers may allow unauthorized data flow through the PSS or its connected peripherals.

T.SIGNAL_LEAK	A connection via the PSS between computers may allow unauthorized data flow through bit-by-bit signaling.
T.RESIDUAL_LEAK	A PSS may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer. More specifically, a PSS may leak user keyboard entries to a PSS-connected computer other than the selected computer in real-time or at a later time.
T.UNINTENDED_SWITCHING	A threat in which the user is connected to a computer other than the one to which they intended to be connected.
T.UNAUTHORIZED_DEVICES	The use of an unauthorized peripheral device with a specific PSS peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers.
T.AUTHORIZED_BUT_UNTRUSTED_DEVICES	The use of an authorized peripheral device with the PSS may still cause unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers. Such threats are possible due to known or unknown device vulnerabilities or due to additional functions within the authorized peripheral device.
T.MICROPHONE_USE	Microphone connected to the TOE used for audio eavesdropping or to transfer data across an air-gap through audio signaling.
T.AUDIO_REVERSED	Audio output device used by an attacker as a low-gain microphone for audio eavesdropping. This threat is an abuse of the computer and TOE audio output path to reverse the analog data flow from the headphones to the computer. The computer then amplifies and filters the weak signal, and then digitizes and streams it to another location.
T.LOGICAL_TAMPER	An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code embedded in the TOE's volatile or non-volatile memory to allow unauthorized information flows between connected devices.
T.PHYSICAL_TAMPER	A malicious human agent could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.
T.REPLACEMENT	A malicious human agent could replace the TOE during shipping, storage, or use with an alternate device that does not enforce the TOE security policies.
T.FAILED	Detectable failure of a PSS may cause an unauthorized information flow, weakening of PSS security functions, or unintended switching.

Table 21 – Threats Addressed - TOEs

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 section describes the security objectives for the TOE.

Security Objective	Definition
O.COMPUTER_INTERFACE_ISOLATION	The TOE must prevent unauthorized data flow to assure that the TOE and/or its connected peripheral devices would not be exploited in an attempt to leak data. The TOE computer interface shall be isolated from all other TOE computer interfaces while TOE is powered.
O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED	The same level of isolation defined in the dataflow objectives must be maintained at all times, including periods while TOE is unpowered.
O.USER_DATA_ISOLATION	User data such as keyboard entries should be switched (i.e., routed) by the TOE only to the computer selected by the user. The TOE must provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
O.NO_USER_DATA_RETENTION	The TOE shall not retain user data after it is powered down.
O.PURGE_TOE_KB_DATA_WHILE_SWITCHING	The TOE shall purge all user keyboard data from computer interfaces following channel switching and before interacting with the new connected computer.
O.NO_DOCKING_PROTOCOLS	The use of docking protocols such as Dock Port, USB docking, and Thunderbolt etc. is not allowed in the TOE.
O.NO_OTHER_EXTERNAL_INTERFACES	The TOE may not have any wired or wireless external interface with external entities (external entity is an entity outside the TOE evaluated system, its connected computers and peripheral devices).
O.NO_ANALOG_AUDIO_INPUT	Shared audio input peripheral functions (i.e., analog audio microphone input or line input) are not allowed in the TOE
O.UNIDIRECTIONAL_AUDIO_OUT	The TOE shall be designed to assure that reverse audio signal attenuation will be at least 30 dBv measured with 200 mV and 2V input pure sinus wave at the extended audio frequency range including negative swing

	signal. The level of the reverse audio signal received by the selected computer shall be minimal to assure that the signal level generated by headphones will be well under the noise floor level.
O.COMPUTER_TO_AUDIO_ISOLATION	The audio dataflow shall be isolated from all other TOE functions. Signal attenuation between any TOE computer interface and any TOE audio interface shall be at least 45 dBv measured with 2V input pure sinus wave at the extended audio frequency range including negative swing signal.
O.USER_AUTHENTICATION_ISOLATION	The user authentication function shall be isolated from all other TOE functions.
O.USER_AUTHENTICATION_RESET	Unless the TOE emulating the user authentication function, upon switching computers, the TOE shall reset (turn off and then turn on) the power supplied to the user authentication device for at least 1 second
O.USER_AUTHENTICATION_ADMIN	If the TOE is capable of being configured after deployment with user authentication device qualification parameters then such configuration may only performed by an administrator.
O.AUTHORIZED_SWITCHING	The TOE shall allow only authorized switching mechanisms to switch between connected computers and shall explicitly prohibit or ignore unauthorized switching mechanisms.
O.NO_AMBIGUOUS_CONTROL	If the TOE allows more than one authorized switching mechanism, only one method shall be operative at any given time to prevent ambiguous commands.
O.CONTINUOUS_INDICATION	The TOE shall provide continuous visual indication of the computer to which the user is currently connected.
O.KEYBOARD_AND_MOUSE_TIED	The TOE shall ensure that the keyboard and mouse devices are always switched together
O.NO_CONNECTED_COMPUTER_CONTROL	The TOE shall not allow TOE control through a connected computer.
O.PERIPHERAL_PORTS_ISOLATION	The TOE shall prevent data flow between peripheral devices of different SPFs and the TOE peripheral device ports of different SPFs shall be isolated.
O.DISABLE_UNAUTHORIZED_PERIPHERAL	The TOE shall only allow authorized peripheral device types (See Annex C) per peripheral device port; all other devices shall be identified and then rejected or ignored by the TOE.
O.DISABLE_UNAUTHORIZED_ENDPOINTS	The TOE shall reject unauthorized peripheral devices connected via a USB hub. Alternatively, the TOE may reject all USB hubs.

O.KEYBOARD_MOUSE_EMULATED	The TOE keyboard and pointing device functions shall be emulated (i.e., no electrical connection other than the common ground is allowed between peripheral devices and connected computers).
O.KEYBOARD_MOUSE_UNIDIRECTIONAL	The TOE keyboard and pointing device data shall be forced to unidirectional flow from the peripheral device to the switched computer only.
O.UNIDIRECTIONAL_VIDEO	TOEs that support VGA, DVI or HDMI video shall force native video peripheral data (i.e., red, green, blue, and TMDS lines) to unidirectional flow from the switched computer to the connected display device.
O.UNIDIRERCTIONAL_EDID	TOEs that support VGA, DVI, Display Port or HDMI video shall force the display EDID peripheral data channel to unidirectional flow and only copy once from the display to each one of the appropriate computer interfaces during the TOE power up or reboot sequence. The TOE must prevent any EDID channel write transactions initiated by connected computers.
O.DISPLAYPORT_AUX_FILTERING	TOEs that support DisplayPort video shall prevent (i.e., filter or otherwise disable) the following auxiliary channel traffic: EDID write, USB, Ethernet, Audio return channel, UART and MCCS. Alternatively, the TOE may prevent the AUX channel from operating at Fast AUX speed (675/720 Mbps).
O.TAMPER_EVIDENT_LABEL	The TOE 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 TOE and continue to be available during the TOE deployment. The TOE shall be labeled with at least one visible and one invisible unique identifying tamper-evident marking that can be used to authenticate the device. The TOE manufacturer must maintain complete list of manufactured TOE articles and their respective identification markings' unique identifiers.
O.ANTI_TAMPERING	The TOE shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the TOE would be evident. This shall be accomplished through the use of an always-on active anti-tampering system that serves to permanently disable the TOE should its enclosure be opened. The TOE shall use an always-on active anti-tampering system to permanently disable the TOE in case physical tampering is detected.
O.ANTI_TAMPERING_BACKUP_POWER	The anti-tampering system must have a backup power source to enable tamper detection while

	the TOE is unpowered.
O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER	A failure or depletion of the anti-tampering system backup power source shall trigger TOE to enter tampered state.
O.ANTI_TAMPERING_INDICATION	The TOE shall have clear user indications when tampering is detected.
O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE	Once the TOE anti-tampering is triggered, the TOE shall become permanently disabled. No peripheral-to-computer data flows shall be allowed.
O.NO_TOE_ACCESS	The TOE shall be designed so that access to the TOE firmware, software, or its memory via its accessible ports is prevented.
O.SELF_TEST	The TOE shall perform self-tests following power up or powered reset.
O.SELF_TEST_FAIL_TOE_DISABLE	Upon critical failure detection the TOE shall disable normal operation of the whole TOE or the respective failed component.
O.SELF_TEST_FAIL_INDICATION	The TOE shall provide clear and visible user indications in the case of a self-test failure.

Table 22 – Security Objectives for the TOE

Notes:

1. Objective O.USER_AUTHENTICATION_TERMINATION is not applicable to the TOE per referenced PP as it does not support emulated user authentication device function.

3.2 Security Objectives for the Operational Environment

The following section describes the Security Objectives for the Operational Environment.

Environment Security Objective	Definition
OE. NO_TEMPEST	The operational environment will not require the use of TEMPEST approved equipment.
OE. NO_SPECIAL_ANALOG_CAPABILITIES	The operational environment will not require special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.
OE.PHYSICAL	The operational environment will provide physical security, commensurate with the value of the TOE and the data it contains.
OE.TRUSTED_ADMIN	The operational environment will ensure that appropriately trained and trusted TOE Administrators and users are available to administer, configure and use the TOE.

Table 23 – Security Objectives for the Operational Environment

3.3 Rationale

The following section showcases that each listed threat, OSP, and assumption are addressed by at minimum one security objective for the TOE, which in turn enforces the OSPs, counteract threats, and asserts assumptions. The following table is taken from the claimed protection profile.

3.3.1 Security Objectives Rationale - TOE

Threats, Policies, and Assumptions	Summary	Objectives and rationale
Cross Computer Flow	Data Flow Isolation	
T.DATA_LEAK **A connection, via the TOE, between connected computers may allow unauthorized data transfer through the TOE or its connected peripherals.**	O.COMPUTER_INTERFACE_ISOLATION The TOE must prevent unauthorized data flow to assure that the TOE and/or its connected peripheral devices would not be exploited in an attempt to leak data. The TOE computer interface shall be isolated from all other TOE computer interfaces while TOE is powered.	**O.COMPUTER_INTERFACE_ISOLATION** partially mitigates that threat through the prevention of potential data flows between the different computer interfaces in the TOE. The assurance of isolation between the TOE computer ports prevents data leakages between TOE connected computers directly between the computer interfaces.
	O.COMPUTER_INTERFACE_ISOLATION_UNPOWERED The same level of isolation defined in the dataflow objectives must be maintained at all times, including periods while TOE is unpowered.	**O.COMPUTER_INTERFACE_ISOLATION_UNPOWERED** counters this threat through the prevention of data flow between TOE computer interfaces during periods that TOE is unpowered. The TOE and its connected computers may have independent power sources or different power management policies. Computer interface isolation in TOE unpowered state must be equal or better than computer interface isolation in TOE powered state.
	O.USER_DATA_ISOLATION User data such as keyboard entries should be switched (i.e., routed) by the TOE only to the computer selected by the user. The TOE must provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.	**O.USER_DATA_ISOLATION** mitigates that threat by ensuring that user data in the TOE will only flow to the user selected computer. To prevent user data leakage, it is critical that user data from the peripheral input device will flow only to the user selected computer. A leakage of user data to another computer interface may disclose classified user information. For example, user credentials typed by the user while the TOE is connected to the secret computer may not leak to any other computer interface to prevent disclosure of classified credentials through another non-classified (and potentially compromised) computer.
	O.NO_DOCKING_PROTOCOLS The use of docking protocols such as Dock Port, USB docking, and Thunderbolt etc. is not allowed in the TOE. Note: MHL 3.0 and higher or USB Type C	**O.NO_DOCKING_PROTOCOLS** mitigates that threat by preventing the use of complex protocols capable of supporting unsecure traffic. As peripheral protocols become more

	is allowed in the TOE only if within the TOE the protocol is separated into one video only protocol (such as HDMI) and one peripheral protocol (such as USB).	capable, multiple functions may be combined into a single physical interface. The use of such protocols in the TOE shall be limited as the protection and isolation cannot be assured with such protocols when peripheral devices are frequently switched. Such switching may cause data leakages between connected computers through docking protocols. Composite protocols such as Display Port, MHL and USB Type C may be used if the TOE is capable of mitigating and effectively removing content other than video and audio.
	O.NO_OTHER_EXTERNAL_INTERFACES The TOE may not have any wired or wireless external interfaces with external entities (external entity is an entity outside the TOE evaluated system, its connected computers and peripheral devices).	**O.NO_OTHER_EXTERNAL_INTERFACES** counters this threat by ensuring that the TOE would not support external interfaces that may inject code or data into the authorized traffic flowing through it. The presence of a data reception function (wired or wireless) inside the TOE may cause unauthorized data flow or signal leak between external entities and sensitive connected computers and networks. It also counters this threat by ensuring that the TOE would not support external interface that may enable data flow to external entities through wired or wireless transmission. The presence of a data transmission function (wired or wireless) inside the TOE may cause unauthorized data flow or signal leak between classified and the non-classified computers and networks.
	O.USER_AUTHENTICATION_ISOLATION The user authentication function shall be isolated from all other TOE functions.	**O.USER_AUTHENTICATION_ISOLATION** mitigates that threat by ensuring that the bidirectional user authentication traffic would not be abused to leak data across the TOE between connected computers. User authentication device requires a bidirectional channel between the device and the connected computer through the TOE. That channel may contain classified user information. The TOE must prevent leakage of this data to other TOE interfaces.
	O.USER_AUTHENTICATION_RESET Unless the TOE emulating the user authentication function, upon switching computers, the TOE shall reset (turn off and then turn on) the power supplied to the user authentication device for at least 1 second.	**O.USER_AUTHENTICATION_RESET** mitigates that threat by ensuring that all state and volatile memory in the connected user authentication device will be deleted (through power recycling reset) prior to connecting to a new computer.

	O.PERIPHERAL_PORTS_ISOLATION The TOE shall prevent data flow between peripheral devices of different SPFs. The TOE peripheral device ports of different SPFs shall be isolated (See Annex D, Table 1, Flows F and G).	**O.PERIPHERAL_PORTS_ISOLATION** counters this threat by ensuring that peripheral ports are isolated to prevent unauthorized data flow between peripheral ports. It is assumed in this PP that all standard peripheral devices may be untrusted; therefore, the TOE shall protect the system from attacks that may exploit such devices to enable unauthorized data flows. Since the TOE may switch peripheral devices of different Shared Peripheral Functions (SPFs) to different computers, data flow between these devices must be protected to prevent unauthorized data flow between connected computers.
T.SIGNAL_LEAK **A connection, via the TOE, between computers may allow unauthorized data transfer through bit-by-bit signaling.**	O.COMPUTER_INTERFACE_ISOLATION The TOE must prevent unauthorized data flow to assure that the TOE and/or its connected peripheral devices would not be exploited in an attempt to leak data. The TOE computer interface shall be isolated from all other TOE computer interfaces.	**O.COMPUTER_INTERFACE_ISOLATION** mitigates that threat by ensuring that the computer interfaces would not be abused for signaling attack. The existence of an unauthorized data flow in the TOE between two computer interfaces may cause signaling leakages across the TOE or its connected peripherals. As computers connected to the TOE may have wide security gap, this may cause classified data (not necessarily user data) to leak to non-classified (potentially compromised) computers.
	O.NO_OTHER_EXTERNAL_INTERFACES The TOE may not have any wired or wireless external interfaces with external entities (external entity is an entity outside the TOE evaluated system, its connected computers and peripheral devices).	**O.NO_OTHER_EXTERNAL_INTERFACES** mitigates that threat by ensuring that the TOE does not contain external interfaces that may inject data into the user data. Such functions may be abused to signal injected data into a connected computer. O.NO_OTHER_EXTERNAL_INTERFACES further mitigates that threat by ensuring that the TOE does not contain any wired or wireless external interface that may export data to outside entity. Such functions may be abused to signal sensitive data from a connected computer.
	O.NO_ANALOG_AUDIO_INPUT Shared audio input peripheral functions (i.e., analog audio microphone input or line input) are not allowed in the TOE.	**O.NO_ANALOG_AUDIO_INPUT** counters this threat by preventing the passage of the highly-sensitive analog audio input or microphone signals through the TOE. This limitation is important in order to prevent exploitation of the connected computer audio codec function to detect, filter, amplify and detect weak signals inside or around the TOE to perform a signaling attack.

	O.UNIDIRECTIONAL_AUDIO_OUT A TOE with an audio switching function shall enforce unidirectional flow of analog signals between the connected computer and the TOE audio peripheral device output. A TOE with an audio switching function shall be designed to assure that reverse signal attenuation will be at least 30 dBv measured with 200 mV and 2V input pure sinus wave at the extended audio frequency range including negative swing signal. The level of the reverse audio signal received by the selected computer shall be minimal to assure that the signal level generated by headphones will be well under the noise floor level.	**O.UNIDIRECTIONAL_AUDIO_OUT** counters this threat by preventing the exploitation of the analog audio output to receive signaled data from a connected computer. Analog audio output in standard computers may be exploited to become audio input in some audio codecs. Audio devices such as headphones may also be used as low-gain dynamic microphone. If the TOE design assures that analog audio reverse signal attenuation is below the noise floor level then the audio signal may not be recovered from the resulted audio stream. This will prevent potential abuse of headphones connected to the TOE for audio eavesdropping. The values selected in the objective was set by analysis and validated by empirical results.
	O.COMPUTER_TO_AUDIO_ISOLATION The audio data flow shall be isolated from all other TOE functions. Signal attenuation in the extended audio frequency range between any TOE computer interface and any TOE audio interface shall be at least 45 dBv measured with 2V input pure sinus wave at the extended audio frequency range including negative swing signal.	**O.COMPUTER_TO_AUDIO_ISOLATION** counters this threat by assuring that analog audio output converted to input by a malicious driver would not pick up signals from other computer interfaces. A TOE design that assures that audio signal would not be leaking to any other TOE interface can effectively prevent a potential signaling leakage across the TOE through the analog audio. The values selected in the objective was set by analysis and validated by empirical results.
	O.NO_CONNECTED_COMPUTER_CONTROL The TOE shall not allow TOE control through a connected computer.	**O.NO_CONNECTED_COMPUTER_CONTROL** reduces the threat by preventing high speed signaling attacks that abuse TOE channel switching. A malicious signaling attack on the TOE may be accelerated if a compromised connected computer is capable of controlling the TOE selected channel. Bit-by-bit leakages may occur at the rate of one or multiple bits per TOE switch. This rate may increase to several kilobytes per second if the TOE is allowed to be controlled by a connected computer.
	O.USER_AUTHENTICATION_RESET Unless the TOE emulating the user authentication function, upon switching computers, the TOE shall reset (turn off and then turn on) the power supplied to the user authentication device for at least 1 second.	**O.USER_AUTHENTICATION_RESET** mitigates this threat by eliminating potential state memory in the connected user authentication device after switching to a new computer. Power recycling of the connected user authentication device assures that states and volatile registers will be erased while the TOE switches between computers.

		Testing showed that all USB powered authentication devices would reset if powered down for 1 second. In case that specific USB device would not properly reset, vendor may implement longer power down intervals.
T.RESIDUAL_LEAK **A PSS may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer. More specifically, a PSS may leak user keyboard entries to a PSS-connected computer other than the selected computer in real-time or at a later time.**	O.NO_USER_DATA_RETENTION The TOE shall not retain user data after it is powered down. It should be noted that user data does not include the TOE or peripherals configuration and therefore such data may remain in the TOE after it is powered off.	**O.NO_USER_DATA_RETENTION** counters this threat by preventing user data retention at the TOE when it is being powered off. As TOE may be reused inside the organization to serve different users / roles at different time, it is critical that no user information will be stored in the TOE after it is being powered off.
	O.PURGE_TOE_KB_DATA_WHILE_SWITCHING The TOE shall purge all user keyboard data from computer interfaces following channel switching and before interacting with the new connected computer.	**O.PURGE_TOE_KB_DATA_WHILE_SWITCHING** assures that when TOE is switched, user keyboard data will not flow to the previously selected computer. It mitigates this threat by deleting user keyboard data while switching between channels.
Unintended Switching	**Control and Monitoring**	
T.UNINTENDED_SWITCHING **A threat in which the user is connected to a computer other than the one to which they intended to be connected.**	O.AUTHORIZED_SWITCHING The TOE shall allow only authorized switching mechanisms to switch between connected computers and shall explicitly prohibit or ignore unauthorized switching mechanisms. Authorized switching mechanisms shall require physical, zero-distance touch and include push-buttons, touch screen and mouse or cursor control. Unauthorized switching mechanisms include keyboard shortcuts, also known as "hotkeys," automatic scanning and voice activation.	**O.AUTHORIZED_SWITCHING** mitigates this threat by preventing unauthorized switching methods that may cause user confusion and loss of situational awareness. A TOE with unauthorized switching mechanisms may cause misalignment between the actual TOE state and the user understanding of the TOE state.
	O.NO_AMBIGUOUS_CONTROL If the TOE allows more than one authorized switching mechanism, only one method shall be operative at any given time to prevent ambiguous commands.	**O.NO_AMBIGUOUS_CONTROL** mitigates this threat by preventing TOE control mechanisms that are not well-defined. Ambiguous TOE control may cause cases of unintended switching of the TOE. The TOE controls must be unambiguous to prevent user confusion or misinterpretation of the TOE state.
	O.CONTINUOUS_INDICATION The TOE shall provide continuous visual indication of the computer to which the user is currently connected.	**O.CONTINUOUS_INDICATION** counters this threat by preventing the loss of TOE indications that may lead to user confusion. TOE monitoring must be shown at all times to reduce the risk of user confusion or misinterpretation of the TOE state. It should be noted that the user may take a break or get interrupted by multiple activities and therefore reliance on user

		memory to define the TOE state should be avoided.
	O.KEYBOARD_AND_MOUSE_TIED The TOE shall ensure that the keyboard and mouse devices are always switched together (i.e., they cannot be assigned to different peripheral groups) in order to prevent operational difficulties.	O.KEYBOARD_AND_MOUSE_TIED Counters this threat by preventing a split between keyboard and mouse in the TOE, thus eliminating the potential user confusion caused by such a split. The TOE may enable grouping of peripheral devices (e.g., audio output may be switched separately from keyboard). However, separation of keyboard and mouse may cause user confusion and could result in cases of unintended TOE switching.
Peripheral Device Threats	**Connected Peripheral Devices**	
T.UNAUTHORIZED_DEVICES **The use of unauthorized peripheral devices with a specific TOE peripheral port may allow unauthorized information flows between connected devices or enable an attack on the TOE or its connected computers.**	O.PERIPHERAL_PORTS_ISOLATION The TOE shall prevent data flow between peripheral devices of different SPFs. TOE peripheral device ports of different SPFs shall be isolated (See Annex D, Table 1, Flows F and G).	**O.PERIPHERAL_PORTS_ISOLATION** mitigates this threat by eliminating potential electronic or logic linkage between the various TOE peripheral device ports. A TOE with peripheral port isolation will provide a higher level of protection from malicious or unauthorized peripheral devices.
	O.DISABLE_UNAUTHORIZED_PERIPHERAL The TOE shall only allow authorized peripheral device types (See Annex C) per peripheral device port; all other devices shall be identified and then rejected or ignored by the TOE.	**O.DISABLE_UNAUTHORIZED_PERIPHERAL** mitigates this threat by disabling unauthorized peripheral devices based on device profiling. Such peripheral device disabling is an effective means against the use of unauthorized peripheral devices.
	O.DISABLE_UNAUTHORIZED_ENDPOINTS The keyboard and pointing device peripheral ports of the TOE shall reject any composite USB devices with endpoints other than those authorized for that specific port (See Annex C). Device rejection shall be accomplished either by completely disabling the connected device or disabling just the unauthorized endpoint(s). Similarly, the TOE shall reject unauthorized peripheral devices connected via a USB hub (alternatively, the TOE may reject all USB hubs).	**O.DISABLE_UNAUTHORIZED_ENDPOINTS** Assures that TOE connected peripheral devices with unauthorized functions (i.e., endpoints) are disabled and therefore would not be used. TOE rejection of unauthorized peripheral devices or functions within the devices is an effective means against the intended or unintended use of such devices or functions.
	O.USER_AUTHENTICATION_ADMIN If the TOE is capable of being configured after deployment with user authentication device qualification parameters then such configuration may only performed by an administrator.	**O.USER_AUTHENTICATION_ADMIN** mitigates this threat by assuring that only the administrator will be able to modify the accepted user authentication device profile (for TOE that supports configurable user authentication device profiling). This prevents unauthorized users from modifying the profile and

		potentially allowing the usage of a malicious or unsecure USB device.
T.AUTHORIZED_BUT_UNTRUSTED_DEVICES **The use of authorized peripheral devices with the TOE may still cause unauthorized information flows between connected devices or enable an attack on the TOE or its connected computers. Such threats are possible due to known or unknown vulnerabilities or due to additional functions within the authorized peripheral device.** **All authorized peripheral devices are treated as untrusted under this PP.**	O.KEYBOARD_MOUSE_EMULATED The TOE keyboard and pointing device functions shall be emulated (i.e., no electrical connection other than the common ground is allowed between peripheral devices and connected computers).	O.KEYBOARD_MOUSE_EMULATED Assures that authorized devices such as keyboard and mice would not be abused to store data while switched between computers. Malicious computers connected to the TOE may exploit certain volatile or non-volatile memory effects in the connected keyboard and pointing device peripherals to temporarily store data. Such temporary data storage may be used to transfer data across connected computers. The use of emulated functions in the TOE is an effective method to assure that only the essential functions of the peripheral device will be supported.
	O.KEYBOARD_MOUSE_UNIDIRECTIONAL The TOE keyboard and pointing device data shall be forced to unidirectional flow from the peripheral device to the switched computer only. Such unidirectional flow enforcement shall be implemented in the TOE through physical (i.e., hardware) methods and not through logical (i.e., firmware dependent) methods (See Annex D, Table 1, Flow B).	**O.KEYBOARD_MOUSE_UNIDIRECTIONAL** counters this threat by assuring that any attempt to store data in the keyboard and mouse by a compromised computer or TOE function will be blocked effectively through a physical barrier (as opposed to software). The TOE shall force keyboard and mouse traffic to unidirectional flow from the peripheral device to the connected computer only. If reverse flow is authorized, then the keyboard and mouse may be abused by a compromised connected computer to store data and as a result, leak data between connected computers.
	O.UNIDIRECTIONAL_VIDEO TOEs that support VGA, DVI or HDMI video shall force native video peripheral data (i.e., red, green, blue, and TMDS lines) to unidirectional flow from the switched computer to the connected display device (See Annex D, Table 1, Flow I2).	**O.UNIDIRECTIONAL_VIDEO** mitigates the threat by preventing any potential reversal of the video path in the TOE that may be abused to transfer video or other data from computer-to-computer through the TOE. The TOE shall force native video traffic to unidirectional flow from the computer to the peripheral only. If reverse flow is authorized through the TOE, then logical tampering of the connected display may cause unauthorized data flow.
	O.UNIDIRERCTIONAL_EDID TOEs that support VGA, DVI, Display Port or HDMI video shall force the display EDID peripheral data channel to unidirectional flow and only copy once from the display to each one of the appropriate computer interfaces during the TOE power up or reboot sequence. The TOE must prevent any EDID channel	**O.UNIDIRERCTIONAL_EDID** mitigates this threat by preventing abuse of shared displays to transfer data between connected computers. All display peripheral devices in use today have a bidirectional interface protocols (e.g., EDID channel in DVI, VGA, HDMI interfaces or AUX channel in Display Port). If the TOE forces a

	write transactions initiated by connected computers.	unidirectional data flow from display to computers only, then the display may not be abused to transfer data across connected computers.
	O.USER_AUTHENTICATION_RESET Unless the TOE emulating the user authentication function, upon switching computers, the TOE shall reset (turn off and then turn on) the power supplied to the user authentication device for at least 1 second.	**O.USER_AUTHENTICATION_RESET** mitigating that threat by preventing potential data transfer between computers through known or unknown volatile memory in an authorized user authentication device.
Device Tampering	**Tamper Mitigation**	
T.LOGICAL_TAMPER **An attached device (computer or peripheral) with malware or otherwise under the control of a malicious user could modify or overwrite code embedded in TOE volatile or non-volatile memory to allow unauthorized information flows between connected devices.**	O.NO_TOE_ACCESS The TOE shall be designed so that access to the TOE firmware, software, or its memory via its accessible ports is prevented. This should be accomplished by offering no access to modify the TOE or its memory. To mitigate the risk that a potential attacker will tamper a TOE and then reprogram it with same or tampered functionality, the TOE external and internal interfaces shall be locked for code read and write. The programmable TOE components programming ports must be permanently disabled for both read and write operations. TOE operation code may not be upgradeable through any of the TOE external or internal ports.	**O.NO_TOE_ACCESS** counters the threat of logical tamper by assuring that the TOE would not have external or internal ports that provide programming access or firmware reading of internal components. Logical TOE tampering may be leveraged by the following TOE functions: 1. Internal or external access to the TOE firmware, software or memory. Such access may be used by potential attacker to modify the TOE security functions. 2. Programmer port reading or writing access to the TOE circuitry. Such open access may be abused by an attacker to read modify and write TOE firmware in an attempt to clone, switch or tamper a TOE. 3. Firmware upgrade function. Such function may be abused by an attacker to read, modify and write TOE firmware in an attempt to clone, switch or tamper a TOE.
T.PHYSICAL_TAMPER **A malicious human agent could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.**	O.ANTI_TAMPERING The TOE shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the TOE would be evident. This shall be accomplished through the use of an always-on active anti-tampering system that serves to permanently disable the TOE should its enclosure be opened. The TOE shall use an always-on active anti-tampering system to permanently disable the TOE in case physical tampering is detected.	**O.ANTI_TAMPERING** mitigates this threat by assuring that any attempt to physically tamper the TOE will cause it to become permanently disabled and will provide indications that user cannot ignore.
	O.ANTI_TAMPERING_BACKUP_POWER The TOE anti-tampering system must	**O.ANTI_TAMPERING_BACKUP_POWER** assures that the active anti-tampering

	have a backup power source to enable tamper detection while the TOE is unpowered.	function would continue to operate at all time – even when the TOE is unpowered. TOE physical tampering protection must be continuously operating to effectively prevent physical tampering while the TOE is unpowered. Without such function, TOE power may be interrupted by the attacker in order to gain access to the TOE internal circuitry without triggering the anti-tampering system.
	O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER A failure or depletion of the anti-tampering system backup power source shall trigger TOE to enter tampered state.	**O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER** counters this threat by ensuring that any case of backup power source failure causes permanent tampering to prevent an attacker from abusing effects such as temperature exposure or time that may affect battery or super-capacitors used by the TOE anti-tampering system in order to gain access to the TOE internal circuitry.
	O.ANTI_TAMPERING_INDICATION The TOE shall have clear user indications when tampering is detected.	**O.ANTI_TAMPERING_INDICATION** mitigates this threat by assuring that an event of physical TOE tampering while in service will be discovered by the user and reported to the proper security functions in the organization. Clear TOE tampering indication, together with proper user training and internal procedures, will increase the probability that a tampered TOE will be properly detected.
	O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE Once the TOE anti-tampering is triggered, the TOE shall become permanently disabled. No peripheral-to-computers data flows shall be allowed.	**O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE** counters this threat by assuring that a tampered TOE will not continue to be used and possibly leak data. Permanent TOE disabling is critical in order to assure that the TOE would not be returned to normal service after it has been tampered.
	O.TAMPER_EVIDENT_LABEL The TOE 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 TOE and continue to be available during the TOE deployment.	**O.TAMPER_EVIDENT_LABEL** provides a higher level of assurance that the TOE was not physically tampered during transit or while in service. A tamper evident label is an effective means to provide clear visual indication of physical TOE tampering and also to assure the authenticity of the TOE.

	The TOE shall be labeled with at least one visible and one invisible unique identifying tamper-evident marking that can be used to authenticate the device. The TOE manufacturer must maintain complete list of manufactured TOE articles and their respective identification markings' unique identifiers.	
T.REPLACEMENT **A malicious human agent could replace the TOE during shipping, storage, or use with an alternate device that does not enforce the TOE security policies.**	O.TAMPER_EVIDENT_LABEL The TOE 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 TOE and continue to be available during the TOE deployment. The TOE shall be labeled with at least one visible and one invisible unique identifying tamper-evident marking that can be used to authenticate the device. Compliant TOE manufacturer must maintain complete list of manufactured TOE articles and their respective identification markings' unique identifiers.	**O.TAMPER_EVIDENT_LABEL** provides a higher level of assurance that the TOE was not physically tampered during transit or while in service. A tamper evident label is an effective means to provide clear visual indication of physical TOE tampering and also to assure the authenticity of the TOE.
Unsafe Failure	**Fail-Secure and Self-Testing**	
T.FAILED **Detectable failure of a TOE causing an unauthorized information flow or weakening of TOE security functions.**	O.SELF_TEST The TOE shall perform self-tests following power up or powered reset. The self-testing should at least cover: 1. The basic integrity of the TOE hardware and firmware; 2. The basic computer-to-computer isolation (See Annex D, Table 1, Flows J and K); and 3. The other critical security functions (i.e., user control and anti-tampering). For example, the following steps may be used to test basic isolation during power up: 1. The TOE is switched to channel 1; 2. A test packet is sent to the computer connected to channel 1; and The self-test function checks that all other ports are not receiving any data.	**O.SELF_TEST** mitigates the threat by increasing the probability that a critical TOE failure affecting security would be discovered. It is also reduces the time that the TOE would continue to operate with such failure. The TOE shall be equipped with a self-test function in order to detect failures of underlying security mechanisms used by the TOE and in order to provide clear user indications in case such a failure is detected.

	O.SELF_TEST_FAIL_TOE_DISABLE Upon critical failure detection the TOE shall disable normal operation of the whole TOE or the respective failed component.	**O.SELF_TEST_FAIL_TOE_DISABLE** counters this threat by assuring that upon TOE failure detection, the user would not be able to continue using the TOE, thus reducing the potential security damage of a failure. If the TOE resumed normal operation after critical failure detection, the user may not be aware of the failure and as a result, data may leak through the TOE.
	O.SELF_TEST_FAIL_INDICATION The TOE shall provide clear and visible user indications in the case of a self-test failure. Such indication will preferably include details about the detected failure and its severity.	**O.SELF_TEST_FAIL_INDICATION** counters this threat by providing proper user guidance in case the TOE detects a failure. The indication should be used to guide immediate TOE disconnection from its working environment to prevent further potential security damages. If the TOE does not provide clear failure indication after critical failure detection, the user may not be aware of the failure and as a result, data may leak through the TOE.

Table 24 – Security Objectives Rationale - TOE

3.3.2 Security Objectives Rationale - Operational Environment

Threats, Policies, and Assumptions	Summary	Objectives and rationale
A.NO_TEMPEST **It is assumed that the computers and peripheral devices connected to the TOE are not TEMPEST approved.**	OE. NO_TEMPEST The operational environment will not require the use of TEMPEST approved equipment.	**OE. NO_TEMPEST** upholds this assumption by ensuring that the operational environment does not impose requirements for TEMPEST approved equipment.
A.NO_SPECIAL_ANALOG_CAPABILITIES **It is assumed that the computers connected to the TOE are not equipped with special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.**	OE. NO_SPECIAL_ANALOG_ CAPABILITIES The operational environment will not require special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.	**OE. NO_SPECIAL_ANALOG_CAPABILITIES** upholds this assumption by ensuring that the operational environment does not impose requirements for special analog data collection cards or peripherals.

A.PHYSICAL **Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.**	OE.PHYSICAL The operational environment will provide physical security, commensurate with the value of the TOE and the data it contains.	**OE.PHYSICAL** upholds this assumption by ensuring that the operational environment provides physical security, commensurate with the value of the TOE and the data it contains.
A.TRUSTED_ADMIN **TOE Administrators and users are trusted to follow and apply all guidance in a trusted manner.**	OE.TRUSTED_ADMIN The operational environment will ensure that appropriately trained and trusted TOE Administrators and users are available to administer, configure and use the TOE.	**OE.TRUSTED_ADMIN** upholds this assumption by ensuring that only appropriately trained and trusted administrators and users will be exercising TOE functions.
A.TRUSTED_CONFIG **Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.**	OE.TRUSTED_ADMIN The operational environment will ensure that appropriately trained and trusted TOE Administrators and users are available to administer, configure and use the TOE.	**OE.TRUSTED_ADMIN** upholds this assumption by ensuring that only appropriately trained and trusted administrators and users will be configuring the TOE.

Table 25 – Security Objectives Rationale - 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 meets the criteria of the SFRs listed in Section 4.2 of the claimed Protection Profile. The TOE also meets some of the optional/selection-based SFRs (refer to Annexes F and G of the PSS PP). The SFRs have been replicated below for clarity. Table 26 below displays the SFR IDs and their corresponding definitions. Additional SRF ID details are shown below.

SFR ID	Name
FDP_IFC.1(1)	Subset information flow control
FDP_IFF.1(1)	Simple security attributes
FDP_IFC.1(2)	Subset information flow control
FDP_IFF.1(2)	Simple security attributes
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_RIP.1(1)	Subset Residual information protection
FPT_PHP.1	Passive detection of a physical attack
FPT_PHP.3	Resistance to physical attack

FPT_FLS.1	Failure with preservation of secure state
FPT_TST.1	TSF testing
FTA_CIN_EXT.1	Continuous indications
Optional Requirements (Annex F)	
FAU_GEN.1	Audit data generation
FDP_RIP.1(2)*	Subset Residual information protection (memory)
FIA_UAU.2	User identification before any action
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behavior
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
Selection based Requirements (Annex G)	
FTA_ATH_EXT.1	User authentication device reset

Table 26 – TOE SFR Overview

*designated as an optional requirement as per NIAP TD 0144

4.1.2 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: No dependencies.

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, and [assign whitelist and blacklist definitions for the TOE user authentication device qualification function, Restore Factory Default, Dump Log, Select Mode (non-Matrix models only), and change Access Credential]*]

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)

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*peripheral device SFP*] on
[Subjects: *Peripheral devices*
Objects: *Console ports*
Operations: *allow connection, disallow connection*].

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3(3) Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [*peripheral device SFP*] to objects based on the following:
[Subjects: *Peripheral devices*
Subject security attributes: *peripheral device type*
Objects: *Console ports*
Object security attributes: *none*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*The TOE shall query the connected peripheral device upon initial connection or upon TOE power up and allow connection for authorized peripheral devices in accordance with the table in Annex C of* ***the PSS*** *PP*].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*none.*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

[*The TOE peripheral device interface (console) port shall reject any peripheral device with unauthorized values*].

Application Notes:

It should be noted that the TOE USB keyboard and USB mouse console ports may be interchangeable or combined into one USB composite device port.

FDP_IFC.1(1) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(1) Simple security attributes

FDP_IFC.1.1(1) The TSF shall enforce the [*User Data Protection SFP*] on
[Subjects: *TOE computer interfaces, TOE peripheral device interfaces*
Information: *User data transiting the TOE*
Operations: *Data flow between subjects*].

FDP_IFF.1(1) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1(1) Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1(1) The TSF shall enforce the [User Data Protection SFP] based on the following types of subject and information security attributes:
[*Subject: TOE computer interfaces*
Subject security attributes: user selected computer interface
Subject: TOE peripheral device interfaces
Subject security attributes: none
Information: User data transiting the TOE
Information security attributes: none].

FDP_IFF.1.2(1) The TSF shall permit information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
[*The user makes a selection to establish a data flow connection between the peripheral device interfaces and one computer interface based on the following rules:*

1. *The attribute User Selected Computer determines the operation Allowed Data Flow such that the only permitted data flows are as listed in the table below:*

Value of User Selected Computer	*Allowed Data Flow*
n	*User keyboard peripheral device interface data flowing from peripheral device interface to computer interface #n;* *User mouse peripheral device interface data flowing from peripheral device interface to computer interface #n;* *User display peripheral device interface data flowing from computer interface #n to one or more user display peripheral device interfaces;* *User authentication peripheral device data flowing bidirectional between computer interface #n and user authentication device peripheral interface; and* *Analog audio output data flowing from computer interface #n to the audio peripheral device interface;*

2. *When the user changes the attribute by selecting a different computer, this causes the TOE to change the data flow accordingly.*
3. *The TOE support**s** multiple instances of the peripheral devices shown in the table above, or a subset of these peripheral devices.*][2]

FDP_IFF.1.3(1) The TSF shall enforce the following additional information flow control SFP rules if the TOE supports user authentication devices:

[Following an event of the user changing the attribute by selecting a different computer, the TOE must reset the power to the connected user authentication device].

FDP_IFF.1.4(1) The TSF shall explicitly authorize an information flow based on the following rules: [*no additional rules*].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules:
[1. The TSF shall deny any information flow between TOE peripheral device interfaces and TOE non-selected computer interfaces.
2. The TSF shall deny any data flow between an external entity and the TOE computer interfaces.
3. The TSF shall deny any user data flow between the TOE and an external entity].

[2] The devices supported by each TOE model are identified in section 1.6.1, particularly in Table 8 with details (for example, protocols and number of monitors) in Tables 5, 6, 7, 9, 10, and 11

Application Notes:

Note that an external entity is any device that is not part of the evaluated TOE system, its connected computers or connected peripheral devices.
Therefore, with regard to data flow between the TOE and an external entity:

a. TOE status information such as currently selected computer number or firmware version is not user data and therefore may be transmitted to other (external) entities;
b. KVM and KM cables, extenders or adapters connected to a TOE computer interface or to a peripheral interface are not considered external entities and are therefore excluded from this requirement.

FDP_IFC.1(2) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(2) Simple security attributes

FDP_IFC.1.1(2) The TSF shall enforce the [*Data Isolation SFP*] on
[Subjects: *TOE computer interfaces, TOE peripheral interfaces*
Information: *data transiting the TOE*
Operations: *data flows between computer interfaces*].

Application Notes:

The Data Isolation SFP shall be enforced on data transiting the TOE wherein this data may be:

a. User data – this is typically text typed by the user on the connected keyboard, but may be other types of user information, such as display video; and
b. Other data transiting the TOE – a generalized view of data that may be the result of a hostile action attributable to a threat agent acting from within one or more of the TOE connected computers.

It should be noted that data transiting the TOE does not refer to data generated by the TOE such as TOE monitoring or control information (for example: user selected computer number or name).

FDP_IFF.1(2) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1(2) Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1(2) The TSF shall enforce the [*Data Isolation SFP*] based on the following types of subject and information security attributes:
[Subject: *TOE interfaces*
Subject security attributes: *Interface types (Allowed TOE interface types are listed in Annex C of* ***the PSS*** *PP. Power source and connected computer interfaces are also applicable interface types.)*
Subject: *TOE peripheral device interfaces*

Subject security attributes: *none*
Information: *data transiting the TOE*
Information security attributes: *data types. (The TSF shall enforce the data isolation SFP on the following data types:*

a. *User keyboard key codes;*
b. *User pointing device commands;*
c. *Video information (User display video data and display management data);*
d. *Audio output data; and*
e. *User authentication device data.)*].

Application Note:

Note that the following TOE interface protocols are specifically prohibited:

a. Microphone audio input;
b. Dock Port;
c. USB Docking;
d. Thunderbolt; and
e. Other docking protocols.

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*1. During normal TOE operation, the TSF shall permit only user entered keyboard key codes, and user input mouse commands to flow between the TOE keyboard and mouse peripheral device interfaces and the TOE selected computer interface. No flow is permitted between the selected computer interface and the TOE keyboard and mouse peripheral device interfaces.*
2. The TSF shall permit information flow and TSF resources sharing between two TOE user peripheral interfaces of the same Shared Peripheral group. Both functions may share the same interface].

Application Notes:

A Shared Peripheral group refers to user peripherals that are switched together as a group. For example, the user keyboard and user mouse shall be switched together and are therefore in the same Shared Peripheral group.

Data flow between the keyboard and the mouse peripheral interfaces is allowed (ports can be shared or interchangeable).

Normal TOE operation occurs at any time when the TOE is powered on and it is not:

a. Initializing; or
b. In self-test; or

c. Being configured; or
d. In tampered state; or
e. In self-test failed state.

FDP_IFF.1.3(2) The TSF shall enforce the [*No additional rules*].

FDP_IFF.1.4(2) The TSF shall explicitly authorize an information flow based on the following rules: [*No additional rules*].

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules:

[*1. The TSF shall deny any information flow between TOE Computer Interfaces, except those allowed by the User Data Flow rules;*
2. The TSF shall deny data flow other than keyboard entries and mouse reports between the TOE keyboard and mouse peripheral device interfaces and the TOE selected computer interface;
3. The TSF shall deny power flow between the selected computer interface and TOE keyboard and mouse peripheral device interfaces;
4. The TSF shall deny information flow from the TOE selected computer interface to the TOE keyboard and mouse peripheral device interface;
5. The TSF shall deny data flow of user authentication device data transiting the TOE to non-selected TOE computer interfaces;
6. The TSF shall assure that the user authentication device computer interfaces are not shared with any other TOE peripheral function interface (keyboard, mouse etc.);
7. The TSF shall deny information flow between two TOE user peripheral interfaces in different Shared Peripheral groups;
8. The TSF shall deny analog audio information flow between the TOE selected computer audio interface and the user audio device peripheral interface when a microphone peripheral device is intentionally or unintentionally connected to the TOE audio peripheral device interface;
9. The TSF shall enforce unidirectional information flow between the TOE selected computer audio interface and the user audio device peripheral interface. Bidirectional information flow shall be denied;
10. The TSF shall deny all AUX Channel information flows other than link negotiation, link training and EDID reading;
11. The TSF shall deny any information flow from the TOE display peripheral device interface and the selected computer interface with the exception of EDID information that may be passed once at TOE power up or after recovery from TOE reset;
12. The TSF shall deny an information flow between the selected computer display interface and the TOE display peripheral device interface on the EDID channel;
13. The TSF shall recognize and enable only those peripherals with an authorized interface type as defined in Annex C of the PSS PP. Information flow to all other peripherals shall be denied; and
14. All denied information flows shall also be denied when the TOE's power source is removed].

Note:
Points 10, 11 and 12 refer to KVM TOE only.

Application Notes:

To properly comply with the isolation requirements in this PP, It is recommended that the TOE will be designed with the mouse and keyboard peripheral device interfaces electrically and logically isolated from the connected computer interfaces to reduce the risk of potential exploitation of these devices to transfer data through local data storage or state memory. This level of isolation may be met through various methods, including through USB host and USB device emulation.
Note that the keyboard LEDs may be supported by local TOE indications but not through the keyboard LEDs.

FDP_RIP.1(1) Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1(1) The TSF shall ensure that any previous information content of a resource is made unavailable [

- Immediately after TOE switches to another selected computer;
- and on start-up of the TOE for]

the following objects:[*a TOE computer interface*]

Application Notes:

User data held in any TOE component with non-volatile memory is made unavailable to any TOE computer interface upon the next TOE power on. User keyboard data held in any TOE component is made unavailable to the next connected TOE computer interface when the TOE is switched to a different computer.

FDP_RIP.1(2) Subset residual information protection (memory)

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1(2) The TOE shall have a purge memory or Restore Factory Defaults function accessible to the user to delete all TOE stored configuration and settings.

4.1.4 Class FIA: Identification and Authentication

FIA_UAU.2 User identification before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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 user.

Application notes:

The Administrator shall be authenticated through logon or a specially assigned key before access to administrative functions is provided by the TOE.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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 user.

Application notes:

The Administrator shall be identified through logon or a specially assigned key before access to administrative functions is provided by the TOE.

4.1.5 Class FMT: Security Management (FMT)

The TOE is not required to maintain a separate management role. However, it may provide the following optional management roles:

a. **Administrative configuration** - Functionality to configure certain aspects of TOE operation that should not be available to the general user population. Requires administrator identification and authentication (logon).
b. **User configuration** - Functionality to enable user configuration of certain aspects of TOE operation. Shall be available to all users. No user identification or authentication is required by this PP.

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions.

FMT_MOF.1.1 The TSF shall restrict the ability to [*perform*] the functions [modify TOE user authentication device filtering (CDF) whitelist and blacklist*, [Restore Factory Default, Dump Log, Select Mode (non-Matrix models only), and change Access Credential]*] to [*the authorized administrators*].

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TOE shall be capable of performing the following management functions:

a. The TOE shall provide authorized administrators the option to assign whitelist and blacklist definitions for the TOE user authentication device qualification function.
b. The TOE shall provide authorized administrators the option to [*Restore Factory Default, Dump Log, Select Mode (non-Matrix models only), and change Access Credential*].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*users, administrators*].

Application notes:

There is no requirement in this PP that user shall be authenticated by the TOE.

4.1.6 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state by disabling the TOE when the following types of failures occur: [*failure of the power on self-test, failure of the anti-tampering function*].

Application Notes:

Disabling the TOE shall provide assurance that, as a minimum, no peripheral device is connected to any computer.

FPT_PHP.1 Passive detection of a physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist [a physical attack on the TOE for the purpose of gaining access to the internal components, or to damage the anti-tampering battery] to the [TOE Enclosure] by becoming permanently disabled.

Application Notes:

'Becoming permanently disabled' is interpreted to mean that all connected peripheral devices shall not function.

The design of the TOE enclosure and anti-tampering functions shall assure that any attempt to open the enclosure enough to allow access to the internal components will activate the anti-tampering function.

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self-tests that includes as minimum:

a. Test of the basic TOE hardware and firmware integrity; and

b. Test of the basic computer-to-computer isolation; and

c. Test of critical security functions (i.e., user control and anti-tampering).

[During initial startup, [*upon reset button activation*]] to demonstrate the correct operation of [the TSF].

FPT_TST.1.2 The TSF shall provide users with the capability to verify the integrity of [the TSF functionality].

FPT_TST.1.3 The TSF shall provide users with the capability to verify the integrity of [the TSF].

Application Notes:

The TOE shall provide visible user indications in case of Self-test failure.

4.1.7 Class FTA: TOE Access

FTA_ATH_EXT.1 User authentication device reset

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_ATH_EXT.1.1 The TSF shall reset the power supplied to the user authentication device for at least one second when the user switches the device from one computer to another.

Application Notes:

It is assumed that the user authentication device is not powered by an external power source.

FTA_CIN_EXT.1 Continuous indications

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_CIN_EXT.1.1 The TSF shall display a continuous visual indication of the computer to which the user is currently connected, including on power up, [on reset].[3]

Application Notes:

"On reset" must be selected if the TOE provides a reset option.

The selection may be omitted if a reset function is not provided by the TOE. A TOE may be PP compliant without providing this option. In this case, the evaluator is not required to perform the tests associated with this option.

4.2 Rationale for TOE Security Requirements

The following section maps the SFRs to Security Objectives and describes the rationale used for the mapping (derived directly from the claimed PP).

4.2.1 TOE Security Functional Requirements Mapping

Table 27 below lists all TOE security objectives and the respective security functional requirements (SFRs) that address these security objectives.

Objective	SFRs	Notes
[O.COMPUTER_INTERFACE_ISOLATION]	FDP_IFC.1(1) FDP_IFF.1(1)	
[O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED]	FDP_IFC.1(1) FDP_IFF.1(1)	
[O.USER_DATA_ISOLATION]	FDP_IFC.1(1) FDP_IFF.1(1)	
[O.NO_USER_DATA_RETENTION]	FDP_RIP.1(2)	
[O.PURGE_TOE KB_DATA_WHILE_SWITCHING]	FDP_RIP.1(1)	
[O.NO_DOCKING_PROTOCOLS]	FDP_IFC.1(1) FDP_IFF.1(1)	
[O.NO_OTHER_EXTERNAL_INTERFACES]	FDP_IFC.1(2) FDP_IFF.1(2)	
[O.NO_ANALOG_AUDIO_INPUT]	FDP_IFC.1(1) FDP_IFF.1(1)	
[O.UNIDIRECTIONAL_AUDIO_OUT]	FDP_IFC.1(1) FDP_IFF.1(1)	

[3] Reset function and Restore Factory Default are the same in IPGARD TOEs

[O.COMPUTER_TO_AUDIO_ISOLATION]	FDP_IFC.1(1) FDP_IFF.1(1)	This objective is touched on, but not met by these SFRs.
[O.USER_AUTHENTICATION_ISOLATION]	FDP_IFC.1(1) FDP_IFF.1(1)	
[O.USER_AUTHENTICATION_RESET]	FDP_IFF.1(1) FTA_ATH_EXT.1	
[O.USER_AUTHENTICATION_ADMIN]	FMT_SMF.1 b FMT_MOF.1 FMT_SMR.1 FIA_UAU.2 FIA_UID.2	
[O.AUTHORIZED_SWITCHING]	FDP_IFC.1(2) FDP_IFF.1(2)	
[O.NO_AMBIGUOUS_CONTROL]	FDP_IFC.1(2) FDP_IFF.1(2)	
[O.CONTINUOUS_INDICATION]	FTA_CIN_EXT.1	
[O.KEYBOARD_AND_MOUSE_TIED]	FDP_ACC.1 FDP_ACF.1	
[O.NO_CONNECTED_COMPUTER_CONTROL]	FDP_IFC.1(1) FDP_IFF.1(1)	
[O.PERIPHERAL_PORTS_ISOLATION]	FDP_IFC.1(1) FDP_IFF.1(1)	
[O.DISABLE_UNAUTHORIZED_PERIPHERAL]	FDP_ACC.1 FDP_ACF.1	
[O.DISABLE_UNAUTHORIZED_ENDPOINTS]	FDP_ACC.1 FDP_ACF.1	
[O.KEYBOARD_MOUSE_EMULATED]	FDP_ACC.1 FDP_ACF.1	

[O.KEYBOARD_MOUSE_UNIDIRECTIONAL]	FDP_ACC.1 FDP_ACF.1	
[O.UNIDIRECTIONAL_VIDEO]	FDP_IFC.1(1) FDP_IFF.1(1)	
[O.UNIDIRERCTIONAL_EDID]	FDP_IFC.1(1) FDP_IFF.1(1)	
[O.NO_TOE_ACCESS]	FPT_PHP.3 FPT_FLS.1	
[O.TAMPER_EVIDENT_LABEL]	FPT_PHP.1	
[O.ANTI_TAMPERING]	FPT_PHP.3	
[O.ANTI_TAMPERING_BACKUP_POWER]	FPT_PHP.3	Implied, but not directly stated in the SFR
[O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER]	FPT_PHP.3	
[O.ANTI_TAMPERING_INDICATION]	FPT_PHP.1	
[O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE]	FPT_PHP.3 FPT_FLS.1	
[O.SELF_TEST]	FPT_TST.1	
[O.SELF_TEST_FAIL_TOE_DISABLE]	FPT_TST.1 FPT_FLS.1	
[O.SELF_TEST_FAIL_INDICATION]	FPT_TST.1	

Table 27 – SFR and Security Objectives Mapping

4.3 Rationale for IT Security Requirement Dependencies

This section identifies the SFRs and their dependencies for the TOE. Any dependency that is not met is accompanied by rationale to provide an explanation for any unmet criteria

SFR	Dependencies	Dependency Satisfied/Rationale
FDP_IFC.1(1)	FDP_IFF.1(1)	Yes
FDP_IFF.1(1)	FDP_IFC.1(1)	Yes
	FMT_MSA.3	No. The security attributes associated with the

		Data Isolation Security Function Policy (SFP) are limited to the interface types and data types. The interface type is determined by the type of peripheral device attached to the TOE, and the data type is determined by that interface. These attributes are not subject to security management. Therefore, this SFR and its dependent Security management SFRs are not appropriate for this TOE type.
FDP_IFC.1(2)	FDP_IFF.1(2)	Yes
FDP_IFF.1(2)	FDP_IFC.1(2)	Yes
	FMT_MSA.3(1)	No. The security attributes associated with the User Data Protection SFP are limited to the user selected computer interface. The value is user selected and not subject to security management. Therefore, this SFR and its dependent Security management SFRs are not appropriate for this TOE type.
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1	Yes
	FMT_MSA.3(3)	No. The security attributes associated with the peripheral device SFP are limited to the peripheral device type. The value is determined by what has been connected to the TOE, and is not subject to security management. Therefore, this SFR and its dependent Security management SFRs are not appropriate for this TOE type.
FDP_RIP.1(1)	none	Not applicable
FPT_PHP.1	none	Not applicable
FPT_PHP.3	none	Not applicable
FPT_FLS.1	none	Not applicable
FPT_TST.1	none	Not applicable
FTA_CIN_EXT.1	none	Not applicable
Optional Requirements (Annex F)		
FAU_GEN.1	none	Not applicable
FDP_RIP.1(2)	none	Not applicable

FIA_UAU.2	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UID.2	none	Not applicable
FMT_MOF.1	FMT_SMR.1	Yes
	FMT_SMF.1	Yes
FMT_SMF.1	none	Not applicable
FMT_SMR.1	FIA_UID.1	Yes
Selection based Requirements (Annex G)		
FTA_ATH_EXT.1	none	Not applicable
FTA_ATH_EXT.2	none	Not applicable

Table 28 – TOE Security Functional Requirements and Dependencies

4.4 Security Assurance Requirements

The TOE SARs, summarized in Table 29, identify the management and evaluative activities required to address the threats identified in Section 2 in PP 3.0.

Assurance Class	Assurance Component ID	Assurance Components Description
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative user guidance
Tests	ATE_IND.1	Independent testing - conformance
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Vulnerability Assessment	AVA_VAN.1	Vulnerability analysis

Table 29 – 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 4, September 2012.
- [CC2] - Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
- [CC3] - Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
- [CEM] - Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.

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

5.2 PP Conformance Claims

This ST claims exact conformance to the NIAP PP listed below.

Protection Profile: Protection Profile for Peripheral Sharing Switch, Version: 3.0 dated Feb 13, 2015 and the following NIAP Technical Decisions:

1. TD0083 - Vulnerability Survey Assurance Component (AVA_VAN.1) in PSS PP v3.0, published date 02/29/2016
2. TD0086 - DisplayPort to HDMI Conversion Functionality, published date 03/10/2016
3. TD0136 – FDP_RIP.1.1 – Refinement, published date 12/16/2016
4. TD0141 – FMT_MOF.1.1 & FMT_SMF.1.1 – Test Mapping, published date 01/20/2017. Archived – N/A
5. TD0144 – FDP_RIP.1.1 – Purge Memory and Restore Factory Defaults Optional, published date 02/06/2017
6. TD0251 – FMT_MOF.1.1 – Added Assignment, published date 10/26/2017
7. TD0298 – Update to FDP_IFF.1 Assurance Activities, published date 02/06/2017

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 requirements of the claimed PP are met. The ST is an instantiation of the claimed PP.

This ST contains all of the requirements in section 4 of the PP as well as some requirements from Annex F and Annex G of the PP. No additional requirements (from the CC parts 2 or 3) were added in this ST. Further, no requirements in section 4 of the PP are omitted from this ST.

This ST meets all assurance requirements defined in the PP and all applicable PP assurance tests were conducted in this ST.

6 Extended Components Definition

6.1 Family FTA_ATH_EXT: User Authentication Device Reset and Termination

The extended family belongs to the FTA: TOE access class and has been created to describe reset and termination activities associated with the use of a user authentication device peripheral. FTA_ATH_EXT.1 and FTA_ATH_EXT.2 are modeled after FTA_SSL.4, User-initiated termination.

Family Behavior

This family defines the requirements for the use of an authentication device, including the reset and termination of authentication devices.

Component Leveling

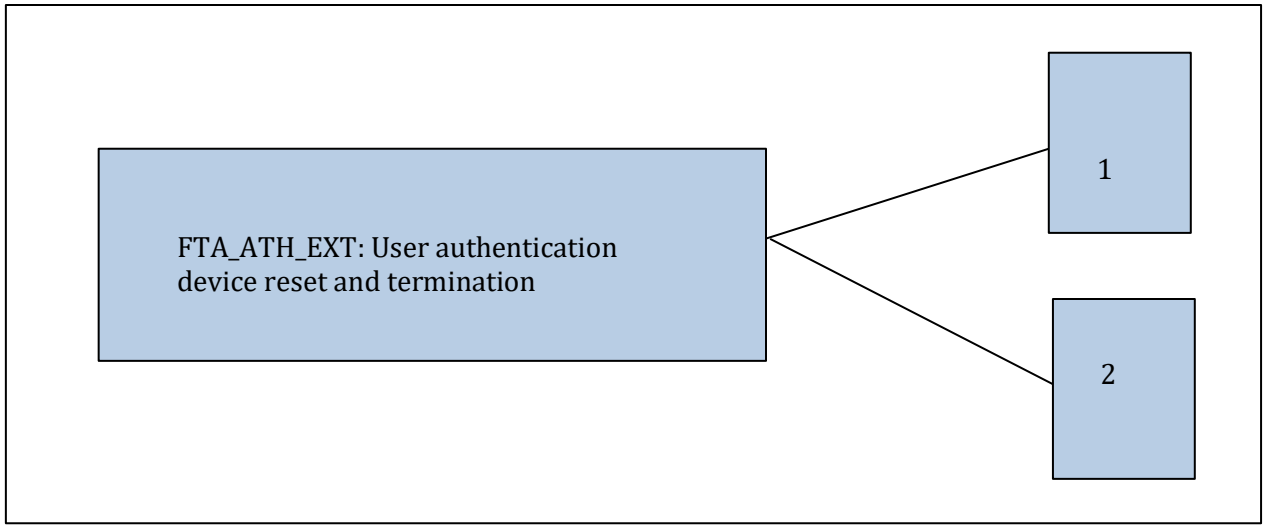


Figure 3: FTA_ATH_EXT: User authentication device reset and termination

Management

There are no management activities foreseen for either FTA_ATH_EXT.1 or FTA_ATH_EXT.2.

Audit

There are no auditable events foreseen for either FTA_ATH_EXT.1 or FTA_ATH_EXT.2.

FTA_ATH_EXT.1 User Authentication Device Reset

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_ATH_EXT.1.1 The TSF shall reset the power supplied to the user authentication device for at least one second when the user switches the device from one computer to another.

Application Notes:

It is assumed that the user authentication device is not powered by an external power source.

FTA_ATH_EXT.2 User Authentication Device Session Termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_ATH_EXT.2.1 The TSF shall ensure that the user authentication session is terminated in all connected computers when the user terminates one authentication session or when the TOE is powered off.

Application Notes:

The user authentication device is no longer considered to be in use when the session is manually terminated by the user. An example of this is the user removing a smartcard.

6.2 Family FTA_CIN_EXT: Continuous Indications

The extended family belongs to the FTA: TOE Access class and has been created to provide for a continuous indication of the connected computer port group. FTA_CIN_EXT.1 is modeled after FTA_TAB.1.

Family Behavior

This family defines the requirements for continuous indications. This family may be used to specify that the TOE must provide an indication of its operational state.

Component Leveling

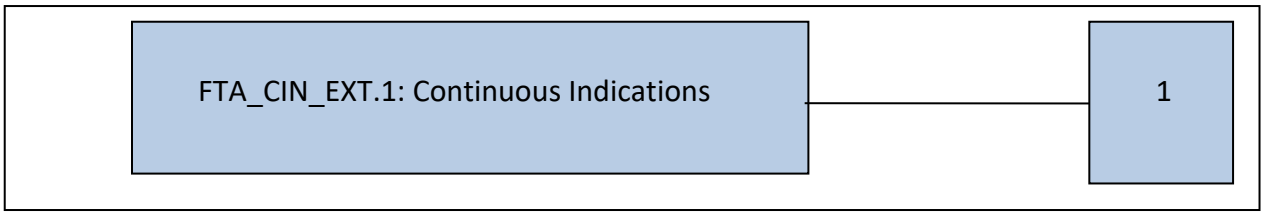


Figure 4: FTA_CIN_EXT: Continuous indications

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

FTA_CIN_EXT.1 Continuous Indications

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_CIN_EXT.1.1 The TSF shall display a continuous visual indication of the computer to which the user is currently connected, including on power up, [selection: on reset].

7 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 27 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.

7.1 TOE Keyboard and Mouse Functionality

The TOE implements the Data Isolation Security Function Policy (SFP) as outlined in Section 4 of the claimed Protection Profile.

[O.COMPUTER_INTERFACE_ISOLATION]: FDP_IFC.1(1) and FDP_IFF.1(1)
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.

[O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED]: FDP_IFC.1(1) and FDP_IFF.1(1)
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.

[O.USER_DATA_ISOLATION]: FDP_IFC.1(1) and FDP_IFF.1(1)
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 in KVM. A secondary multiplexer is used in Matrix to allow only one set of keyboard and mouse operation. Each secure multiplexor 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.

[O.PERIPHERAL_PORTS_ISOLATION]: FDP_IFC.1(1) and FDP_IFF.1(1)
The keyboard and mouse processor is programmed in firmware only to accept 108-key keyboard, 3-button mouse USB devices. Incorrect USB or manipulated composite devices will be refused by the TOE peripheral interface ports. 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.

[O.KEYBOARD_AND_MOUSE_TIED]: FDP_ACC.1 and FDP_ACF.1
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, video, USB/CAC) or other external interfaces.

[O.KEYBOARD_MOUSE_EMULATED]: FDP_ACC.1 and FDP_ACF.1
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.KEYBOARD_MOUSE_UNIDIRECTIONAL]: FDP_ACC.1 and FDP_ACF.1
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. Embedded Keyboard LEDs are not supported by the TOE.

[O.DISABLE_UNAUTHORIZED_PERIPHERAL]: FDP_ACC.1 and FDP_ACF.1
[O.DISABLE_UNAUTHORIZED_ENDPOINTS]: FDP_ACC.1 and FDP_ACF.1
The keyboard and mouse processor is programmed in firmware only to accept basic keyboard and mouse USB devices. Wireless keyboard and mouse are not allowed by the TOE. 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. Only USB host peripheral devices are allowed by TOE keyboard and mouse host emulators. Basic USB 1.1/2.0 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. If a connected device attempts to enumerate as multiple devices at varying time intervals – the TOE will not enumerate the device. All other devices / endpoints will be rejected by the TOE.

[O.NO_USER_DATA_RETENTION]: FDP_RIP.1(2)
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.

[O.PURGE_TOE KB_DATA_WHILE_SWITCHING]: FDP_RIP.1(1)
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 and 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.

[O.SELF_TEST]: FPT_TST.1
[O.SELF_TEST_FAIL_TOE_DISABLE]: FPT_TST.1 and FPT_FLS.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.

7.2 TOE External Interfaces Security Functions

[O.NO_OTHER_EXTERNAL_INTERFACES]: FDP_IFC.1(2) and FDP_IFF.1. (2)
The TOE only supports AC/DC power, USB keyboard and mouse, KVM Video (DVI in/DVI out, DP 1.2 in/DP 1.2 out, HDMI 1.4 in/HDMI 1.4 out or VGA in/VGA out via adapter), 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.

[O.NO_DOCKING_PROTOCOLS]: FDP_IFC.1(1) and FDP_IFF.1(1)
Docking protocols are not supported by the TOE.

[O.NO_ANALOG_AUDIO_INPUT]: FDP_IFC.1(1) and FDP_IFF.1(1)
Analog microphone inputs are not supported by the TOE. 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 user peripheral device. Audio data from the connected peripheral devices to the connected computer is blocked by the audio data diodes. In addition to these uni-directional audio diodes, the LM4880 analog output amplifier enforces uni-directional data flow with internal transistors to prevent microphone access to the computer.

7.3 TOE Audio Subsystem Security Functions

Electrical isolation of the audio subsystem from all other TOE interfaces prevents data leakages to and from the audio paths.

[O.NO_ANALOG_AUDIO_INPUT]: FDP_IFC.1(1) and FDP_IFF.1(1)
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.

[O.UNIDIRECTIONAL_AUDIO_OUT]: FDP_IFC.1(1) and FDP_IFF.1(1)
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. Audio data from the connected peripheral devices to the connected computer is blocked by the audio data diodes.

[O.COMPUTER_TO_AUDIO_ISOLATION]: FDP_IFC.1(1) and FDP_IFF.1(1)
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.PERIPHERAL_PORTS_ISOLATION]: FDP_IFC.1(1) and FDP_IFF.1(1)
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.

[O.NO_USER_DATA_RETENTION]: FDP_RIP.1(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.

[O.SELF_TEST]: FPT_TST.1
[O.SELF_TEST_FAIL_TOE_DISABLE]: FPT_TST.1 and FPT_FLS.1
[O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE]: FPT_PHP.3 and FPT_FLS.1
When the TOE is not powered, an audio isolation relay is opened to isolate the audio input ports from all internal TOE circuitry. 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.

7.4 TOE Video Subsystem Security Functions

The TOE video data flow path is composed of three uni-directional paths:

- Read EDID path
- Write EDID path
- Uni-directional video path

The TOE is designed to read the connected monitor's EDID upon power up for a short period of time. The monitor must be connected to the video output connector located in the console space at the back of the TOE.

If the read EDID from the connected monitor is identical to the current stored EDID in the TOE then EDID write function will be skipped.

The TOE indicates current EDID read/write processes to the user by flashing the front panel's LEDs. Port one green and push button blue LEDs will both begin to flash for about 10 seconds. When the LEDs stop flashing, the EDID data has been read by the processor and has been written to all EDID emulators for each connected computer video channel. If the TOE has more than one video board (such as dual-head and quad-head models), then the TOE will continue to read/write the EDIDs of the connected monitors and indicate the progress of the process by flashing the next port selections green and push button blue LEDs respectively. Table 30 below shows a time estimate for EDID read/write for all TOE models.

	Single Head	Dual Head	Quad Head
1-Port	10		

2-Port	10	20	
4-Port	10	20	40
8-Port	10	20	

Table 30 – EDID Read/Write Time Chart

EDID READ

During EDID read, the EDID I2C isolation switch closes and EDID data is read from the EDID EEPROM of the monitor by the TOE processor. The EDID multiplexor is set its isolated option to establish electrical and physical isolation between the processor and the rest of the TOE EDID emulators, preventing possible bi-directional communication between the monitor and TOE. Note: all computers must be disconnected from the TOE before attempting to read/write EDID information.

EDID Write

The I2C isolation switch between the EDID EEPROM on the monitor and the TOE processor is opened to prevent any bi-directional communication between the connected computers and the TOE. The EDID multiplexor is then set to the first EDID emulator of the TOE. The processor then transmits the EDID data to the EDID emulator. Once the EDID data has been transmitted, the EDID multiplexor switches to the next EDID emulator. The process repeats itself until the processor has written to all EDID emulators in the TOE.

Normal Operation

All attempted threats made from a connected computer to the TOE will be stopped by the TOE architecture. Each connected computer video channel has its own emulated EDID EEPROM chip. Each independent EDID EEPROM chip isolates all video data provided by the 4 connected computers.

The following features implemented in the TOE video subsystem (depending on the TOE model and video protocols supported):

[O.USER_DATA_ISOLATION]: FDP_IFC.1(1) and FDP_IFF.1(1)

Each connected computer has its own TOE isolated channel with its own EDID emulator and video input port. Data flows from the input video source through its respective EDID emulator and out of the monitor display port.

[O.COMPUTER_INTERFACE_ISOLATION]:FDP_IFC.1(1) and FDP_IFF.1(1)

Each video input interface is isolated from one another using different EDID ICs, power planes, ground planes, and electronic components in each independent channel.

[O.PERIPHERAL_PORTS_ISOLATION]: FDP_IFC.1(1) and FDP_IFF.1(1)

The TOE supports DVI, DP 1.2 and HDMI 1.4 video input and output (depending on the TOE model).

[O.UNIDIRECTIONAL_EDID]: FDP_IFC.1(1) and FDP_IFF.1(1)

The TOE video subsystem prevents MCCS write commands through independent, read only emulated EDID EEPROMs. The TOE processor reads the EDID data from the monitor and then individually writes this EDID data to each independent emulator during power up. All changes in display after the EDID read/write process are ignored. There are switches in the internal circuitry

to prevent connected computers from writing to their respective EDID emulators. The TOE will reject invalid EDID display devices.

[O.UNIDIRECTIONAL_VIDEO]: FDP_IFC.1(1) and FDP_IFF.1(1)
The TOEs support that VGA, DVI, DP or HDMI video force native Analog video data (red, green, and blue channels) and TMDS digital video data (1 Clock signal, red, green, blue channels) to unidirectional flow from the switched computer to the connected display device.

[O.DISPLAYPORT_AUX_FILTERING]: FDP_IFC.1(1) and FDP_IFF.1(1)
The AUX channel between the PC and the monitor is completely disconnected in all TOEs that do support DP video inputs and DP video output (SDPN models). All AUX channels from each computer are connected to internal FPGA that simulates monitors. The simulated AUX is preloaded in the FPGA during manufacturing and can never be changed.

[O.SELF_TEST]: FPT_TST.1
[O.SELF_TEST_FAIL_TOE_DISABLE]: FPT_TST.1 and FPT_FLS.1
[O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED]: FDP_IFC.1(1) and FDP_IFF.1(1)
When TOE is unpowered, all video signals are isolated electrically and logically from the TOE. If the TOE anti-tampering is triggered or TOE self-testing has failed, the same video signal isolation occurs inside the TOE. The emulated EDID EEPROMs are still powered by their respective computers, but cannot communicate with the TOE due to hardware component isolation.

[O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE]: FPT_PHP.3 and FPT_FLS.1
If anti-tampering is triggered on the TOE, all video channels are permanently isolated and all EDID information is erased from the TOE.

7.5 TOE Administration and Security Management Tool

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. See table 16 above for supported features by administrator and user.

7.6 TOE User Authentication Device Subsystem Security Functions

The TOE is shipped with default Fixed Device Filtration (FDF) for the CAC port. The filter is set at default to allow only standard smart-card reader, PIV/CAC USB 1.1/2.0 token or biometric reader. All devices must be bus powered only (no external power source allowed).

CDF (Configurable Device Filtration)

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.

[O.COMPUTER_INTERFACE_ISOLATION]: FDP_IFC.1(1) and FDP_IFF.1(1)
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.

[O.USER_DATA_ISOLATION]: FDP_IFC.1(1) and FDP_IFF.1
Each CAC computer interface channel has its own isolated circuitry and power plane. All data channels are electrically and logically isolated to prevent data leakage.

[O.PERIPHERAL_PORTS_ISOLATION]: FDP_IFC.1(1) and FDP_IFF.1
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. 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.

[O.NO_USER_DATA_RETENTION]: FDP_RIP.1(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.

[O.USER_AUTHENTICATION_ADMIN]: FMT_SMF.1 b, FMT_MOF.1, FMT_SMR.1, FIA_UAU.2 and FIA_UID.2
Only an identified and authenticated 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.[4]

[O.USER_AUTHENTICATION_RESET]: FDP_IFF.1. (1) and FTA_ATH_EXT.1
The power of the CAC port for user authentication devices is being reset for duration of 1,000ms when ports are switched, 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 100µF requires 200µs to drop from 5V to 2V and 250µs to drop from 5V to under 1.8V. Since the

[4] Registration of a USB CAC/peripheral device is part of Administration and Security Management Tool outlined in section 7.5 above

power disconnect time has been set to 1,000ms, it allows the CAC device to be completely discharged and erase any internal information.

[O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED]: FDP_IFC.1(1) and FDP_IFF.1(1)
[O.SELF_TEST]: FPT_TST.1
[O.SELF_TEST_FAIL_TOE_DISABLE]: FPT_TST.1 and FPT_FLS.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 multiplexor. If the TOE fails during self testing or TOE anti-tampering is triggered, the same multiplexor will isolate all channels as during non-powered operation to prevent data leakage. All open authentication sessions will be disconnected during channel isolation.

7.7 TOE User Control and Monitoring Security Functions

All user monitoring and control of the TOE is performed through the TOE front panel LED illuminated push-buttons. These buttons are tied to the TOE system controller functionality.

[O.CONTINUOUS_INDICATION]: FTA_CIN_EXT.1
All push-buttons for selecting computer channels are internally illuminated via LEDs. The current selected channel is indicated by the illumination of the current channel push-button LED (the other channel LEDs remain off). 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.[5]

[O.AUTHORIZED_SWITCHING]: FDP_IFC.1(2) and FDP_IFF.1(2)
[O.NO_AMBIGUOUS_CONTROL]: FDP_IFC.1(2) and FDP_IFF.1(2)
All TOE models include push buttons for TOE computer channel selection. KVM TOE models configured in KM mode can also use cursor control to change selected channels. In the evaluated configuration, ambiguous control is prevented by configuring the TOE to temporarily disable one selection method when the other method is used. Additionally, when cursor control is used, the selected channel is unambiguous because the TOE will emit an audio indication when a switch has occurred.

[O.NO_CONNECTED_COMPUTER_CONTROL]: FDP_IFC.1(1) and FDP_IFF.1(1)
No user channel selection control by connected computer is allowed by the TOE. Only the TOE push-buttons or peripheral mouse can change the current state of the TOE.

[O.SELF_TEST]: FPT_TST.1
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.

[5] See section 1.6.2.6.5 above for detailed information about Restore Factory Default (reset)

7.8 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 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 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_PHP.3 and FPT_FLS.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.

[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.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.

[O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE]: FPT_PHP.3 and FPT_FLS.1
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 multiplexors to isolation and opening all data relays. All stored information on the TOE is also erased.

[O.ANTI_TAMPERING_INDICATION]: FPT_PHP.1
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

[O.ANTI_TAMPERING_BACKUP_POWER]: FPT_PHP.3

The TOE power supply controls the anti-tampering system during powered operation. When the TOE is not supplied, a backup battery located on the TOE circuit board keeps the anti-tampering system powered. The battery is rated for an operation life of 10 years.

[O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER]: FPT_PHP.3
Once the backup battery on the TOE depletes to a certain voltage level, the anti-tampering function will trigger. This permanently disables the TOE.

7.9 TOE Self-Testing and Security Audit

[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.
4. Test the data traffic isolation between ports.

[O.SELF_TEST_FAIL_TOE_DISABLE]: FPT_TST.1 and FPT_FLS.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.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.

[O.ANTI_TAMPERING]: FAU_GEN.1.1 and FAU_GEN.1.2
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:

1	ALO	Administrator Log On
2	ALF	Administrator Log Off
3	ARM	Arming A/T System
4	CAC	CAC Configuration
5	EDL	EDID Learn
6	LGD	LOG Dump
7	PWU	Power Up
8	PXX	Select Mode 01(KVM), 02(KM), 03(Custom) uploaded

9	RCA	Rejected CAC Device
10	AFD	Restore Factory Default
11	RKM	Rejected Keyboard or Mouse
12	STS	Self-Test
13	TMP	Device Tampered, Review by MFR only
14	ULO	User Log On
15	ULF	User Log Off

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). Note that the 'Custom' value for Select Mode is only available on DisplayPort models.

Appendix A – Product's Model Name Structure

X	XX	X	-	X	X	-	X
S = Secure	DV = DVI DP = DisplayPort UH = HDMI to HDMI HD = HDMI DM = DVI Preview Screen	N = NIAP		1 Ports 2 Ports 4 Ports 8 Ports	S = Single Head Video D = Dual Head Video Q = Quad Head Video 2 = 2 Consoles Matrix 4 = 4 Consoles Matrix		P = With CAC X = Matrix w/CAC (null) = No CAC

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. It also is responsible for communications with the Video board. No other source can independently power the Controller Board Main MCU other than the TOE.

Memory type:

1. Flash Firmware:
    - 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 :
    - The Main MCU has dedicated flash EEPROM to save all registration of USB devices, and a log of operations.
3. SRAM:
    - 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.

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:
    - All Emulation MCU firmware that controls its operation is saved in its own dedicated flash memory.

2. SRAM:
    - 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.

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:
    - 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.

Device: CAC USB Host Controller - SL811HS and **ARM Cortex**
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:
    - 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.

Video PCBA: DVI/DP

Device: Video Board Main MCU - ATxmega256A3U-AU and STM32 ARM
Manufacturer: Atmel, ST
Type: Microcontroller

Functions:
The Video Board Main MCU is responsible for all the operations of the video board, and communications with the Controller Board Main MCU. All devices on the video board are controlled by the Video Board Main MCU. No other source can independently power the Video Board Main MCU other than the TOE.

Memory type:

1. Flash Firmware:
    - All Video Board Main MCU firmware that controls its operation is saved in its own dedicated firmware flash block. This firmware cannot be changed by any user or programmer. Video Board Main MCU firmware is erased if anti-tampering is triggered.
2. SRAM:
    - The Video Board Main MCU uses SRAM memory to run the entire video board during TOE operation. 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.

Device: EDID Emulator
Manufacturer: Atmel - AT24C04C-SSHM-T, Atmel - AT24C08C-SSHM-T, Microchip - 24LC04B-I/SN, Microchip - 24LC08B-I/SN
Type: EEPROM

Functions:
The EDID Emulator is responsible for all EDID storage, used for emulation on the video board. All the EDID emulators are powered by their respective computers or the TOE, however all communications channels are disabled if TOE is not powered.

Upon triggering of the tamper detection functionality, all EDID emulation is disabled. This will prevent a connected computer from seeing the TOE as a display adapter so no video signal is output to the TOE.

Memory - Atmel - AT24C04C-SSHM-T or Microchip - 24LC04B-I/SN:

- SERIAL 4Kb 400KHz EEPROM

- The EDID EEPROM is 4K bit electrically erasable
- Programmable memory (EEPROM), organized as 512 x 8 bits.

Memory - Atmel - AT24C08C-SSHM-T or Microchip - 24LC08B-I/SN:

- SERIAL 8Kb 400KHz EEPROM
- The EDID EEPROM is 8K bit electrically erasable
- Programmable memory (EEPROM), organized as 1024 x 8 bits.

Front Panel PCBA

The front panel board has no ROM or RAM functionality.