BAE Systems

Secure KVM Gen2 8560943-2

Security Target

Version 1.0

2023-01-10

Prepared for:

BAE Systems
450 Pulaski Road
Greenlawn, NY 11740

Prepared by:

Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
Columbia, Maryland 21046

Not Export Controlled per: ES-C4ISR-092722-0182

Revision History		
Version	**Author**	**Modifications**
0.1	Leidos	Initial Version
0.2	Leidos	Incorporated additional information from BAE Systems
0.3	Leidos/BAE Systems	Added additional details on self-tests and part numbers
0.4	Leidos/BAE Systems	Clarifications and additional details added
1.0	Leidos/BAE Systems	Updated for submission based on internal review

Table of Contents

List of Figures and Tables

1 Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is BAE Systems Secure KVM Gen2.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements(Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8)

1.1 Security Target, Target of Evaluation, and Common Criteria Identification

ST Title: BAE Systems Secure KVM Gen2, 8560943-2 Security Target

ST Version: Version 1.0

ST Date: 2023-01-10

Target of Evaluation (TOE) Identification: BAE Systems Secure KVM Gen2, 8560943-2 consisting of the following:

- 3 transmitter (Tx) modules: BAE Systems PN 8561040-5, -6, -7; Top level firmware/software version 2.1 (same for each dash number)
- Receiver module (Rx): BAE Systems PN 8561038-2; Top level firmware/software version 2.1
- Optical Switch Assembly: BAE Systems PN 8561041-2
    - Optical Switch Circuit Card Assembly: BAE Systems PN 8552755-1; Firmware/software version 97453A
    - Power Distribution Board: BAE Systems PN 8583117-1; Contains no firmware/software
- Keyboard: BAE Systems PN 8552758-2; Firmware/software version 755604B, 625679B (contains wired remote control for the TOE channel selection mechanism and status indicators which is locally separate from the USB HID keyboard but contained in the same physical chassis)
- Power Control Panel: BAE Systems PN 8561142-2: Contains no firmware/software

TOE Developer: BAE Systems

Evaluation Sponsor: BAE Systems

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1 Revision 5, April 2017
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1 Revision 5, April 2017
  - Part 3 Conformant

This ST and the TOE it describes claims exact conformance to the *PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and Video/Display Devices*, version 1.0, 19 July 2019 [CFG-KM-VI], which includes the following Protection Profile and PP-Modules:

- *Protection Profile for Peripheral Sharing Device*, Version 4.0, 19 July 2019 [PSD], including the following optional and selection-based SFRs: FDP_SWI_EXT.2, and FTA_CIN_EXT.1.
- *PP-Module for Keyboard/Mouse Devices*, Version 1.0, 19 July 2019 [MOD-KM], including the following optional and selection-based SFRs: FDP_FIL_EXT.1/KM, FDP_RIP.1/KM, and FDP_SWI_EXT.3.
- *PP-Module for Video/Display Devices*, Version 1.0, 19 July 2019 [MOD-VI], including the following selection-based SFRs: FDP_CDS_EXT.1, FDP_IPC_EXT.1, and FDP_SPR_EXT.1/DP.

The following NIAP Technical Decisions are applicable to the claimed Protection Profile and Modules:

- TD0686 – DisplayPort CEC Testing
- TD0620 – EDID Read Requirements
- TD0593 – Equivalency Arguments for PSD
- TD0586 – DisplayPort and HDMI Interfaces in FDP_IPC_EXT.1
- TD0584 – Update to FDP APC_EXT.1 Video Tests
- TD0583 – FPT_PHP.3 modified for PSD remote controllers
  This TD is not applicable to the TOE because the TOE does not claim FPT_PHP.3.
- TD0539 – Incorrect Selection Trigger in FTA_CIN_EXT.1 in MOD_VI_V1.0
  The TOE does not fit the Combiner Use Case so this TD is not applicable to the TOE.
- TD0518 – Typographical Error in Dependency Table
- TD0514 – Correction to MOD_VI FDP_APC_EXT.1 Test 3 Step 6
- TD0507 – Clarification on USB Plug Type
- TD0506 – Missing Steps to Disconnect and Reconnect Display

1.3 Conventions

The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, with additional extended functional components.

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections, iterations, and refinements. This document retains all operations completed by the PP author (i.e. selections/assignments they already filled out). These are formatted as italicized text.

This document uses the following font conventions to identify iterations, extended SFRs and operations performed by the ST author:

- **Refinement** operation (denoted by **bold text** and underline) is used to add details to a requirement, and thus further restricts a requirement.
- **Selection** operation (denoted by italicized ***bold*** text): is used to select one or more options provided by the [CC] in stating a requirement. Selection operations completed in the PP are shown in brackets.
- **Assignment** operation (denoted by **bold** text) is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment. Assignments within Selections are denoted by italicized ***bold*** text).
- **Iteration** operation is identified with a slash ('/') and an identifier (e.g. "/KM"). Additional iterations made by the ST author are identified with an identifier within parenthesis (e.g. "(DP)").
- **Extended** SFRs are identified by having a label "EXT" after the SFR name.

1.3.1 Terminology

Table 1: Terms and Definitions

Term	Definition
Assurance	Grounds for confidence that a TOE meets the SFRs.
Authorized Peripheral	A Peripheral Device that is both technically supported and administratively permitted to have an active interface with the PSD.
Combiner (multi-viewer)	A PSD with video integration functionality that is used to simultaneously display output from multiple personal computers (PCs).
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
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.
Display	A device that visually outputs user data, such as a monitor.
Interface	A shared boundary across which two or more Devices exchange information through a Connection.

Term	Definition
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 Interface	The PSD's physical receptacle or port for connecting to a Peripheral Device.
Peripheral/Peripheral Device	A Device with access that can be Shared or Filtered by a PSD.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
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.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	Implementation-independent documentation that describes a TOE, its Operational Environment, and its claimed security functionality.
Selected Computer	A Connected Computer that has Active Interfaces with the PSD.
Supported Peripheral	A Peripheral Device that is technically supported by the PSD.
Target of Evaluation(TOE)	A product or component, consisting of hardware, software, and/or firmware, that claims to implement certain security functionality in a specific and well-defined manner.
TOE Security Functionality (TSF)	The combined hardware, software, and firmware capabilities of a TOE that are responsible for implementation of its claimed SFRs.
TOE Security Functionality Interface (TSFI)	Any external interface between the TOE and its Operational Environment that has a security-relevant purpose or is used to transmit security-relevant data.
TOE Summary Specification (TSS)	Documentation contained within the Security Target that provides the reader with a description of how the TOE implements the claimed SFRs.
User	A person that interacts with a PSD (or a process or mechanism acting on behalf of a person).
User Authentication Device	A Peripheral Device that is used to affirm the identity of a User attempting to authenticate to a computer (e.g., smart card reader, biometric authentication device, proximity card reader).

Term	Definition
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)

1.3.2 Acronyms

Table 2: Acronyms

Acronym	Definition
ARC	Audio Return Channel
AUX	Display Port Auxiliary Channel
BIT	Built-in Test
CAC	Common Access Card
CCA	The TOE's Optical Switch Circuit Card Assembly
CEC	Consumer Electronics Control
DVI	Digital Visual Interface
EDID	Extended Display Identification Data
EEPROM	Electrically Erasable Programmable Read-Only Memory
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
HD	High Definition
HDCP	High-bandwidth Digital Content Protection
HDMI	High Definition Multimedia Interface
HEAC	HDMI Ethernet Audio Control
HEC	HDMI Ethernet Channel
HID	Human Interface Device
HPD	Hot Plug Detect
IT	Information Technology
KVM	Keyboard, Video, and Mouse
LED	Light-Emitting Diode
MCCS	Hot Plug Detect
PC	Personal Computer
PCP	Power Control Panel
PSD	Peripheral Sharing Device
SFP	Security Function Policy
USB	Universal Serial Bus
VESA	Video Electronics Standards Association

2 TOE Description

2.1 Product Overview

The TOE is the BAE Systems Secure KVM Gen2, BAE Systems part number 8560943-2. The TOE consists of the KVM and a keyboard functioning as a remote controller device, that together function as a Peripheral Sharing Device and includes console ports and computer ports. The KVM facilitates the switching of a local keyboard, trackball and two displays (one with a touch panel) to three host computers. The KVM control switching function, located on the keyboard, is wired to the main KVM component and functions as a remote controller device. The switching control connection is separate from the keyboard USB connection. The keyboard has its own tamper detection separate from the main KVM component.

A single set of peripherals, including a trackball, keyboard, and two video displays, connect to the TOE. One of the displays contains a touch panel interface. The TOE's computer ports are connected to three separate computers. The user can then securely switch the connected console peripherals between any of the connected computers while preventing unauthorized data flows or leakage between computers. The TOE's remote controller provides manual port switching by simultaneously pressing the function key (FN) with the desired computer selection key to bring the KVM focus to the desired computer.

2.2 TOE Overview

The TOE is the BAE Systems Secure KVM Gen2 that allows users to connect a single set of peripherals to its console ports to interact with multiple computers that are connected to it via its computer ports. Controls on the keyboard remote controller device allow the user to select which of the connected computers is 'active' such that the peripherals connected to the TOE can be used to interact with the selected computer.

The TOE's console ports support USB keyboard input, USB trackball input, USB touch panel input, and DisplayPort output.

The TOE's computer ports support TMDS video input and USB HID output.

2.3 TOE Architecture

The BAE Systems Secure KVM Gen2 consists of three identical transmitter (Tx) modules for connecting to three separate host computers, one receiver (Rx) module and one optical switch. The Tx modules, Rx module, and optical switch are all housed within a single modular chassis that uses bars and tamper-evident seals to maintain its integrity. Additionally, the TOE includes LED status indicators, CAPS and SCRL lock keys, and a remote controller switching function located on the keyboard. The TOE boundary includes the firmware running on the peripheral keyboard.

The keyboard remote controller is connected to the main KVM unit with two non-standard RS-232 connectors. One interface goes to the KVM Rx and uses a non-standard, circular push-pull type connector. The other RS-232 interface is unidirectional (transmit only) and goes to the optical switch module. The connector on the optical switch module is a DB-9 connector, but it uses a non-standard pinout. The RS-232 messages from the keyboard to the Rx and optical switch are identical and are sent simultaneously. Because the remote controller is part of the TOE, these interfaces are considered internal interfaces and are used for the switching control and for receiving the keyboard CAPS & SCROLL lock indicator data.

The TOE's external interfaces are:

- One Combo D-9W4 connector for the Power interface.
- Three inputs to the Switch (one for selected computer interface).
- Two video DisplayPort interfaces to the dual DisplayPort monitors
- One USB interface for touch panel data from the single lower display.
- Two USB interfaces for USB Keyboard[1], USB Trackball.

Note that the KVM also has a fiber optic I/O interface for a fourth transmitter module located remote to the "main" KVM chassis. This interface and the fourth transmitter module are not part of the TOE.

The host computers themselves are not part of the TOE. The video display devices and the USB user data input keys on the keyboard device are not part of the TOE.

The BAE Systems Secure KVM Gen2 has the following characteristics:

- Two DVI-D input ports for dual display DisplayPort output
- Six HDMI input ports for dual display DisplayPort output

Two of the host computers convert DisplayPort video signals to HDMI using the DisplayPort dual mode feature provided by the host computer's graphics card. The TOE provides signaling to the host computer's graphics card over the DisplayPort cable so that it activates this feature. This feature is a standard feature of DisplayPort since 2013 when Video Electronics Standards Association (VESA) released the Dual-Mode 1.1 standard. The third host computer sends DVI-D video to the TOE. The TOE receives the HDMI and DVI-D signals and converts them for output as DisplayPort protocol to the connected video displays. The Extended Display Identification Data (EDID) of the connected displays are statically loaded into memory during manufacturing and do not need to be read during boot.

The Secure KVM Switch product is designed to connect a keyboard, trackball, and two video displays to three separate computers. The user can then switch the connected peripherals between any of the connected computers using the FN+ button corresponding to the host computer on the keyboard device. The selected computer is always identifiable by blue LED associated with the applicable selection button.

To interface with connected computers, the Secure KVM Switch product supports USB connections for the keyboard, trackball, touch panel input, and DisplayPort input for the computer video display interfaces.

The user keyboard and trackball data connect to the TOE's receiver component using a USB cable that contains separate wiring for the two interfaces. The touch panel data connects to the TOE using a separate cable. The keyboard, trackball, and touch panel data are then switched together to the selected computer. The user's touch panel data inputs are treated as mouse data. The TOE connects to one USB port on the host computer and all USB data (keyboard, trackball, and touch panel) are transmitted to the host computer over this same USB cable.

[1] The USB Keyboard device contains the KVM Switching function and is therefore part of the TOE. Therefore, the RS-232 interface between the keyboard and the main KVM component is considered an internal interface.

The Secure KVM Switch product is designed to enforce the allowed and disallowed data flows between user peripheral devices and connected computers as specified in [PSD]. Data leakage is prevented across the TOE to avoid compromise of the user's information. The Secure KVM Switch product automatically clears the internal TOE keyboard and mouse buffers.

The data flow of USB keyboard/trackball/touch panel is controlled by the TOE's Optical Switch Circuit Card Assembly (CCA). The selection is done through commands received via the RS-232 interface. Details of the data flow architecture are provided in the proprietary Secure KVM Isolation Document. All keyboard, trackball, display and touch panel connections are filtered first, and only authorized devices will be allowed. The TOE emulates data from the authorized USB keyboard, trackball and touch screen to USB data for computer sources.

The TOE's proprietary design ensures there is no possibility of data leakage from a user's peripheral output device to the input device and that no unauthorized data flows from the monitor to a connected computer. The keyboard and mouse are always switched together. There is no possibility of data leakage between computers or from a peripheral device connected to a console port to a non-selected computer. Each connected computer contains its own independent USB controller, processing memory and GPU.

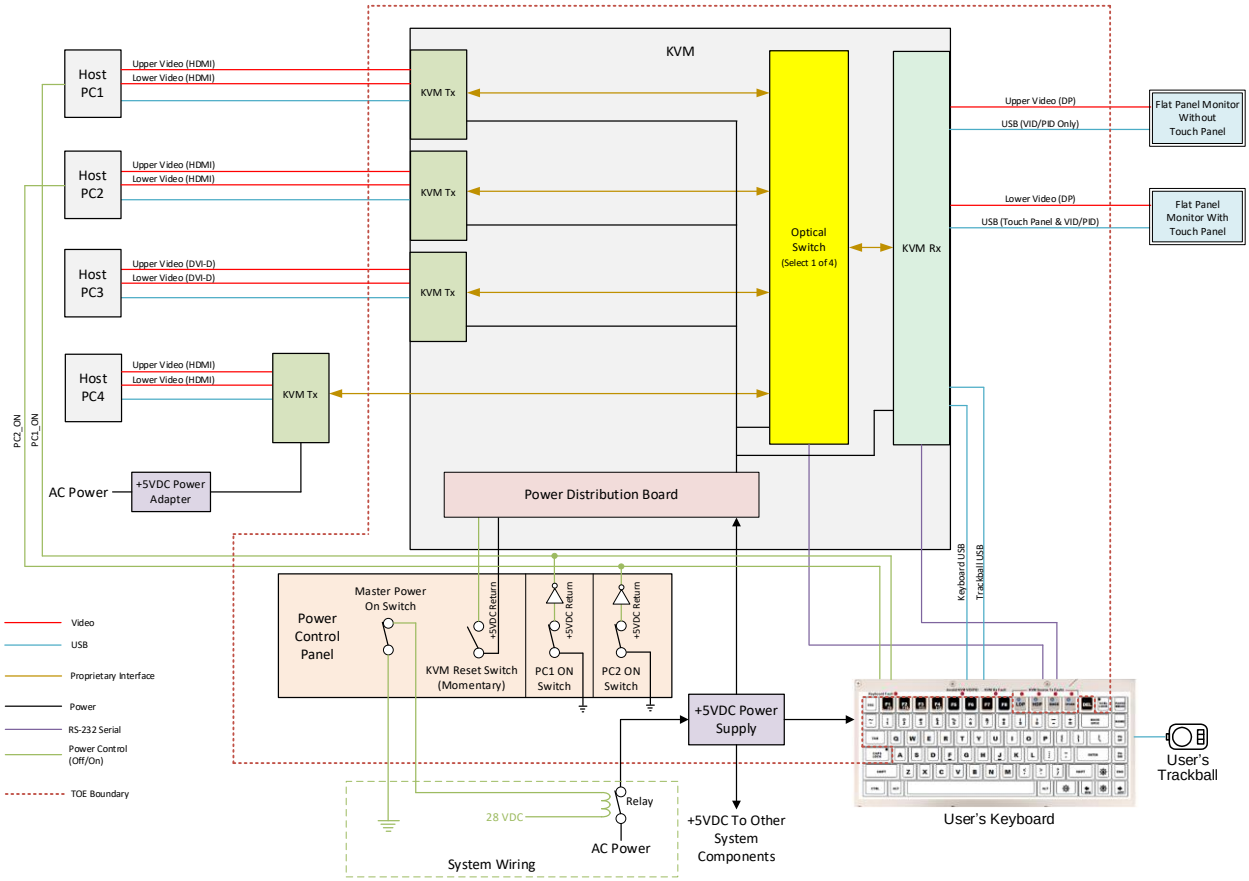
All Secure KVM Switch components, including the keyboard that houses the remote control, feature tamper-evident labels. Software security features include restricted USB connectivity, an isolated channel per port that makes it impossible for data transmission between computers, and automatic clearing of the keyboard, trackball and touch panel buffers.

A detailed description of the TOE security features can be found in Section 6 (TOE Summary Specification).

2.3.1 Physical Boundary

Figure 1 shows the BAE Systems Secure KVM Gen2 in its environment. Its three transmitters, receiver, optical switch, and power control panel are all housed within a single physical chassis assembly. The user keyboard is a purpose-built USB peripheral keyboard that includes channel selection functionality and KVM status indicators, and caps/scroll lock status indicators. While physically part of the keyboard, this portion of it functions as a wired remote control as it interfaces with the rest of the TOE from a physically and logically distinct interface from the USB HID interface used for keyboard inputs. The power control panel is physically separate from the main chassis but only carries electrical power.

Figure 1: BAE Systems Secure KVM Gen2



Note: The Operational Environment includes the peripheral trackball and monitors. The peripheral keyboard includes firmware which is in the TOE boundary because it functions as the wired remote control for the TOE.

The TOE includes the following components:

- Three identical transmitter (Tx) modules for three host computers:
    - Tx receives DVI-D or HDMI video from host computer and converts it from copper input to fiber optic output.
    - The Tx also converts USB between copper and fiber optic signals.
    - Each Tx has tamper evident seals.
- RX Receiver module
    - Converts video from fiber optic input to copper output and DVI-D or HDMI to DisplayPort for output to displays.

  - Converts USB copper interfaces, including the touch panel's RS-232-over-USB interface, to USB HID reports over fiber optic cable.
  - Has tamper evident seals.
- Optical switch
  - Connects user's video and USB interfaces to selected host computer.
  - Protected by tamper evident seals.
- Power Distribution Board
  - Accepts +5V DC power from the external power supply and distributes it to each of the KVM modules.
  - Accepts a KVM Reset signal and causes the KVM to reset itself.
  - Protected by tamper evident seals
- Keyboard:
  - Remote Controller function on the keyboard – provides the user switching function to switch between the host computers by simultaneously depressing the FN key + Host Select Key. The switching control function uses a RS-232 interface to the main KVM unit that is a separate interface from the user's USB keyboard data interface.
  - Keyboard lock indicators (SCRL, CAPS) – located on the keyboard.
  - Keyboard fault indicators (Keyboard, Invalid KVM VID/PID, KVM Rx, KVM Source TX (4)).
  - Keyboard has a tamper evident seals.
- Off/On Power Control Panel (PCP)
  - Includes the Master On/Off Power Control pull to engage toggle switch, KVM Reset momentary toggle switch and pull-to-engage toggle switches for PC1 and PC2 power.
- +5VDC Power supply that provides power to the KVM and keyboard.
- Documentation identified in Section 2.5 below.

The TOE is delivered with a purpose-built trackball (part number 1072378P-5) and a set of proprietary purpose-built cables for the various connections: KVM connections to the PCs, and internal component connections. These include:

- Keyboard connectors: color-coded keyboard connectors for:
  - +5VDC Power: a 4-pin circular push-pull connector, color code red. Mating cable part number 8564980-1.

- LED brightness signal, PC1_ON and PC2_ON signals[2]: an 8-pin circular push-pull connector, color code green. Mating cable part number is also 8564980-1.
- Data and Control Signals: a 12-pin circular push-pull connector, color code blue, supporting Keyboard/Trackball USB and RS-232 Serial Input/Output Signals. Mating cable part number 8564979-1.
- Handgrip – a 5-pin circular push-pull connector, color code yellow, for connecting the Handgrip directly to PC1 via the keyboard (not switched)[3]. Mating cable part number 8564978-1.

- Optical Switch Assembly connectors:
  - Control Connector (J1): a DB-9 with pin contacts (male) and contains the RS-232 interface. Mating cable part number 8564979-1.
  - Power Connector (J2): a combo D-9W4 connector that is mounted to the power distribution board and contains +5VDC power. Mating cable part number 8564980-1.
  - Connector (J3) for fourth Tx: a fiber-optic LC union for connecting two fiber optic cables. External mating cable part number 8569787-1. Provides video and USB interface to the external Tx module that is not part of the TOE.
  - KVM Reset Connector (J4): a 2-pin circular push-pull connector that contains the KVM Reset signal from the Power Control Panel. Mating cable part number 8584296-1.

  Power Distribution Board:

    - KVM Reset Connector: a 4-pin header type connector. Mating cable part number is 8584717-1, other end connects to external KVM Reset Connector J4.
    - KVM Internal Power Connectors: 4-pin and 6-pin header type connectors. Mating cable part numbers are 8560344-6 through -10. Other end of cables connect to the three Tx modules, the Rx and the optical switch board.

  - Optical Switch CCA:
    - Power Connector: a 2-pin header type connector. Mating cable part number is 8560344-10. Other end connects to the Power Distribution Board.
    - Fiber optic input and output connectors (P1-P5). These connectors are on fiber optic umbilical cables that are mounted directly to the optical switch CCA. Each is labeled to show where it connects.

[2] The keyboard uses the PC1_ON and PC2_ON signals to prevent the operator from selecting Host PC1 or Host PC2 if they are powered off.

[3] The Handgrip, the Handgrip connection, and its cable are not part of the TOE.

- Transmitter connectors:
    - J1, J2 video input DisplayPort receptacle connectors. Mating cable part numbers 8560342-3 thru -6 for DP++ (HDMI) video, cable P/N 8560342-7 and -8 for DVI-D video.
    - USB connector J3 -a circular push-pull connector with socket contacts (female). Mating cable part numbers 8564978-1, -2 and P/N 8560343-1. Each is labeled to show where it connects.
    - Fiber optic connector J5 - Part of a fiber optic transceiver. Connects to one of the fiber optical umbilical cables from the optical switch CCA. Refer to the optical switch CCA connector description for more information.
    - Input power connector J6 - A 5-pin circular push-pull type with pin contacts (male). Mating cable part numbers are 8560344-6, -7 and -8. Each is labeled to show where it connects.
    - JTAG connector J8 – A 14-pin header type connector. This connector is an internal connector used only during the development process and is not externally accessible.
- Receiver connectors:
    - DP output interfaces (J1 and J2) - DisplayPort receptacle connectors. Mating cable part numbers are 8560342-1 and 8560342-2.
    - Keyboard and Trackball USB connector J5 - An 8-pin circular push-pull type connector with socket contacts (female). Contains the keyboard USB signals and the trackball USB signals on separate contacts. Mating cable part number is also 8564979-1.
    - Flat Panel Monitor USB connector J6 - An 8-pin circular push-pull type connector with socket contacts (female). Contains the USB signals for the two monitors. USB for the upper monitor is only used for VID/PID check. USB for the lower monitor is used for VID/PID check and touch panel data. Mating cable part number is 8574677-1.
    - Fiber optic connector J8 - an LC dual connector that is part of a fiber optic transceiver. Connects to LC connector P5 on a fiber optical umbilical cable from the optical switch board.
    - Input power connector J9 - A 5-pin circular push-pull type with pin contacts (male). Mating cable part number is 8560344-9.
    - JTAG connector J10– A 14-pin header type connector. This connector is an internal connector used only during the development process and is not externally accessible.

  Note: Although Rx connectors J4, J5 and J6 are the same connector type, they are keyed differently so the mating cables cannot be attached to the wrong connector.

All keyboard and KVM USB interfaces use circular push/pull connectors for USB that do not allow a standard keyboard or trackball device to be hooked directly to the KVM with standard commercial cables. The keyboard has an umbilical cable with a 9-pin Dsub connector with socket contacts. Since standard commercial trackballs have standard USB connectors, not 9-pin Dsub connectors, the only

things that can be connected to the keyboard are the trackball provided with the TOE and the handgrip which is not part of the TOE. This is also enforced by the KVM's whitelist; only devices that are in the KVM whitelist are allowed to be connected to the KVM either directly or via the keyboard. The cable sets supplied with the TOE are considered part of the operational environment along with the switched PCs and peripheral devices.

2.4 Logical Boundary

This section summarizes the security functions provided by the TOE:

- User Data Protection
- Protection of the TSF
- TOE Access

2.4.1 User Data Protection

The TOE controls and isolates information flowing between the peripheral device interfaces and a computer interface. The peripheral devices supported include USB keyboard, USB trackball, and DisplayPort with touch panel. The TOE accepts TMDS video waveform outputs from connected computers and converts them to DisplayPort for output to peripheral monitors.

The TOE authorizes peripheral device connections with the TOE console ports based on the peripheral device's VID/PID.

The TOE ensures that any previous information content of a resource is made unavailable upon the deallocation of the resource from a TOE computer interface prior to the TOE switching to another selected computer and on start-up or reset of the TOE.

2.4.2 Protection of the TSF

The TOE runs a suite of self-tests during initial startup and after activating the reset switch that includes a test of the basic TOE hardware and firmware integrity and a test of critical security functions (i.e., user control). The TOE provides users with the capability to verify the integrity of the TSF and the TSF functionality. The TOE contains status indicators to inform the user of a self-test failure.

The TOE preserves a secure state by disabling the TOE's external and internal interfaces when there is a failure of the power on self-test.

The TOE provides unambiguous detection of physical tampering that might compromise the TSF with tamper evident unique labels.

2.4.3 TOE Access

The TOE displays a continuous visual indication of the computer to which the user is currently selected, including on power up, and on reset.

2.5 TOE Documentation

There are several documents that provide information and guidance for the deployment and usage of the TOE. In particular, the following guides reference the security-related guidance material for all devices in the evaluated configuration.

Guidance Documentation:

- BAE Systems Generation 2 Keyboard/Video/Mouse (KVM) User's Manual, Part Number 8560943-2, January 10, 2023

TOE Documentation:

- BAE Systems Secure KVM Gen2 8560943-2 Isolation Documentation and Assessment, Version 1.0, 2022-11-02 (Proprietary)
    - **Note**: The BAE Systems Secure KVM Gen2 8560943-2 Isolation Documentation and Assessment is **proprietary** as permitted by PSD 4.0 Annex D.1 Isolation Document and Assessment.
    - The isolation document supplements the Security Target Section 6 TOE Summary Specification in order to demonstrate the TOE provides isolation between connected computers. In particular, the isolation document describes how the TOE mitigates the risk of each unauthorized data flow listed in PSD 4.0 Annex D and Evaluation Activities specified in the PP v4.0 and modules.

3 Security Problem Definition

This security target includes by reference the Security Problem Definition from the [PSD] and [MOD-VI]. The Security Problem Definition consists of threats that a conformant TOE is expected to address and assumptions about the operational environment of the TOE.

In general, the [PSD] has presented a Security Problem Definition appropriate for peripheral sharing devices. The BAE Systems Secure KVM Gen2 supports KVM (USB Keyboard/Mouse, and DisplayPort) peripheral switch. As such, the [PSD] Security Problem Definition applies to the TOE.

4 Security Objectives

Like the Security Problem Definition, this Security Target includes by reference the Security Objectives from the [PSD], [MOD-VI], and [MOD-KM].

The [PSD] and [MOD-VI] security objectives for the operational environment are reproduced below, since these objectives characterize technical and procedural measures each consumer must implement in their operational environment.

In general, the [PSD] has presented a Security Objectives statement appropriate for peripheral sharing devices. Consequently, the [PSD] security objectives are suitable for the TOE.

4.1 Security Objectives for the Operational Environment

Table 3: Security Objectives for the Operational Environment

Objective	Description
OE.NO_SPECIAL_ANALOG_CAPABILITIES (from [MOD-VI])	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.
OE. NO_TEMPEST (from [PSD])	The operational environment will not use TEMPEST approved equipment.
OE.NO_WIRELESS_DEVICES (from [PSD])	The operational environment will not include wireless keyboards, mice, audio, user authentication, or video devices.
OE.PHYSICAL (from [PSD])	The operational environment will provide physical security, commensurate with the value of the PSD and the data that transits it.
OE.TRUSTED_ADMIN (from [PSD])	The operational environment will ensure that trusted PSD Administrators and users are appropriately trained.
OE.TRUSTED_CONFIG (from [PSD])	The operational environment will ensure that administrators configuring the PSD and its operational environment follow the applicable security configuration guidance.

5 IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the Protection Profile: [PSD] and the modules: [MOD-KM], and [MOD-VI], and include some of the optional and selection-based SFRs. As a result, refinements and operations already performed in that PP and modules are not identified (e.g., highlighted) here, rather the requirements have been copied from that PP and any residual operations have been completed herein. Of particular note, the [PSD] and modules made a number of refinements and completed some of the SFR operations defined in the CC and that PP should be consulted to identify those changes if necessary.

The SARs are the set of SARs specified in [PSD].

5.1 Extended Requirements

All of the extended requirements in this ST have been drawn from the [PSD] and the modules: [MOD-KM] and [MOD-VI]. The [PSD] and modules define the following extended SFRs and since they are not redefined in this ST, the [PSD] and associated modules should be consulted for more information concerning those extensions.

- FDP_APC_EXT.1 – Active PSD Connections
- FDP_CDS_EXT.1 – Connected Displays Supported
- FDP_FIL_EXT.1/KM – Device Filtering (Keyboard/Mouse)
- FDP_IPC_EXT.1 – Internal Protocol Conversion
- FDP_PDC_EXT.1 – Peripheral Device Connection
- FDP_PDC_EXT.2/KM – Authorized Devices (Keyboard/Mouse)
- FDP_PDC_EXT.2/VI – Peripheral Device Connection (Video Output)
- FDP_PDC_EXT.3/KM – Authorized Connection Protocols (Keyboard/Mouse)
- FDP_PDC_EXT.3/VI – Authorized Connection Protocols
- FDP_RIP_EXT.1 – Residual Information Protection
- FDP_SPR_EXT.1/DP – Sub-Protocol Rules (DisplayPort Protocol)
- FDP_SWI_EXT.1 – PSD Switching
- FDP_SWI_EXT.2 – PSD Switching Methods
- FDP_SWI_EXT.3 – Tied Switching
- FDP_UDF_EXT.1/KM – Unidirectional Data Flow (Keyboard/Mouse)
- FDP_UDF_EXT.1/VI – Unidirectional Data Flow (Video Output)
- FPT_FLS_EXT.1 – Failure with Preservation of Secure State
- FPT_NTA_EXT.1 – No Access to TOE
- FPT_TST_EXT.1 – TSF Testing
- FTA_CIN_EXT.1 – Continuous Indications

5.2 TOE Security Functional Requirements

This section identifies the TOE Security Functional Requirements for the PSD 4.0, and modules [MOD-KM] and [MOD-VI].

Table 4 identifies the SFRs that are satisfied by the TOE.

Table 4: TOE Security Functional Components

Requirement Class	Requirement Component
FDP: User Data Protection	FDP_APC_EXT.1/KM – Active PSD Connections (Keyboard/Mouse)
	FDP_APC_EXT.1/VI – Active PSD Connections (Video/Display)
	FDP_CDS_EXT.1 – Connected Displays Supported
	FDP_FIL_EXT.1/KM – Device Filtering (Keyboard/Mouse)
	FDP_IPC_EXT.1 – Internal Protocol Conversion
	FDP_PDC_EXT.1 – Peripheral Device Connection
	FDP_PDC_EXT.2/KM – Authorized Devices (Keyboard/Mouse)
	FDP_PDC_EXT.2/VI – Peripheral Device Connection (Video Output)
	FDP_PDC_EXT.3/VI – Authorization Connection Protocols (Video Output)
	FDP_PDC_EXT.3/KM – Authorized Connection Protocols (Keyboard/Mouse)
	FDP_RIP.1/KM – Residual Information Protection (Keyboard Data)
	FDP_RIP_EXT.1 – Residual Information Protection
	FDP_SPR_EXT.1/DP – Sub-Protocol Rules (DisplayPort Protocol)
	FDP_SWI_EXT.1 – PSD Switching
	FDP_SWI_EXT.2 – PSD Switching Methods
	FDP_SWI_EXT.3 – Tied Switching
	FDP_UDF_EXT.1/KM – Unidirectional Data Flow (Keyboard/Mouse)
	FDP_UDF_EXT.1/VI – Unidirectional Data Flow (Video Output)
FPT: Protection of the TSF	FPT_FLS_EXT.1 – Failure with Preservation of Secure State
	FPT_NTA_EXT.1 – No Access to TOE
	FPT_PHP.1 – Passive Detection of Physical Attack
	FPT_TST.1 – TSF Testing
	FPT_TST_EXT.1 – TSF Testing
FTA: TOE Access	FTA_CIN_EXT.1 – Continuous Indications

5.2.1 User Data Protection (FDP)

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

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 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 by the ST author to apply to the keyboard/mouse interface per section 5.1.2 of the Keyboard/Mouse PP-Module.*

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

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 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 by the ST author to apply to the video interface per section 5.1.2 of the Video/Display PP-Module.*

5.2.1.3 Connected Displays Supported (FDP_CDS_EXT.1)

FDP_CDS_EXT.1.1 The TSF shall support [***multiple connected displays***] at a time.

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

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.

5.2.1.5 Internal Protocol Conversion (FDP_IPC_EXT.1)[4]

FDP_IPC_EXT.1.1 The TSF shall convert the [*DisplayPort*] protocol at the [***DisplayPort peripheral display interface(s)***] 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***].

Application Note: *This SFR was modified by TD0586 to allow for HDMI in -> DP out, as per the Issue Description. The TOE only accepts TMDS waveform video signal data (part of HDMI) from host computers and outputs the video as DisplayPort.*

5.2.1.6 Peripheral Device Connection (FDP_PDC_EXT.1)

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.

5.2.1.7 Authorized Devices (Keyboard/Mouse) (FDP_PDC_EXT.2/KM)

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

- ***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 KM Module**] and [

- ***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.

[4] Modified by TD0586

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

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

- ***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 VI Module**] and [

- ***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.

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

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*].

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

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

FDP_PDC_EXT.3.2/VI[5] The TSF shall apply the following rules to the supported protocols: [the TSF shall read the connected display EDID information **up to** once during power-on or reboot].

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

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

5.2.1.12 Residual Information Protection (FDP_RIP_EXT.1)

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

[5] The refinement in this requirement was made as per TRRT #1055.

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

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].

5.2.1.14 PSD Switching (FDP_SWI_EXT.1)

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

5.2.1.15 PSD Switching Methods (FDP_SWI_EXT.2)

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 [***wired remote control***].

5.2.1.16 Tied Switching (FDP_SWI_EXT.3)

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.

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

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.

Application Note: *Per the PP-Module, it is permissible for USB data to enter the TOE via a computer port for the purpose of reporting state changes (e.g. caps/scroll lock toggle) as long as this data does not ultimately exit the TOE through the input peripheral interface.*

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

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.

5.2.2 Protection of the TSF (FPT)

5.2.2.1 Failure with Preservation of Secure State (FPT_FLS_EXT.1)

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 [***no other failures***].

5.2.2.2 No Access to TOE (FPT_NTA_EXT.1)

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***].

5.2.2.3 Passive Detection of Physical Attack (FPT_PHP.1)

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.

5.2.2.4 TSF Testing (FPT_TST.1)

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 ***[no other functions]***].

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

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

5.2.2.5 TSF Testing (FPT_TST_EXT.1)

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.

5.2.3 TOE Access (FTA)

5.2.3.1 Continuous Indications (FTA_CIN_EXT.1)

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[6] The TSF shall implement the visible indication using the following mechanism: easily visible graphical and/or textual markings of each source video on the display, [***a button, a panel with lights***].

Application Note: *The selected computer is indicated with a panel with lights that corresponds to the computer selection buttons. Each port has its own Port LED.*

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***].

Application Note: *As indicated in FTA_CIN_EXT.1.2, the TOE has a light panel that shows the selected computer by backlighting (in blue) the selected button corresponding to the selected computer. There is no situation in which the selected computer will be indicated with the light panel and a different computer will be indicated with the selection button.*

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are included by reference from the [PSD].

Table 5: Assurance Components

Requirement Class	Requirement Component
Security Target (ASE)	Conformance Claims (ASE_CCL.1)
	Extended Components Definition (ASE_ECD.1)
	ST Introduction (ASE_INT.1)
	Security Objectives (ASE_OBJ.2)
	Derived Security Requirements (ASE_REQ.2)
	Security Problem Definition (ASE_SPD.1)
	TOE Summary Specification (ASE_TSS.1)
Development (ADV)	Basic Functional Specification (ADV_FSP.1)
Guidance Documents (AGD)	Operational User Guidance (AGD_OPE.1)
	Preparative Procedures (AGD_PRE.1)
Life Cycle Support (ALC)	Labeling of the TOE (ALC_CMC.1)
	TOE CM Coverage (ALC_CMS.1)
Tests (ATE)	Independent Testing – Conformance (ATE_IND.1)

[6] TD0539 clarifies that the mandatory selection (refined by the VI-Module) applies if the TOE fits the Combiner Use Case selecting “multiple connected displays” in FDP_CDS_EXT.1.1. The TOE does not fit the Combiner User Case but rather selects “multiple connected displays” because dual displays from a single source video feed are supported. Therefore, the selection does not apply.

Requirement Class	Requirement Component
Vulnerability Assessment (AVA)	Vulnerability Survey (AVA_VAN.1)

6 TOE Summary Specification

This chapter describes the following security functions:

- User Data Protection
- Protection of the TSF
- TOE Access

6.1 User Data Protection

The TOE enforces data isolation and the User Data Protection SFP on TOE computer interfaces and TOE peripheral device interfaces by controlling the data flow and user data transiting the TOE.

The TOE supports the following types of devices: USB Keyboard, Trackball, and DisplayPort monitor (with touch panel). All other devices are rejected. The TOE accepts TMDS waveform video signals at the computer interface using a physical DisplayPort connector. The TOE converts the TDMS video to DisplayPort for display on the peripheral monitors. The TOE does not support audio.

The TOE ensures that any previous information content of a resource is made unavailable upon the deallocation of the resource from the TOE computer interfaces immediately after a TOE is switched to another selected computer and on start-up of the TOE.

The Appendix A Letter of Volatility provides assurance that no user data remains in the TOE after power down.

The Tx modules are connected through an optical switch to the Rx module. Only one Tx module is active at a time over the fiber optic link. The only host computer data that the Tx can send to the Rx are video and CAPS Lock and Scroll Lock indicator On/Off status.

6.1.1 FDP_APC_EXT.1 (All Iterations); FDP_UDF_EXT.1/KM – Unidirectional Data Flow (Keyboard/Mouse); FDP_UDF_EXT.1/VI – Unidirectional Data Flow (Video Output)

The TOE routes video data only from the selected computer to the attached peripherals and routes the keyboard, mouse, and touch panel data unidirectionally and only to the selected computer from the attached peripherals.

The transmitters output EDID from inside the TOE to the Host Computers. No EDID comes from the monitors and there are no data channels from the monitors to the connected computers other than the touch panel data described below. This ensures there will is no unauthorized video or video sub-protocol data flow from the monitor to a connected computer.

All Keyboard, trackball and touch panel connections are filtered first, and only the authorized devices pre-defined in the TOE's whitelist will be allowed. The data input by the authorized USB Keyboard, Trackball, Touch Panel will be emulated by TOE to USB data for computer sources.

Keyboard Caps Lock and Scroll Lock indications are displayed on the keyboard wired to the switch (the PSD). The keyboard does not have a NUM lock key. They are controlled via the TOE side channel RS-232 interface connected to the keyboard and therefore the two LEDs are an extension of the TOE. Those are

the only keyboard LEDs that can be changed by a connected computer. There is no mechanism by which the TOE can transmit data to the keyboard via its USB interface.

No data or electrical signals flow between connected computers at any time. The TOE employs optical isolation and physically separate enclosed transmitter modules to prevent data and electrical signal flow between computers. Each connected computer contains its own independent USB controller, processing memory, and GPU.

No data transits the TOE when the KVM is powered off or when the KVM is in a failure state.

6.1.2 FDP_CDS_EXT.1 – Connected Displays Supported

The TOE supports two connected displays from a single source video feed (dual head). Because of this, the single selected source video feed is always the same channel and indication of the selected channel is through the channel selection LEDs on the PSD remote controller.

6.1.3 FDP_FIL_EXT.1/KM – Device Filtering (Keyboard/Mouse); FDP_IPC_EXT.1 – Internal Protocol Conversion; FDP_PDC_EXT.3/KM – Authorized Connection Protocols (Keyboard/Mouse); FDP_PDC_EXT.3/VI – Authorized Connection Protocols (Video Output); FDP_SPR_EXT.1/DP – Sub-Protocol Rules (DisplayPort Protocol)

The TOE supports authorized USB keyboard, mouse (trackball), and video (with and without touch panel) peripherals as defined in ***Table 6: Supported protocols by port*** below. Keyboard/mouse peripherals are filtered and emulated. Device filtering for keyboard/mouse interfaces is fixed. The specific keyboard/trackball/video that are designed to work with the TOE are specified at manufacturing time and are permanently whitelisted.

Whitelisted devices are authorized devices for the keyboard/trackball/video interfaces in peripheral device connections. Keyboard/trackball/video devices that are not whitelisted are unauthorized devices. The TOE does not define blacklists and therefore it is not possible for whitelisted devices to also be blacklisted devices.

The TOE emulates data from authorized USB Keyboard and Mouse protocol as well as touch panel interfaces to USB connected computers.

The TOE is designed to be used in a purpose-built environment where the monitors attached to the PSD are purpose-built and known to the vendor at the time of initial deployment. Because of this, the PSD is designed such that as part of the initial deployment process, the EDID of the connected displays are statically loaded into memory and do not need to be read during boot since substitution is not possible. The TOE ensures that no data transmission of any kind can occur over the EDID channel and therefore the EDID channel cannot be used as a side channel to transmit data through the PSD. The TOE also rejects all MCCS communications as well as DPCD-based communications over the DisplayPort AUX channel (CEC, HDCP). The only video signal processed by the TOE that originates from connected computers is the TMDS waveform signal. Link training and HPD from display to computer are only indirectly permitted via communications from the display only going to the KVM Rx. A separate HPD goes from each KVM Tx to its respective host computer. Additional details are provided in the proprietary Isolation Documentation.

6.1.4 FDP_PDC_EXT.1 – Peripheral Device Connection; FDP_PDC_EXT.2/KM – Authorized Devices (Keyboard/Mouse); FDP_PDC_EXT.2/VI – Peripheral Device Connection (Video Output)

The TOE allows the authorized devices and protocols for the PSD Console Ports as identified in the table below upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

The TOE does not allow any other user data transmission to or from any other external entities including wireless devices. The TOE only recognizes those peripherals with an authorized interface type as described below and all other peripherals will be denied both upon TOE power up and upon connection of a peripheral device to a powered-on TOE. Any unauthorized devices connected to a TOE peripheral USB port triggers the Invalid KVM VID/PID LED on the keyboard. Additionally, the displays will show an "Invalid VID/PID" error message. Host computer selection LEDs are located on the Keyboard and provide a continuous visual indication of the status of the function associated with that port.

Specifically the TOE supports the following peripherals on the console interfaces:

Table 6: Supported protocols by port

PSD Console Port	Authorized Devices	Authorized Protocol
Keyboard	QWERTY purpose-built wired keyboard.	USB 2.0
Display	Monitors (specific models known by vendor prior to assembly so that EDID information can be pre-written)	DisplayPort 1.2 (output to display) DisplayPort 1.2 (physical interface that carries TMDS waveform signal)
Mouse/Pointing Device	Purpose-built 4-button wired trackball. Connects to the keyboard using a 9-pin Dsub connector. The keyboard routes the trackball USB data to the KVM on a USB interface that is separate from the keyboard USB data. Touchscreen (lower monitor only).	USB 2.0 USB 2.0

Additionally, the KVM has interfaces for +5VDC power and a power-on reset signal. LED indicators on each KVM module provide general status information. Each component has its own power source connection. The pull to engage Reset switch is located on the PCP. The PCP also provides three pull to engage power switches and three power LEDs: one for the entire system, one for the PC1 and one for the PC2. LEDs are also located on the Keyboard include Caps and Scroll Lock (Green), fault indicator (RED) LEDs and Port status (BLUE) indicators of the source selections. The fault indicators are:

- Keyboard Fault (Internal BIT)
- Invalid KVM VID/PID
- KVM Rx (Receiver) Fault
- KVM Source Tx (Transmitter) Faults (one above each KVM Source Selection key).

The KVM Source LEDs indicate Host Computer Port selection/connection status.

6.1.5 FDP_RIP.1/KM – Residual Information Protection (Keyboard Data), FDP_RIP_EXT.1 – Residual Information Protection

No user data is written to TOE non-volatile memory or storage. User keyboard data is purged and not available to the next connected TOE computer interface prior to switching to the new source computer. The data input by the authorized keyboard/trackball/touch panel will be kept in the TOE's authorized keyboard/trackball/touch panel buffers. The TOE purges any user data in these non-volatile memory locations after a power up or reset.

User data coming from the USB user input devices is not stored in non-volatile memory on any TOE component. Details of user data storage in the volatile memory is provided in the proprietary Isolation Documentation.

The TOE provides pull to engage Power On/Off and Reset switches located on the PCP on the front of the cabinet allowing the user to delete the Keyboard/trackball/touch panel buffers. The switch then powers on the TOE, which performs power-on self-test.

The Letter of Volatility provided in Appendix A identifies the TOE components that have non-volatile memory and provides details of the memory and its use.

6.1.6 FDP_SWI_EXT.1 – PSD Switching; FDP_SWI_EXT.2 – PSD Switching Methods; FDP_SWI_EXT.3 – Tied Switching

The keyboard, mouse, and video ports are always switched together to the same connected computer using push buttons on the wired PSD remote control.

The TOE's KVM is enclosed within a cabinet and the switching mechanism is provided as toggle buttons on a keyboard that are wired back to the main chassis enclosed within the cabinet. The switching connection is separate from the keyboard USB connection. The toggle buttons for the selected computer are physically adjoining the keyboard but are directly wired to the TOE through a dedicated channel and are not "keyboard buttons" that communicate with the TOE over USB. The switching messages communicate with the KVM over a separate serial channel.

Switching can only be performed by the user pressing the function key simultaneously with the key selection that corresponds with the computer they wish to connect with. These buttons are labeled with their corresponding connected computer.

There are no options to switch peripherals independently from the keyboard and mouse. The TOE does not allow switching to be initiated through automatic port scanning, control through a connected computer, or control through keyboard shortcuts.

6.2 Protection of the TSF

In order to mitigate potential tampering and replacement, the TOE is designed to ensure that any replacement or physical modification is evident, and that any logical modification is prevented. Access to the TOE firmware, software, or its memory via its accessible ports is prevented with the allowable exception that EDID memory for Video is available to connected computers. No access is available to modify the TOE or its memory. All of the programmable memory in the KVM Tx and Rx modules, except for the memory containing the Linux file system, is hard soldered to the board. The Linux file system is stored in a Secure Digital High Capacity (SDHC) card that is mounted in cage. All of the programmable memory in the Tx and Rx modules is set to write protect mode prior to shipment by means of internal DIP switches and is not externally accessible. The programmable memory in the KVM Optical Switch Board is hard soldered to the board and is not externally accessible. Thus, the KVM's operational code is not upgradeable through any of its external ports. Upgrading the operational code is only possible by removing and opening a KVM module, but that puts the module's tamper-evident labels into the tampered state. The keyboard's programmable memory is not accessible via any of its external ports. The keyboard's operational code can only be upgraded by opening the keyboard, but that puts the keyboard's tamper-evident labels into the tampered state.

Each TOE component has its own tamper-evident label(s) printed with its own unique serial number and the vendor's specific design. Any attempts to open the KVM component enclosures sufficient to gain access to internal components will change the labels to a tampered state. Approximately half of the tamper-evident front labels on the Tx and Rx modules attach to the module covers; the other half wraps around the edge and attaches to the side. Approximately half of the rear label also attaches to the module cover and wraps around to the side. Therefore, the module cover cannot be even partially opened from the front, rear or side without putting a tamper-evident label into the tampered state. The optical switch module, which contains the optical switch board and power distribution board, has a metal bar across its front side that is held in place with screws on both sides that go into the KVM chassis. Two tamper-evident labels cover the two screws at both ends of the metal bar. Thus, the optical switch module cannot be removed without putting the labels into the tampered state. The keyboard has its own label on the bottom of the keyboard covering the circuitry. A tampered state can be determined in two ways. If someone tampers with the unit and replaces a torn label with a new label, that can be detected because the replacement label would not have the same vendor design and would have a different serial number. Additionally, the design of each label includes a hologram that when ripped is visually evident and cannot be re-assembled without it being obvious.

6.2.1 FPT_FLS_EXT.1 – Failure with Preservation of Secure State

The TOE preserves a secure state by disabling external and internal interfaces when the following types of failures occur: failure of the power-on and run-time self-test. The behavior as described below for FPT_TST.1 will occur if the Secure KVM Switch self-test fails.

6.2.2 FPT_NTA_EXT.1 – No Access to TOE

The TOE firmware, software, and memory is not accessible from the TOE's external ports, with the following exception:

- the Extended Display Identification Data (EDID) memory for Video is made available to the connected computers.

6.2.3 FPT_PHP.1 – Passive Detection of Physical Attack

Each TOE component has its own tamper-evident label(s), each label printed with its own unique serial number and the vendor's specific design. Each transmitter and receiver module is sealed with its own labels, one on the front and one in the rear. Approximately half of each label attaches to the module's cover, and the other half wraps around the module's edge and attaches to the module's side. This ensures the module cover cannot even be partially opened from the front, rear or side without putting a tamper-evident label into the tampered state. The fourth transmitter located outside of the main KVM chassis is protected in the same way; it has its own tamper-evident labels that do not allow its cover to be opened without putting the labels into the tampered state. The KVM's optical switch module, which contains the optical switch CCA and power distribution board, has a metal bar across its front side that is held in place with screws on both sides that go into the KVM chassis. Two tamper-evident labels cover the two screws at both ends of the metal bar. Thus, the optical switch module cannot be removed without putting the labels into the tampered state. The keyboard has its own labels on the bottom of the keyboard covering the circuitry. The PCP does not have a tamper label since it only provides power on/off signals to the TOE and does not pass any data.

The labels on the front and back of the KVM as well as the label on the bottom of the keyboard are clearly visible. All labels are in the form of tamper-evident tape to provide visual indications of intrusion to the enclosures. Any attempt to open the KVM component enclosures sufficient to gain access to internal components will change the labels to a tampered state.

6.2.4 FPT_TST.1 – TSF Testing and FPT_TST_EXT.1 – TSF Testing

The Secure KVM Switch TOE self-tests include memory tests, firmware integrity tests, and tests of push-button functioning. The TOE executes self-tests during boot (after a power-on or the reset switch is toggled) and executes some self-tests during run-time. The self-test function runs independently at each one of the TOE components following power up and reset. The KVM performs self-tests first before enabling the peripheral switching function. Before self-tests have completed successfully, the data paths between peripherals and connected computers are blocked and no data flow is allowed. External and internal interfaces are disabled following a self-test failure. Each TOE component performs its own self-tests and the results are sent to the Keyboard remote controller indicators.

The KVM enters a failure state when any of the power-on/reset or run-time self-tests fail except the Tx/Rx link up, VID/PID and QWERTY key stuck checks, which do not cause the TOE to be in an unsecure state. Note that the manual reset function applies to the KVM only.

The TOE runs the following self-tests:

<u>Power-On Self-Tests</u>

- KVM SDRAM Tx memory test: The memory controller performs a calibration procedure on the SDRAM during power-on initialization. A memory test failure occurs if the memory controller detects values falling outside of the allowed range. Upon failure, the KVM Tx will be in a failure state (inoperable).
- Rx SDRAM memory test: The memory controller performs a calibration procedure on the SDRAM during power-on initialization. A memory test failure occurs if the memory controller detects values falling outside of the allowed range. Upon failure, the KVM will be in a failure state (inoperable).

- KVM Tx communication with EEPROMs: Verify that EEPROMs can be read. Upon failure, the KVM Tx will be in a failure state (inoperable).
- KVM Rx communication with EEPROMs: Verify that EEPROMs can be read. Upon failure, the KVM will be in a failure state (inoperable).
- KVM Tx communication with video re-timer: Verify that the registers in the video re-timer can be written to and read from. Upon failure, the KVM Tx will be in a failure state (inoperable).
- KVM Rx communication with video re-driver: Verify that the registers in the video re-driver can be written to and read from. Upon failure, the KVM will be in a failure state (inoperable).
- KVM Rx communication with phase-lock loop chips: Verify that the registers in the phase-lock loop chips can be written to and read from. Upon failure, the KVM will be in a failure state (inoperable).
- KVM Rx communication with USB hub: Verify that that the USB link between the processor and the USB hub is up. Upon failure, the KVM will be in a failure state (inoperable).
- KVM Rx VID/PID check: Verify that the connected USB peripheral devices have a whitelisted VID/PID. Upon failure, the associated USB port is disabled.
- Keyboard memory test: The keyboard microcontroller writes a block of predefined data into SRAM and then reads the block out to compare if it is identical. The keyboard fault LED illuminates if the test fails. As long as the memory failure persists, the keyboard remains in a non-operational state. The keyboard can only be recovered by recycling power.

Run-Time Self-Tests

- Keyboard memory test: The keyboard microcontroller writes a block of predefined data into SRAM and then reads the block out to compare if it is identical. The keyboard fault LED illuminates if the test fails. As long as the memory failure persists, the keyboard remains in a non-operational state. The keyboard can only be recovered by recycling power.
- Keyboard KVM selection stuck key test: If a keyboard KVM selection key remains actuated for 30 seconds or more, the keyboard illuminates its keyboard fault LED and it sends a shutdown message to the KVM causing the KVM to disable itself and become non-operational.
- Keyboard watchdog: A watchdog timer causes the keyboard to reboot in the event that the processor fails to reset it in time. A persistent failure causes the keyboard to continually reboot. This is observed by the keyboard LEDs repeatedly illuminating and extinguishing and leaving the keyboard non-operational.
- Keyboard QWERTY stuck key test: If a keyboard QWERTY key remains actuated for 30 seconds or more, the keyboard illuminates its keyboard fault LED. No further action is taken because the QWERTY keys are not part of the TOE and the TOE remains in a secure state.
- KVM Tx fiber optic transceiver presence: Verify that the fiber optic transceiver is present and active. Upon failure, the KVM Tx will be in a failure state (inoperable).
- KVM Tx/Rx link up: If the link over the fiber optic cable between the Rx and the selected Tx is not up, the keyboard will illuminate the corresponding Tx Fault LED. No further action is taken because no data can transit the TOE when the Tx/Rx link is down and, therefore, the TOE remains in a secure state.
- KVM Tx/Rx communication: When the Tx/Rx link is up, verify that the Rx and Tx are communicating with each other over the fiber optic link. Upon failure, the KVM will be in a failure state (inoperable).
- KVM Tx correct response to Rx: When the Tx/Rx link is up, the Rx verifies that the Tx is responding properly. Upon failure, the KVM will be in a failure state (inoperable).

- KVM Rx VID/PID check: If a new USB peripheral device is connected, verify that the peripheral device has a whitelisted VID/PID. Upon failure, the associated USB port is disabled.

Additional details on the self-tests including which components perform the test are provided below.

The fault status indicators on the KVM Keyboard are as follows:

- Keyboard Fault LED – e.g. a Key stuck test failure.
- Invalid KVM VID/PID
- KVM Rx (Receiver) Fault
- KVM Source Tx (Transmitter) Faults (one above each KVM Source Selection key – total of 4).

When a self-test failure is detected, the corresponding LED will display a red LED.

All self-test failures may be recoverable by initiating a power cycle of the Secure KVM Switch. If the failures continue then the device will remain in the failure state described below. Although the TOE does not shut down completely when a self-test failure occurs, the TOE protects itself by disabling external and internal interfaces to ensure that the TOE remains in a secure state.

Users can verify the integrity of the TOE by triggering a self-test (e.g. by powering on or rebooting the TOE using the reset switch) and examining the Keyboard LEDs for self-test failures as identified above.

6.3 TOE Access

The TOE display a continuous visual indication of the computer to which the user is currently connected, and displays the indicator on power up, and on reset.

6.3.1 FTA_CIN_EXT.1 – Continuous Indications

The Port LEDs on the keyboard remote control provide a continuous visual indication of the selected Port and corresponding selected computer (blue) to which the user is currently connected at all times when the TOE is powered.

Upon successful power-up and reset, the TOE defaults to select PC1, if powered on, and the blue LED indicator for PC1 Source TX source is lit. If PC1 is powered off, the TOE defaults to select PC2. If both PC1 and PC2 are powered off, the TOE defaults to select PC3. The keyboard, which receives the PC1_ON and PC2_ON signals from the Power Control Panel, prevents the TOE from selecting PC1 or PC2 if they are powered off. The indicator showing the selected computer remains lit until switched by the user. The user can switch between the connected computer sources by simultaneously using the function and selector keys. Once the connection is successfully switched, the previously selected source LED indicator is shut off and the newly selected source LED indicator is lit. During power-up and reset, the KVM functions and interfaces are not accessible until the self-tests have successfully completed at which point the blue LED indicator for the default host computer will light.

Indicators for the selected channel are located with the remote control on the top right of the keyboard. The LEDs indicate blue for selected host or red for fault. There is an LED indicator for each of the connected computers. The TOE chassis itself also includes a LNK LED on each transmitter. When a given channel is

selected, the LNK LED for the corresponding transmitter is illuminated. This is the same information that is conveyed on the remote control.

The TOE supports connected displays from a single source video feed (multi-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 Keyboard.

7 Protection Profile Claims

This ST is conformant to the Protection Profile [PSD], including the following optional and selection-based SFRs: FDP_SWI_EXT.2, and FTA_CIN_EXT.1.

The ST is also conformant to the following PP-Modules

- *PP-Module for Keyboard/Mouse Devices*, Version 1.0, 19 July 2019 [MOD-KM], including the following optional and selection-based SFRs: FDP_FIL_EXT.1/KM, FDP_RIP.1/KM, and FDP_SWI_EXT.3
- *PP-Module for Video/Display Devices*, Version 1.0, 19 July 2019 [MOD-VI], including the following selection-based SFRs: FDP_CDS_EXT.1, FDP_IPC_EXT.1, and FDP_SPR_EXT.1/DP

As explained in Section 3, the Security Problem Definition of the [PSD] and modules have been included in this ST by reference.

As explained in Section 4, Security Objectives, the Security Objectives of the [PSD] and modules have been included by reference in this ST.

The following table identifies all the Security Functional Requirements (SFRs) in this ST, drawn from the [PSD], [MOD-KM] and [MOD-VI]. The only operations performed on the SFRs drawn from the [PSD] are assignment and selection operations.

Table 7 identifies the SFRs that are satisfied by the TOE.

Table 7: SFR Protection Profile Sources

Requirement Class	Requirement Component	Source
FDP: User Data Protection	FDP_APC_EXT.1 – Active PSD Connections	[PSD]
	FDP_CDS_EXT.1 – Connected Displays Supported	[MOD-VI]
	FDP_FIL_EXT.1/KM – Device Filtering (Keyboard/Mouse)	[MOD-KM]
	FDP_IPC_EXT.1 – Internal Protocol Conversion	[MOD-VI]
	FDP_PDC_EXT.1 – Peripheral Device Connection	[PSD]
	FDP_PDC_EXT.2/KM – Authorized Devices (Keyboard/Mouse)	[MOD-KM]
	FDP_PDC_EXT.2/VI – Peripheral Device Connection (Video Output)	[MOD-VI]
	FDP_PDC_EXT.3/KM – Authorized Connection Protocols (Keyboard/Mouse)	[MOD-KM]
	FDP_PDC_EXT.3/VI – Authorized Connection Protocols (Video Output)	[MOD-VI]
	FDP_RIP.1/KM – Residual Information Protection (Keyboard Data)	[MOD-KM]
	FDP_RIP_EXT.1 – Residual Information Protection	[PSD]
	FDP_SPR_EXT.1/DP – Sub-Protocol Rules (DisplayPort Protocol)	[MOD-VI]
	FDP_SWI_EXT.1 – PSD Switching	[PSD]
	FDP_SWI_EXT.2 – PSD Switching Methods	[PSD]
	FDP_SWI_EXT.3 – Tied Switching	[MOD-KM]

Requirement Class	Requirement Component	Source
	FDP_UDF_EXT.1/KM – Unidirectional Data Flow (Keyboard/Mouse)	[MOD-KM]
	FDP_UDF_EXT.1/VI – Unidirectional Data Flow (Video Output)	[MOD-VI]
FPT: Protection of the TSF	FPT_FLS_EXT.1 – Failure with Preservation of Secure State	[PSD]
	FPT_NTA_EXT.1 – No Access to TOE	[PSD]
	FPT_PHP.1 – Passive Detection of Physical Attack	[PSD]
	FPT_TST.1 – TSF Testing	[PSD]
	FPT_TST_EXT.1 – TSF Testing	[PSD]
FTA: TOE Access	FTA_CIN_EXT.1 – Continuous Indications	[PSD]

8 Rationale

This security target includes by reference the [PSD], [MOD-KM], and [MOD-VI] Security Problem Definitions, Security Objectives, and Security Assurance Requirements. The security target makes no additions to the [PSD] or listed modules assumptions. The [PSD] and listed module's security functional requirements have been reproduced with the Protection Profile operations completed. Operations on the security requirements follow [PSD] and the module's application notes and assurance activities. Consequently, [PSD] and the module's rationale applies but is incomplete. The TOE Summary Specification rationale below serves to complete the rationale required for the security target.

8.1 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. Table 8 demonstrates the relationship between security requirements and security functions.

Table 8: Security Functions vs. Requirements Mapping

Specifications	User Data Protection	Protection of the TSF	TOE Access
FDP_AFL_EXT.1	X		
FDP_APC_EXT.1	X		
FDP_CDS_EXT.1	X		
FDP_FIL_EXT.1/KM	X		
FDP_IPC_EXT.1	X		
FDP_PDC_EXT.1	X		
FDP_PDC_EXT.2/KM	X		
FDP_PDC_EXT.2/VI	X		
FDP_PDC_EXT.3/KM	X		
FDP_PDC_EXT.3/VI	X		
FDP_RIP.1/KM	X		

Specifications	User Data Protection	Protection of the TSF	TOE Access
FDP_RIP_EXT.1	X		
FDP_SPR_EXT.1/DP	X		
FDP_SWI_EXT.1	X		
FDP_SWI_EXT.2	X		
FDP_UDF_EXT.1/KM	X		
FDP_UDF_EXT.1/VI	X		
FPT_FLS_EXT.1		X	
FPT_NTA_EXT.1		X	
FPT_PHP.1		X	
FPT_TST.1		X	
FPT_TST_EXT.1		X	
FTA_CIN_EXT.1			X

Appendix A Letter of Volatility

Item No.	Component Function	Component type, Manufacturer, and Part number	Memory Type	Memory Size	Memory Technology	User Data
1.	Transmitter and Receiver Boot PROM. Also stores EDID, video re-timer re-driver parameters and phase-lock look parameters	Boot PROM Micron Technology MT25QL01GBBB	Flash	1 Gb	Non-volatile	No user data
2	Transmitter and Receiver Glue Logic CPLD (Configuration Image)	CPLD Lattice Semiconductor LCMXO2-256ZE-SG32C	Internal Flash	71 Kb	Non-volatile	No user data
3.	Transmitter and Receiver Glue Logic CPLD (Runtime Configuration)	CPLD Lattice Semiconductor LCMXO2-256ZE-SG32C	Internal SRAM	2 Kb	Volatile	No user data
4.	Transmitter and Receiver Xilinx FPGA Runtime Memory	FPGA Xilinx XCZU7EV-2FFVF1517E	Internal SRAM	256 KB	Volatile	Yes, Video, USB HID reports
5.	Transmitter and Receiver Xilinx FPGA Cache Memory	FPGA Xilinx XCZU7EV-2FFVF1517E	Internal SRAM	256 KB L1 Cache, 1 MB L2 Cache	Volatile	No user data

6.	Transmitter CPU DRAM	DRAM Micron Technology MT40A1G16RC (or equivalent)	DRAM	2 x 16 Gb	Volatile	No user data
7.	Receiver CPU DRAM	DRAM Micron Technology MT40A1G16RC (or equivalent)	DRAM	2 x 16 Gb	Volatile	No user data
8.	Receiver Upper Display Video	DRAM Micron Technology MT40A1G16RC (or equivalent)	DRAM	2 x 16 Gb	Volatile	Yes, Upper display video
9.	Receiver Lower Display Video	DRAM Micron Technology MT40A1G16RC (or equivalent)	DRAM	2 x 16 Gb	Volatile	Yes, Lower Display Video
10.	Transmitter and Receiver Linux File System Storage	SDHC Card Kingston 31663-023,A00LF (or equivalent)	SDHC Card	32 GB	Non-volatile	No user data
11.	Not used in both Transmitter and Receiver	Serial EEPROM Atmel AT24C512B	Serial EEPROM	2x 512 Kb	Non-volatile	No user data
12.	Optical Switch Calibration Data	Serial EEPROM Microchip 25LC256-H/SN	EEPROM	256 Kb	Non-volatile	No user data
13.	Optical Switch Processor program storage	Microcontroller NXP LPC2148FBD64	Flash	512 KB	Non-volatile	No user data

14.	Keyboard Backlight Brightness Controller Code	Microcontroller Microchip PIC16F676T	Internal SRAM	64 Bytes	Volatile	No user data
15.	Keyboard Data Memory	Microcontroller Microchip PIC18F45K50	Internal SRAM	2 KB	Volatile	Yes, keystroke data
16.	Keyboard Memory- Not Used	NXP MMA8453Q	SRAM	3 Bytes	Volatile	No user data
17.	Keyboard Backlight Brightness Controller Code Storage	Microcontroller Microchip PIC16F676T	Internal Flash	1 KB	Non-Volatile	No user data
18.	Keyboard Backlight Brightness Levels	Microcontroller Microchip PIC16F676T	Internal EEPROM	128 Bytes	Non-Volatile	No user data
19.	Keyboard Main CPU Program Memory	Microcontroller Microchip PIC18F45K50	Internal Flash	32 KB	Non-Volatile	No user data
20.	Keyboard Main CPU Background Brightness Settings (Shared With Background Brightness Controller)	Microcontroller Microchip PIC18F45K50	Internal EEPROM	256 Bytes	Non-Volatile	No user data
21.	Keyboard Memory – Not Used	NXP MMA8453Q	Internal One-Time Programmable ROM	3 Bytes	Non-Volatile	No user data
22.	Keyboard VID/PID Storage	EEPROM STM M93C76	EEPROM	2 x 1 KB	Non-Volatile	No user data

All components are powered by the Secure KVM only with the exception of the keyboard components that are powered by the keyboard.

As identified in the above table, no user data is stored in Non-Volatile memory and some user data is stored in Volatile memory. User data in Volatile memory is purged from the buffers when the TOE is powered down or reset with the following exceptions. The keyboard is not subject to the reset function and therefore user data in the Keyboard Data Memory may remain in data buffers until power to TOE is shutdown.