High Security Labs Secure KVM and Matrix Security Target

Release Date:	July 12, 2019
Document ID:	HDC11543
Revision:	4.5
Prepared By:	Aviv Soffer, High Security Labs ltd

Contents

Table of Figures

List of Tables

Document Revisions

Rev.	Date	Author	Changes
3.01	Feb 17, 2015	Aviv Soffer, High Sec Labs	Submitted for initial review to CSC
3.02	March 4, 2015	Aviv Soffer, High Sec Labs	Fixed some models, added graphics, responded to CSC Observation Report dated March 3, 2015
3.03	April 7, 2015	Aviv Soffer, High Sec Labs	Revised document per committee review Excel sheet
3.04	April 28, 2015	Aviv Soffer, High Sec Labs	Revised logical boundary section. This version is used as a baseline for all 3 STs submitted together.
3.05	June 3, 2015	Aviv Soffer, High Sec Labs	Removed reference to EAL. Removed. "at least equal to or stronger than what defined in the PP" Removed.
3.06	July 6, 2015	Ronit Pasternak, High Sec Labs	Updated Revision info
3.07	Aug 11, 2015	Aviv Soffer, High Sec Labs	Revision after updating per ECR-Package-DPF_TC_CJT-1500807
3.08	Aug 14, 2015	Aviv Soffer, High Sec Labs	ST restructuring – chapters 1, 4 and 7
3.09	Aug 17, 2015	Aviv Soffer, High Sec Labs	Response to evaluator comments received today
3.10	Aug 18, 2015	Aviv Soffer, High Sec Labs	Response to evaluator comments received today
3.11	Aug 19, 2015	Aviv Soffer, High Sec Labs	Response to evaluator comments received today
3.12	Aug 21, 2015	Aviv Soffer, High Sec Labs	Accepted changes and fix format, bad references and typos
3.13	Sep 5, 2015	Aviv Soffer, High Sec Labs	Split into x6 STs
3.14	Jan 28, 2016	Aviv Soffer, High Sec Labs	Revised based on the validation team comments dated Sept 14, Sept 28, Oct 2, Oct 5, Oct 17, Nov 1st and Jan 28, 2016.
3.15	March 20, 2019	Aviv Soffer, High Sec Labs	Resubmission to CCTL.
4.1	April 1, 2019	Aviv Soffer, High Sec Labs	Submitted to NIAP validation team
4.2	May 3, 2019	Aviv Soffer, High Sec Labs	Corrected based on comments from validation team
4.3	May 9, 2019	Aviv Soffer, High Sec Labs	Corrected for latest TDs
4.4	May 23, 2019	Aviv Soffer, High Sec Labs	Corrected for latest TDs and evaluator comments.
4.5	July 12, 2019	Aviv Soffer, High Sec Labs	Address Evaluator Comments

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 principally defines:

- A security problem expressed as a set of assumptions about the security aspects of the environment; a list of threats which the product is intended to counter; and any known rules with which the product must comply (in Chapter 3, Security Problem Definition).
- A set of security objectives and a set of security requirements to address that problem (in Chapters 4 and 5, Security Objectives and IT Security Requirements, respectively).
- The IT security functions provided by the Target of Evaluation (TOE) that meet the set of requirements (in Chapter 6, TOE Summary Specification).

The structure and content of this ST complies with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 6.

1.1 ST and TOE Identification

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

ST Title	High Security Labs Secure KVM and Matrix Security Target
ST Evaluation by	DXC.technology, Security Testing & Certification Lab
Revision Number	4.5
ST Publish Date	July 12, 2019
ST Authors	Aviv Soffer, High Security Labs ltd
TOE Identification	See tables 2 below
Keywords	KVM, Secure, , Isolator, HSL, High Sec Labs, Protection Profile 3.0, Mini-Matrix

Table 1 – ST identification

1.2 PP Identification

Validated Protection Profile – NIAP Peripheral Sharing Switch for Human Interface Devices Protection Profile, Version 3.0, February 13, 2015.

1.3 TOE Overview

1.3.1 High Level TOE Architecture

The High Sec Labs Secure Peripheral Sharing Switches (PSS) allows the secure sharing of a single set of peripheral components such as keyboard, Video Display and Mouse/Pointing devices among multiple computers through standard USB, DVI, HDMI, and DisplayPort interfaces.

The High Sec Labs third-generation Secure PSS product uses multiple isolated microcontrollers (one microcontroller per connected computer) to emulate the connected peripherals in order to prevent various methods of attacks such as: display signaling, keyboard signaling, power signaling etc. Figure 1 below show a simplified block diagram of the TOE keyboard and mouse data path. Full-time Host Emulator (HE) communicates with the user keyboard through bi-directional protocols such as USB. Host Emulator converts the user key-strokes into unidirectional serial data. That unidirectional serial data is passed through the data switch that selects between computer A and computer B based on the user channel selection. Isolated Device Emulators (DE) are connected to the data switch on one side and to their respective computers on the other side. Each key-stroke is converted by the selected DE into a bi-directional stream such as USB to communicate with the computer.

The products are also equipped with multiple unidirectional flow forcing devices to assure adherence to the organizational confidentiality policy through strict isolation of connected computers.

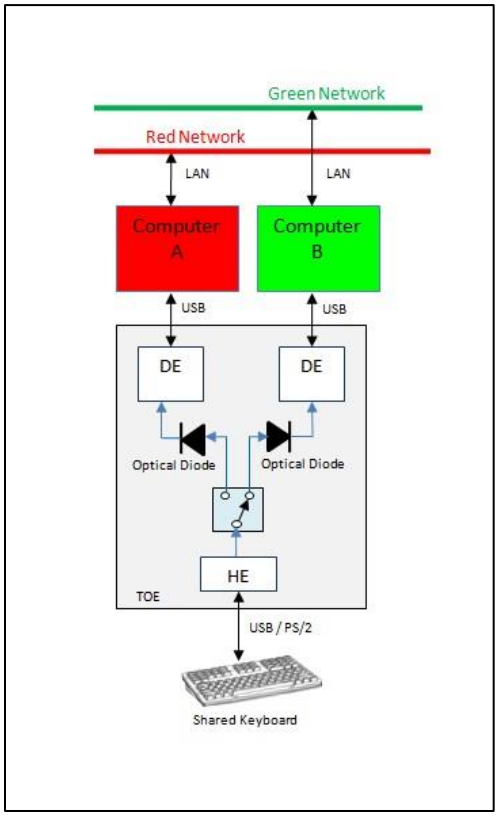

Figure 1 – Simplified block-diagram of 2-Port KVM TOE

The High Sec Labs Secure PSS product lines are available in 2, 4, 8 or 16 port models with single or dual-head (displays). Products include traditional KVM switching devices, as well as KVM matrix products.

The High Sec Labs Secure PSS works with standard Personal Computers, portable computers, servers or thin-clients. Connected computers usually running operating systems such as Windows or Linux and have ports for USB keyboard, USB mouse, DVI-I video, DVI-D video, HDMI video, DisplayPort video, audio (input and output), and USB Common Access Card (CAC) or Smart-Card reader.

The TOE is intended to be used in a range of security settings (i.e. computers coupled to a single TOE can vary from non-classified Internet connected to those protected in accordance with national security policy). Any data leakage across the TOE may cause severe damage to the organization and therefore must be prevented.

Unlike older Secure PSS security schemes that mostly protected user information transitioning through the TOE, the modern approach addresses the broader risk of the TOE compromising the air-gap between the computers connected to it (and possibly compromising their connected networks) either through the TOE itself or through a peripheral connected to it.

A summary of the High Sec Labs Secure PSS security features can be found in Table 7 below. A detailed description of the TOE security features and how it is mapped to the claimed PP SFRs, can be found in Section 7, TOE Summary Specification.

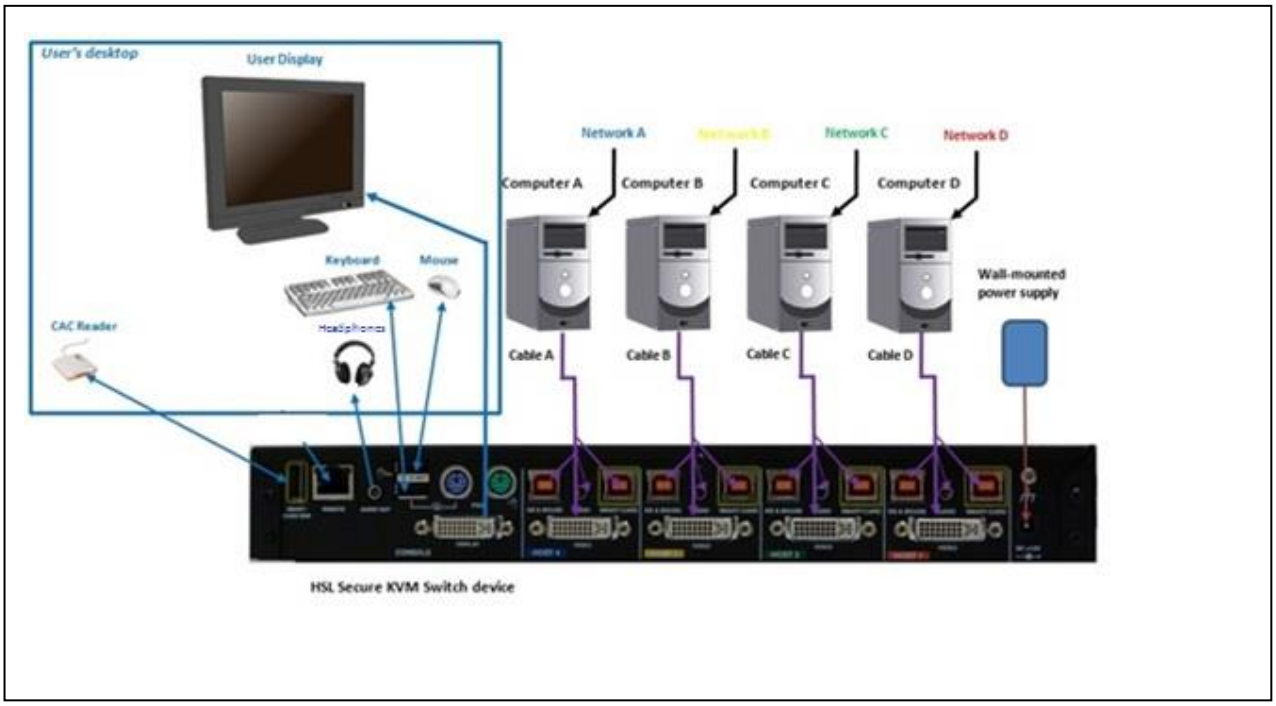

Figure 2 – Typical example of KVM TOE installation

1.3.2 KVMs TOE Details

1.3.2.1 *Evaluated KVM Products*

Model	P/N	Description	Eval. Version
2-Port			
SK21D-3	CGA10107	HSL Secure SH KVM Switch 2-Port DVI-I video, PP 3.0	33303-C4C4
SK21P-3	CGA10108	HSL Secure SH KVM Switch 2-Port DisplayPort video, PP 3.0	33303-C4C4
SK21H-3	CGA10109	HSL Secure SH KVM Switch 2-Port 4K HDMI video, PP 3.0	33303-C4C4
SX22D-3	CGA10110	HSL Secure SH Mini-Matrix KVM 2-Port x 2 DVI-I video, PP 3.0	33303-C4C4
SX22H-3	CGA10111	HSL Secure SH Mini-Matrix KVM 2-Port x 2 HDMI video, PP 3.0	33303-C4C4
DK22H-3	CGA10113	HSL Secure DH KVM Switch 2-Port 4K HDMI video, PP 3.0	33303-C4C4
DK22P-3	CGA10114	HSL Secure DH KVM Switch 2-Port DisplayPort video, PP 3.0	33303-C4C4
DK22D-3	CGA10115	HSL Secure DH KVM Switch 2-Port DVI-I, PP 3.0	33303-C4C4
DK22PD-3	CGA10116	HSL Secure DH KVM Switch 2-Port DVI-I and DisplayPort, PP 3.0	33303-C4C4
4-Port			
SK41D-3	CGA10129	HSL Secure SH KVM Switch 4-Port DVI-I video, PP 3.0	33303-C4C4
SK41DU-3	CGA10130	HSL Secure SH KVM Switch 4-Port DVI-I video, w/fUSB (2), PP 3.0	33333-C4C4
SK41P-3	CGA10131	HSL Secure SH KVM Switch 4-Port DisplayPort video, PP 3.0	33303-C4C4
SK41PU-3	CGA10132	HSL Secure SH KVM Switch 4-Port DisplayPort video, w/fUSB, PP 3.0	33333-C4C4
SK41H-3	CGA10133	HSL Secure SH KVM Switch 4-Port 4K HDMI video, PP 3.0	33303-C4C4
SK41HU-3	CGA10134	HSL Secure SH KVM Switch 4-Port 4K HDMI video, w/fUSB, PP 3.0	33333-C4C4
DK42D-3	CGA10135	HSL Secure DH KVM Switch 4-Port DVI-I video, PP 3.0	33303-C4C4
DK42DU-3	CGA10136	HSL Secure DH KVM Switch 4-Port DVI-I video, w/fUSB, PP 3.0	33333-C4C4
DK42P-3	CGA10137	HSL Secure DH KVM Switch 4-Port DisplayPort video, PP 3.0	33303-C4C4
DK42PU-3	CGA10138	HSL Secure DH KVM Switch 4-Port DisplayPort video, w/fUSB, PP 3.0	33333-C4C4
DK42H-3	CGA10139	HSL Secure DH KVM Switch 4-Port HDMI video, PP 3.0	33303-C4C4
DK42HU-3	CGA10140	HSL Secure DH KVM Switch 4-Port HDMI video, w/fUSB, PP 3.0	33333-C4C4
SX42DU-3	CGA10143	HSL Secure SH Mini-Matrix KVM 4-Port DVI video, w/fUSB, PP 3.0	33333-C4C4
SX42PU-3	CGA10144	HSL Secure SH Mini-Matrix KVM 4-Port DisplayPort video, w/fUSB, PP 3.0	33333-C4C4
SX42HU-3	CGA10145	HSL Secure SH Mini-Matrix KVM 4-Port HDMI video, w/fUSB, PP 3.0	33333-C4C4
8/16-Port			
SK81DU-3	CGA10149	HSL Secure SH KVM Switch 8-port DVI video w/fUSB, PP 3.0	33333-C4C4
DK82DU-3	CGA10150	HSL Secure DH KVM Switch 8-port DVI video w/fUSB, PP 3.0	33333-C4C4
SK161DU-3	CGA10151	HSL Secure SH KVM Switch 16-port DVI video w/fUSB, PP 3.0	33333-C4C4

Table 2 – Secure KVM and Matrix TOE identification

Notes:

(1) fUSB = Filtered USB port (having Configurable Device Filtration - CDF).

(2) SH = Single Head, DH = Dual Head.

(3) Mini-matrix and Dual-head TOE are considered KVM.

(4) All products listed above are having USB 1.0 / 2.0 interfaces for peripheral devices. The USB interfaces support Low speed, Fast and high-speed USB protocols.

(5) See Appendix A for details about HSL model numbering.

1.3.2.2 *Common Criteria Product type*

The KVM TOE is a device classified as a "Peripheral Sharing Switch" for Common Criteria. The TOE includes both hardware and firmware components.

HSL KVM TOE is satisfying the referenced PP Annex B Use Case 1.

1.3.2.3 *Peripheral Device Supported by the KVM TOE*

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

Console Port	Authorized Devices
Keyboard	1. Any wired keyboard and keypad without internal USB hub or composite device functions; 2. KVM extender; 3. USB to PS/2 adapter; and 4. Barcode reader.
Mouse / Pointing device	1. Any wired mouse, or trackball without internal USB hub or composite device functions. 2. Touch-screen; 3. Multi-touch or digitizer; 4. KVM extender.
Audio out	1. Analog amplified speakers; 2. Analog headphones; 3. Digital audio appliance.
Display	1. Display; 2. Projector; 3. Video or KVM extender.
User authentication device	1. Smartcard, CAC reader; 2. Token; 3. Biometric reader; 4. Any other qualified device if PSS supports configurable user authentication device filtering. 5. PSS internal function listed above.

Table 3 – Peripheral Devices supported by the KVM TOE

1.3.2.4 *Protocols supported by the KVM TOE*

The following table maps the TOE covered by this ST to the protocols supported.

First table (table 4) identifies the TOE console interface protocols supported. The second table below (table 5) identifies the TOE computer (host) interface protocols supported.

Model	Console Keyboard	Console Mouse	Console Audio	Console Display			Console DPP
	USB 1.1/2.0	USB 1.1/2.0	Analog stereo output	DVI-I	DP	HDMI	USB 1.1/2.0
2-Port							
SK21D-3	●	●	●	●			
SK21P-3	●	●	●		●		
SK21H-3	●	●	●			●	
SX22D-3	●	●	●	●			
SX22H-3	●	●	●			●	
DK22H-3	●	●	●			●	
DK22P-3	●	●	●	●			
DK22D-3	●	●	●	●	●		
DK22PD-3	●	●	●		●	●	
4-Port							
SK41D-3	●	●	●	●			
SK41DU-3	●	●	●	●			●
SK41P-3	●	●	●		●		
SK41PU-3	●	●	●		●		●
SK41H-3	●	●	●			●	
SK41HU-3	●	●	●			●	●
DK42D-3	●	●	●	●			
DK42DU-3	●	●	●	●			●
DK42P-3	●	●	●		●		
DK42PU-3	●	●	●		●		●
DK42H-3	●	●	●			●	
DK42HU-3	●	●	●			●	●
SX42DU-3	●	●	●	●			●
SX42PU-3	●	●	●		●		●
SX42HU-3	●	●	●			●	●
8/16-Port							
SK81DU-3	●	●	●	●			●
DK82DU-3	●	●	●	●			●
SK161DU-3	●	●	●	●			●

Table 4 – Protocols supported by the KVM TOE Console Ports

Model	Host Keyboard and Host Mouse	Host Audio	Host Display			Host DPP
	USB 1.1/2.0	Analog stereo input	DVI-I	DP	HDMI	USB 1.1/2.0
2-Port						
SK21D-3	●	●	●			
SK21P-3	●	●			●	
SK21H-3	●	●			●	
SX22D-3	●	●	●			
SX22H-3	●	●			●	

DK22H-3	●	●			●	
DK22P-3	●	●	●			
DK22D-3	●	●	●		●	
DK22PD-3	●	●			●	
4-Port						
SK41D-3	●	●	●			
SK41DU-3	●	●	●			●
SK41P-3	●	●			●	
SK41PU-3	●	●			●	●
SK41H-3	●	●			●	
SK41HU-3	●	●			●	●
DK42D-3	●	●	●			
DK42DU-3	●	●	●			●
DK42P-3	●	●			●	
DK42PU-3	●	●			●	●
DK42H-3	●	●			●	
DK42HU-3	●	●			●	●
SX42DU-3	●	●	●			●
SX42PU-3	●	●			●	●
SX42HU-3	●	●			●	●
8/16-Port						
SK81DU-3	●	●	●			●
DK82DU-3	●	●	●			●
SK161DU-3	●	●	●			●

Table 5 – Protocols supported by the KVM TOE Computer Ports

1.3.2.5 *KVM TOE and Environment Components*

The following paragraphs describe the various KVM TOE type typical operational environment and external interfaces.

It should be noted that although in most figures below four host computer channels are shown, TOE may have two, three, four or eight channels depending on product derivative. KVM TOE also my support a single display, multiple displays or multiple displays through video matrix.

Figure 3 illustrates a high-level block diagram of the TOE system 1a showing 4-channels Secure DVI, HDMI or DP KVM TOE 5a, coupled to four host computers 6a to 6d typically coupled to four isolated networks (not shown here) and coupled to the user console devices 3, 4, 66 and 40.

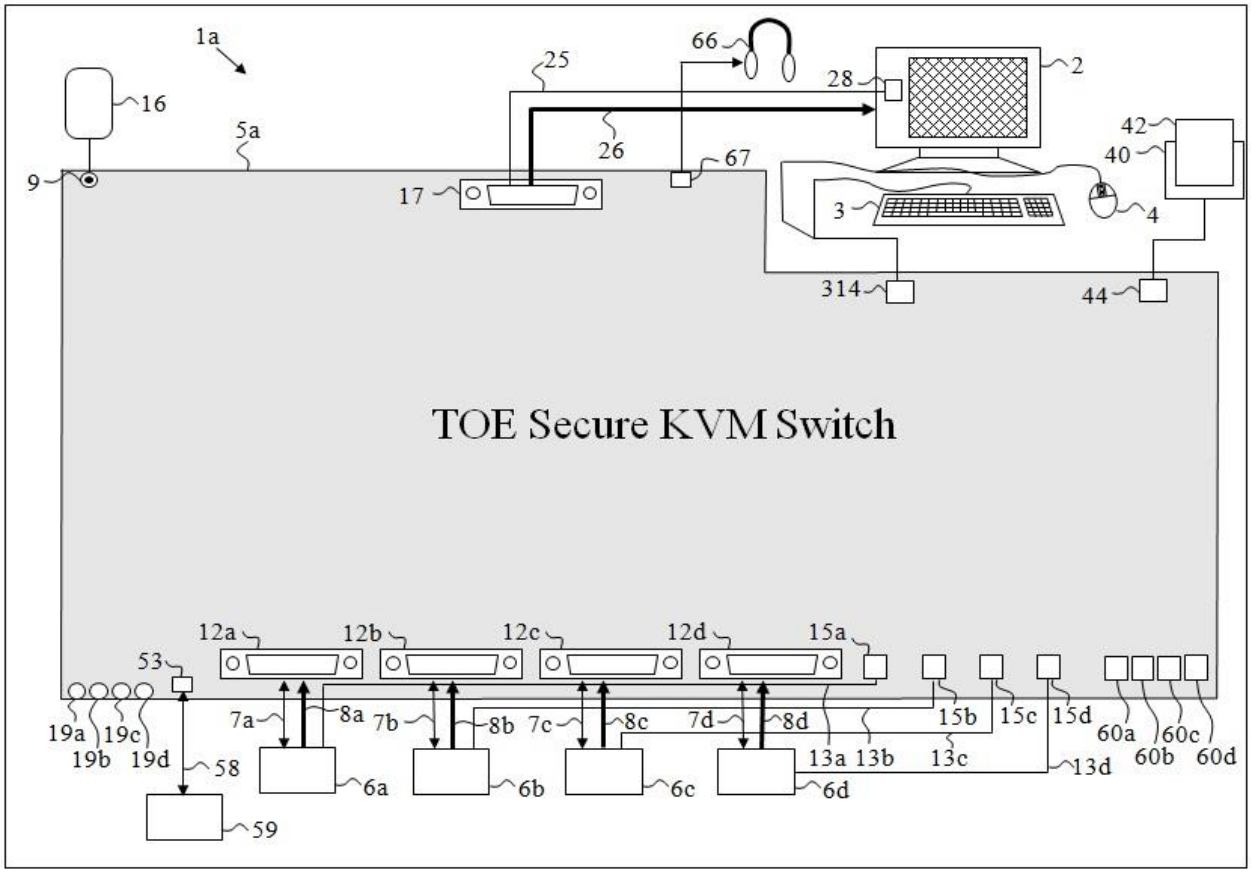

Figure 3 - Secure KVM Switch TOE external interfaces diagram

User console devices illustrated here and in the next figures are:

- User display 2 coupled to TOE peripheral interface video output 17;
- User headphones or amplified speakers 66 coupled to TOE peripheral interface audio out 67;
- User USB keyboard 3 coupled to TOE keyboard peripheral interfaces 314;
- User USB mouse 4 coupled to TOE pointing-device peripheral interfaces 314;
- User USB authentication device or other defined USB device 40 coupled to TOE dedicated peripheral port device interface 44;

This KVM TOE 5a functions as a conventional switch that allows a single user to interact with one of the four coupled computers 6a to 6d through selection made with TOE front panel pushbuttons 19a to 19d respectively. This KVM TOE supports a single user display 2 through switching function to display only one user selected channel at a time.

An optional wired Remote Desktop Controller (RDC) or Basic Remote Controller (BRC – simplified basic wired remote controller) 59 may be coupled to the TOE 5a through RDC port 53 to enable remote monitoring and control of the TOE from remote locations (not covered by the current evaluation).

KVM TOE Computer interface cables (some sown in figure 3 above) are special cables supplied with the TOE. Video cables 7x and 8x are coupled to the TOE computer video interface port 12x respectively. Keyboard and mouse USB cables 13x are coupled to the TOE KM computer interface ports 15x respectively. Additional USB DPP cables (not shown in the figure above) are coupled to the TOE DPP computer interface ports 60x.

Any one of the connected computers 6x may be used to access user configuration and administrator configuration mode through simple text editor. User or administrator can interact with the TOE through keyboard 3, mouse 4 and display 2. In addition, keyboard 3 may be used to enter various TOE operational settings using keyboard shortcuts. These shortcuts are defined in the appropriate user guidance documentation.

External AC/DC wall mounted power supply 16 is coupled to the TOE DC power jack 9 to provide power. It should be noted that some TOE (4-Port and higher) are having internal AC/DC power supply and therefore in these TOE AC cable is connected to AC power jack at the TOE rear panel.

The three 8/16 port KVM TOE models (SK81DU-3, DK82DU-3 and SK 161DU-3) are sharing the same internal modules – these TOEs are having respectively:

- A single instance of 8-Port DVI video board;
- Two instances of 8-port DVI video boards connected in parallel; and
- Two instances of 8-Port DVI video boards connected in series.

Dual-head or Mini-Matrix KVM TOE

Figure 4 illustrates a high-level block diagram of the KVM TOE system 1d showing four-channels Dual-Head or Mini-Matrix Secure KVM Switch TOE 5d, coupled to four host computers 6a to 6d that are typically coupled to four isolated networks (not shown here) and coupled to the user console devices 2p, 2s, 3, 4, 66 and 40.

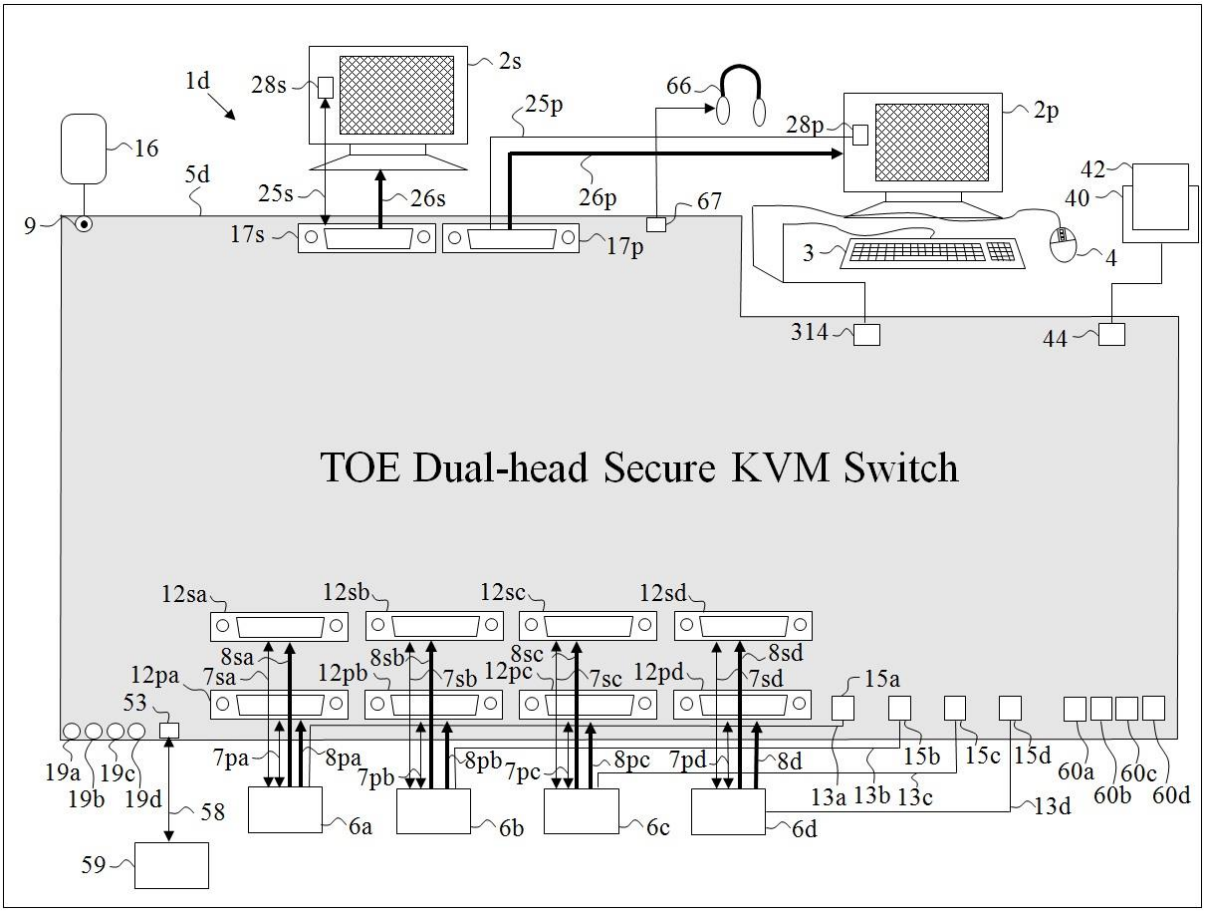

Figure 4 – Dual-Head or Mini-Matrix Secure KVM Switch TOE external interfaces diagram

This TOE functions as a keyboard and mouse switch that allows a single user to interact with one of the four coupled computers 6a to 6d through selection made with push buttons 19a to 19d respectively. In this TOE each coupled host computer 6a to 6d is capable of driving two user displays 2p (primary display) and 2s (secondary display). TOE 5d switches the two video outputs of each host computer into the two user displays 2p and 2s synchronously with the keyboard 3, mouse 4, User authentication device reader 40 and headset 66.

1.3.2.6 *Logical Scope of the KVM TOE*

1.3.2.6.1 Basic KVM TOE Functions Overview

Secure KVMs are used to enable a single user having a single set of peripherals to operate in an environment having multiple isolated computers. KVM switches keyboard, mouse, display, audio, and other peripheral devices to one user selected computer.

The following table provides the various KVM TOE features and services that were verified in the current evaluation.

No.	Function / Service provided by the KVM TOE
1.	Mapping user display to selected computer
2.	Mapping user keyboard and mouse to selected computer
3.	Mapping user audio device to selected computer
4.	Isolating source computer from user peripherals
5.	Mapping user USB peripheral device to selected computer
6.	Freeze user USB device to one channel
7.	Freeze user audio device to selected computer
8.	Administrator access to management, configuration and log functions
9.	Cursor tracking switching functions
10.	Restore factory defaults function

Table 6 – KVM TOE features and services

1.3.2.6.2 Administrative and User configuration of the KVM TOE

The KVM TOE enable user configuration of various operational parameters. User may modify these parameters using predefined keyboard shortcuts.

The KVM TOE enable identified and authenticated administrators' configuration of various operational and security parameters. Multiple administrators are supported by this TOE. Access requires user name and password authentication. This access may be performed using one of the following two methods (as further explained in the relevant TOE administrator guidance):

1. Using connected computer and text editor application; and
2. Using special USB configuration loading cable and special configuration utility software.

1.3.2.6.3 KVM TOE Security Functions Overview

The KVM TOE is comprised of many security features. The following table maps the various security features supported by the KVM TOE. It also provides information whether that feature was tested, audited or not covered in the current evaluation.

No.	Security functions	Tested / Audited / Not Covered
Keyboard and Mouse Security features		
1.	Host and device emulation of the user keyboard and mouse preventing direct access to peripherals	Tested
2.	Galvanic isolation between computer KM interfaces	Reviewed but not tested
3.	Rejection of unqualified USB devices or endpoints hiding inside composite device or USB hub	Tested
4.	KM Isolation maintained when TOE is powered off	Tested
5.	Optical unidirectional data flow diodes in the USB data path	Reviewed but not tested
6.	TOE blocks USB traffic other than valid keyboard and mouse commands	Tested
7.	TOE is having local Caps lock, Num lock and scroll lock LEDs. Keyboard LEDs commands are blocked by TOE	Tested
8.	Keyboard always switched together with mouse	Tested
9.	TOE purges keyboard buffer while switching	Tested
10.	KM peripheral switch is designed for fail-secure operation	Reviewed but not tested
11.	KM power domains isolated to prevent power signalling	Tested
Display Security Features		
12.	TOE emulation of EDID with display reading only at power up	Tested
13.	Display circuitry and interfaces isolated from all other TOE circuitry	Reviewed but not tested
14.	TOE blocks all EDID and MCCS write transactions	Tested
15.	TOE EDID emulators are independently powered to prevent power signalling	Tested
16.	Display EDID is checked before use or display will be rejected	Not covered
17.	Display qualification status LED indicator	Tested
18.	Native video traffic enforced to unidirectional flow	Tested
Audio Security Features		
19.	Microphone connection protection through bias voltage blocking	Tested
20.	TOE support only audio output switching	Tested
21.	Fail-secure audio channel switching circuitry to prevent data leaking in case of single component failure	Reviewed but not tested

22.	Electrical isolation between audio interfaces and other computer interfaces	Tested
23.	Combination of electromechanical and solid-state relays assures adequate isolation between audio interfaces of selected and non-selected computers	Reviewed but not tested
24.	Analog audio diodes to enforce unidirectional audio data flow from selected computer to audio peripheral device	Tested
User Authentication Device Security Features (applicable for TOE that supports fUSB)		
25.	User authentication support as default FDF (Fixed Device Filtering) set to filter only user authentication devices such as smart-card readers, tokens and biometric readers	Tested
26.	CDF (Configurable Device Filtering) can be enabled and configured by authenticated administrators only	Tested
27.	User authentication device computer interface ports are electrically and logically isolated	Tested
28.	Isolation between user authentication data and all other TOE traffic	Reviewed but not tested
29.	User authentication device power is interrupted upon switching computers to cause device reset	Tested
30.	Device qualification status LED indicator	Tested
Tampering protection features		
31.	Active, always-on anti-tampering triggered by enclosure coupled sensors	Tested
32.	Failure or depleting of the anti-tampering battery would cause TOE anti-tampering triggering	Tested
33.	TOE anti-tampering triggering causes TOE isolation of all computers and peripheral device interfaces	Tested
34.	Anti-tampering triggering generating visible user indications	Tested
35.	Anti-tampering is loaded with unique secret key during production	Reviewed but not tested
36.	Anti-tampering triggering causes micro-fuse to burn to assure that TOE is permanently destroyed	Reviewed but not tested
37.	Stainless steel metal chassis to protect from mechanical intrusion	Tested
38.	Log function to provide auditable trail for all TOE security events	Tested
39.	TOE is equipped with one or more Holographic Tamper Evident Labels with unique identification code/numbers	Tested
40.	TOE microcontroller protected against firmware read, modification and rewrite	Reviewed but not tested
Self-testing security features		
41.	TOE is having self-testing function that is enforced prior to power up	Tested
42.	Failure of the self-testing will cause TOE affected part to become isolated	Tested

43.	Failure of the self-testing will generate visible user indications	Tested
44.	Self-test perform isolation and firmware integrity testing prior to TOE power up	Reviewed but not tested
Other security features		
45.	TOE channel selection push buttons are numbered and self-illuminated to provide clear user indication of currently selected channel	Tested
46.	TOE does not support docking protocols	Tested
47.	The TOE manufacturer maintains a complete list of manufactured TOE articles and their respective identification markings' unique identifiers	Reviewed but not tested
48.	TOE does not store user data on non-volatile memory	Reviewed but not tested
49.	TOE has restore factory defaults switch that delete all stored configuration (except for log and administrators credentials)	Tested
50.	TOE designed, manufactured and delivered in security controlled environment	Reviewed but not tested

Table 7 – KVM TOE Security features

Notes:

1. Tested – feature or function was tested during TOE evaluation.
2. Reviewed but not tested – feature or function described in the TSS or AGD to meet PP Assurance Activities but not otherwise covered by AA testing.
3. Not covered - feature or function was not tested or otherwise verified during TOE evaluation.
4. For more detailed information on each security function is available in Section 7 of this ST.

1.4 Physical Scope and Boundary

1.4.1 Overview

The TOE is a peripheral sharing switch that is configured as KVM or Mini-Matrix.

The physical boundary of the TOE consists of:

- One HSL Secure KVM Switch or Matrix; Typically (but not necessarily) made internally of system controller board and video board (refer to table 2 above for model and hardware version);
- The firmware embedded inside the TOE that is permanently programmed into the TOE multiple microcontrollers (refer to table 2 above for firmware version);
- The log, state and settings data stored in the TOE;
- The TOE power supply that is shipped with the product (or integrated inside some of the products having 4 ports or more);
- The TOE computer interface cables that are shipped with the product (refer to table 8 below);
- The accompanying User Guidance and Administrator Guidance can be downloaded from High Sec Labs website: http://highseclabs.com/page/?pid=23 at any time.

The evaluated TOE configuration does not include any peripherals or computer components, but do include supplied computer interface cables attached to the TOE. Figures 1 and 2 above and table 8 below depicts the TOE and its typical installation environment.

It should be noted that some TOE models support multiple instances of the same peripheral for example Dual Head KVM and Matrix TOE models that support two or more instances of user displays.

It also should be noted that some TOE models support only a partial set of peripheral devices. For example some KVM TOE models do not support user authentication devices (parts are not populated on the board).

1.4.2 Evaluated Environment

This table identifies hardware components and indicates whether or not each component is in the TOE or Environment.

TOE / Environment	Component	Description
TOE	Selectable product from table 2 above.	TOE Hardware and firmware
Environment	Standard USB	Console USB user mouse port
Environment	Standard USB	Console USB user keyboard port
Environment	Standard USB User Authentication Device. Any other predefined USB device based on the Configurable Device Filtration (CDF) settings.	Console user authentication device interface
Environment	Standard computer display (VGA, DVI, HDMI, DisplayPort depending on TOE product)	Console user display interface

<table>
<tr><td>TOE</td><td>HSL KVM Cables (as needed):

<table><tr><th>P/N</th><th>Description</th></tr><tr><td>CWR05117</td><td>KVM Cable short (1.8 m), USB Type-A to USB Type-B, Black</td></tr><tr><td>CWR05116</td><td>KVM Cable short (1.8 m), Audio out, DPP, Black</td></tr><tr><td>CWR05205</td><td>KVM Cable short (1.8 m), DVI-A to VGA, USB, Black</td></tr><tr><td>CWR05114</td><td>KVM Cable short (1.8 m), DVI-D to DVI-D Single-Link, USB, Black</td></tr><tr><td>CWR05115</td><td>KVM Cable short (1.8 m), DVI-D to DVI-D Dual-Link, USB, Black</td></tr><tr><td>HWR08154</td><td>KVM Cable short (1.8m), HDMI to HDMI, USB, Black</td></tr><tr><td>CWR05113</td><td>KVM Cable short (1.8 m), DVI-D to DVI-D Single-Link, USB, Audio out, DPP, Black</td></tr><tr><td>CWR06246</td><td>KVM Cable short (1.8 m), DP to DP, USB A to USB B, Black</td></tr></table></td><td>Cables for connection of computers to TOE computers</td></tr>
<tr><td>TOE</td><td>Special Administrator Configuration Loading Cable (as needed):

<table><tr><th>P/N</th><th>Description</th></tr><tr><td>HWR06579</td><td>HSL USB Type-A to USB Type-A Configuration Loading Cable, 1.8m, Black</td></tr></table></td><td>USB-A to USB-A Configuration Loading Cable</td></tr>
<tr><td>Environment</td><td>Standard amplified stereo speakers or analog headphones</td><td>Audio output console port</td></tr>
<tr><td>Environment</td><td>Standard PC, Server, portable computer, tablet, thin-client or zero-client running any operating system; or
KVM extender connected to remote platform.</td><td>Connected computers</td></tr>
</table>

Table 8 - Evaluated TOE and Environment Components

1.5 Guidance Documents

The following guidance documents are provided with the TOE upon delivery in accordance with PP:

- Product user's manual
- Administrators guide

All documentation delivered with the product or available for download from HSL web-site is relevant to and within the scope of the TOE – for additional information see paragraph 1.4.1 above.

1.6 TOE Features Outside of Evaluation Scope

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

- TOE cable connected remote control unit that provides user monitoring and control of the TOE from remote locations – device called Remote Desktop Controllers (RDC) is not covered by this evaluation.
- USB Configuration Utility (UCU) software used with some models to configure the fUSB, Dedicated Peripheral Port (DPP) filtration parameters.
- Remote Fiber or Copper extender that may be used to extend the user console and RDC.

1.7 Document Organization

Security Target Introduction (Section 1)

Section 1 provides identification of the TOE and ST, an overview of the TOE, an overview of the content of the ST, document conventions, and relevant terminology. The introduction also provides a description of the TOE security functions as well as the physical and logical boundaries for the TOE, the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE.

Conformance Claims (Section 2)

Section 2 provides applicable Common Criteria (CC) conformance claims, Protection Profile (PP) conformance claims and Assurance Package conformance claims.

Security Problem Definition (Section 3)

Section 3 describes the threats, organizational security policies, and assumptions pertaining to the TOE and the TOE environment.

Security Objectives (Section 4)

Section 4 identifies the security objectives for the TOE and its supporting environment as well as a rationale describing how objectives are sufficient to counter the threats identified for the TOE.

Extended Components Definition (Section 5)

Section 5 presents the components needed for the ST but not present in Part II or Part III of the Common Criteria Standard.

Security Requirements (Section 6)

Section 6 presents the Security Functional Requirements (SFRs) met by the TOE, and the security functional requirements rationale. In addition, this section presents Security Assurance Requirements (SARs) met by the TOE, as well as the assurance requirements rationale.

Summary Specification (Section 7)

This section describes the security functions provided by the TOE and how they satisfy the security functional requirements. It also describes the security assurance measures for the TOE and the rationale for the assurance measures.

1.8 Document Conventions

The CC defines four operations on security functional requirements. The descriptions below define the conventions used in this ST to identify these operations. When NIAP interpretations are included in requirements, the additions from the interpretations are displayed as refinements.

Assignment: **indicated with bold text**

Selection: indicated with underlined text

Note that this ST follows the conventions used in the referenced PP regarding selection based SFRs and therefore only requirements appearing in Annex G of the PP are underlined.

Refinement: ***additions indicated with bold text and italics deletions indicated with strike-through bold text and italics***

Iteration: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MSA.1a)

Extended: indicated as per the applicable PP (e.g. FTA_CIN_EXT.1)

1.9 Document Terminology

Please refer to CC Part 1 Section 4 for definitions of commonly used CC terms.

1.9.1 ST Specific Terminology

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 touchscreen, which displays user data.
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 a single connected computer.
Keyboard	A Human Interface Device (HID) such as a keyboard, keypad or other text entry device.
KM	A PSS that switches only the keyboard and pointing 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).
Remote Desktop Controller (RDC)	Device connected to the TOE with a cable that enables remote user to control and monitor the TOE.
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.

Video Wall	Consists of multiple computer monitors, video projectors, or television sets tiled together contiguously or overlapped in order to form one large display.

Table 9 - ST Specific Terminology

1.9.2 Acronyms

Acronym	Meaning
AUX	DisplayPort Auxiliary Channel
CAC	Common Access Card
CCID	Chip Card Interface Device (USB Organization standard)
CCTL	Common Criteria Test Lab
CDC	Communication Device Class
CODEC	Coder-Decoder
dBv	A measurement of voltages ratio – decibel volt
DC	Direct Current
DP	DisplayPort
DVI	Digital Visual Interface
EDID	Extended Display Identification Data
FDF	Fixed Device Filtration
HDMI	High Definition Multimedia Interface
HEAC	HDMI Ethernet Audio Control
HID	Human Interface Device
HSL	High Sec Labs (the manufacturer of the TOE)
IP	Internet Protocol
USB Keep-Alive NAK transaction	USB 2.0 standard handshake PID (1010B) – Receiving device cannot accept data or transmitting device cannot send data.

KM	Keyboard, Mouse
KVM	Keyboard, Video and Mouse
LED	Light-Emitting Diode
LoS	Line-of-Sight
MCCS	Monitor Control Command Set
MHL	Mobile High-Definition Link
MSC	Mass Storage Class
mV	millivolt
OSD	On-Screen Display
PC	Personal Computer
PIN	Personal Identification Number
PSS	Peripheral Sharing Switch
S/PDIF	Sony/Philips Digital Interface Format
SP	Special Publication
SPF	Shared Peripheral Functions
TMDS	Transition-Minimized Differential Signaling
UART	Universal Asynchronous Receiver / Transmitter
USB	Universal Serial Bus
V	Volt
VESA	Video Electronics Standards Association
VGA	Video Graphics Array

Table 10 - Acronyms

2 Conformance Claims

This section describes the conformance claims of this Security Target.

2.1 Common Criteria Conformance Claims

The Security Target is based upon:

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.
5. All International interpretations with effective dates on or before July 1st, 2019.

This Security Target claims the following CC conformance:

- Part 2 extended
- Part 3 conformant

This ST strictly conforms to the requirements of PP – all PP requirements are met. This ST is an instantiation of the PP. The TOE covered in this ST demonstrates Exact Compliance with the 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.

With respect to assurance, this ST contains the exact assurance requirements defined in the PP. Furthermore all applicable assurance activities stated in the PP were performed.

2.2 Protection Profile (PP) Claims

This ST claims exact compliance to the following PP:

Protection Profile: Peripheral Sharing Switch Protection Profile

Version: 3.0 dated Feb 13, 2015.

2.3 Technical decisions

This ST and TOE addresses the following technical decisions:

TD0083 - AVA_VAN.1 – Applied.

TD0086 - FDP_IFF.1.5 – Applied.

TD0136 - FDP_RIP.1.1 – Applied.

TD0144 - FDP_RIP.1.1 - Applied.

TD0251 - FMT_MOF.1.1 - Applied.

TD0298 - FDP_IFF.1 Assurance Activities – Not applicable

Rationale:

TD0298 changes the testing Assurance Activities for the SFR, but not the SFR. The FDP_IFF.1 requirement is not changed in the ST and is still applicable to the TOE. However, the test steps added by the new TD are not applicable to the TOE under evaluation. These procedures apply to a TOE that supports DisplayPort video format passed through the switch. A TOE that supports DisplayPort through conversion to other video formats through an external cable or dongle should not be tested using these procedures or test steps. All TOE models under evaluation support DisplayPort input by converting DisplayPort to HDMI and therefore are not affected by the TD changes in part 2 of test 4.4. If necessary, the evaluation team is prepared to raise a TRRT to request concurrence or a formal decision based on this rationale.

2.4 Package Claims

Package Claims are not part of the referenced PP.

3 Security Problem Definition

This section describes assumptions about the operational environment in which the TOE is intended to be used and represents the conditions for the secure operation of the TOE.

Note: The content in this section is appears in the Security Problem Definition of the claimed PSS PP and is copied here for completeness.

3.1 Secure Usage Assumptions

The Security Objectives and Security Functional Requirements defined in subsequent sections of this Security Target are based on the condition that all of the assumptions described in this section are satisfied.

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 11 – Secure usage assumptions

3.2 Threats

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.

TOE 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 TOE is an intentional attack designed to leak data between two connected computers. A remote attacker may abuse one hacked computer connected to the TOE 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 TOE to the hacked computer on the other side of the TOE (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 TOE 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 TOE via various signaling methods. Signaling methods refer to the use of simple bit-by-bit effects used to transfer data across the TOE while in use or while the TOE 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 TOE. For example, if one computer connected to the TOE is attempting to power cycle its USB (Universal Serial Bus) port power and another computer connected to the TOE 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 TOE in these cases may be unrelated to the data entered or received by the specific user. Data may leak through the TOE without user awareness when the user is performing normal operational tasks or while the TOE is left powered on and unattended.

It should also be noted that the scope of threats in the referenced 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, video signal leakage through the TOE 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.

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 TOE, but not selected.

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 TOE 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" to switch computers is not allowed in the TOE (note that the use of keyboard shortcuts for other purposes such as TOE

configuration is allowed). Similarly, a scanning function commonly used in commercial switches is not supported by the TOE.

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 TOE 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 TOE).

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.

Audio threats in TOE may be resulted from the following:

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.

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.

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.

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.

3.2.1 Threats Addressed by the different TOE

"Threats to Security" Section 2 of the claimed Protection Profile identifies the following threats to the assets against which specific protection within the TOE is required:

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 12 – Threats addressed by the different TOEs

3.2.2 Threats addressed by the IT Operating Environment

The Protection Profile claimed identifies no threats to the assets against which specific protection within the TOE environment is required.

3.3 Organizational Security Policies

The Protection Profile claimed identifies no Organizational Security Policies (OSPs) to which the TOE must comply.

4 Security Objectives

This chapter describes the security objectives for the TOE and the Operational Environment. The security objectives are divided between TOE Security Objectives (for example, security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (for example, security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 Security Objectives for the TOE

This section defines the IT security objectives that are to be addressed by the TOE.

Security Objective	Definition as applied to KVM type TOE
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 DockPort, USB docking, 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 TOE 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	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	TOE CDF 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	Only one switching 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	The TOE 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	The TOE 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.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 13 - TOE Security Objectives definitions (derived from the PP)

Notes:

1. Objective O.USER_AUTHENTICATION_TERMINATION is not applicable to the Secure KVM and Matrix TOE per referenced PP as it does not support emulated user authentication device function.
2. O.DISPLAYPORT_AUX_FILTERING is not applicable for HSL KVM TOEs as none of the TOE support DisplayPort display (Native DisplayPort format video).

4.2 Security Objectives for the Operational Environment

The following IT security objectives for the environment are to be addressed by the Operational Environment by technical means.

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 14 - Operational Environment Security Objectives (from the PP)

4.3 Rationale

This section demonstrates that each threat, organizational security policy, and assumption are mitigated by at least one security objective for the TOE, and that those security objectives counter the threats, enforce the policies, and uphold the assumptions.

Threats, Policies, Assumptions: / Objectives:	T.DATA_LEAK	T.SIGNAL_LEAK	T.RESIDUAL_LEAK	T.UNINTENDED_SWITCHING	T.UNAUTHORIZED_DEVICES	T.AUTHORIZED_BUT_UNTRUSTED_DEVICES	MICROPHONE_USED	AUDIO_REVERSED	T.LOGICAL_TAMPER	T.PHYSICAL_TAMPER	T.REPLACEMENT	T.FAILED	A.NO_TEMPEST	A.NO_SPECIAL_ANALOG_CAPABILITIES	A.PHYSICAL	A.TRUSTED_ADMIN	A.TRUSTED_CONFIG
O.COMPUTER_INTERFACE_ISOLATION	•	•															
O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED	•																
O.USER_DATA_ISOLATION	•																
O.NO_USER_DATA_RETENTION			•														
O.PURGE_TOE_KB_DATA_WHILE_SWITCHING			•														
O.NO_DOCKING_PROTOCOLS	•																
O.NO_OTHER_EXTERNAL_INTERFACES	•	•															
O.NO_ANALOG_AUDIO_INPUT		•					•	•									
O.UNIDIRECTIONAL_AUDIO_OUT		•					•	•									
O.COMPUTER_TO_AUDIO_ISOLATION		•						•									
O.USER_AUTHENTICATION_ISOLATION	•																
O.USER_AUTHENTICATION_RESET	•	•				•											
O.USER_AUTHENTICATION_ADMIN					•												
O.AUTHORIZED_SWITCHING				•													
O.NO_AMBIGUOUS_CONTROL				•													

O.CONTINUOUS_INDICATION				●												
O.KEYBOARD_AND_MOUSE_TIED				●												
O.NO_CONNECTED_COMPUTER_CONTROL		●														
O.PERIPHERAL_PORTS_ISOLATION	●				●											
O.DISABLE_UNAUTHORIZED_PERIPHERAL					●											
O.DISABLE_UNAUTHORIZED_ENDPOINTS					●											
O.KEYBOARD_MOUSE_EMULATED						●										
O.KEYBOARD_MOUSE_UNIDIRECTIONAL						●										
O.UNIDIRECTIONAL_VIDEO						●										
O.UNIDIRERCTIONAL_EDID						●										
O.TAMPER_EVIDENT_LABEL										●	●					
O.ANTI_TAMPERING										●						
O.ANTI_TAMPERING_BACKUP_POWER										●						
O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER										●						
O.ANTI_TAMPERING_INDICATION										●						
O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE										●						
O.NO_TOE_ACCESS									●							
O.SELF_TEST												●				
O.SELF_TEST_FAIL_TOE_DISABLE												●				
O.SELF_TEST_FAIL_INDICATION												●				
OE. NO_TEMPEST													●			
OE. NO_SPECIAL_ANALOG_CAPABILITIES														●		
OE.PHYSICAL															●	
OE.TRUSTED_ADMIN																● ●

Table 15 - Sufficiency of Security Objectives

Notes:

1. Cells marked in ● are indicating an objective that appears in the PP and shall be met by the KVM and Matrix TOEs.
2. Rational for objectives not met is given in table 16 at the next paragraph.

4.3.1 TOE Security Objectives Rationale

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 DockPort, USB docking, Thunderbolt etc. is not allowed in the TOE. Note: MHL 3.0 and higher or USB Type C 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).	**O.NO_DOCKING_PROTOCOLS** mitigates that threat by preventing the use of complex protocols capable of supporting unsecure traffic. As peripheral protocols become more 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 DisplayPort, 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	**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

	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).	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 prevent 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	**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).

	physical (i.e., hardware) methods and not through logical (i.e., firmware dependent) methods (See Annex D, Table 1, Flow B).	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, DisplayPort 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.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 DisplayPort). If the TOE forces a 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	**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.

	authentication device for at least 1 second.	
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.	**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.

	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 TOE anti-tampering system must have a backup power source to enable tamper detection while the TOE is unpowered.	**O.ANTI_TAMPERING_BACKUP_POWER** assures that the active anti-tampering 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. 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.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.
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	**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.

	manufactured TOE articles and their respective identification markings' unique identifiers.	
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 16 – TOE Security Objectives rationale

4.3.2 Security Objectives Rationale for the 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	**OE.TRUSTED_ADMIN** upholds this assumption by ensuring that only appropriately trained and trusted administrators and users will be exercising TOE functions.

	users are available to administer, configure and use the TOE.	
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 17 – Operational Environment Security Objectives rationale

4.4 Rationale for Organizational Policy Coverage

There are no Organizational Policies for this TOE.

5 Extended Components Definition

The Extended Components Definition describes components for security objectives which cannot be translated or could only be translated with great difficulty to existing requirements.

The following extended requirements were depicted from Annex H of the PP.

Extended Security Functional Requirements	
FTA_CIN_EXT	Continuous Indications
FTA_ATH_EXT	User Authentication Device Reset and Termination

Table 18 - Extended SFR Components

5.1 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

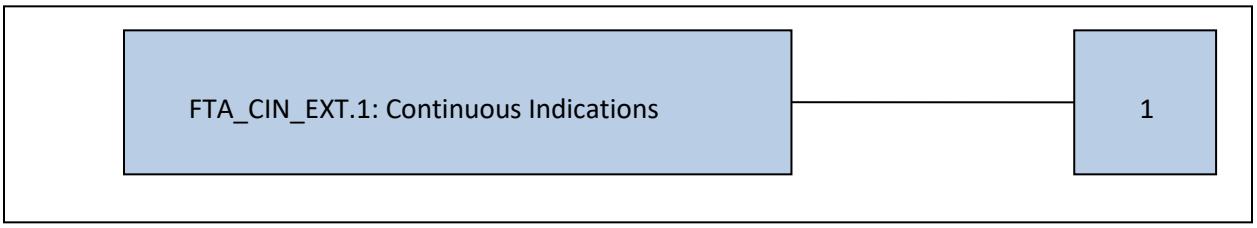

Figure 5 - FTA_CIN_EXT.1: Continuous Indications

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

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*].

5.2 Class 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. Both FTA_ATH_EXT.1 is 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

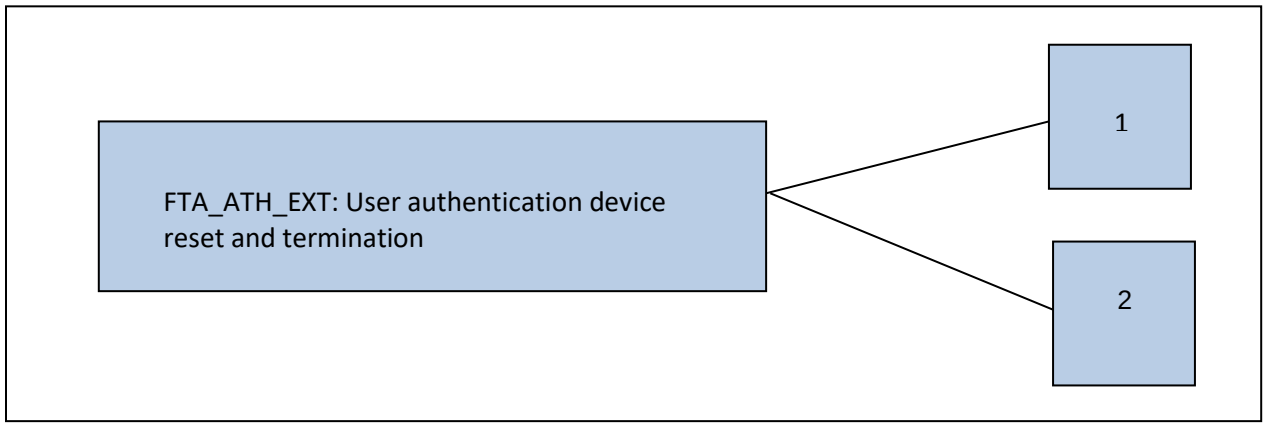

Figure 6 - FTA_ATH_EXT: User authentication device reset and termination

Management

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

Audit

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

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.

6 Security Requirements

This section defines the IT security requirements that shall be satisfied by the TOE or its environment. The CC divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.

- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

These requirements are discussed separately within the following subsections.

6.1 Security Functional Requirements for the TOE

The security requirements that are levied on the TOE are specified in this section of the ST.

6.1.1 Overview

The TOE satisfies the SFRs delineated in "Target of Evaluation Security Requirements," Section 4.2 of the claimed Protection Profile. The SFRs have been reproduced here for convenience.

Functional Component ID	Functional Component 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	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	Extended: Continuous Indications
Optional Requirements (Annex F)	
FAU_GEN.1	Audit data generation
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 19 - TOE Security Functional Requirements summary

6.1.2 Class: User Data Protection (FDP)

6.1.2.1 *User Data Information Flow Requirements*

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 will 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*].

6.1.2.2 *Information flow control functions (FDP_IFF)*

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 will 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 will permit an 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	*This ST will claim the following data-flow claims based on applicable TOE groups:* *[Selection]* *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 #1 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 will causes the TOE to change the data flow accordingly.*
3. *The specific TOE implementation will allow splitting of the user control to different shared peripheral groups. For example, the user authentication device selected computer may be #2, while the keyboard and mouse selected computer device may be #1. In this case, each selection will be clearly indicated.*
4. *The TOE supports multiple instances of the peripheral devices shown in the table above, or a subset of these peripheral devices.*]

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

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 will explicitly authorize an information flow based on the following rules: [*no additional rules*].

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

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 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.

6.1.3 Data Isolation Requirements

6.1.3.1 *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 will 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 will 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.
c. 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).

6.1.3.2 *Information flow control functions (FDP_IFF)*

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 will 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 this 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 will 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 not supported by the TOE:

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

FDP_IFF.1.2(2) The TSF will 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 will 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 will be permitted between the selected computer interface and the TOE keyboard and mouse peripheral device interfaces. 2. The TSF will permit information flow and TSF resources sharing between two TOE user peripheral interfaces of the same Shared Peripheral group*].

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 are 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 will enforce the [*No additional rules*].

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

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

[*1. The TSF will deny any information flow between TOE Computer Interfaces, except those allowed by the User Data Flow rules;*

2. The TSF will 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 will deny power flow between the selected computer interface and TOE keyboard and mouse peripheral device interfaces;

4. The TSF will deny information flow from the TOE selected computer interface to the TOE keyboard and mouse peripheral device interface;

5. The TSF will deny data flow of user authentication device data transiting the TOE to non-selected TOE computer interfaces;

6. The TSF will assure that the user authentication device computer interfaces are not shared with any other TOE peripheral function interface (keyboard, mouse etc.);

7. The TSF will 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 this 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].

6.1.3.3 *Access Control policy (FDP_ACC)*

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 will enforce the [*peripheral device SFP*] on
[Subjects: *Peripheral devices*
Objects: *Console ports*
Operations: *allow connection, disallow connection*].

6.1.3.4 *Access control functions (FDP_ACF)*

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 will 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 will enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*The TOE will 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 referenced PP*].

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

FDP_ACF.1.4 The TSF will explicitly deny access of subjects to objects based on the following additional rules:
[*The TOE peripheral device interface (console) port will reject any peripheral device that is not identified as an authorized device in table 20 below*].

TOE Console Port	Authorized Devices	Authorized Protocols
Keyboard	• Any wired keyboard and keypad without internal USB hub or composite device functions; • USB hub and composite devices are allowed as TOE can filter USB endpoints (if at least one endpoint is a keyboard or mouse HID class). In such case TOE will disable all other endpoints; • Wireless keyboards are not allowed; • KVM extender; • PS/2 to USB adapter; and • Barcode reader.	• USB
Mouse / Pointing device	• Any wired mouse or trackball without internal USB hub or composite device functions; • USB hub and composite devices are allowed as TOE can filter USB endpoints (if at least one endpoint is a keyboard or mouse HID class). In such case TOE will disable all other endpoints; • Touch-screen; • Multi-touch or digitizer; • KVM extender.	• USB

User authentication device	• Smartcard, CAC reader; • Token; • Biometric reader; • Any other qualified device if PSS supports configurable user authentication device filtering and that specific USB device is both whitelisted and not blacklisted. Note that user authentication device must be powered by the TOE. External power source is prohibited.	• USB
Audio out	• Analog amplified speakers; • Analog headphones; • Digital audio appliance. Note that the use of analog microphone or line-in audio devices is strictly prohibited.	• Analog audio output; • Digital audio (for example SPDIF); • Digital audio embedded inside the video.
Display	• Display; • Projector; • Video or KVM extender. Note that the use of wireless video transmitters with the TOE is not allowed.	• VGA; • DVI; • HDMI; • DisplayPort up to version 1.1; • DisplayPort higher than version 1.1.

Table 20 - Authorized peripheral devices (derived from referenced PP table 12)

6.1.3.5 *Residual Information Protection (FDP_RIP)*

FDP_RIP.1 Subset Residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1(1) **[Refinement]** The TSF will ensure that any previous information content of a resource is made unavailable ~~upon the~~:

- **immediately after TOE switch to another selected computer;**
- **and on start-up of the TOE for**

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

Notes:

For additional information refer to the Letter Of Volatility issued by High Sec Labs in Annex C of this document.

6.1.4 Class: Protection of the TSF (FPT)

6.1.4.1 *Passive Detection of a Physical Attack (FPT_PHP)*

FPT_PHP.1 Passive detection of a physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.1.1 The TSF provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

6.1.5 Resistance to Physical Attack

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 **[Refinement]** The TSF will 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 ~~responding automatically such that the SFRs are always enforced~~ **becoming permanently disabled.**

Application Notes:

Since once TOE was tampered, there is no practical way to test or to assure that the various complex isolation requirements listed above are met, the preferred option is to isolate all peripherals from all

computers completely. For this reason the SFR above was modified to use the stronger requirement of permanent disabling. Performing this isolation permanently assures that the TOE would not remain in service after tampering attempt.

6.1.5.1 *Failure with Preservation of Secure State (FPT_FLS)*

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF will 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*].

6.1.5.2 *TSF Testing (FPT_TST)*

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 **[Refinement]** The TSF will run a suite of self-tests that includes:

- **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 will provide users with the capability to verify the integrity of [the TSF functionality].

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

Application Notes:

The TOE will provide visible user indications in case of Self-test failure through front panel LEDs.

6.1.6 TOE Access (FTA_CIN_EXT)

FTA_CIN_EXT.1 Extended: Continuous Indications

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.1.7 F.1.2 Class: Security Audit (FAU)

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_GEN.1.1 The TSF will 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* [assignment: all administrative functions claimed in FMT_MOF.1 and FMT_SMF.1]]

FAU_GEN.1.2 The TSF will 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].

6.1.8 F.1.3 Class: Identification and authentication (FIA)

FIA_UAU.2 User identification before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.2 User identification before any action

FIA_UAU.2.1 The TSF will require each **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Notes:

The Administrator will 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 will require each **administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Notes:

The Administrator is identified through logon before access to administrative functions is provided by the TOE.

6.1.9 F.2.1 Class: Security Management (FMT)

The TOE provides the following management roles:

a. **Administrative configuration** - Functionality to configure certain aspects of TOE operation that are 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. Available to all users. No user identification or authentication is required.

6.1.9.1 *Management of Functions in TSF (FMT_MOF)*

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles; and
FMT_SMF.1 Specification of Management Functions.

FMT_MOF.1.1 The TSF will restrict the ability to [*perform*] the functions [*modify TOE user authentication device filtering (CDF) whitelist and blacklist*, *none*] to [*the authorized administrators*].

Application Note: If there are additional management functions performed by the TOE (including those specified in Section 4.2.4, FMT_SMF), they should be added in the assignment.

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 will provide authorized administrators the option to assign whitelist and blacklist definitions for the TOE user authentication device qualification function,
b. [*and the ability to define specific data flow rules for specific computer interfaces*].

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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

6.1.10 G.1 - Class FTA_ATH_EXT: User Authentication Device Reset and Termination

6.1.10.1 *G.1.1 User authentication device reset*

FTA_ATH_EXT.1 **User authentication device reset**

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_ATH_EXT.1.1 The TSF will 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.

6.2 Rationale For TOE Security Requirements

The section below demonstrates the tracing of Security Functional Requirements to Security Objectives and describes the applicable rationale based on direct reference from the claimed Protection Profile.

6.2.1 TOE Security Functional Requirements Tracing & Rationale

Objective	SFRs	TOE shall comply with SFRs / Not applicable
[O.COMPUTER_INTERFACE_ISOLATION]	FDP_IFC.1(1) FDP_IFF.1(1)	TOE shall comply with SFRs.
[O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED]	FDP_IFC.1(1) FDP_IFF.1(1)	TOE shall comply with SFRs.
[O.USER_DATA_ISOLATION]	FDP_IFC.1(1) FDP_IFF.1(1)	TOE shall comply with SFRs.
[O.NO_USER_DATA_RETENTION]	FDP_RIP.1	TOE shall comply with SFRs.
[O.PURGE_TOE KB_DATA_WHILE_SWITCHING]	FDP_RIP.1	TOE shall comply with SFRs.
[O.NO_DOCKING_PROTOCOLS]	FDP_IFC.1(1) FDP_IFF.1(1)	TOE shall comply with SFRs.
[O.NO_OTHER_EXTERNAL_INTERFACES]	FDP_IFC.1(2) FDP_IFF.1. (2)	TOE shall comply with SFRs.
[O.NO_ANALOG_AUDIO_INPUT]	FDP_IFC.1(1) FDP_IFF.1(1)	TOE shall comply with SFRs.
[O.UNIDIRECTIONAL_AUDIO_OUT]	FDP_IFC.1(1) FDP_IFF.1(1)	TOE shall comply with SFRs.
[O.COMPUTER_TO_AUDIO_ISOLATION]	FDP_IFC.1(1) FDP_IFF.1(1)	TOE shall comply with SFRs.
[O.USER_AUTHENTICATION_ISOLATION]	FDP_IFC.1(1) FDP_IFF.1(1)	TOE shall comply with SFRs.
[O.USER_AUTHENTICATION_RESET]	FDP_IFF.1. (1) FTA_ATH_EXT.1	TOE shall comply with SFRs.
[O.USER_AUTHENTICATION_ADMIN]	FMT_SMF.1 b FMT_MOF.1 FMT_SMR.1	TOE shall comply with SFRs.
[O.AUTHORIZED_SWITCHING]	FDP_IFC.1(2) FDP_IFF.1(2)	TOE shall comply with SFRs.
[O.NO_AMBIGUOUS_CONTROL]	FDP_IFC.1(2) FDP_IFF.1(2)	TOE shall comply with SFRs.
[O.CONTINUOUS_INDICATION]	FTA_CIN_EXT.1	TOE shall comply with SFRs.
[O.KEYBOARD_AND_MOUSE_TIED]	FDP_ACC.1 FDP_ACF.1	TOE shall comply with SFRs.

[O.NO_CONNECTED_COMPUTER_CONTROL]	FDP_IFC.1(1) FDP_IFF.1(1)	TOE shall comply with SFRs.
[O.PERIPHERAL_PORTS_ISOLATION]	FDP_IFC.1(1) FDP_IFF.1(1)	TOE shall comply with SFRs.
[O.DISABLE_UNAUTHORIZED_PERIPHERAL]	FDP_ACC.1 FDP_ACF.1	TOE shall comply with SFRs.
[O.DISABLE_UNAUTHORIZED_ENDPOINTS]	FDP_ACC.1 FDP_ACF.1	TOE shall comply with SFRs.
[O.KEYBOARD_MOUSE_EMULATED]	FDP_ACC.1 FDP_ACF.1	TOE shall comply with SFRs.
[O.KEYBOARD_MOUSE_UNIDIRECTIONAL]	FDP_ACC.1 FDP_ACF.1	TOE shall comply with SFRs.
[O.UNIDIRECTIONAL_VIDEO]	FDP_IFC.1(1) FDP_IFF.1(1)	TOE shall comply with SFRs.
[O.UNIDIRERCTIONAL_EDID]	FDP_IFC.1(1) FDP_IFF.1(1)	TOE shall comply with SFRs.
[O.NO_TOE_ACCESS]	FPT_PHP.3 FPT_FLS.1	TOE shall comply with SFRs.
[O.TAMPER_EVIDENT_LABEL]	FPT_PHP.1	TOE shall comply with SFRs.
[O.ANTI_TAMPERING]	FPT_PHP.3	TOE shall comply with SFRs.
[O.ANTI_TAMPERING_BACKUP_POWER]	FPT_PHP.3	TOE shall comply with SFRs.
[O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER]	FPT_PHP.3	TOE shall comply with SFRs.
[O.ANTI_TAMPERING_INDICATION]	FPT_PHP.1	TOE shall comply with SFRs.
[O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE]	FPT_PHP.3 FPT_FLS.1	TOE shall comply with SFRs.
[O.SELF_TEST]	FPT_TST.1	TOE shall comply with SFRs.
[O.SELF_TEST_FAIL_TOE_DISABLE]	FPT_TST.1 FPT_FLS.1	TOE shall comply with SFRs.
[O.SELF_TEST_FAIL_INDICATION]	FPT_TST.1	TOE shall comply with SFRs.

Table 21 - SFR and Security Objectives Mapping with TOE compliance requirements

Objective	SFR	Rationale
[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.	FDP_IFC.1(1) FDP_IFF.1(1)	FDP_IFC.1(1) and FDP_IFF.1(1) satisfies the "Computer interface isolation" objective by enforcing the user data protection SFP. This policy defines the allowed and disallowed data flows between peripheral and computer interfaces. It is specifically disallowing any data flow between different computer interfaces.
[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.	FDP_IFC.1(1) FDP_IFF.1(1)	FDP_IFC.1(1) and FDP_IFF.1(1) satisfies the "Computer interface isolation TOE unpowered" objective by further enforcing the user data protection SFP even when the TOE is unpowered. This policy defines the allowed and disallowed data flows between peripheral and computer interfaces. It is specifically disallowing any data flow between different computer interfaces when TOE is unpowered. Also see in FDP_IFF.1.5(2), Denied data flow rule #14 that defines the data isolation requirements 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.	FDP_IFC.1(1) FDP_IFF.1(1)	FDP_IFC.1(1) and FDP_IFF.1(1) satisfies the "Computer interface isolation" objective by enforcing the user data protection SFP. This policy defines the allowed and disallowed data flows between peripheral and computer interfaces. It is specifically allowing data flow from peripheral device to the selected computer. It is specifically disallowing data flow from peripheral device to non-selected computer and therefore it satisfying the user data isolation objective.
[O.NO_USER_DATA_RETENTION] The TOE shall not retain user data after it is powered down.	FDP_RIP.1	FDP_RIP.1 satisfies the "No user data retention" objective by preventing TOE from storing user data on non-volatile memory.
[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.	FDP_RIP.1	FDP_RIP.1 satisfies the "Purge TOE keyboard data while switching "objective by enforcing the requirement that during TOE power up and new computer selection, user data in the TOE will be deleted.
[O.NO_DOCKING_PROTOCOLS]	FDP_IFC.1(1) FDP_IFF.1(1)	FDP_IFC.1(1) and FDP_IFF.1(1) satisfies the "No docking protocols" objective by defining the allowed and disallowed TOE interface protocols.

The use of docking protocols such as DockPort, USB docking, Thunderbolt etc. is not allowed in the TOE.		Docking protocols are specifically disallowed by these SFRs application note.
[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).	FDP_IFC.1(2) FDP_IFF.1. (2)	FDP_IFC.1(2) and FDP_IFF.1. (2) Satisfies the "No other external interfaces" objectives by enforcing the "Data isolation SFP" on the TOE external interfaces. More specifically the TSF shall deny any data flow between an external entity and the TOE computer interfaces. In addition it requires that the TSF shall deny any user data flow between the TOE and an external entity. The exclusion of other external interfaces prevents these unauthorized data flows.
[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.	FDP_IFC.1(1) FDP_IFF.1(1)	The FDP_IFC.1(1) and FDP_IFF.1(1) satisfies the "No analog audio input" objective by requiring the TOE would specifically not support analog audio input (microphone in or line in). The SFR defined positive (allowed) interfaces. The specific requirement appears in the application note paragraph a. Also see in FDP_IFF.1.5(2), Denied data flow rule #13 that refers to Annex C of the PP.
[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 sine 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.	FDP_IFC.1(1) FDP_IFF.1(1)	The FDP_IFC.1(1) and FDP_IFF.1(1) satisfies the "Unidirectional audio out" objective by defining in FDP_IFF.1.5(2),Denied data flow rule #9 that the audio shall be enforced to unidirectional flow from the computer interface to the peripheral device interface only. The objective testing methodology and isolation targets are defined in the appropriate assurance activities for that SFR.
[O.COMPUTER_TO_AUDIO_ISOLATION] The audio data flow 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 sine wave at the extended audio frequency range including negative swing signal.	FDP_IFC.1(1) FDP_IFF.1(1)	The FDP_IFC.1(1) and FDP_IFF.1(1) satisfies the "Computer to audio isolation" objective by defining in FDP_IFF.1.5(2), Denied data flow rule #1 that The TSF shall deny any information flow between TOE Computer Interfaces, except those allowed by the User Data Flow rules. Audio to other functions data flow is specifically not authorized by the same SFR. The objective testing methodology and isolation targets are defined in the appropriate assurance activities for that SFR.
[O.USER_AUTHENTICATION_ISOLATION]	FDP_IFC.1(1)	

The user authentication function shall be isolated from all other TOE functions.	FDP_IFF.1(1)	The FDP_IFC.1(1) and FDP_IFF.1(1) satisfies the "User authentication isolation" objective by defining in FDP_IFF.1.5(2), Denied data flow rule #6 defining that the TSF shall assure that the user authentication device computer interfaces are not shared with any other TOE peripheral function interface (keyboard, mouse etc.).
[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.	FDP_IFF.1(1)	FDP_IFF.1(1) satisfying the User authentication reset" objective by setting the requirement in FDP_IFF.1.3(1) that the TSF shall enforce the rule:" If the TOE user authentication device function is not emulated - 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"
	FTA_ATH_EXT.1	The extended requirement FTA_ATH_EXT.1 satisfies the "User authentication reset" objective by setting the requirement that 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.

[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.	FMT_SMF.1 b	FMT_SMF.1 satisfies the "User authentication admin" objective by setting the requirement that the TOE shall be capable of performing the following management functions: a. If the TOE supports configurable user authentication device filtering (CDF) – then it shall provide authorized administrators the option to assign whitelist and blacklist definitions for the TOE user authentication device qualification function, b. TOE may provide any additional TOE management functions.
	FMT_MOF.1	FMT_MOF.1 defines the rule that the TSF shall restrict the ability to perform the functions modify TOE user authentication device filtering (CDF) whitelist and blacklist to the authorized administrators and therefore limiting the access to this function to authenticated administrators only.
	FMT_SMR.1	FMT_SMR.1 defines the rule that the TSF shall maintain the roles users, and administrators. This role must be defined in order to enable it to perform administrative functions.
[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.	FDP_IFC.1(2) FDP_IFF.1(2)	The assurance activities for FDP_IFC.1(2) and FDP_IFF.1(2) requires that the evaluator will examine the TOE to verify that it supports only authorized switching methods. In particular the evaluator shall verify that the TOE does not receive channel switching commands from keyboard shortcuts.
[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.	FDP_IFC.1(2) FDP_IFF.1(2)	FDP_IFF.1(2)-2 requires that the user will use one selection mechanism (and only one) to select the connected computer value n. Multiple user selection mechanisms would violate the "No ambiguous control" objective.
[O.CONTINUOUS_INDICATION] The TOE shall provide continuous visual indication of the computer to which the user is currently connected.	FTA_CIN_EXT.1	The FTA_CIN_EXT.1 extended requirement satisfies the "Continuous indication" objective by enforcing that the TOE shall display a continuous visual indication of the computer to which the user is currently connected, including on power up.
[O.KEYBOARD_AND_MOUSE_TIED] The TOE shall ensure that the keyboard and mouse devices are always switched together	FDP_ACC.1	FDP_ACC.1 enables positive identification of the keyboard and mouse peripheral devices are connected to the TOE keyboard and mouse ports and therefore assure that when these two ports are switched, it would be the keyboard and the mouse that will be tied together and not any other USB device.
	FDP_ACF.1	FDP_IFF.1.2(2) application note stating (as an example) that the keyboard and mouse

		functions must be in the same SPF and therefore must be switched together.
[O.NO_CONNECTED_COMPUTER_CONTROL] The TOE shall not allow TOE control through a connected computer.	FDP_IFC.1(1) FDP_IFF.1(1)	FDP_IFF.1.2(1) requires that the user makes a selection to establish a data flow connection between the peripheral device interfaces and one computer interface… This requirement indirectly satisfying the "No connected computer control" objective by prohibiting TOE channel selection by a connected computer that may have automated selection or may be controlled by a different user.
[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.	FDP_IFC.1(1) FDP_IFF.1(1)	The FDP_IFC.1(1) and FDP_IFF.1(1) satisfies the "Peripheral ports isolation" objective by defining in FDP_IFF.1.5(2), Denied data flow rule #1 defining that the TOE shall deny any information flow between TOE Computer Interfaces, except those allowed by the User Data Flow rules explicitly defined in other data flow rules by the SFR.
[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.	FDP_ACC.1	FDP_ACC.1 satisfies the "Disable unauthorized peripheral" objective by enforcing the "peripheral device SFP" on the TOE console ports. This policy enables the TOE to either allow connection, or disallow connection of console port connected peripheral device based on the rules defined in FDP_ACF.1 SFR below.
	FDP_ACF.1	FDP_ACF.1.4 satisfies the "Disable unauthorized peripheral device" objective by enforcing the following SFP rule: The TOE peripheral device interface (console) port shall reject any peripheral device with unauthorized values.
[O.DISABLE_UNAUTHORIZED_ENDPOINTS] The TOE shall reject unauthorized peripheral devices connected via a USB hub. Alternatively, the TOE may reject all USB hubs.	FDP_ACC.1	FDP_ACC.1 satisfies the "Disable unauthorized endpoints" objective by enforcing the "peripheral device SFP" on the TOE console ports. This policy enables the TOE to either allow connection, or disallow connection of console port connected peripheral device based on the rules defined in FDP_ACF.1 SFR below.
	FDP_ACF.1	FDP_ACF.1.4 satisfies the "Disable unauthorized endpoints" objective by enforcing the following SFP rule: The TOE peripheral device interface (console) port shall reject any peripheral device with unauthorized values. FDP_ACF.1.2 further requires that: "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 this PP". Annex C of the PP specifically defining the rules regarding USB endpoints:

		USB hub and composite devices are allowed if: The PSS can filter USB endpoints; and At least one endpoint is a keyboard or mouse HID class; and All other endpoints are disabled.
[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).	FDP_ACC.1	FDP_ACC.1 partially satisfying the "Keyboard and mouse emulated" objective by enforcing qualification rules on the peripheral devices connected to the TOE keyboard and mouse console ports. Such rules are essential in order to assure that the device connected (and emulated), are actually the keyboard and mouse and no other USB devices.
	FDP_ACF.1	FDP_ACF.1 satisfies the "Keyboard and mouse emulated" objective by setting the requirement that the TOE peripheral device interface (console) port shall reject any peripheral device with unauthorized values. The qualification of the connected keyboard and mouse device requires that the host function will be emulated. Furthermore, FDP_IFF.1.5(2) rule #2 requires that 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. This requirement can only be fulfilled if the keyboard and mouse emulated objective is met.
[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.	FDP_IFC.1(1) FDP_IFF.1(1)	The FDP_IFC.1(1) and FDP_IFF.1(1) satisfies the "Keyboard and mouse unidirectional" objective by defining in FDP_IFF.1.5(2), Denied data flow rules #3 and #4 that the TOE shall enforce unidirectional data flow from the keyboard and mouse peripheral device interfaces and the computer interface to the peripheral device interface. The prevention of power flow support the option that power modulation by computer will be used to signal data across the TOE.
[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.	FDP_IFC.1(1) FDP_IFF.1(1)	The FDP_IFC.1(1) and FDP_IFF.1(1) satisfies the "Unidirectional video" objective by defining in FDP_IFF.1.5(2), Denied data flow rule #11 that the TOE shall enforce unidirectional data flow from the computer video interface to the display interface only.
[O.UNIDIRERCTIONAL_EDID] TOEs that support VGA, DVI, DisplayPort or HDMI video shall force the display EDID peripheral data channel to unidirectional flow and only copy once from the display to	FDP_IFC.1(1) FDP_IFF.1(1)	The FDP_IFC.1(1) and FDP_IFF.1(1) satisfies the "Unidirectional EDID" objective by defining in FDP_IFF.1.5(2), Denied data flow rule #11 that the TOE shall enforce unidirectional data flow from the computer video interface to the

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.		display interface with the exception of EDID that may be copied from display to computer interfaces once during TOE power up.
[O.NO_TOE_ACCESS] 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.	FPT_PHP.3	FPT_PHP.3 requires that the TOE will actively resist a physical attack for the purpose of gaining access to the internal components, or to damage the anti-tampering battery by causing the TOE to become permanently disabled.
	FPT_FLS.1	FPT_FLS.1 requires that a failure of the TOE anti-tampering function would cause the TOE to become permanently disabled. This requirement is critical in order to assure that a TOE with potential physical tampering would not continue to be used.
[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 unique identifying tamper-evident marking that can be used to authenticate the device. The TOE manufacturer must maintain a complete list of manufactured TOE articles and their respective identification markings' unique identifiers.	FPT_PHP.1	FPT_PHP.1 requires that the TOE will have an unambiguous detection of physical tampering that might compromise the TSF. Furthermore it requires that the TOE shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred. One or more Tamper Evident Labels located in critical locations on the TOE enclosure would satisfy this SFR and objective.
[O.ANTI_TAMPERING] The TOE shall use an always-on active anti-tampering system to permanently disable the TOE in case physical tampering is detected.	FPT_PHP.3	FPT_PHP.3 satisfies the anti-tampering objective by requiring that the TOE will be equipped with a function that would actively resist a physical attack for the purpose of gaining access to the internal components.
[O.ANTI_TAMPERING_BACKUP_POWER] The anti-tampering system must have a backup power source to enable tamper detection while the TOE is unpowered.	FPT_PHP.3	FPT_PHP.3 satisfies the anti-tampering backup power source objective by requiring that the TOE anti-tampering function will be always on (even when 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.	FPT_PHP.3	FPT_PHP.3 satisfies the anti-tampering backup power source failure objective by requiring that the TOE anti-tampering function will trigger the anti-tampering if it detected that the backup power source has failed.
[O.ANTI_TAMPERING_INDICATION] The TOE shall have clear user indications when tampering is detected.	FPT_PHP.1	FPT_PHP.1 satisfies the anti-tampering triggering indications objective by requiring that the TOE shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

[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.	FPT_PHP.3	FPT_PHP.3.1 satisfies the "Anti-tampering permanently disables TOE" objective by setting the requirement that the TSF shall resist a physical attack …. by TOE <u>becoming permanently disabled</u>.
	FPT_FLS.1	FPT_FLS.1 requiring that once anti-tampering function was triggered, as a minimum, no peripheral device is connected to any computer.
[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.	FPT_PHP.3	FPT_PHP.3 satisfies the "No TOE access" objective by requiring that TOE will be equipped with an always-on active anti-tampering function that prevent external access to the TOE programming ports. FPT_FLS.1 adds to the previous SFR the assurance that in case of an anti-tampering backup power source failure, the anti-tampering function will be triggered.
	FPT_FLS.1	
[O.SELF_TEST] The TOE shall perform self-tests following power up or powered reset.	FPT_TST.1	FPT_TST.1 SFR defines the TOE self-testing coverage and schedule (before every power up cycle).
[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.	FPT_TST.1	FPT_TST.1 SFR defines the expected result in case of self-test failure – TOE shall become disabled. All inputs shall be isolated from all outputs.
	FPT_FLS.1	FPT_FLS.1 requires that failure of the TOE power on self-test, failure of the anti-tampering function will cause at least isolation of the peripheral devices and connected computers to preserve secure state.
[O.SELF_TEST_FAIL_INDICATION] The TOE shall provide clear and visible user indications in the case of a self-test failure.	FPT_TST.1	FPT_TST.1 requires that TOE will provide proper user indications in case of self-test failure.

Table 22 - Objective to SFRs Rationale

6.3 Rationale for IT Security Requirement Dependencies

This section includes a table of all the security functional requirements and their dependencies and a rationale for any dependencies that are not satisfied.

SFR	Dependencies	Dependency Satisfied/Rationale
FDP_IFC.1 (1)	FDP_IFF.1 (1)	Yes

SFR	Dependencies	Dependency Satisfied/Rationale
FDP_IFF.1 (1)	FDP_IFC.1 (1)	Yes
	FMT_MSA.3	No
FDP_IFC.1 (2)	FDP_IFF.1 (2)	Yes
FDP_IFF.1 (2)	FDP_IFC.1 (2)	Yes
	FMT_MSA.3(1)	No
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1	Yes
	FMT_MSA.3(3)	No
FDP_RIP.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
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	Satisfied by FIA_UID.2
Selection based Requirements (Annex G)		
FTA_ATH_EXT.1	none	Not applicable

Table 23 - SFR Dependencies satisfied

6.4 Dependencies Not Met

6.4.1 FMT_MSA.3 - Static attribute initialization

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.

6.4.2 FMT_MSA.3(1) and FMT_MSA.3(3) - Static attribute initialization

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.

6.5 Security Assurance Requirements

The table below is provides a list of claimed assurance components for each class.

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
Vulnerability Assessment	AVA_VAN.1	Vulnerability analysis
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage

Table 24 - SAR list

7 TOE Summary Specification

This section presents an overview of the security functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

7.1 TOE keyboard and mouse security functions

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

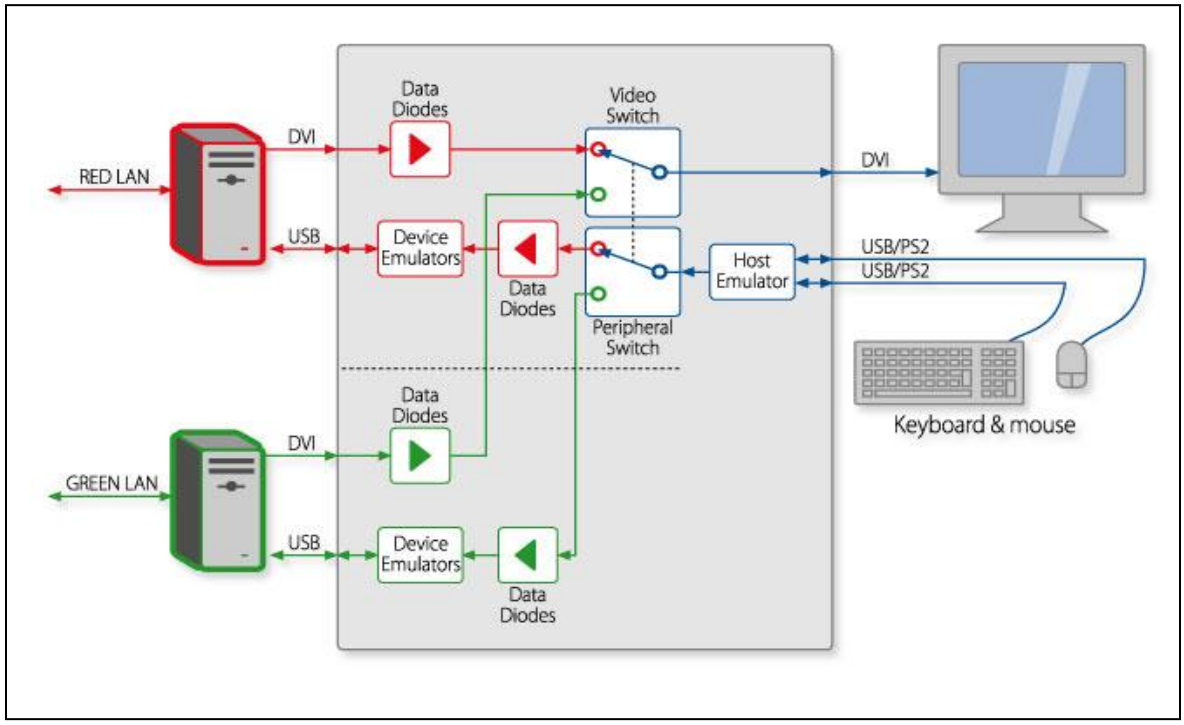

Figure 7 – Simplified block diagram of 2-Port KVM TOE

The TOE keyboard and mouse data flow path design is based on the following features (refer to figure 7 above for components location):

a. Isolated keyboard and mouse USB device emulators per connected computer to prevent direct interface between the TOE shared peripheral devices and connected computers. Device Emulators are microcontrollers that receive serial stream representing the keyboard and mouse commands on one side and interact with connected computer via USB bus on the other side. The use of isolated device emulator (one per computer) assures that connected computers will not interact electrically or logically with shared TOE or peripheral resources.
b. Each device emulator is powered by its own connected computer. Power domains of different computer interfaces are independent and isolated behind unidirectional data diodes.
c. TOE uses host (computer) emulators to interface with connected keyboard and mouse peripheral devices, thus isolating external peripherals from TOE internal circuitry and from connected

computers. An attempt of connected computer to target shared peripheral device or internal TOE circuitry must defeat first these host and device emulators.

d. Data exchange from host emulators to device emulators is limited to basic HID transactions through the use of limited serial protocol between TOE host emulators and device emulators. No other data may flow between emulators as it is not supported by the limited protocol.
e. Optical data diodes to enforce unidirectional data flow of serial data between TOE host emulators and device emulators. Optical data diodes are located before each device emulator channel to assure that each channel is completely isolated (electrically and logically) from other channel or from other TOE functions. No data flow is possible between the device emulators (connected computers) and host interfaces (peripheral devices).
f. Multiplexer (Peripheral switch) to enable selection of just one keyboard / mouse serial data source at any given time. Note that in the TOE this multiplexer is 3 positioned – third position is isolation (not connected). The third position is used when TOE is tampered or when self-test has failed to disable the keyboard and mouse stream.
g. Keyboard and mouse data flow is not combined or connected to any other TOE data flow. The keyboard and mouse functions are completely isolated from all other functions (audio, video etc.). There are no shared microcontrollers or any other electronic components. No other external interfaces are coupled to the keyboard and mouse data flow paths.
h. Keyboard and mouse are always switched together in the TOE. There is no administrator or user configuration that enables control split between keyboard and mouse functions.
i. Keyboard and mouse host emulators can only enumerate USB HID (Human Interface Devices). No other devices or endpoints are supported.
j. If connected device will attempt to enumerate as different devices in different time – the TOE will not enumerate the device at all. All other devices / endpoints will be rejected by the TOE. BadUSB or manipulated composite devices will be rejected by the TOE keyboard and mouse interface ports.
k. When the TOE is powered off, the optical data diodes are powered off and therefore no data flow is possible between the keyboard and mouse peripheral devices and computer interfaces.
l. During TOE switching from one computer to another, the system controller function assures that the keyboard and mouse stacks are deleted and that the first 100 milliseconds of commands received from the keyboard after switching are ignored (deleted). This is done to delete keyboard microcontroller buffer accumulation of cached commands from previous channel.
m. Keyboard LEDs are supported by local TOE indications but not through the keyboard embedded LEDs. Keyboard traffic is unidirectional but device emulators can detect each individual computer state and pass this information via secure multiplexer to the TOE front panel LEDs.
n. USB hub and composite devices are authorized as all evaluated TOE can filter USB endpoints; Note that devices having integrated USB hub and composite devices will be supported by the TOE only if the connected device has at least one endpoint which is a keyboard or mouse HID class; In such case the TOE will disable all other endpoints.
o. Wireless keyboards are not allowed per applicable user guidance.
p. Wireless mice are not allowed per applicable user guidance.
q. TOE Keyboard and mouse USB console ports are interchangeable.

This keyboard / mouse peripheral data path design provides the level of assurance that is required by the referenced PP.

The above features assure that the TOE satisfies the following PP objectives and security functional requirements:

i. [O.COMPUTER_INTERFACE_ISOLATION] → FDP_IFC.1(1) and FDP_IFF.1(1) (limited to keyboard and mouse data flows).
ii. [O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED] → FDP_IFC.1(1) and FDP_IFF.1(1) (limited to keyboard and mouse data flows).
iii. [O.USER_DATA_ISOLATION] → FDP_IFC.1(1) and FDP_IFF.1(1) (limited to keyboard and mouse data flows).
iv. [O.KEYBOARD_AND_MOUSE_TIED] → FDP_ACC.1 and FDP_ACF.1.
v. [O.PERIPHERAL_PORTS_ISOLATION] → FDP_IFC.1(1) and FDP_IFF.1(1) (limited to keyboard and mouse data flows).
vi. [O.DISABLE_UNAUTHORIZED_PERIPHERAL] → FDP_ACC.1 and FDP_ACF.1 (limited to keyboard and mouse data flows).
vii. [O.DISABLE_UNAUTHORIZED_ENDPOINTS] → FDP_ACC.1 and FDP_ACF.1 (limited to keyboard and mouse data flows).
viii. [O.KEYBOARD_MOUSE_EMULATED] → FDP_ACC.1 and FDP_ACF.1.
ix. [O.KEYBOARD_MOUSE_UNIDIRECTIONAL] → FDP_ACC.1 and FDP_ACF.1.

Keyboard user data is not stored on TOE non-volatile memory. All USB stacks are implemented in the TOE using SRAM (Static Random Access Memory) – a volatile memory that clears data once TOE is powered down.

The above features assure that the TOE satisfies the following PP objectives and security functional requirements:

i. [O.NO_USER_DATA_RETENTION] → FDP_RIP.1 (limited to keyboard and mouse data).
ii. [O.PURGE_TOE KB_DATA_WHILE_SWITCHING] → FDP_RIP.1.

7.2 TOE external interface security functions

a. The TOE supports only the following external interfaces protocols (as required by referenced PP):
   - USB keyboard and mouse;
   - Analog audio output;
   - User authentication device or other assigned USB devices (TOE model specific);
   - Power (AC or DC); and
   - Video (VGA, DVI, HDMI, DisplayPort or MHL video only);
b. The TOE audio out switching includes a unidirectional data flow diode to assure that microphone would not be supported. Audio data is forced to flow only from the selected connected computer to the user peripheral device. Audio data from connected peripheral device back to connected computer is blocked by the audio data diodes. There are two diodes in parallel to handle right side and left side audio signals (stereo).

c. Microphone bias is blocked by the TOE audio path to disable electrets microphone if connected to computer microphone input interface. The TOE does not support docking protocols. It does not support analog microphone or audio line inputs.

The above features assure that the TOE satisfies the following PP objectives and security functional requirements:

i. [O.NO_DOCKING_PROTOCOLS] → FDP_IFC.1(1) and FDP_IFF.1(1)
ii. [O.NO_OTHER_EXTERNAL_INTERFACES] → FDP_IFC.1(2) and FDP_IFF.1. (2)
iii. [O.NO_ANALOG_AUDIO_INPUT] → FDP_IFC.1(1) and FDP_IFF.1(1)

7.3 TOE Audio Subsystem security functions

The TOE audio data flow path is electrically isolated from all other functions and interfaces to prevent signaling data leakages to and from the audio paths.

Audio paths include:

a. The audio switching is controlled by the TOE system controller function through dedicated unidirectional command lines. Audio signals cannot be digitized or otherwise sampled by any TOE circuitry.
b. TOE is having separate interface per computer. Each interface is electrically isolated from other interfaces or other TOE circuitry;
c. TOE audio Switching multiplexer uses a combination of mechanical relays and solid state multiplexer to assure high off isolation;
d. Audio unidirectional flow data diodes (two) to prevent audio data flow from audio device to selected computer; and
e. Separate channel selection control by the user with optional freeze function. When the TOE is unpowered, an audio isolation relay is open up to isolate the audio inputs (computer interfaces) from all other circuitry and interfaces. TOE self-test failure or anti-tampering activation will de-energize the same audio isolation relay to isolate the audio inputs. TOE audio subsystem does not store, convert or delay any audio data flows. There is no risk of audio overflow while switching between channels.
f. The use of analog microphone or line-in audio devices is strictly prohibited per user guidance. All TOE that support analog audio out switching will reject a microphone through the following two methods:
    a. Analog audio data diode that forces data to flow only from computer to connected audio peripheral device; and
    b. Microphone DC bias barrier that blocks electrets microphone DC bias if deliberately or inadvertently the TOE is being connected to connected computer microphone input jack.

The above features assure that the TOE satisfies the following PP objectives and security functional requirements:

i. [O.NO_ANALOG_AUDIO_INPUT] → FDP_IFC.1(1) and FDP_IFF.1(1).
ii. [O.UNIDIRECTIONAL_AUDIO_OUT] → FDP_IFC.1(1) and FDP_IFF.1(1).
iii. [O.COMPUTER_TO_AUDIO_ISOLATION] → FDP_IFC.1(1) and FDP_IFF.1(1).

iv. [O.PERIPHERAL_PORTS_ISOLATION] → FDP_IFC.1(1) and FDP_IFF.1(1) (limited to audio data flows).
v. [O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE] → FPT_PHP.3 and FPT_FLS.1 (limited to audio data flows).
vi. [O.SELF_TEST] → FPT_TST.1 (limited to audio data flows).
vii. [O.SELF_TEST_FAIL_TOE_DISABLE] FPT_TST.1 and FPT_FLS.1 (limited to audio data flows).
viii. [O.NO_USER_DATA_RETENTION] → FDP_RIP.1 (limited to audio user data).

7.4 TOE video subsystem security functions

The TOE video data flow path is made of a unidirectional video and EDID paths.

To further illustrate the KVM TOE video subsystem security functions, the following figure show a simplified block-diagram of the TOE in various operating mode.

In figure 8 below, the TOE video controller function reads the connected display EDID EEPROM content through the closed isolation switch. No video is shown on display as the main video mux is switch to the fifth (isolated) state.

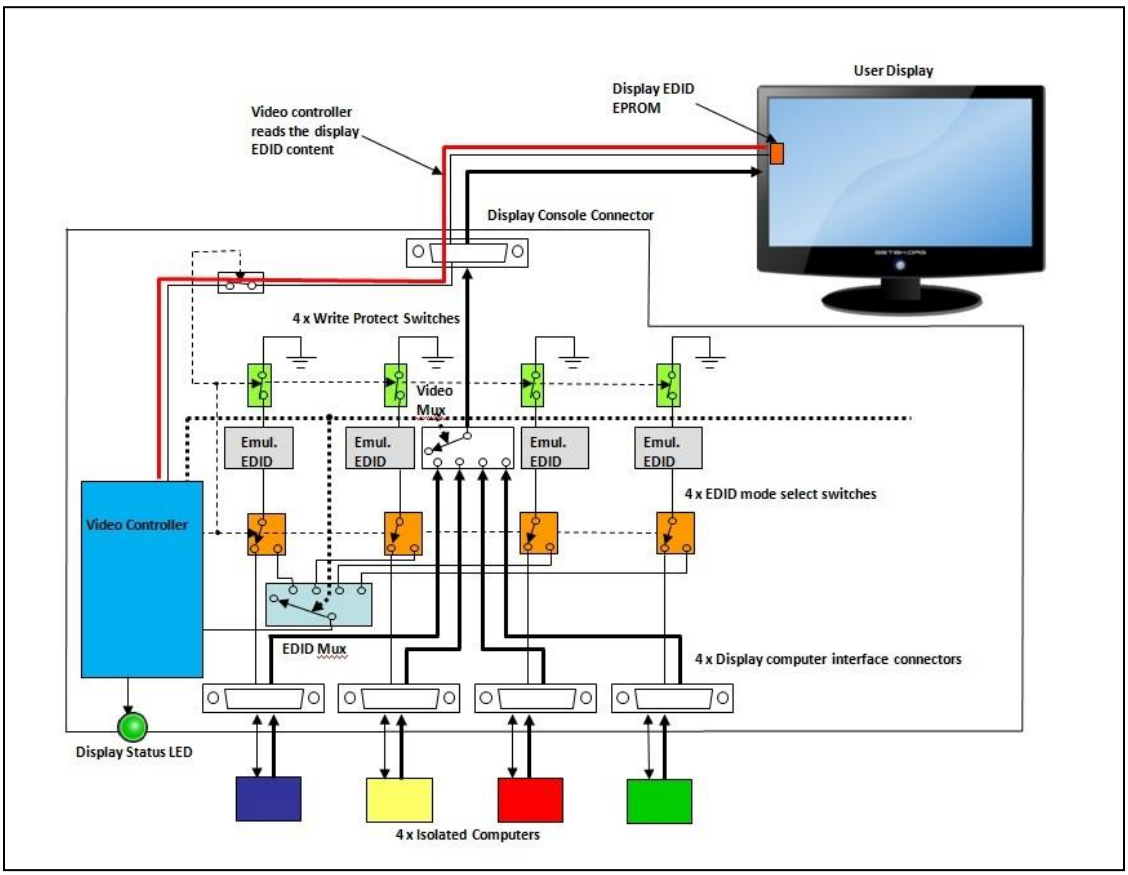

Figure 8 – Block diagram of KVM TOE video sub-system during display EDID read

This operating mode only occurs as the TOE is being powered up. The display EDID is not read at any other time while the TOE is operating. The video controller function is checking the EDID content to verify that it is valid and usable. If data is not valid – it will stop the programming sequence and wait for display change (next Hot Plug event).

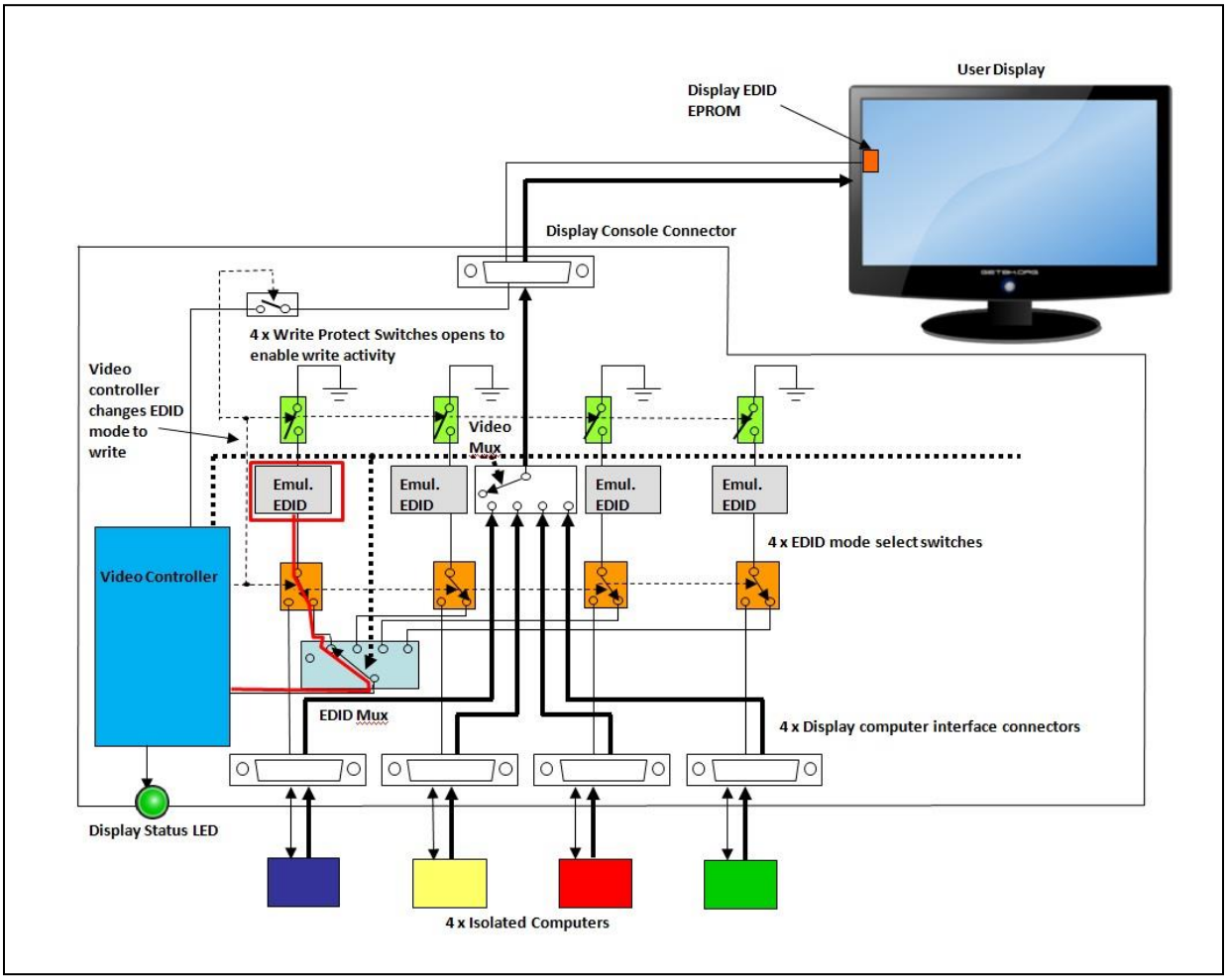

Figure 9 – Block diagram of KVM TOE video sub-system during display EDID write

Figure 9 illustrate the same TOE sub-system while the video controller function (blue) is writing the EDID content into the first channel emulated EDID EEPROM chip (gray). All thick lines in this figure are native video lines. All thin lines are I2C lines. The EDID mux (light blue) is coupling the I2C lines to the first EDID mode switch (orange). The first EDID mode switch is switching the video controller I2C lines to the first emulated EDID EEPROM chip (gray). The chip write protect switch (green) is opened to enable writing. Video controller uses the I2C lines to write the first emulated EDID EEPROM chip. Once writing operation completed and verified, the video controller function will switch the EDID mux to the next channel and the operation will repeat until all chips are programmed. Only when this write operation was successfully completed, the video controller will switch to normal operating mode as can be seen in figure 16 below.

In this mode the 4 Emulated EDID EEPROM chips are switched to their respective computers to enable read. The 4 write protect switches (green) are switched back to protected mode to prevent any attempt to write the EEPROM or transmit MCCS commands.

In this mode each computer interface is completely independent. The power to each emulated EDID EEPROM is received from its respective computer through the video cable. The main video mux is then switched to the user selected computer to enable proper video display of that computer.

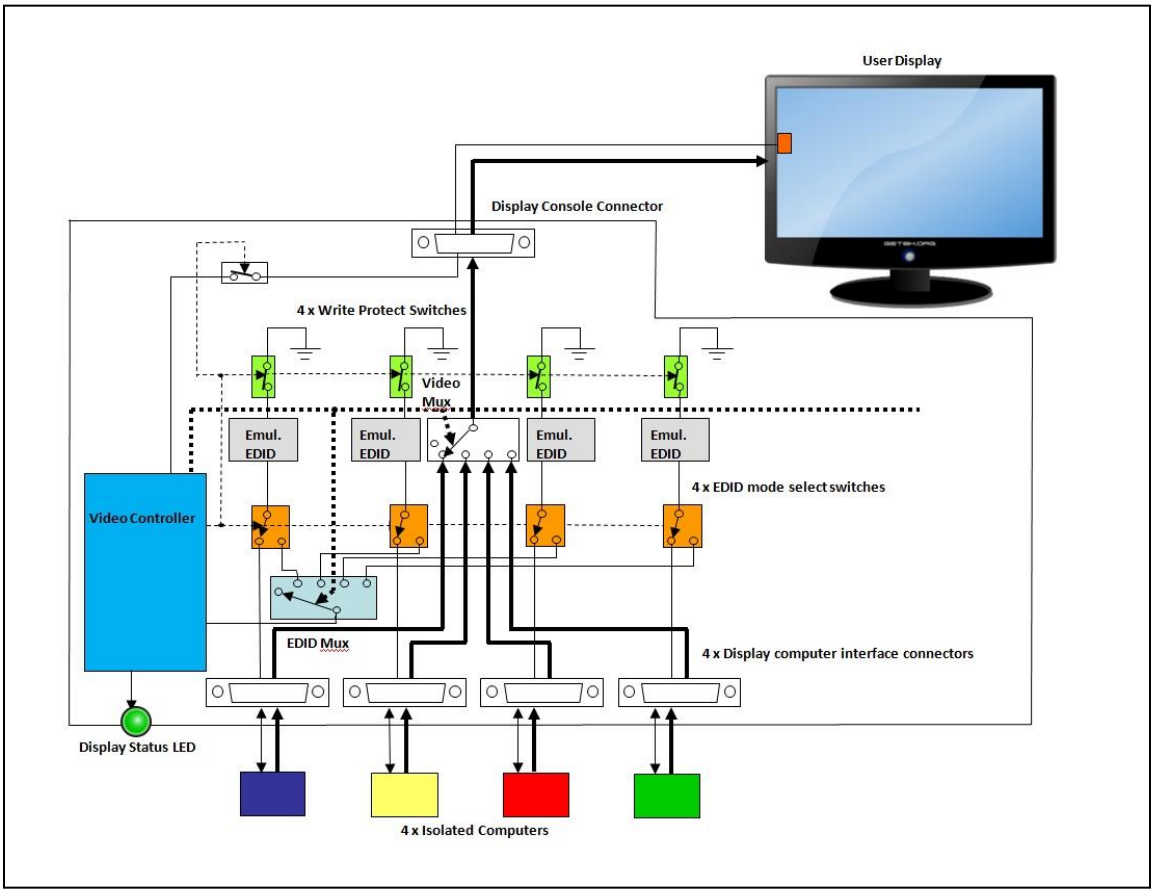

Figure 10 – Block diagram of KVM TOE video sub-system during normal mode

As shown in figure 10 above, during TOE normal operation, any attempt of one or more connected computer to attack, program, and signal or otherwise affect the EDID channel will be blocked by this architecture. Each computer effect will be contained in its own emulated EDID EEPROM.

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

a. Video input interfaces are isolated from one another. Isolation is achieved through the use of different power and ground planes, different electronic components and different emulated EDID chips per channel.
b. EDID function is emulated by independent emulation EEPROM chip for each computer channels. These chips are loaded with content read from the connected display once the TOE is powering up. All changes in display after that are ignored.
c. TOE will reject display devices having non-valid EDID content. Proper user indications provided by the TOE rear panel display status LED.

d. TOE supports Display Port 1.1, 1.2 and 1.3. TOE video function filters the AUX channel by converting it to I2C EDID only. DisplayPort video is converted into HDMI video stream and I2C EDID lines that being connected to the same emulated EDID EEPROM functions as shown in figures 8 – 10 above). All AUX channel threats are mitigated through the conversion from DisplayPort to HDMI protocols. All types of traffic not authorized by the referenced PP including USB, Ethernet, MCCS and EDID write are blocked by this TOE function as the emulated EEPROM would only support valid EDID read requests from connected computers. Note that HEAC and CEC functions are not connected in these TOEs and therefore not supported.
e. TOE video subsystem blocks MCCS write transactions through the emulated EDID EEPROMs. Emulated EEPROMs only supports EDID read transactions. As shown in figure 10 – emulated EDID EEPROMs cannot be written by their respective computers. The write protect switch will prevent such operation.
f. When TOE is unpowered or after TOE anti-tampering was triggered or after TOE self-testing has failed – all video signals are isolated (inputs from inputs and from outputs) by the active video re-drivers. Emulated EDID EEPROMs may still operate as it is powered by its respective computer, but isolation will remain the same as can be seen in figure 10 above.

The above features assure that the TOE satisfies the following PP objectives and security functional requirements:

i. [O.COMPUTER_INTERFACE_ISOLATION] → FDP_IFC.1(1) and FDP_IFF.1(1) (limited to video data flows).
ii. [O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED] → FDP_IFC.1(1) and FDP_IFF.1(1) (limited to video data flows).
iii. [O.USER_DATA_ISOLATION] → FDP_IFC.1(1) and FDP_IFF.1(1) (limited to video data flows).
iv. [O.PERIPHERAL_PORTS_ISOLATION] → FDP_IFC.1(1) and FDP_IFF.1(1) (limited to video data flows).
v. [O.UNIDIRECTIONAL_VIDEO] → FDP_IFC.1(1) and FDP_IFF.1(1).
vi. [O.UNIDIRERCTIONAL_EDID] → FDP_IFC.1(1) and FDP_IFF.1(1).
vii. [O.SELF_TEST] → FPT_TST.1 (limited to video data flows).
viii. [O.SELF_TEST_FAIL_TOE_DISABLE] → FPT_TST.1 and FPT_FLS.1 (limited to video data flows).
ix. [O.NO_USER_DATA_RETENTION] → FDP_RIP.1 (limited to video user data).

7.5 TOE User authentication device subsystem security functions

TOE may support User Authentication Device function (called DPP or fUSB). These products are configured by default as FDF (Fixed Device Filtration) with filter set to qualify only the following devices:

- Standard smart-card reader USB token or biometric authentication device having USB smart-card class interface complying with USB Organization standard CCID Revision 1.1 or ICCID Revision 1.0.

Note that device must be bus powered;

At any time after production, qualified administrator after successfully logging-in to the TOE administrative function may switch the TOE to CDF (Configurable Device Filtration) mode trough loading any white-list/black-list or traffic rules. Traffic rules are only related to preventing DPP from being switched to the currently selected computer. While in this mode, the TOE may qualify any USB 1.1, 2.0 or 3.0 based on the following one or more criterions:

1. USB Class;
2. USB Sub-class;
3. USB Protocol;
4. USB device ID;
5. USB Vendor ID;
6. USB Serial number;

The DPP function features (refer to figure 6 above area H):

a. Isolated computer interfaces 60x per connected computers 6x respectively. Each DPP computer interface 60x is using independent circuitry and power planes. There is no shared circuitry or logical functions with other ports or other TOE functions.
b. Qualification microcontroller 52 drives the mode select switch 54 that initially routes the device USB to the microcontroller.
c. The qualification microcontroller uses the predefined USB qualification parameters and compares them with the discovered USB device 40 parameters. In case that the parameters are matching – device is qualified.
d. If device 40 is qualified, the qualification microcontroller 52 switches the mode switch 54 to the USB multiplexer 56. The USB multiplexer 56 receives channel selected commands 23 from the system controller function 20 to allow proper selection of connected computer selected by the user.
e. The user authentication device data paths in the TOE are fully isolated from all other user data paths and functions.
f. TOE will only enumerate and enable peripheral devices that are predefined by authenticated administrator. Before and during USB session, the device enumeration set of details is being compared with pre-stored values to determine if the device can be qualified or should be rejected. The CDF definitions may define one or more device characteristics such as: USB device class, protocol, sub-protocol, VID, PID, serial number etc.
g. Once the user switches the connected computer, the TOE resets the user authentication device through power supply switching (temporary power dip as defined by the referenced PP). This is done through High-side Power switches on the System Controller board that switches 5V power to the DPP device jack. Load FET transistor is shorting the supply voltage to the ground to assure that all capacitance in the TOE or in the connected device would be quickly discharged and go below 2V as required by the PP.
h. The TOE does not emulate or process user authentication device data. No data retention is possible.
i. When TOE is unpowered or after TOE anti-tampering was triggered or after TOE self-testing has failed – all user authentication device data paths are isolated (switched off) through peripheral mux. Such disconnection will disconnect open authentication sessions per USB CCID standard.
j. The only traffic rules that can be set by the administrator are related to preventing user authentication device (DPP or CAC) from accessing a specific selected computer. It is only negative rules for the DPP/CAC. This means that the TOE blocks all USB devices other than user authentication by default. This is done to provide the most secure setting by default. Any white listing is reducing initial negative parameters. Any black listing is adding more parameters to the list I the TOE.
k. TOE User authentication port implementation is operating by default as Fixed device filtering – TOE will allow only user authentication devices.

l. TOE having fUSB function enable administrator configuration that switch the TOE to Configurable device filtering mode – TOE will allow any USB device based on configurable rules (for example whitelist and blacklist). Refer to the PP FDP_IFF.1.5(2) rules 5 and 6 and Annex C table 12 comment 6.
m. User authentication device must be powered by the TOE. External power source is prohibited per applicable user guidance.

The above features assure that the TOE satisfies the following PP objectives and security functional requirements:

a. [O.COMPUTER_INTERFACE_ISOLATION] → FDP_IFC.1(1) and FDP_IFF.1(1) (limited to user authentication device data flows).
b. [O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED] → FDP_IFC.1(1) and FDP_IFF.1(1) (limited to user authentication device data flows).
c. [O.USER_DATA_ISOLATION] → FDP_IFC.1(1) and FDP_IFF.1(1) (limited to user authentication device data flows).
d. [O.PERIPHERAL_PORTS_ISOLATION] → FDP_IFC.1(1) and FDP_IFF.1(1) (limited to user authentication device data flows).
e. [O.USER_AUTHENTICATION_ISOLATION] → FDP_IFC.1(1) and FDP_IFF.1(1).
f. [O.USER_AUTHENTICATION_RESET] → FDP_IFF.1. (1) and FTA_ATH_EXT.1.
g. [O.USER_AUTHENTICATION_ADMIN] → FMT_SMF.1 b, FMT_MOF.1 and FMT_SMR.1.

7.6 TOE User control and monitoring security functions

TOE is controlled and monitored by the user through front panel illuminated push-buttons and switches. These controls and indications are coupled to the TOE system controller function. This function features:

a. Internally illuminated push-buttons for computer channel selection. User may attach labels with computer name near push-buttons.
b. Additional white LEDs per channel to indicate audio and user authentication device channel selection.
c. Freeze function push-button and LED to enable audio and user authentication device channel freeze and to provide freeze status indication. This implementation allows user to split the TOE control as defined in the referenced PP.
d. TOE does not support keyboard shortcuts for channel selection or automatic port scanning. There are no firmware or hardware functions to support such unauthorized TOE control features.
e. All TOE user control methods are authorized by the referenced PP.
f. TOE does not enable user channel selection control by connected computer. No interface capable of this function provided by the TOE.
g. Channel selection indications provided by the TOE cannot be dimmed or disabled. Indications are continuous and are visible to the user at any time using the TOE.
h. The communication, configuration and integrity of the TOE front panel are being tested during power up self-testing. During power up until the TOE successfully passed the self-test, no channel is selected and therefore no TOE state provided to the user.
i. After self-test passed at all times that the TOE is operative, front panel indications are provided and cannot be turned off or dimmed by the user in any way.

j. All TOE have Restore to Factory Default recessed switch (exact location of this switch described in the applicable user and administrative guidance). Once this switch is pressed while the TOE is powered up and in normal operation, the following events will happen:
    1. All peripheral devices will be disconnected from selected computers;
    2. Front panel indications will blink all together;
    3. The TOE will reset and perform normal power up and self-test sequence (no user indications while powering up and self-testing);
    4. Then the TOE will resume normal operation while all settings and internal cache except for log are reset to the factory defaults. User indications will resume normal behavior at this stage unless TOE failed the self-test.
    5. **Note that administrator credentials and log data are not erased by this function**.

The above features assure that the TOE satisfies the following PP objectives and security functional requirements:

i. [O.AUTHORIZED_SWITCHING] → FDP_IFC.1(2) and FDP_IFF.1(2)
ii. [O.NO_AMBIGUOUS_CONTROL] → FDP_IFC.1(2) and FDP_IFF.1(2)
iii. [O.CONTINUOUS_INDICATION] → FTA_CIN_EXT.1
iv. [O.NO_CONNECTED_COMPUTER_CONTROL] →FDP_IFC.1(1) and FDP_IFF.1(1)

7.7 TOE Tampering protection

a. All TOE microcontrollers are running from internal protected flash memory. Firmware cannot be updated by the user through external tools.
b. Firmware cannot be read or rewrite through JTAG tools by internal interfaces. Firmware execution performed on SRAM with proper protection from external access and tampering of code or stacks.
c. The TOE enclosure was designed specifically to prevent physical tampering. It features stainless steel welded chassis and panels that prevent external access through bending or brute force.
a. Always-on anti-tampering system mechanically coupled to the TOE enclosure to detect and attempt to access the TOE internal circuitry.
b. Anti-tampering is powered by the TOE power supply and by a backup battery. If battery is depleted or failing – the anti-tampering function will trigger and the TOE will become permanently disabled.
c. The TOE anti-tampering function is irreversible. Once it is triggered – TOE will be permanently disabled through melting of internal (on-die) micro-fuse.
d. All TOE interfaces and user functions are disabled and proper user indications are shown through sequentially blinking front panel LEDs.
e. TOE is equipped with special holographic Tampering Evident Labels that located in critical location on the TOE enclosure. Any attempt to access the TOE internal circuitry would cause permanent visible damage to one or more TEL. Each label is numbered with unique number that recoded by the manufacturer during TOE production.
f. During production, each TOE receives a unique secret key (long unique number) that is securely stored in crypto-memory chip. This secret key is required to enable normal TOE boot and power up. If the secret key is missing or incorrect (cannot be authenticated by the TOE system controller) then the TOE will enter isolated mode and TOE will provide tampering indications. The anti-tampering sensors interrupting the power to the crypto memory and as a result delete the secret

key once sensors are momentarily interrupted. In addition, once the secret key cannot be authenticated, the TOE System Controller function burns a microscopic fuse on its die that causes irreversible change in the operating program.

g. All anti-tampering production and in-service events are recorded in TOE internal non-volatile memory with time and date tags to enable traceable audit through one of the two supported methods:
   I. Using special USB cable supplied as an optional accessory by the vendors, PC may be connected to the TOE. Using administrator user name and password, authorized administrator may download the stored log files into text or Excel file; and
   II. If TOE support keyboard then the keyboard device emulator may be used to type the log data into text editor application such as Notepad running in a connected computer. This function also requires administrator identification and authentication through proper user name password entry through the connected keyboard.

The above features assure that the TOE satisfies the following PP objectives and security functional requirements:

i. [O.NO_TOE_ACCESS] → FPT_PHP.3 and FPT_FLS.1
ii. [O.TAMPER_EVIDENT_LABEL] → FPT_PHP.1
iii. [O.ANTI_TAMPERING] → FPT_PHP.3
iv. [O.ANTI_TAMPERING_BACKUP_POWER] → FPT_PHP.3
v. [O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER] → FPT_PHP.3
vi. [O.ANTI_TAMPERING_INDICATION] → FPT_PHP.1
vii. [O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE] → FPT_PHP.3 and FPT_FLS.1

7.8 TOE Self-testing and Log

TOE is equipped with self-testing function that operating while TOE is being powered up prior to normal use. The self-test function is running independently at each one of the TOE microcontrollers following power up.

a. If the self-testing function has failed, the TOE will provide proper user indications and will disable normal operation while isolating all / or affected peripheral devices and connected computers.
b. The self-testing function checks the integrity of the TOE microcontroller firmware, the anti-tampering function, and the control functions.
c. The self-testing function further test computer ports isolation by running test packets at different interfaces and attempting to detect traffic at all other interfaces.
d. All failures detected by the self-testing are recorded in the TOE log file together with time tags. Log content cannot be deleted by user or administrator.

The above features assure that the TOE satisfies the following PP objectives and security functional requirements:

i. [O.SELF_TEST] → FPT_TST.1
ii. [O.SELF_TEST_FAIL_TOE_DISABLE] → FPT_TST.1 and FPT_FLS.1

iii. [O.SELF_TEST_FAIL_INDICATION] → FPT_TST.1

TOE is equipped with event log non-volatile memory that stores information about abnormal security related events. There are two log storage spaces that differ in their operational logic:

1. **Critical log area** –This log area stores the following data in fixed structure:
    a. **T**he product registration information (once during production);
    b. The anti-tampering arming event (once during production);
    c. Tampering events detected (may be up to 6 possible event flags, each with data and time);
    d. The last admin log-on information (one event); and
    e. The last self-test failure information (one event with error codes).
2. **Non-critical log –** This log area holds a maximum of 32 lines of data. Every new event will delete the oldest line. This area holds the following data:
    a. **A**dministrator log in and changes made;
    b. Changes in administrator user name or password;
    c. Rejection of USB devices;
    d. Self-test failures;
    e. CDF (black-list / white-list) and traffic rules uploading; and
    f. Power up and down cycles.

Log can be extracted by one of the 3 options (in the first two options log can only be read – it cannot be written or delete):

i. Using special programming cable and software utility running on a connected PC. Administrator log-in is needed.
ii. Using connected PC and Notepad. Log can be dumped to the notepad. Again administrator log-on is needed.
iii. If the device was tampered then no external communication is possible. In the factory, the vendor may de-solder the part and extract the memory content using low-level tools.

The above features assure that the TOE satisfies the following PP objectives and security functional requirements:

i. [O.ANTI_TAMPERING] → FAU_GEN.1.1 and FAU_GEN.1.2

Annex A – HSL Model Numbering

The following text explains the HSL model numbering of secure KVM, KM, Matrix, Filters, Isolators and MDRs.

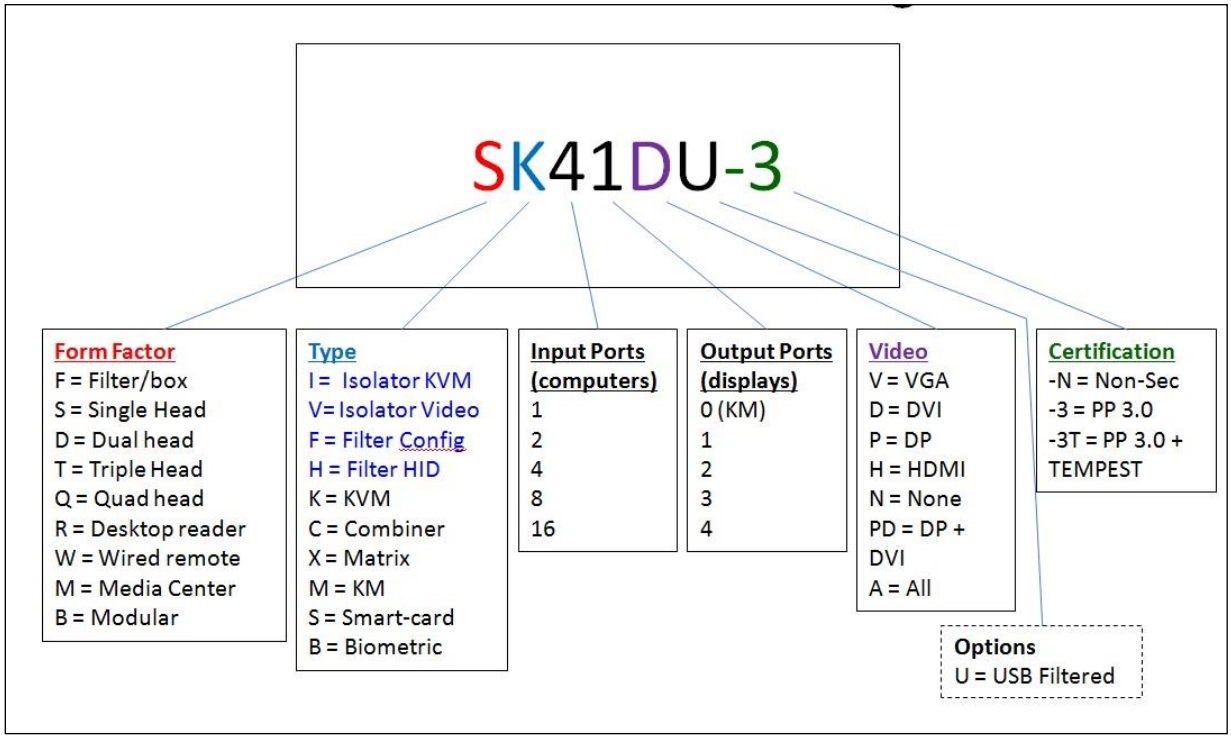

Figure 11 – HSL Secure products model numbering

Annex B – Removed

Annex B – Letter of Volatility

The following pages capture the Letter of Volatility issued by High Sec Labs for the TOE.

HighSecLabs
Highest Security Solutions Ltd.

Letter of Volatility

The table below provides volatility information and memory types for the High Sec Labs Secure KVM and Matrix as part of the documentation required for compliance with NIAP Peripheral Sharing Switch Protection Profile Rev 3.0. Please note that there are no remnants of user data retained in the device when the power is turned off.

Product Model	No. of devices in each product	Function, MFR and P/N	Storage Type	Size	Volatility	Contains User Data
SK21D-3 SK21P-3 SK21H-3 SX22D-3 SX22H-3 DK22H-3 DK22P-3 DK22D-3 DK22PD-3	1	System Controller, Host emulators; ST Microelectronics STM32F207ICH6	Embedded SRAM[1]	128KB	Volatile	May contain user data
			Embedded Flash[2]	256KB	Non-Volatile	No user data
			Embedded EEPROM	4 KB	Non-Volatile	No user data
			OTP Memory	512 bytes	Non-Volatile	No user data
	1	Video Controller; ST Microelectronics STM32L151CBU6	Embedded SRAM[1]	16KB	Volatile	No user data
			Embedded Flash[2]	128KB	Non-Volatile	No user data
			Embedded EEPROM	4 KB	Non-Volatile	No user data
	2	Device emulators; ST Microelectronics STM32L151CBU6	Embedded SRAM[1]	16KB	Volatile	May contain user data
			Embedded Flash[2]	128KB	Non-Volatile	No user data
			Embedded EEPROM	4 KB	Non-Volatile	No user data
	1	RTC (Real Time Clock); Intersil; ISL1209IU10Z-TK	RAM[3]	2 Bytes	Non-Volatile[2]	No user data
	1	Anti-tampering; Atmel; AT88SC0204CA-SU	Crypto memory EEPROM[4]	256 Byte	Non-Volatile	No user data
	2	EDID Emulator; ST Microelectronics M24C02-WMN6TP	EEPROM[5]	2 KB	Non-Volatile	No user data
SK41D-3 SK41DU-3 SK41P-3 SK41PU-3 SK41H-3 SK41HU-3 DK42D-3 DK42DU-3 DK42P-3 DK42PU-3	1 or 2	System Controller, Host emulators, DPP Controller (optional); ST Microelectronics STM32F207ICH6	Embedded SRAM[1]	128KB	Volatile	May contain user data
			Embedded Flash[2]	256KB	Non-Volatile	No user data
			Embedded EEPROM	4 KB	Non-Volatile	No user data
			OTP Memory	512 bytes	Non-Volatile	No user data
	1 in SH or 2 in	Video Controller;	Embedded SRAM[1]	16KB	Volatile	No user data

DK42H-3 DK42HU-3 SX42DU-3 SX42PU-3 SX42HU-3	DH models	ST Microelectronics STM32L151CBU6	Embedded Flash[2]	128KB	Non-Volatile	No user data
			Embedded EEPROM	4 KB	Non-Volatile	No user data
	4 in SH or 8 in DH models	Device emulators; ST Microelectronics STM32L151CBU6	Embedded SRAM[1]	16KB	Volatile	May contain user data
			Embedded Flash[2]	128KB	Non-Volatile	No user data
			Embedded EEPROM	4 KB	Non-Volatile	No user data
	1	RTC (Real Time Clock); Intersil; ISL1209IU10Z-TK	RAM[3]	2 Bytes	Non-Volatile[2]	No user data
	1	Anti-tampering; Atmel; AT88SC0204CA-SU	Crypto memory EEPROM[4]	256 Byte	Non-Volatile	No user data
	4 in SH or 8 in DH models	EDID Emulator; ST Microelectronics M24C02-WMN6TP	EEPROM[5]	2 KB	Non-Volatile	No user data
SK81DU-3 DK82DU-3 SK161DU-3	1 or 2	System Controller, Host emulators, DPP Controller (optional); ST Microelectronics STM32F207ICH6	Embedded SRAM[1]	128KB	Volatile	May contain user data
			Embedded Flash[2]	256KB	Non-Volatile	No user data
			Embedded EEPROM	4 KB	Non-Volatile	No user data
			OTP Memory	512 bytes	Non-Volatile	No user data
	1 in SH or 2 in DH models	Video Controller; ST Microelectronics STM32L151CBU6	Embedded SRAM[1]	16KB	Volatile	No user data
			Embedded Flash[2]	128KB	Non-Volatile	No user data
			Embedded EEPROM	4 KB	Non-Volatile	No user data
	8 in SH or 16 in DH /16P models	Device emulators; ST Microelectronics STM32L151CBU6	Embedded SRAM[1]	16KB	Volatile	May contain user data
			Embedded Flash[2]	128KB	Non-Volatile	No user data
			Embedded EEPROM	4 KB	Non-Volatile	No user data
	1	RTC (Real Time Clock); Intersil; ISL1209IU10Z-TK	RAM[3]	2 Bytes	Non-Volatile[2]	No user data
	1	Anti-tampering; Atmel; AT88SC0204CA-SU	Crypto memory EEPROM[4]	256 Byte	Non-Volatile	No user data
	8 in SH or 16 in DH /16P models	EDID Emulator; ST Microelectronics M24C02-WMN6TP	EEPROM[5]	2 KB	Non-Volatile	No user data

Notes:

[1] SRAM stores USB Host stack parameters and up to 4 last key-codes. Data is erased when the KVM is being powered off. It is also erased whenever the user switches channels. Device emulators are powered by the individual connected computers and therefore devices are powered as long as the connected computer is powered.

[2] Flash is used to store firmware code and contains no user data. Flash is permanently locked by fuses after initial programming to prevent rewriting (becoming ROM). It is an integral part of the ST Microcontroller together with SRAM and EEPROM.

[3] Memory is volatile but it is powered from a battery backup. It contains anti-tampering unique device authentication keys and events log.

[4] Crypto memory is used to store device unique authentication keys for anti-tampering.

[5] EEPROM is used to store operational parameters (display Plug & Play) and contains no user data. These devices are powered by the individual computers connected to the TOE and therefore are powered as long as powered computer is connected.

If any additional information is required, please contact me directly:

Aviv Soffer
CEO
High Sec Labs ltd.,
Tel: +972-4-9591191
Email: aviv@highseclabs.com
Signature:

Date: Sep 13, 2015,
Revision C
Document No. HDC11577

Annex C – Letter of Declaration – Spectre / Meltdown Vulnerability

The following page capture the Letter of Declaration issued by High Security Labs as mitigation for Spectre /Meltdown vulnerabilities.

We are aware of the recent industry-wide announcement regarding vulnerabilities with certain advanced microprocessors.

As an active member of the Cybersecurity vendor community we are currently analyzing the impact of Spectre and Meltdown vulnerabilities on our current and past products.

We specifically addressed the vulnerabilities of Speculative Processors to Cache Timing Side-Channel Mechanism.

So far we completed the analysis of all of our current and past secure KVM products. Based on this analysis Belkin acknowledge that:

1. None of our current and past secure KVM products is using Intel or AMD processors.
2. None of our current and past secure KVM products is using ARM Cortex-A8, Cortex-A9, and Cortex-A15 architectures that are affected by the Spectre and Meltdown vulnerabilities.
3. None of our current and past secure KVM products is using other processor, DSP or ASIC that is currently known to be affected by the Spectre and Meltdown vulnerabilities.

Annex D – Tamper Evident Label

Below is the spec for HSL's tamper evident label. The labels are placed on the TOE so it is impossible to open the TOE mechanical cover without removing the labels. Physical tampering is indicated if the label reveals a 'VOID' message or if the label is thorn. The label is not altered during normal use of the device.