National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

BAE Systems Secure KVM Gen2 8560943-2

Report Number: **CCEVS-VR-11304-2023**

Dated: **January 12, 2023**

Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

James Donndelinger

DeRon Graves

Fernando Guzman

Marybeth Panock

The Aerospace Corporation

Common Criteria Testing Laboratory

Justin Fisher

Josh Marciante

Armin Najafabadi

Allen Sant

Leidos
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the BAE Systems Secure KVM Gen2 8560943-2 peripheral sharing device. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. It applies only to the specific version and configuration of the product as evaluated and as documented in the Security Target (ST).

The evaluation of the BAE Systems Secure KVM Gen2 8560943-2 switch (Secure KVM) was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in January 2023. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Leidos.

The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 5 **Error! Reference source not found.** and the evaluation activities specified in the following materials:

- *Protection Profile for Peripheral Sharing Device*, Version 4.0, 19 July 2019 (PP_PSD_V4.0) or [PSD]
  - including the following optional and selection-based SFRs: FTA_CIN_EXT.1.
- *PP-Module for Keyboard/Mouse Devices*, Version 1.0, 19 July 2019 (MOD_KM_V1.0)
  - 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_V1.0)
  - including the following selection-based SFRs: FDP_CDS_EXT.1, FDP_IPC_EXT.1, 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
- TD0539 – Incorrect Selection Trigger in FTA_CIN_EXT.1 in MOD_VI_V1.0
- 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

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The BAE Systems Secure KVM Gen2 is a purpose-built peripheral sharing device that allows for securely sharing one set of peripherals between multiple computers. The KVM includes console ports and computer ports. The console ports are used to connect a single set of peripherals (keyboard, trackball, flat panel display, and flat panel display with touch panel) to three separate computers in the evaluated configuration. 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 supports manual port switching using a wired remote control that is embedded in the purpose-built console keyboard. Operating the remote control commands, the KVM to connect its peripherals to the selected computer.

This report is intended to assist the end-user of this product and any security certification agent for that end-user to determine the suitability of this Information Technology (IT) product in their environment. End-users should review the ST [6] , (which is where specific security claims are made) as well as this VR (which describes how those security claims were evaluated, tested, and any restrictions that may be imposed upon the evaluated configuration) to help in that determination. Prospective users should carefully read the Assumptions and Clarification of Scope in section 4 and the Validator Comments in section 10, where any restrictions on the evaluated configuration are highlighted.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PP had been completed successfully and that the product satisfied all of the security functional and assurance requirements as stated in the ST.

Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the BAE Systems Secure KVM Gen2 8560943-2 Security Target.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL) (https://www.niap-ccevs.org/Product/).

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluated Product	BAE Systems Secure KVM Gen2 8560943-2
Sponsor & Developer	BAE Systems plc 450 Pulaski Road Greenlawn, NY 11740
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	January 12, 2023
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 5, April 2017
PP	Protection Profile for Peripheral Sharing Device, Version 4.0 PP-Module for Keyboard/Mouse Devices, Version 1.0 PP-Module for Video/Display Devices, Version 1.0
Evaluation Personnel	Justin Fisher, Leidos Josh Marciante, Leidos Armin Najafabadi, Leidos Allen Sant, Leidos

Item	Identifier
Validation Personnel	James Donndelinger: Senior Validator, The Aerospace Corporation DeRon Graves: Lead Validator (Trainee), The Aerospace Corporation Fernando Guzman: ECR Team (Trainee), The Aerospace Corporation Marybeth Panock: Lead Validator. The Aerospace Corporation

Table 1: Evaluation Details

The following table identifies the evaluated Security Target and TOE.

Name	Description
ST Title	BAE Systems Secure KVM Gen2 8560943-2 Security Target
ST Version	v1.0
Publication Date	January 10, 2023
TOE Developer	BAE Systems plc
TOE Reference	BAE Systems Secure KVM Gen2 (part number 8560943-2)
TOE Software Version	Firmware version v2.1
Keywords	KVM Switch, Peripheral Sharing Switch

Table 2: Security Target Identification

2.1 Organizational Security Policies

There are no Organizational Security Policies for the *Protection Profile for Peripheral Sharing Device* [5].

3 Assumptions, Threats, and Clarifications of Scope

3.1 Assumptions

The ST identifies the following assumptions about the use of the product:

- Computers and peripheral devices connected to the PSD are not TEMPEST approved.
- The environment provides physical security commensurate with the value of the TOE and the data it processes and contains.
- The environment includes no wireless peripheral devices.
- Users are trusted to follow and apply all guidance in a trusted manner.
- Personnel configuring the PSD and its operational environment follow the applicable security configuration guidance.
- 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.
- 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.
- 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.

3.2 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter the following threats.

- A connection via the PSD between one or more computers may allow unauthorized data flow through the PSD or its connected peripherals.
- A connection via the PSD between one or more computers may allow unauthorized data flow through bit-by-bit signaling.
- A PSD may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer.
- A PSD may connect the user to a computer other than the one to which the user intended to connect.
- 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.

- 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.
- A malicious user or human agent could physically modify the PSD to allow unauthorized information flows.
- 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.
- Detectable failure of a PSD may cause an unauthorized information flow or weakening of PSD security functions.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific hardware products, and firmware versions identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation. Any additional non-security related functional capabilities of the product, even those described in the ST, were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM **Error! Reference source not found.** defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

The BAE Systems Secure KVM Gen2 consists of three identical transmitter (Tx) modules for connecting with three host computers, one receiver (Rx) module, 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 within the 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. The messages use a specific format and require parity checks. 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 are Host PC1, Host PC2, and Host PC3 (selected computer interfaces).
    - Host PC1, Host PC2, and Host PC3 are copper interfaces, each consisting of two video interfaces and one USB 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 for Host PC4 located remote to the "main" KVM chassis. This interface and the Host PC4 transmitter are not part of the TOE. See Figure 1.

The workstation cabinet that the KVM resides within, and 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 product includes a handgrip device that is

[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.

connected to the keyboard using a USB connector. This device is not switched and does not use the KVM. The handgrip is out of scope and not part of the TOE.

Host PC1 and Host PC2 output 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. HDMI uses the TMDS waveform. Host PC4 sends DVI-D, which also uses the TMDS waveform, to the TOE. The TOE receives the TMDS video streams 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.

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) that switches the data over a fiber-optic connection. 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. Host PC1 and Host PC2 share a common -48VDC power supply that is inside the workstation, but each computer has its own input power filtering. Host PC3 has its own power supply.

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.

4.2 Physical Boundary

The figure below shows a high-level diagram of the TOE in its operational environment. The main chassis of the TOE consists of an optical switch, power distribution board, three transmitters and a receiver. The peripheral keyboard is a standard HID class device that interfaces with the TOE over USB. However, it also has a remote control function with channel switch keys and status indicators physically embedded into it; these are considered to be the TOE's wired remote control, which communicates with the TOE over an RS-232 data path that is physically and logically isolated from the USB HID peripheral signals.

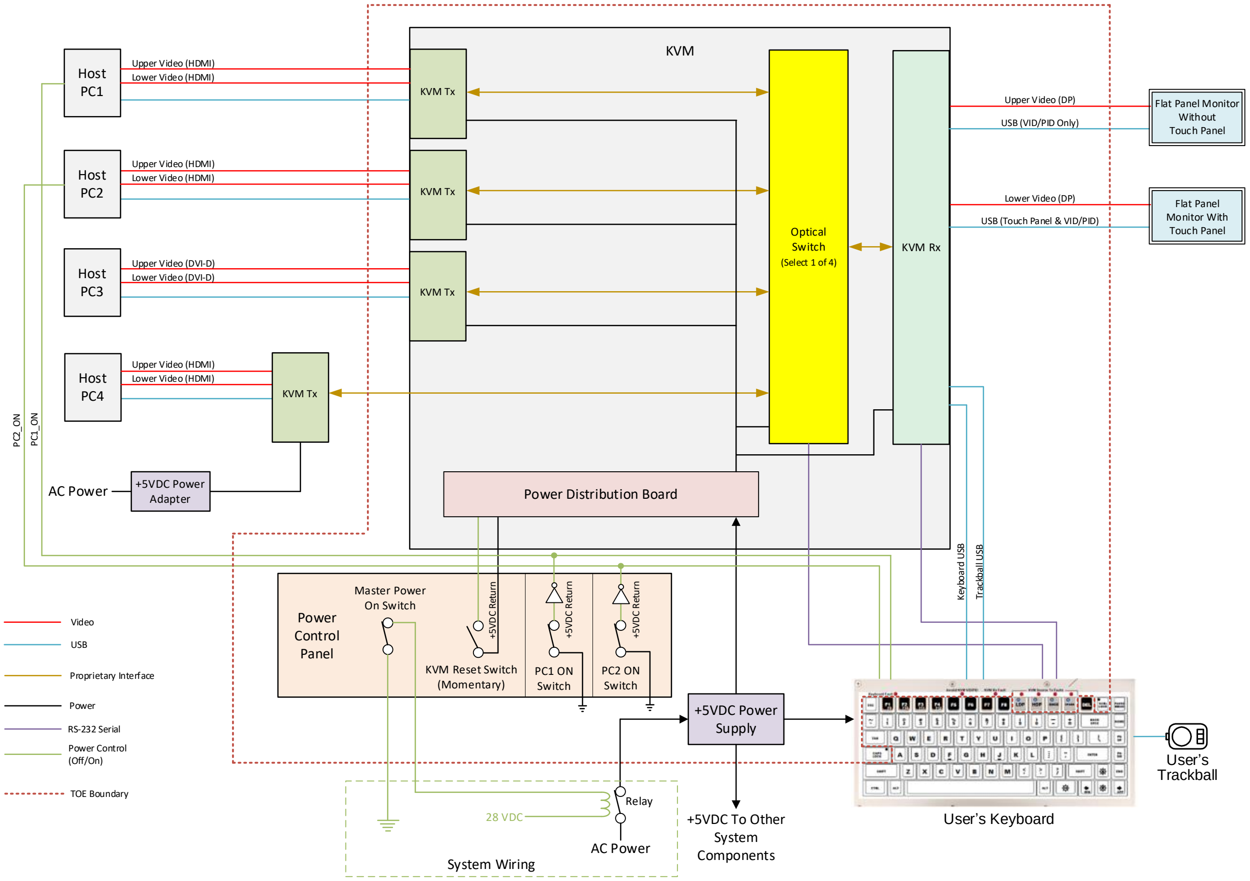

Figure 1 Simplified block diagram of the TOE

5 Security Policy

The TSF enforces the following TOE functional policies as specified in the ST.

5.1 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 two DisplayPort monitors, one with touch panel. The TOE accepts TMDS video waveform outputs from connected computers over DisplayPort which is processed by the TOE and converted 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.

5.2 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.

5.3 TOE Access

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

6 Documentation

The vendor documentation examined during the course of the evaluation is as follows:

- BAE Systems Generation 2 Keyboard, Video, Mouse Switch (KVM) User's Guide (P/N: 8560943-2), January 10, 2023
- BAE Systems Secure KVM Gen2 8560943-2 Security Target, Version 1.0, January 10, 2023
- BAE Systems Secure KVM Gen2 8560943-2 Isolation Documentation and Assessment, Version 1.0, November 2, 2022 (BAE Systems Proprietary)

The isolation document supplements the Security Target in order to demonstrate the how 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.

The documentation listed above is the only documentation that should be trusted to install, administer, or use the TOE in its evaluated configuration. Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated. To use the product in the evaluated configuration, the product must be configured as specified in the guidance documentation listed above.

Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 Evaluated Configuration

7.1 Evaluated Configuration

The evaluated version of the TOE consists of the BAE Systems Secure KVM Gen2 (part number 8560943-2) deployed in its operational environment which includes the purpose-built peripherals intended for use with the TOE as well as the power control system used to deliver electrical power to it. The peripherals specifically include the peripheral keyboard that also contains embedded wired remote control functionality that communicates with the rest of the TOE over a separate data path from the USB HID channel.

The TOE must be deployed as described in section 0 The BAE Systems Secure KVM Gen2 consists of three identical transmitter (Tx) modules for connecting with three host computers, one receiver (Rx) module, 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 within the 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. The messages use a specific format and require parity checks. 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 are Host PC1, Host PC2, and Host PC3 (selected computer interfaces).
  - Host PC1, Host PC2, and Host PC3 are copper interfaces, each consisting of two video interfaces and one USB 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, USB Trackball.

Note that the KVM also has a fiber optic I/O interface for a fourth transmitter module for Host PC4 located remote to the “main” KVM chassis. This interface and the Host PC4 transmitter are not part of the TOE. See Figure 1.

The workstation cabinet that the KVM resides within, and 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 product includes a handgrip device that is connected to the keyboard using a USB connector. This device is not switched and does not use the KVM. The handgrip is out of scope and not part of the TOE.

Host PC1 and Host PC2 output 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. HDMI uses the TMDS waveform. Host PC4 sends DVI-D, which also uses the TMDS waveform, to the TOE. The TOE receives the TMDS video streams 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.

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) that switches the data over a fiber-optic connection. 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. Host PC1 and Host PC2 share a common -48VDC power supply that is inside the workstation, but each computer has its own input power filtering. Host PC3 has its own power supply.

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.

7.2 Physical Boundary

The figure below shows a high-level diagram of the TOE in its operational environment. The main chassis of the TOE consists of an optical switch, power distribution board, three transmitters and a receiver. The peripheral keyboard is a standard HID class device that interfaces with the TOE over USB. However, it also has a remote control function with channel switch keys and status indicators physically embedded into it; these are considered to be the TOE's wired remote control, which communicates with the TOE over an RS-232 data path that is physically and logically isolated from the USB HID peripheral signals.

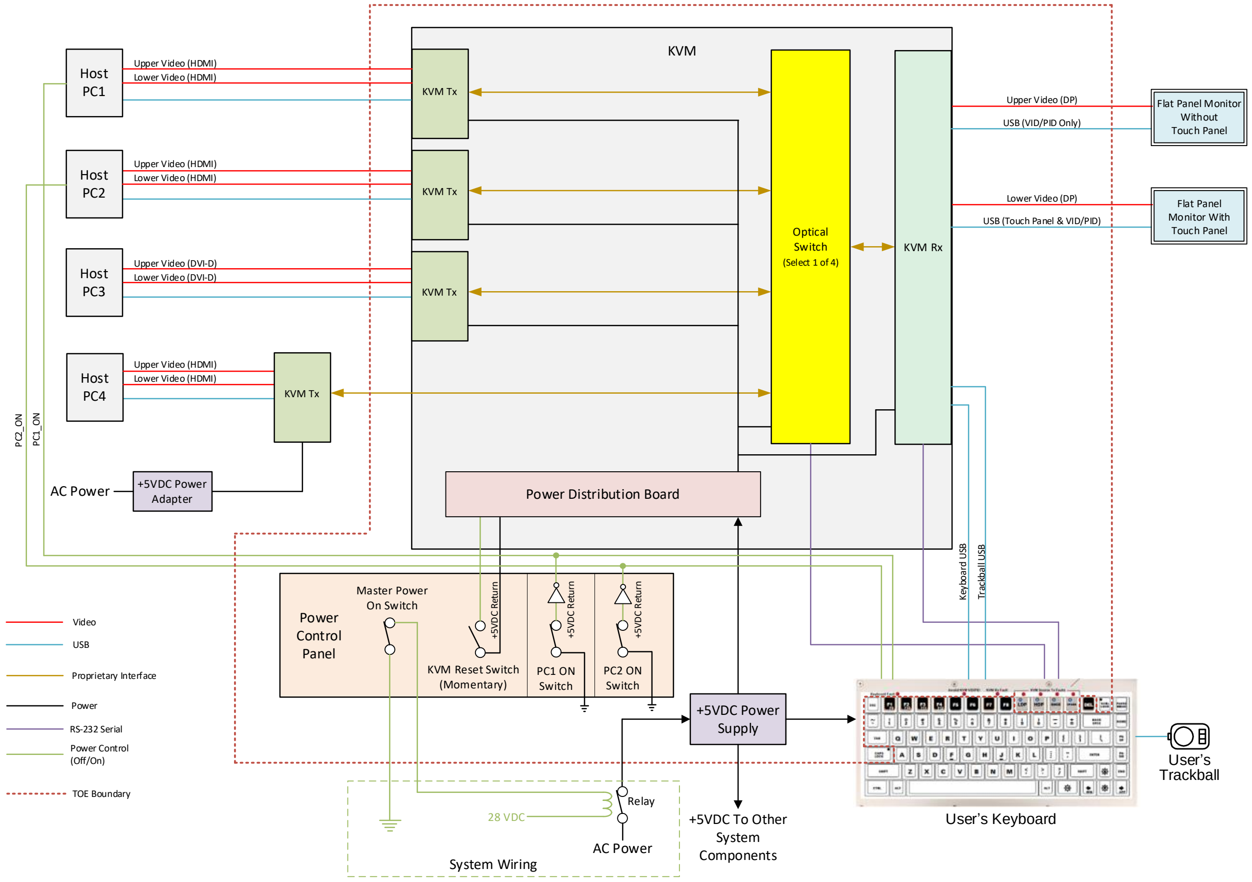

Figure 1 Simplified block diagram of the TOE

of this document and be configured in accordance with the documentation identified in Section 6.

7.3 Excluded Functionality

The fourth transmitter, external to the TOE boundary was excluded from the evaluation. And as such violates one of the security requirements of the PP_PSD_V4.0. However, for this product only, the NIAP Technical Rapid Response Team(TRRT) for Peripheral Sharing Switch approved Technical Query (TQ) 1354. This allows the evaluated product to have a fourth port that a fourth transmitter, referred to by the TOE developer as the "spare transmitter" to be optionally connected. This requires introduction of a standalone transmitter device that is physically separate from the rest of the KVM and outside the TOE boundary.

8 Independent Testing

8.1 Evaluation team independent testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- BAE Systems Secure KVM PSD PP 4.0 Common Criteria Common Criteria Test Report and Procedures, Version 1.1, January 10, 2023

A non-proprietary summary of the test configuration, test tools, and tests performed may be found in:

- Assurance Activities Report for BAE Systems Secure KVM Gen2 8560943-2, Version 1.1, January 10, 2023

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to *Protection Profile for Peripheral Sharing Device* [5].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Protection Profile for Peripheral Sharing Device* [5]. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

The TOE was delivered to Leidos but was deployed at an alternate site outside the AT&E lab. The evaluators ensured that the physical security of the site was sufficient to ensure the legitimacy of test results per NIAP Labgram 078, with information about the preparation and observation of the site submitted to and subsequently approved by NIAP. Independent testing took place at this alternate site in Columbia, Maryland from August 15, 2022 to October 25, 2022.

The evaluators received the TOE in the form of the console workstation that normal customers would receive it with, except where modifications were made to allow the test evaluation activities to be performed.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *Protection Profile for Peripheral Sharing Device* [5] and the claimed PP-Modules were fulfilled.

8.2 Vulnerability Survey

A search of public domain sources for potential vulnerabilities in the TOE did not reveal any known exploitable vulnerabilities. Public domain information relating to the TOE in any capacity was not found. The vulnerability survey also included searches for vulnerabilities relating to potential flaws in KVM technology in general as well as searches relating to communications protocols and third-party components used by the TOE.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Protection Profile for Peripheral Sharing Switch* [5] in conjunction with version 3.1 revision 4 of the CC and the CEM (**Error! Reference source not found.**, **Error! Reference source not found.**, **Error! Reference source not found.**, and **Error! Reference source not found.**). A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The validation team's assessment of the evidence provided by the evaluation team is that the evidence demonstrates the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR) **Error! Reference source not found.**, which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic function specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

Table 3: TOE Security Assurance Requirements

9.1 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Documents related to the examination of the information contained in the TOE Summary Specification.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Evaluation Activities, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Guidance Documents

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Document related to the examination of the information contained in the operational guidance documents.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Evaluation Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work units. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Evaluation Activities in the NDcPP Supporting Documents and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the NDcPP Supporting Documents were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis requirements in the NDcPP Supporting Documents, and that the conclusion reached by the evaluation team was justified.

9.6 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s test activities also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Evaluation Activities in the NDcPP Supporting Document, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the instructions in the BAE Systems Generation 2 Keyboard, Video, Mouse Switch (KVM) User's Guide (P/N: 8560943-2), January 10, 2023. No versions of the TOE and software, either earlier or later were evaluated.

As noted in the Excluded Functionality section 7.2, the 4th port or interface for the fourth transmitter is outside of the TOE boundary. And as such violates one of the security requirements of the PP_PSD_V4.0. However, for this product only, the NIAP Technical Rapid Response Team(TRRT) for Peripheral Sharing Switch approved Technical Query (TQ) 1354. This allows the evaluated product to have a fourth port that a fourth transmitter, referred to by the TOE developer as the "spare transmitter" to be optionally connected. This requires introduction of a standalone transmitter device that is physically separate from the rest of the KVM and outside the TOE boundary. This fourth interface was tested.

As section 7.2 states, there was a deviation from the security requirements of PP_PSD_V4.0. The validators addressed this in multiple ways including use of a TRRT and multiple updates to the Lab provided Isolation Document. Validators requested the Lab discuss the various protocols used and what capabilities they provided. Validators also required the Lab to demonstrate the functionality of the product over the course of multiple sync sessions to ensure understanding and verify that the 4th transmitter could not be "spoofed" by potential intruders.

All other functionality provided, to include software, firmware, or hardware that was not part of the evaluated configuration needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

All other concerns and issues are adequately addressed in other parts of this document.

11 Annexes

Not applicable.

12 Security Target

Name	Description
ST Title	BAE Systems Secure KVM Gen2 8560943-2 Security Target
ST Version	v1.0
Publication Date	January 10, 2023

Table 4: Security Target Identification

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1 Revision 5, April 2017.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

[5] Protection Profile for Peripheral Sharing Device, Version 4.0, 19 July 2019 (PP_PSD_V4.0) or [PSD]

[6] BAE Systems Secure KVM Gen2 8560943-2 Security Target Public Version, Version 1.0, January 10, 2023

[7] BAE Systems Secure KVM Gen2 8560943-2 Security Target Proprietary Version, Version 1.0, January 10, 2023

[8] Assurance Activities Report for BAE Systems Secure KVM Gen2 8560943-2 Public Version, Version 1.1, January 10, 2023

[9] Assurance Activities Report for BAE Systems Secure KVM Gen2 8560943-2 Proprietary Version, Version 1.1, January 10, 2023

[10] BAE Systems Secure KVM PSD PP 4.0 Common Criteria Common Criteria Test Report and Procedures, Version 1.1, January 10, 2023

[11] Evaluation Technical Report for BAE Systems Secure KVM Gen2 8560943-2, Version 1.1, January 10, 2023

[12] BAE Systems Generation 2 Keyboard, Video, Mouse Switch (KVM) User’s Guide (P/N: 8560943-2), Version -, January 10, 2023

[13] *PP-Module for Keyboard/Mouse Devices*, Version 1.0, 19 July 2019 (MOD_KM_V1.0)

[14] *PP-Module for Video/Display Devices*, Version 1.0, 19 July 2019 (MOD_VI_V1.0)