Sekuryx Secure KVM Switch Security Target (Non-CAC Models)

Release Date: August 20, 2021
Revision: 1.06
Author: Steve Barash, Sekuryx

Table of Contents

Table of Figures

List of Tables

Document Revisions

Revision#	Date	By	Updates
1.00	June 5, 2020	Steve Barash, Sekuryx	Initial Document Outline
1.01	July 7, 2020	Steve Barash, Sekuryx	Formatting updates and adding NIAP TDs
1.02	August 1, 2020	Steve Barash, Sekuryx	Responding to comments based on preliminary evaluation
1.03	January 21, 2021	Steve Barash, Sekuryx	Separated requirements based on different supported video protocols
1.04	May 21, 2021	Steve Barash, Sekuryx	Incorporation of NIAP feedback and finalization
1.05	August 6, 2021	Steve Barash, Sekuryx	Incorporation of evaluator feedback
1.06	August 20, 2021	Steve Barash, Sekuryx	Incorporation of NIAP feedback

1 Introduction

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

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

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

Table 1 – ST Composition

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

1.1 ST and TOE Identification

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

ST Title	Sekuryx Secure KVM Switch Security Target (Non-CAC Models)
Revision Number	1.06
ST Publish Date	August 20, 2021
ST Authors	Steve Barash, Sekuryx
TOE Identification	See Tables 5, 6 and 7 below
Keywords	KVM, Secure, Sekuryx, Protection Profile 4.0

Table 2 – ST Identification

1.2 PP Reference Identification

The TOE claims conformance to the following PP-Configuration:

PP-Configuration Reference: PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, and Video/Display Devices (CFG_PSD-AO-KM-VI_V1.0)
PP-Configuration Sponsor: National Information Assurance Partnership (NIAP)
PP-Configuration Version: 1.0
PP-Configuration Date: July 19, 2019

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

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

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

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

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

1.3 Organization

Security Target Introduction (Section 1)

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

Security Problem Description (Section 2)

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

Security Objectives (Section 3)

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

Security Requirements (Section 4)

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

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

Conformance Claims (Section 5)

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

Summary Specification (Section 6)

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

1.4 Conventions

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

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

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

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

1.5 Technical Definitions

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

1.5.1 ST Specific Terminology

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

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

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

Protocol	A set of rules or procedures for transmitting data between electronic devices.
Remote Controller	Remote component of the PSD that extends the controls and indications through a cable.
Secure State	An operating condition in which the PSD disables all connected peripheral and connected computer interfaces when the correctness of its functions cannot be ensured.
Selected Computer	A Connected Computer that has Active Interfaces with the PSD.
Sub-Protocol	A set of common commands flowing within a protocol.
Supported Peripheral	A Peripheral Device that is technically supported by the PSD.
TOE Computer Video Interface	TOE port used to connect the computer or other video source.
Touch Screen	A pointing device Peripheral Device that enable users to touch one or more objects on the screen or to point the cursor device to specific locations.
USB Audio codec	Computer audio peripheral device with USB digital input/output, one or more analog audio outputs and one or more analog audio inputs.
USB Device	USB devices are leafs in the USB tree that are connected to the host.
USB Hub	A device that expands a single USB port into several so there are more ports available to connect devices to a host system.
USB Type-C	Universal Serial Bus (USB) interface that supports DisplayPort video output as an alternate mode.
User	A person that interacts with a PSD (or a process or mechanism acting on behalf of a person).
User Data	Information that the User inputs to the Connected Computer or is output to the User from the Connected Computer (and including user authentication and credential information)
Video Data	Visual and audio information presented to the user through the display device.
Video Wall	A tiled set of displays that allow the video output from a single Selected Computer to be spanned across multiple individual displays.
Whitelist	List containing one or more device attributes that will cause the TOE to accept the devices having that attribute.

Table 3 – ST Technical Definitions

1.5.2 Acronyms

Acronym	Full Definition
ARC	Audio Return Channel

CEC	Consumer Electronics Control
dB	Decibel
dBv	A measurement of voltage ratio to 1 volt
DVI	Digital Visual Interface (standard)
EDID	Extended Display Identification Data
HDCP	High-bandwidth Digital Content Protection
HDMI	High-Definition Multimedia Interface (standard)
HEAC	HDMI Ethernet and Audio Return Channel
HEC	HDMI Ethernet Channel
HID	Human Interface Device
HPD	Hot Plug Detect
KHz	Kilohertz
KM	Keyboard, Mouse
KVM	Keyboard, Video and Mouse
mV	Millivolt
PC	Personal Computer
PSD	Peripheral Sharing Device
PS/2	Personal System/2
MCCS	Monitor Command Control Set
OSP	Organizational Security Policies
PSD	Peripheral Sharing Device
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
S/PDIF	Sony/Philips Digital Interface Format
USB	Universal Serial Bus
VGA	Video Graphics Array (standard)

Table 4 – ST Acronyms

1.6 TOE Overview

1.6.1 TOE Architecture (High Level)

Sekuryx Secure Peripheral Sharing Devices (PSD) provide a secure medium to share a single set of peripheral components such as keyboard, video display and mouse/pointing devices among one or multiple computers over USB, and DisplayPort.

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

Sekuryx Secure KVM port models:

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

Sekuryx Secure KVM video outputs (displays):

- Single head
- Dual-head

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

- USB keyboard – the TOE does not allow USB traffic to flow from the TOE to a connected keyboard via the peripheral port
- USB mouse or other pointing device – the TOE does not allow USB traffic to flow from the TOE to a connected pointing device via the peripheral port
- DisplayPort 1.2 Video Input (computer ports) – the TOE does not allow video traffic to flow from the TOE to a connected computer via the computer port except for those sub-protocols needed to establish initial connectivity between the computer and the peripheral monitor(s)
- DisplayPort 1.2 Video Output (peripheral port) – the TOE does not allow video traffic to flow from a peripheral to the TOE via the peripheral port except for those sub-protocols needed to establish initial connectivity between the computer and the peripheral monitor(s).
- 3.5mm Audio Input (computer ports) – the TOE does not allow audio output to flow from the TOE to a connected computer via the computer ports (i.e. the use of a microphone peripheral is not supported)
- 3.5mm Audio Output (peripheral port) – the TOE does not allow audio input to flow from a peripheral to the TOE via the peripheral port (i.e. the use of a microphone peripheral is not supported)

Tables 5, 6, and 7 below provide a summary of the Sekuryx Secure KVM security features by supported interface types. A detailed description of the TOE security features and how they are mapped to the claimed SFRs can be found in Section 6 (TOE Summary Specification) below.

1.6.2 TOE Details

1.6.2.1 *Evaluated Products*

#	Model Name	Description	Eval. Version
1	CK4-P102	2-Port SH Secure DP KVM w/audio	4.30.001
2	CK4-P202	2-Port DH Secure DP KVM w/audio	4.30.001

Table 5 – Sekuryx 2-Port Secure TOE Identification

#	Model Name	Description	Eval. Version
1	CK4-P104	4-Port SH Secure DP KVM w/audio	4.30.001
2	CK4-P204	4-Port DH Secure DP KVM w/audio	4.30.001

Table 6 – Sekuryx 4-Port Secure TOE Identification

#	Model Name	Description	Eval. Version
1	CK4-P108	8-Port SH Secure DP KVM w/ audio	4.30.001
2	CK4-P208	8-Port DH Secure DP KVM w/ audio	4.30.001

Table 7 – Sekuryx 8-Port Secure TOE Identification

Notes:

- DP = DisplayPort video.
- SH = Single head; DH = Dual head
- Description - Includes text that is printed on a label attached to each device on the bottom.
- Eval. Version – Firmware and hardware revision per each device.
- Sekuryx's model name logic can be found in Appendix A.

1.6.2.2 *Common Criteria Product Type*

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

1.6.2.3 *Peripheral Devices Supported by the TOE*

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

Console Port	Authorized Devices
Keyboard	Wired keyboard and keypad without internal USB hub or composite device functions, unless the connected device has at least one endpoint which is a keyboard or mouse HID class
Display	Display device (e.g. monitor, projector) that uses an interface that is physically and logically compatible with the TOE ports (DisplayPort)
Audio out	Analog amplified speakers, Analog headphones
Mouse / Pointing Device	Any wired mouse or trackball without internal USB hub or composite device functions

Table 8 – Peripheral Devices supported by the TOE

1.6.2.4 *Protocols Supported by the TOE*

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

Model	CK4-P102	CK4-P202
Keyboard USB 1.1/2.0	✓	✓
DP	✓	✓
Mouse USB 1.1/2.0	✓	✓
Audio Analog Stereo	✓	✓

Table 9 – Console Port Protocols (2-Port TOE models)

Model	CK4-P104	CK4-P204
Keyboard USB 1.1/2.0	✓	✓
DP	✓	✓
Mouse USB 1.1/2.0	✓	✓
Audio Analog Stereo	✓	✓

Table 10 – Console Port Protocols (4-Port TOE models)

Model	CK4-P108	CK4-P208
Keyboard USB 1.1/2.0	✓	✓
DP	✓	✓
Mouse USB 1.1/2.0	✓	✓
Audio Analog Stereo Output	✓	✓

Table 11 – Console Port Protocols (8-Port TOE models)

Model	CK4-P102	CK4-P202
Keyboard USB 1.1/2.0	✓	✓
DP	✓	✓
Mouse USB 1.1/2.0	✓	✓
Audio Analog Stereo	✓	✓

Table 12 – Computer Port Protocols (2-Port TOE models)

Model	CK4-P104	CK4-P204
Keyboard USB 1.1/2.0	✓	✓
DP	✓	✓
Mouse USB 1.1/2.0	✓	✓
Audio Analog Stereo	✓	✓

Table 13 – Computer Port Protocols (4-Port TOE models)

Model	CK4-P108	CK4-P208
Keyboard USB 1.1/2.0	✓	✓
DP	✓	✓
Mouse USB 1.1/2.0	✓	✓
Audio Analog Stereo Output	✓	✓

Table 14 – Computer Port Protocols (8-Port TOE models)

1.6.2.5 *Logical Scope of the TOE*

1.6.2.5.1 Basic KVM TOE Function Overview

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

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

TOE Service	Verification
User peripheral isolation from source computer	✓
Admin access to management and log functions	✓
Restore factory defaults function	✓
Mapping user display to chosen computer	✓
Mapping user keyboard and mouse to chosen computer	✓
Mapping user audio device to chosen computer	✓

Table 15 – TOE Services

1.6.2.6 Administrative configuration of the TOE

Table 16 below shows a summary of administrator administrative and security management features. The authenticated Administrator is considered to be the administrator for the PSD PP. See section 6.2 for detailed description of the administration tool architecture.

Menu Option	Administrator
Change Admin Access Credentials	✓
Dump Log	✓
Restore Factory Default (reset)	✓
Terminate Session	✓

Table 16 – TOE Administrator Services and Accessibility

1.6.2.6.1 Change Admin Credentials option allows updating both the username and password.

1.6.2.6.2 Dump Log (auditing) option allows generating a detailed report of security functions such as self test, rejected peripheral USB device connection, restore factory default (reset) and failure to log in.

1.6.2.6.3 Restore Factory Default (reset) option causes the following to occur:

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

1.6.2.6.4 Terminate Session logs out the authenticated Administrator.

1.6.2.7 TOE Security Functions Overview

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

TOE Keyboard and Mouse Security Functions

1. No data is stored in non-volatile memory (SRAM only).
2. USB Keyboard and mouse data flows are converted to a serial data flow channel which is isolated from each connected computer and all TOE internal circuitry.
3. Keyboard and mouse channels are isolated electrically and logically from each connected computer and all TOE internal circuitry.
4. Uni-directional data flow enforced by using uni-directional optical data diodes.
5. Temporary power shut down during channel switching to eliminate previous cached keyboard/mouse commands.
6. Device/Host emulators used to prevent connected computer and peripheral device direct communication/data leakage.

7. Device/Host emulators used to maintain KM emulation system on all channels during TOE operation (enabling non-selected connected computers to have emulation even when the user uses another PC).
8. The TOE rejects all unauthorized peripheral devices.
9. Keyboard LEDs will not turn on despite valid keyboard commands being executed (ex: Caps Lock LED will not turn on) to enforce unidirectional communication.
10. The TOE only allows valid and simple keyboard and mouse commands. All other USB traffic is rejected. All advanced keyboard and mouse devices will have their non-basic features disabled by the TOE.
11. Keyboard and mouse channels remain isolated when the TOE is not powered.

TOE External Interfaces Security Functions

1. No docking protocols supported by the TOE.
2. No analog audio input allowed by peripherals connected to the TOE.
3. Devices allowed by the TOE:
    - Wired USB 1.1/2.0 keyboard and mouse
    - 3.5mm Analog audio output jack
    - DP 1.2 input/DP 1.2 output

TOE Audio Subsystem Security Functions

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

TOE Video Subsystem Security Functions

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

TOE User Control and Monitoring Security Functions

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

Self-Testing

1. TOE self-testing function that forcibly executes prior to system power up.
2. Self-testing function failure temporarily disables normal TOE operation until system reboot and subsequent passing of all self-test functions.

3. Self-testing function failure has visual and audible indications (flashing push-button LEDs, pulsing relays).

Anti-Tampering

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

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

1.7 TOE Scope and Boundary

1.7.1 Overview

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

- Analog audio output
- Keyboard/Mouse input
- Video output

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

No.	Physical Boundary of TOE
1	One Sekuryx Secure KVM Switch
2	The TOE computer interface cables that are shipped with the product
3	The permanently programmed embedded firmware inside the TOE on each microcontroller and processor
4	Log data, settings data, state data stored in the TOE
5	The TOE power supply that is shipped with the product
6	User Guidance Manual. Current version available for download at: https://sekuryx.com/documents-niap4/
7	Administrator Guidance. Current version available for download at: https://sekuryx.com/documents-niap4/

Table 17 – TOE Physical Boundary Composition

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

Note: Some TOE models support the operation of multiple user displays. Specifically, the model names that include “2” after “CK4-P” support the connection of up to two displays to the console ports. This

allows for switching of computers that have multi-monitor display capabilities. Models that do not use this notation in the model name are single head for switchable video output.

The figures below show representative examples of supported TOE models and their connections to peripherals and computers. This includes 2-port and 4-port models. 8-port models behave the same way as 2-port and 4-port models except that additional connected computers are supported.

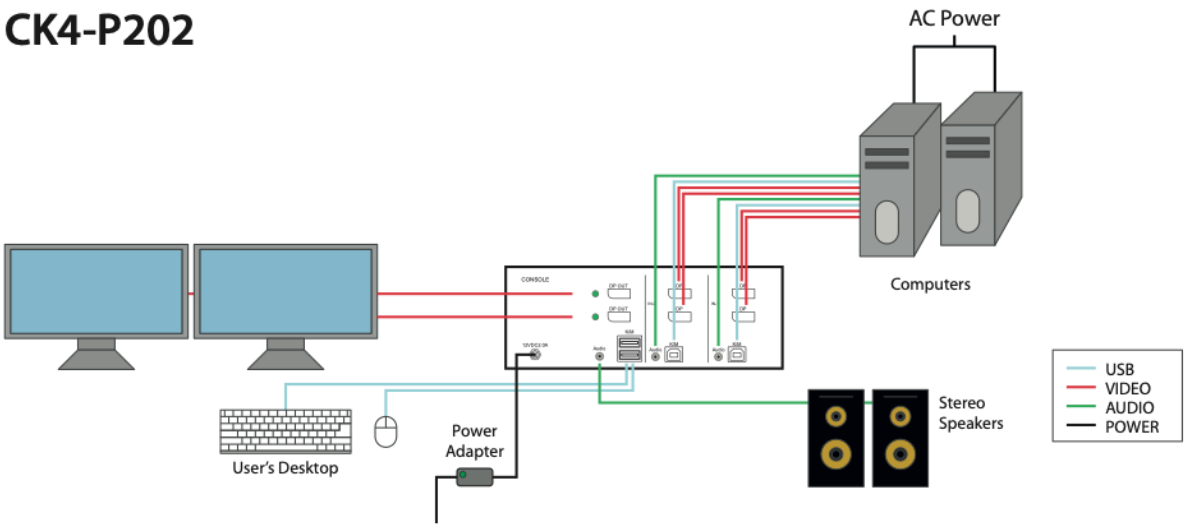

Figure 1: Standard Setup of 2-Port KVM TOE Installation

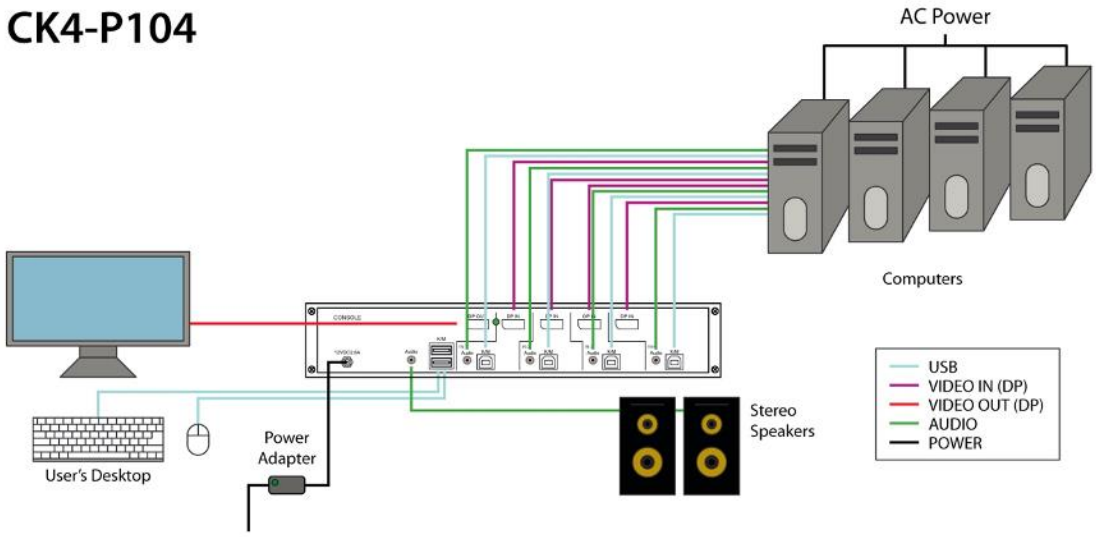

Figure 2: Standard Setup of 4-Port TOE installation

1.7.2 Environment

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

Component	Part Number (P/N)	Description
Each device listed in Tables 5, 6, and 7 above.	Same as model number	TOE Hardware
Sekuryx KVM Cables	CB-5021	KVM/KM Cable (1.8 m), USB Type-A to USB Type-B*
	CB-5022	KVM/KM Cable (1.8 m), Audio out, 3.5mm*
	CB-5050	KVM Cable (1.8 m), DP to DP, USB A to USB B*

Table 18 – TOE Components

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

Component	Description
Standard USB Mouse	Shared Peripheral Hardware
Standard USB Keyboard	Shared Peripheral Hardware
Standard Computer Display(s)	Shared Peripheral Hardware
Audio Device (Speakers: supports 3.5mm connector)	Shared Peripheral Hardware
Standard PC, Server, portable computer or thin client running any operating system	Connected Computer(s)

Table 19 – Environment Components

1.8 Guidance Documents

User manuals for each TOE model and an administrative guide are available for download via the following link: https://sekuryx.com/documents-niap4/. The following documents on the page are relevant to the TOE:

- Sekuryx Secure KVM Administration and Security Management Tool Guide (Non-CAC), Version 1.0, April 6, 2021
- User Manual Sekuryx Secure DP KVM Switch with CAC Port and 4K Ultra-HD Support, Revision 1.0, July 21, 2021

Note that the User Manual references both “CAC” and “Non-CAC” models. For this evaluation, Non-CAC models should be referenced, and so all discussion in the referenced document applies to the TOE except for that relating to the physical CAC port and its logical operation.

1.9 Features Outside of TOE Evaluation Scope

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

There are no items excluded from the TOE.

2 Security Problem Description

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

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

2.1 Assumptions

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

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

PP-Module for Video/Display Devices	
A.NO_SPECIAL_ANALOG_CAPABILITIES	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, or analog video capture function.

Table 20 – Assumptions

2.2 Organizational Security Policies

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

2.3 Threats

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

Threat	Definition
Protection Profile for Peripheral Sharing Device	
T.DATA_LEAK	A connection via the PSD between one or more computers may allow unauthorized data flow through the PSD or its connected peripherals.
T.SIGNAL_LEAK	A connection via the PSD between one or more computers may allow unauthorized data flow through bit-by-bit signaling.
T.RESIDUAL_LEAK	A PSD may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer.
T.UNINTENDED_USE	A PSD may connect the user to a computer other than the one to which the user intended to connect.
T.UNAUTHORIZED_DEVICES	The use of an unauthorized peripheral device with a specific PSD peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSD or its connected computers.
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 or data stored in the PSD's volatile or non-volatile memory to allow unauthorized information flows.
T.PHYSICAL_TAMPER	A malicious user or human agent could physically modify the PSD to allow unauthorized information flows.

T.REPLACEMENT	A malicious human agent could replace the PSD during shipping, storage, or use with an alternate device that does not enforce the PSD security policies.
T.FAILED	Detectable failure of a PSD may cause an unauthorized information flow or weakening of PSD security functions.
PP-Module for Analog Audio Output Devices	
T.MICROPHONE_USE	A malicious agent could use an unauthorized peripheral device such as a microphone, connected to the TOE audio out peripheral device interface to eavesdrop or transfer data across an air-gap through audio signaling.
T.AUDIO_REVERSED	A malicious agent could repurpose an authorized audio output peripheral device by converting it to a low-gain microphone to eavesdrop on the surrounding audio or transfer data across an air-gap through audio signaling.
PP-Module for Keyboard/Mouse Devices	
PP-Module for Video/Display Devices	

Table 21 – Threats

3 Security Objectives

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

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

3.1 Security Objectives for the TOE

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

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

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

O.UNIDIRECTIONAL_INPUT	The TOE shall enforce unidirectional keyboard and/or mouse device's data flow from the peripheral device to only the selected computer.
PP-Module for Video/Display Devices	
O.PROTECTED_EDID	The TOE shall read the connected display Extended Display Identification Data (EDID) once during the TOE power up or reboot sequence and prevent any EDID channel write transactions that connected computers initiate.
O.UNIDIRECTIONAL_VIDEO	The TOE shall enforce unidirectional video data flow from the connected computer video interface to the display interface only.

Table 22 – Security Objectives for the TOE

3.2 Security Objectives for the Operational Environment

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

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

PP-Module for Video/Display Devices	
OE.NO_SPECIAL_ANALOG_CAPABILITIES	The operational environment will not have special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, or a component with digital signal processing or analog video capture functions.

Table 23 – Security Objectives for the Operational Environment

4 Security Requirements

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

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

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

4.1 TOE Security Functional Requirements

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

4.1.1 Overview

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

The SFRs have been replicated below for clarity. Table 24 below displays the SFR IDs, their names, and where they originate from.

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

FDP_IPC_EXT.1	Internal Protocol Conversion	Video/Display Module (selection-based)
FDP_PDC_EXT.1	Peripheral Device Connection	PSD PP (mandatory)
FDP_PDC_EXT.2/AO	Peripheral Device Connection (Audio Output)	Audio Output Module (mandatory)
FDP_PDC_EXT.2/KM	Authorized Devices (Keyboard/Mouse)	Keyboard/Mouse Module (mandatory)
FDP_PDC_EXT.2/VI	Peripheral Device Connection (Video Output)	Video/Display Module (mandatory)
FDP_PDC_EXT.3/KM	Authorized Connection Protocols (Keyboard/Mouse)	Keyboard/Mouse Module (mandatory)
FDP_PDC_EXT.3/VI	Authorized Connection Protocols (Video Output)	Video/Display Module (mandatory)
FDP_PUD_EXT.1	Powering Unauthorized Devices	Audio Output Module (mandatory)
FDP_RIP.1/KM	Residual Information Protection (Keyboard Data)	Keyboard/Mouse Module (selection-based)
FDP_RIP_EXT.1	Residual Information Protection	PSD PP (mandatory)
FDP_RIP_EXT.2	Purge of Residual Information	PSD PP (optional)
FDP_SPR_EXT.1/DP	Sub-Protocol Rules (DisplayPort Protocol)	Video/Display Module (selection-based)
FDP_SWI_EXT.1	PSD Switching	PSD PP (mandatory)
FDP_SWI_EXT.2	PSD Switching Methods	PSD PP (selection-based)
FDP_SWI_EXT.3	Tied Switching	Keyboard/Mouse Module (selection-based)
FDP_UDF_EXT.1/AO	Unidirectional Data Flow (Audio Output)	Audio Output Module (mandatory)
FDP_UDF_EXT.1/KM	Unidirectional Data Flow (Keyboard/Mouse)	Keyboard/Mouse Module (mandatory)
FDP_UDF_EXT.1/VI	Unidirectional Data Flow (Video Output)	Video/Display Module (mandatory)

FIA_UAU.2	User Authentication Before Any Action	PSD PP (optional)
FIA_UID.2	User Identification Before Any Action	PSD PP (optional)
FMT_MOF.1	Management of Security Functions Behavior	PSD PP (optional)
FMT_SMF.1	Specification of Management Functions	PSD PP (optional)
FMT_SMR.1	Security Roles	PSD PP (optional)
FPT_FLS_EXT.1	Failure with Preservation of Secure State	PSD PP (mandatory)
FPT_NTA_EXT.1	No Access to TOE	PSD PP (mandatory)
FPT_PHP.1	Passive Detection of Physical Attack	PSD PP (mandatory)
FPT_PHP.3	Resistance to Physical Attack	PSD PP (optional)
FPT_STM.1	Reliable Time Stamps	PSD PP (optional)
FPT_TST.1	TSF Testing	PSD PP (mandatory)
FPT_TST_EXT.1	TSF Testing	PSD PP (mandatory)
FTA_CIN_EXT.1	Continuous Indications	PSD PP (selection-based)

Table 24 – TOE SFR Overview

4.1.2 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the audit functions;
b. All auditable events for the [*not specified*] level of audit; and
c. [*administrator login, administrator logout, self-test failures, peripheral device acceptance and rejections, [all administrative functions claimed in FMT_MOF.1 and FMT_SMF.1]*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

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

4.1.3 Class FDP: User Data Protection

FDP_AFL_EXT.1 Audio Filtration

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

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

Table 25 – Audio Filtration Specifications

FDP_APC_EXT.1/AO Active PSD Connections (Audio Output)

FDP_APC_EXT.1.1/AO The TSF shall route user data only from the interfaces selected by the user.

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

FDP_APC_EXT.1.3/AO The TSF shall ensure that no data transits the TOE when the TOE is powered off.

FDP_APC_EXT.1.4/AO The TSF shall ensure that no data transits the TOE when the TOE is in a failure state.

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

FDP_APC_EXT.1/KM Active PSD Connections (Keyboard/Mouse)

FDP_APC_EXT.1.1/KM The TSF shall route user data only to the interfaces selected by the user.

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

FDP_APC_EXT.1.3/KM The TSF shall ensure that no data transits the TOE when the TOE is powered off.

FDP_APC_EXT.1.4/KM The TSF shall ensure that no data transits the TOE when the TOE is in a failure state.

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

FDP_APC_EXT.1/VI Active PSD Connections (Video/Display)

FDP_APC_EXT.1.1/VI The TSF shall route user data only from the interfaces selected by the user.

FDP_APC_EXT.1.2/VI The TSF shall ensure that no data **or electrical signals** flow between connected computers whether the TOE is powered on or powered off.

FDP_APC_EXT.1.3/VI The TSF shall ensure that no data transits the TOE when the TOE is powered off.

FDP_APC_EXT.1.4/VI The TSF shall ensure that no data transits the TOE when the TOE is in a failure state.

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

FDP_CDS_EXT.1 Connected Displays Supported

FDP_CDS_EXT.1.1 The TSF shall support [one connected display **for TOE models with CK4-10X model names**, multiple connected displays **for all other TOE models**] at a time.

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

FDP_FIL_EXT.1.1/KM The TSF shall have [fixed] device filtering for [keyboard, mouse] interfaces.

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

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

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

FDP_IPC_EXT.1 Internal Protocol Conversion[1]

FDP_IPC_EXT.1.1 The TSF shall convert the [*DisplayPort*] protocol at the [*DisplayPort computer video interface*] into the [*HDMI*] protocol within the TOE.

FDP_IPC_EXT.1.2 The TSF shall output the [*HDMI*] protocol from inside the TOE to [*peripheral display interface(s)*] as [*[DisplayPort] protocol*].

FDP_PDC_EXT.1 Peripheral Device Connection

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

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

FDP_PDC_EXT.1.3 The TOE shall have no external interfaces other than those claimed by the TSF.

FDP_PDC_EXT.1.4 The TOE shall not have wireless interfaces.

FDP_PDC_EXT.1.5 The TOE shall provide a visual or auditory indication to the User when a peripheral is rejected.

FDP_PDC_EXT.2/AO Peripheral Device Connection (Audio Output)

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

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

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

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

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

[1] As modified by NIAP TD0586

- authorized devices presenting authorized interface protocols as defined in the PP-Module for Video/Display Devices

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

FDP_PDC_EXT.2/KM Peripheral Device Connection (Keyboard/Mouse)

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

- authorized devices as defined in the PP-Module for Audio Output Devices,
- authorized devices as defined in the PP-Module for Video/Display Devices

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

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

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

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

FDP_PDC_EXT.2/VI Peripheral Device Connection (Video Output)

FDP_PDC_EXT.2.1/VI The TSF shall allow connections with authorized devices as defined in [*Appendix E **of the Video/Display Devices Module***] and [

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

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

FDP_PDC_EXT.2.2/VI The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*Appendix E **of the Video/Display Devices Module***] and [

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

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

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

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

FDP_PDC_EXT.3.1/KM The TSF shall have interfaces for the [USB (keyboard), USB (mouse)] protocols.

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

FDP_PDC_EXT.3/VI Authorized Connection Protocols (Video Output)

FDP_PDC_EXT.3.1/VI The TSF shall have interfaces for the [DisplayPort] protocols.

FDP_PDC_EXT.3.2/VI The TSF shall apply the following rules to the supported protocols: [*the TSF shall read the connected display EDID information once during power-on or reboot*].

FDP_PUD_EXT.1 Powering Unauthorized Devices

FDP_PUD_EXT.1.1 The TSF shall not provide power to any unauthorized device connected to the analog audio peripheral interface.

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

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

FDP_RIP_EXT.1 Residual Information Protection

FDP_RIP_EXT.1.1 The TSF shall ensure that no user data is written to TOE non-volatile memory or storage.

FDP_RIP_EXT.2 Purge of Residual Information

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

FDP_SPR_EXT.1/DP Sub-Protocol Rules (DisplayPort Protocol)

FDP_SPR_EXT.1.1/DP The TSF shall apply the following rules for the [*DisplayPort*] protocol:

- block the following video/display sub-protocols:
  - [*CEC,*
  - *EDID from computer to display,*
  - *HDCP,*
  - *MCCS*]
- allow the following video/display sub-protocols:
  - [*EDID from display to computer,*
  - *HPD from display to computer,*
  - *Link Training*].

FDP_SWI_EXT.1 PSD Switching

FDP_SWI_EXT.1.1 The TSF shall ensure that [switching can be initiated only through express user action].

FDP_SWI_EXT.2 PSD Switching Methods

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

FDP_SWI_EXT.2.2 The TSF shall ensure that switching can be initiated only through express user action using [console buttons].

FDP_SWI_EXT.3 Tied Switching

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

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

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

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

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

FDP_UDF_EXT.1/VI Unidirectional Data Flow (Video Output)

FDP_UDF_EXT.1.1/VI The TSF shall ensure [*video*] data transits the TOE unidirectionally from the [*TOE computer video*] interface to the [*TOE peripheral device display*] interface.

4.1.4 Class FIA: Identification and Authentication

FIA_UAU.2 User Identification before Any Action

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

FIA_UID.2 User Identification before Any Action

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

4.1.5 Class FMT: Security Management

FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [*modify the behavior of*] the functions [*administrator authentication, dump log, restore factory default, terminate session*] to [*the authorized administrators*].

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TOE shall be capable of performing the following management functions: [*change administrator access credential, dump log, restore factory default, terminate session*].

FMT_SMR.1 Security Roles

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

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

4.1.6 Class FPT: Protection of the TSF

FPT_FLS_EXT.1 Failure with Preservation of Secure State

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

FPT_NTA_EXT.1 No Access to TOE

FPT_NTA_EXT.1.1 TOE firmware, software, and memory shall not be accessible via the TOE's external ports, with the following exceptions: [the Extended Display Identification Data (EDID) memory of Video TOEs may be accessible from connected computers; the configuration data, settings, and logging data that may be accessible by authorized administrators].

FPT_PHP.1 Passive Detection of Physical Attack

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

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

FPT_PHP.3 Resistance to Physical Attack[2]

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

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

FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

FPT_TST.1 TSF Testing

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

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

[2] As modified by NIAP TD0583

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

FPT_TST_EXT.1 TSF Testing

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

4.1.7 Class FTA: TOE Access

FTA_CIN_EXT.1 Continuous indications

FTA_CIN_EXT.1.1 The TSF shall display a visible indication of the selected computers at all times when the TOE is powered.

FTA_CIN_EXT.1.2 The TSF shall implement the visible indication using the following mechanism: a panel with lights.

Application Note: *The selected computer is indicated with a panel with lights that corresponds to the computer selection buttons.*

FTA_CIN_EXT.1.3 The TSF shall ensure that while the TOE is powered the current switching status is reflected by [multiple indicators which never display conflicting information].

4.2 Rationale for TOE Security Requirement Dependencies

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

- FDP_RDR_EXT.1 (from Keyboard/Mouse Module) – this is an optional SFR that the TSF does not claim to address.
- FDP_SPR_EXT.1/DVI-D (from Video/Display Devices Module) – this is a selection-based SFR that is only claimed if "DVI-D" is selected in FDP_PDC_EXT.3.1/VI. Because this selection is not made, the SFR is appropriately omitted.
- FDP_SPR_EXT.1/DVI-I (from Video/Display Devices Module) – this is a selection-based SFR that is only claimed if "DVI-I" is selected in FDP_PDC_EXT.3.1/VI. Because this selection is not made, the SFR is appropriately omitted.
- FDP_SPR_EXT.1/HDMI (from Video/Display Devices Module) – this is a selection-based SFR that is only claimed if "HDMI" is selected in FDP_PDC_EXT.3.1/VI. Because this selection is not made, the SFR is appropriately omitted.
- FDP_SPR_EXT.1/USB (from Video/Display Devices Module) – this is a selection-based SFR that is only claimed if "USB Type-C with DisplayPort as alternate function" is selected in FDP_PDC_EXT.3.1/VI. Because this selection is not made, the SFR is appropriately omitted.
- FDP_SPR_EXT.1/VGA (from Video/Display Devices Module) – this is a selection-based SFR that is only claimed if "VGA" is selected in FDP_PDC_EXT.3.1/VI. Because this selection is not made, the SFR is appropriately omitted.

In all cases, the omitted SFRs have been excluded from the TSF because they refer to conditional functionality where the TOE did not satisfy the required condition or to optional functionality that may be excluded at the TOE developer's discretion.

4.3 TOE Security Assurance Requirements

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

Assurance Class	Assurance Component ID	Assurance Components Description
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent Testing – Conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Survey

Table 26 – TOE Security Assurance Requirements

5 Conformance Claims

The following section describes the ST Conformance Claims.

5.1 CC Conformance Claims

This ST is compliant with the following CC documents:

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

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

5.2 PP Conformance Claims

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

1. TD0506 - Missing Steps to disconnect and reconnect display, published date 02/28/2020
2. TD0507 - Clarification on USB plug type, published date 03/03/2020
3. TD0514 - Correction to MOD_VI FDP_APC_EXT.1 Test 3 Step 6, published date 05/18/2020
4. TD0518 - Typographical error in Dependency Table, published date 06/15/2020
5. TD0539 - Incorrect selection trigger in FTA_CIN_EXT.1 in MOD_VI_V1.0, published date 07/11/2020
6. TD0557 - Correction to Audio Filtration Specification Table in FDP_AFL_EXT.1, published date 12/08/2020
7. TD0583 – FPT_PHP.3 modified for PSD remote controllers, published date 05/12/2021
8. TD0584 - Update to FDP APC_EXT.1 Video Tests, published date 04/29/2021
9. TD0585 - Update to FDP_APC_EXT.1 Audio Output Tests, published date 04/29/2021
10. TD0586 - DisplayPort and HDMI Interfaces in FDP_IPC_EXT.1, published date 05/11/2021
11. TD0593 - Equivalency Arguments for PSD, published date 06/03/2021

5.3 ST Conformance Requirements

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

The mandatory requirements of the PP and all PP-Modules contained within the PP-Configuration are met. The ST is an instantiation of the claimed PP-Configuration. Additionally, optional

requirements from these materials are claimed as needed and selection-based requirements are claimed where required. The ST does not omit any mandatory requirements, nor does it define or claim any requirements that are not defined in any of the components of the claimed PP-Configuration.

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

6 TOE Summary Specification

This section summarizes the security functions of the TOE and the subsequent Assurance Measures taken to ensure their proper implementation. See Table 24 in Section 4 for the entire list of SFRs that address the security objectives for this TOE. These objectives will be broken down in the subsequent sections for further detail.

6.1 TOE External Interfaces Security Functions

[O.NO_OTHER_EXTERNAL_INTERFACES]: FDP_PDC_EXT.1
[O.REJECT_UNAUTHORIZED_PERIPHERAL]: FDP_PDC_EXT.1
[O.REJECT_UNAUTHORIZED_ENDPOINTS]: FDP_PDC_EXT.1
The TOE only supports AC/DC power, USB keyboard and mouse, KVM video (DP 1.2 in/DP 1.2 out), and analog audio output devices. All other peripheral types are rejected, either physically (because the TOE does not support the required physical interface) or logically (because the TOE does not recognize the connected peripheral as authorized).

6.2 TOE Administration, User Control, and Monitoring Security Functions

[O.AUTHORIZED_USAGE]: FAU_GEN.1, FDP_SWI_EXT.1, FDP_SWI_EXT.2, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_SMF.1, FMT_SMR.1, FPT_STM.1, FTA_CIN_EXT.1
Each TOE is equipped with Administration and Security Management Tool that can be initiated by running an executable file on a computer with keyboard connected to the same computer via the TOE. The tool requires administrator to be successfully identified and authenticated by name and password in order to gain access to any supported feature. The TOE has a menu-driven interface in which the administrator can initiate the supported functions. See below for descriptions of the supported features.

- Change Admin Access Credentials
  - Updates the username and password for the “admin” account
- Dump Log
  - Prints out the last 100 logs the TOE recorded
- Restore Factory Default
  - Resets the administrator credentials to default settings
- Terminate Session
  - Ends the current administrative tool session

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

The administrator account passwords as well as the name of the account itself can both be changed. The restrictions for each are as follows:

- Minimum 4 characters
- Maximum 8 characters

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

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

There are no switching mechanisms that can be engaged using automatic port scanning, control through a connected computer, or control through keyboard shortcuts. The console buttons are the only available switching mechanisms.

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

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

APU	Administrator Credential Update
ALO	Administrator Log On
ALF	Administrator Log Off
ARM	Arming A/T System
EDL	EDID Learn
LGD	LOG Dump
PWU	Power Up
PWD	Power Down
AFD	Restore Factory Default
RKM	Rejected Keyboard or Mouse
STS	Self-Test
TMP	Device Tampered, Review by MFR only

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

The TOE includes an internal system clock function that is used for time stamps of audit records.

For non-isolator TOE models, the TOE indicates the selected channel using a panel of LEDs that are located directly above the channel selection buttons for the connected computer. When the user presses a channel selection button, the corresponding LED will light up to indicate the selected computer. The channel selection buttons are also backlit. During operation, all front panel LED indications cannot be turned off or dimmed by the user in any way including after Restore Factory

Default (reset). This prevents user confusion of current TOE state.[3] When the TOE has booted successfully, it will default to computer 1 being the selected computer.

[O.LEAK_PREVENTION_SWITCHING]: FDP_SWI_EXT.1, FDP_SWI_EXT.2
All switching mechanisms must be deliberately engaged by the user. There are no mechanisms that allow data intended for the selected computer to be transmitted to a different computer, and there are no interfaces that allow data to be transmitted directly between computers.

6.3 TOE Tampering Protection

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

The TOE is designed so that access to the TOE firmware, software, or its memory via its accessible ports is prevented. No access is available to modify the TOE or its memory. To mitigate the risk that a potential attacker will tamper with a TOE and then reprogram it with altered functionality, the compliant TOE external and internal interfaces are locked for code read and write. The programmable components of the TOE's programming ports are permanently disabled for both read and write operations. The TOE's operational code may not be upgradeable through any of the TOE external or internal ports.

[O.NO_TOE_ACCESS]: FPT_NTA_EXT.1
The TOE is designed to prevent any physical or logical access its internal memory. All TOE microcontrollers run from internally protected flash memory. The TOE firmware is read/write protected, inaccessible by JTAG interfacing, and cannot be modified or updated by any external tools. All firmware is executed on SRAM and protected against external access/modification of code or stacks.

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

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

[O.TAMPER_EVIDENT_LABEL]: FPT_PHP.1
Each TOE has one uniquely labeled front panel holographic tamper evident label (TEL) placed over the boundary between the upper and lower half of the TOE enclosure. The TEL has a recorded unique serial number that is monitored for TOE authentication purposes. Any attempt to access the internals of the TOE will cause permanent visible damage to the TEL.

[O.ANTI_TAMPERING]: FPT_PHP.1 FPT_PHP.3
In addition to the TEL on the front panel, the TOE is physically designed to trigger the anti-tampering system once opened. The TOE enclosure is composed of all-around reinforced stainless steel construction, which shields it from outside intrusion through brute physical force. There is also a

[3] See section 1.6.2.6.3 above for detailed information about Restore Factory Default (reset)

mechanical switch on the inside of the TOE that triggers the anti-tampering state when the enclosure is manually opened.

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

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

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

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

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

6.4 TOE Self-Testing

[O.SELF_TEST]: FPT_TST.1

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

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

Users verify the integrity of the TSF and its data through these mechanisms. All features of the TOE front panel are tested during power up self-testing. From power up until the termination of the TOE self-test, no channel is selected. This ensures no TOE state is enabled to the user until all self tests have been passed. If all self tests are passed, normal operation is indicated audibly through one beep of the internal alarm followed by one pulse of an internal relay. If any self-tests fail, the TOE is temporarily disabled to the extent that all computer and peripheral ports are deactivated, and the

management interface cannot be accessed. The user can reboot the TOE (power off/power on) to attempt to clear the error state.

[O.SELF_TEST_FAIL_TOE_DISABLE]: FPT_FLS_EXT.1, FPT_TST_EXT.1
If a self-testing function does not meet normal operation requirements (failure), the TOE is temporarily disabled until the issue is resolved and the TOE is rebooted (power off/power on). If the unit is permanently defective, then it must be replaced.

[O.SELF_TEST_FAIL_INDICATION]: FPT_TST_EXT.1
If self-testing fails, all front panel LEDs will turn on to indicate self test failure. TOE normal operation is disabled until the issue is resolved and the system is rebooted. When the system passes all self-testing functions, normal operation is indicated by one beep from the internal speaker and one pulse from an internal TOE relay.

6.5 TOE Audio Subsystem Security Functions

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

[O.COMPUTER_INTERFACE_ISOLATION, O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED, O.USER_DATA_ISOLATION, O.PERIPHERAL_PORTS_ISOLATION, O.REJECT_UNAUTHORIZED_PERIPHERAL]: FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1
When the TOE is not powered, an audio isolation relay is opened to isolate the audio input ports from all internal TOE circuitry. The TOE does not supply power to any device connected to the analog audio output interface. Each connected computer has its own isolated stereo audio channel that flows from the connected computer's audio input port to the analog stereo output port of the TOE. The analog audio output interface is the only physical interface for this function; unauthorized peripherals are either physically incompatible or logically incompatible (as is the case with audio input devices).

[O.UNIDIRECTIONAL_AUDIO_OUT]: FDP_AFL_EXT.1, FDP_APC_EXT.1/AO, FDP_UDF_EXT.1/AO
The use of microphones as input devices is prohibited. All TOE devices support analog audio out switching and all TOE devices will prevent microphone devices. These microphones are stopped through the use of uni-directional audio diodes on both left and right stereo channels (forces data flow from only the computer to the connected audio device) and the LM4880 Boomer analog output amplifier which enforces uni-directional audio data flow. All audio signals are filtered in accordance with the Audio Filtration Specifications table (Table 25) above.

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

Furthermore, uni-directional audio diodes are placed in parallel on both right and left stereo channels to ensure uni-directional data flow from the connected computer to the audio analog output port on the TOE which prevents any reverse audio from leaking. Audio data from the connected

peripheral devices to the connected computer is blocked by the audio uni-directional electronic circuit. Only analog audio is supported, all digital audio will be blocked using a dedicated filter. The output signal is limited to range between 45dB and 75dB.

[O.COMPUTER_TO_AUDIO_ISOLATION]: FDP_APC_EXT.1/AO, FDP_UDF_EXT.1/AO
The TOE system controls the audio switching between each connected computer channel using isolated unidirectional audio buses. The TOE audio interface uses a solid state multiplexer and mechanical relays to ensure audio/computer channel isolation.

[O.NO_USER_DATA_RETENTION]: FDP_RIP_EXT.1, FDP_RIP_EXT.2
The TOE audio subsystem does not delay, store, or convert audio data flows. This prevents any audio overflow during switching between isolated audio channels. The Letter of Volatility in Appendix B identifies all non-volatile memory components of the TOE and the data that is stored on them; these components do not store audio data.

[O.SELF_TEST]: FPT_TST.1
[O.SELF_TEST_FAIL_TOE_DISABLE]: FPT_FLS_EXT.1, FPT_TST_EXT.1
[O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE]: FPT_PHP.3 and FPT_FLS.1
If the TOE fails to pass the audio self test or anti-tampering is triggered, the same audio isolation relay is opened to isolate the audio inputs, preventing data leakage.

6.6 TOE Keyboard and Mouse Functionality

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

[O.COMPUTER_INTERFACE_ISOLATION, O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED, O.USER_DATA_ISOLATION, O.PERIPHERAL_PORTS_ISOLATION, O.REJECT_UNAUTHORIZED_ENDPOINTS, O.REJECT_UNAUTHORIZED_PERIPHERAL]: FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_SWI_EXT.3
In order to completely isolate the keyboard and mouse interfacing for all connected computers, host and device emulators are used to control these peripheral interfacings. The host emulator receives serial commands from the USB keyboard and mouse and stores them in SRAM. These commands are sent through the current channel to its respective isolated microcontroller (the device emulator). The TOE device emulator then interacts with its assigned isolated connected computer via USB. Having separate isolated device emulators assures that the connected computers do not have an electrical or logical information channel with the TOE or peripheral devices. External devices connected to the USB KM ports of the TOE cannot be used to supply power to the TOE.

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

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

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

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

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

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

[O.NO_USER_DATA_RETENTION]: FDP_RIP_EXT.1, FDP_RIP_EXT.2, FDP_RIP.1/KM
TOE Non-Volatile Memory is not used to store keyboard and mouse data. All keyboard and mouse commands are stored on Static Random Access Memory (SRAM). Since SRAM is volatile memory, all data is cleared off the stack when the TOE is powered down and during Restore Factory Default. The buffer for keyboard and mouse data is 128 bits and is continuously read and cleared during use.

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

More information about the keyboard/mouse buffer and its clearing, including the physical components responsible for doing this, can be found in Appendix B below. This Appendix also lists

the non-volatile memory components of the TOE and the data that is stored on them to show that the TOE does not store user data in non-volatile memory.

[O.EMULATED_INPUT]: FDP_PDC_EXT.2/KM, FDP_PDC_EXT.3/KM
Isolated host/device emulators are used to interact with the serial commands sent via keyboard and mouse over USB. The host emulator receives a serial data stream from the tied keyboard and mouse peripherals. This data is passed through a peripheral data diode, optical isolator, and a mechanical relay to the device emulator. This prevents any type of bi-directional communication between the keyboard/mouse and the connected computers.

[O.UNIDIRECTIONAL_INPUT]: FDP_UDF_EXT.1/KM
To ensure uni-directional data flow, data diodes, optical isolators, and mechanical relays are placed in series between the TOE host emulators and device emulators. Each isolated device emulator has its own respective diode, optical isolator and relay to assure electrical/logical data isolation from other data channels and other TOE functions. This can be seen in the TOE by observing the embedded keyboard LEDs of CAPS, Num, and Scroll Lock. When connected to the computer through the TOE, these indicators are not functional as this data is not able to pass between the TOE and the computer and vie-versa. Thus, the use of these embedded keyboard LEDs is not supported by the TOE.

[O.SELF_TEST]: FPT_TST.1
[O.SELF_TEST_FAIL_TOE_DISABLE]: FPT_FLS_EXT.1, FPT_TST_EXT.1
[O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE]: FPT_PHP.3 and FPT_FLS.1
When the TOE is not powered, an isolation relay is opened to isolate the KM input ports from all internal TOE circuitry. If the TOE fails to pass the KM self test or anti-tampering is triggered, the same isolation relay is opened to isolate the KM inputs, preventing data leakage. All stored keyboard and mouse information is erased from the TOE.

6.7 TOE Video Subsystem Security Functions

The TOE enforces requirements for data isolation and peripheral authorization for the video interface.

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

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

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

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

The TOE indicates current EDID read/write processes to the user by flashing the front panel's LEDs. Port one green and push button blue LEDs will both begin to flash for about 10 seconds. When the LEDs stop flashing, the EDID data has been read by the processor and has been written to all EDID emulators for each connected computer video channel. If the TOE has more than one video board (in the case of dual-head models), then the TOE will continue to read/write the EDIDs of the connected

monitors and indicate the progress of the process by flashing the next port selections green and push button blue LEDs respectively. Table 27 below shows a time estimate for EDID read/write for all TOE models.

	Single Head	Dual Head
2-Port	10	20
4-Port	10	20
8-Port	10	20

Table 27 – EDID Read/Write Time Chart

EDID READ

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

EDID Write

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

Normal Operation

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

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

[O.COMPUTER_INTERFACE_ISOLATION, O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED, O.USER_DATA_ISOLATION, O.PERIPHERAL_PORTS_ISOLATION]: FDP_APC_EXT.1/VI

Each connected computer has its own TOE isolated channel with its own EDID emulator and video input port. Data flows from the input video source through its respective EDID emulator and out of the monitor display port. Each video input interface is isolated from one another using different EDID ICs, power planes, ground planes, and electronic components in each independent channel.

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

[O.REJECT_UNAUTHORIZED_PERIPHERAL]: FDP_PDC_EXT.1, FDP_PDC_EXT.2/VI

To ensure the EDID signal cannot be used to transfer unauthorized data, the TOE has the following limitations on EDID:

- The EDID is only learned on power up of the TOE and only from the display.
- During the learning process, all EDID signals are disconnected from the computers and the computers all have hot plug disabled.
- Each computer has a dedicated EEPROM for storing the EDID data. This EEPROM is limited to be Read-Only by the computer and has only 256 bytes of storage, the computer cannot edit it and it can be read only using the protocol of the EDID with its limitations.
- When the learning process is complete, each computer is connected to the Read-Only EDID flash memory. The reading is initiated by the computer after the TOE has completed the learning and programming of the flashes to all the computer ports.
- The transition of the Hotplug signal from "disabled" during learning process triggers the computer to read from the dedicated flash memory of the TOE through the DDC.
- For each supported display protocol, the TOE permits communication of EDID and HPD information from display to computer.

All TOE models support DP 1.2 video input and output. The TOE will convert the DP signal to HDMI inside the TOE. This signal is then converted back to DisplayPort for output to console display. The TOE rejects communication of EDID information from computer to display, as well as CEC, HDCP, and MCCS communications. Link Training is allowed for the DisplayPort interface.

[O.AUTHORIZED_USAGE]: FDP_CDS_EXT.1
The TOE supports connected displays from a single source video feed (either single-head or dual-head). Because of this, the single selected source video feed is always the same channel as all other peripherals, and indication of the selected channel is indicated through the channel selection LEDs on the TOE chassis. This functionality relates to unauthenticated users operating the TOE so it does not relate to the portion of the O.AUTHORIZED_USAGE objective that is satisfied by the administration capability described in section 6.2 above.

[O.UNIDIRECTIONAL_VIDEO]: FDP_UDF_EXT.1/VI
For each supported video protocol, the TOE forces native Analog video data (red, green, and blue channels) and TMDS digital video data (1 Clock signal, red, green, blue channels) to unidirectional flow from the switched computer to the connected display device (or devices, if the TOE supports dual-head and multiple displays are connected to the TOE's console ports).

[O.SELF_TEST]: FPT_TST.1
[O.SELF_TEST_FAIL_TOE_DISABLE]: FPT_FLS_EXT.1, FPT_TST_EXT.1
[O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE]: FPT_PHP.3 and FPT_FLS.1
When TOE is unpowered, all video signals are isolated electrically and logically from the TOE. If the TOE anti-tampering is triggered or TOE self-testing has failed, the same video signal isolation occurs inside the TOE. The emulated EDID EEPROMs are still powered by their respective computers, but cannot communicate with the TOE due to hardware component isolation.

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

[O.NO_USER_DATA_RETENTION]: FDP_RIP_EXT.1
No data is stored by the TOE in regards to user video data (as opposed to EDID data that is used to interface with a connected video peripheral). The Letter of Volatility in Appendix B identifies all

non-volatile memory components of the TOE and the data that is stored on them; these components do not store buffered video data.

[O.REJECT_UNAUTHORIZED_PERIPHERAL]: FDP_PDC_EXT.1, FDP_PDC_EXT.2/VI, FDP_PDC_EXT.3/VI, FDP_IPC_EXT.1, FDP_SPR_EXT.1/DP
The TOE rejects unauthorized video peripherals through the physical port and filtering of video signals received. Physically, the TOE will only accept a video connector which fits specifications of the unit, which is DisplayPort for P models. The connectors that are not for the specified unit will not be able to connect and send signals to the TOE. The Pin out for each video interface is different which ensures that no other physical connector can be used. The video signals themselves are also ensured to adhere to the specifications. A VGA signal, for example, is analog and cannot be read by the digital standard of DisplayPort. The TMDS signal of HDMI and DVI cannot be read by the DisplayPort interface. The power level and the HPD signal for the various connections are also different across the board which will reduce any risk. Another thing to note the PC in the system is specifically an input device and can only receive certain signals from the monitor. On top of these obstructions, the TSF ensures that any signal which does not match the protocol of the intended video signal depending on the device, will be completely ignored by the TOE.

The DisplayPort AUX channel between the PC and the monitor is completely disconnected. The AUX channel from the computer is connected to an internal FPGA that simulates a monitor. The simulated AUX is preloaded in the FPGA during manufacturing and can never be changed.

[O.PROTECTED_EDID]: FDP_PDC_EXT.2/VI, FDP_SPR_EXT.1/DP
The TOE video subsystem prevents MCCS write commands through independent, read only emulated EDID EEPROMs. The TOE processor reads the EDID data from the monitor and then individually writes this EDID data to the emulator during power up. All changes in display after the EDID read/write process are ignored. There are switches in the internal circuitry to prevent the connected computer from writing to its EDID emulator. The TOE will reject invalid EDID display devices, regardless of which physical device types are supported by the particular TOE model.

Appendix A – Product's Model Name Structure

KVM

XXX-	XXX	X	XX
CK4 = CyberKVM NIAP 4.0	P=DP	1=Single Head	02=2 Port
		2=Dual Head	04=4 Port
			08=8 Port

Appendix B – Letter of Volatility

Main PCBA: USB

Device: Controller Board Main MCU - ATxmega256A3U-AU
Manufacturer: Atmel
Type: Microcontroller

Functions:
The Controller Board Main MCU is responsible for controlling the operations of the USB, Keyboard and Mouse, and front panel board. It also is responsible for communications with the Video board. No other source can independently power the Controller Board Main MCU other than the TOE.

Memory type:

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

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

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

Device: Emulation MCU - PIC18F25J50-I/SS
Manufacturer: Microchip
Type: Microcontroller

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

Memory type:

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

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

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

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

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

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

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

Memory Type:

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

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

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

Video PCBA: DP

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

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

Memory type:

1. Flash Firmware 2KB EEPROM, 64KB Programmable Flash (non-volatile):
    - All Video Board Main MCU firmware that controls its operation is saved in its own dedicated firmware flash block. This firmware cannot be changed by any user or programmer. Video Board Main MCU firmware is erased if anti-tampering is triggered.
2. SRAM (volatile):
    - The Video Board Main MCU uses SRAM memory to run the entire video board during TOE operation. The SRAM is erased as soon as the external power supply is disconnected. All SRAM is erased if anti-tampering is triggered. No user data is stored inside the SRAM when the power is disconnected from the TOE, or if anti-tampering has been triggered.

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

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

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

Memory - Atmel - AT24C04C-SSHM-T or Microchip - 24LC04B-I/SN (non-volatile):

- SERIAL 4KBIT 400KHZ EEPROM
- The EDID EEPROM is 4K bit electrically erasable
- Programmable memory (EEPROM), organized as 512 x 8 bits.

Memory - Atmel - AT24C08C-SSHM-T or Microchip - 24LC08B-I/SN (non-volatile):

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

When the Restore Factory Default operation is performed, all the EDID information stored in the local memory is erased and brought to its initial state. After first operation, the TOE will detect a new display, all computers will be disconnected, and the TOE will learn the new display, store in its EDID memory for each computer.

Front Panel PCBA

The front panel board has no ROM or RAM functionality.