National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Raritan Secure KVM Switch Series with CAC

Report Number: **CCEVS-VR-VID11323-2023**

Dated: **April 20, 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

Daniel Faigin
Fernando Guzman
Meredith Martinez
The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos
Columbia, MD

Table of Contents

List of Figures

List of Tables

1 Executive Summary

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 Security Target (ST) [5][1], (which is where specific security claims are made) as well as this Validation Report (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.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Raritan Secure KVM Switch Series with CAC of peripheral sharing switches. It presents the evaluation results, their justifications, and the conformance results. This 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. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the Raritan Secure KVM Switch Series with CAC peripheral sharing switches was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in April 2023. 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 [4] and the assurance activities specified in the PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/MouseDevices, User Authentication Devices, and Video/Display Devices, 19 July 2019 including the following components:

- Base-PP: Protection Profile for Peripheral Sharing Device, Version 4.0
  - including the following optional and selection-based SFRs: FAU_GEN.1, FDP_RIP_EXT.2, FDP_SWI_EXT.2, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_SMF.1, FMT_SMR.1, FPT_PHP.3, FPT_STM.1, and FTA_CIN_EXT.1.
- PP-Module: PP-Module for Analog Audio Output Devices, Version 1.0, 19 July 2019
- PP-Module: PP-Module for Keyboard/Mouse Devices, Version 1.0, 19 July 2019
  - including the following optional and selection-based SFRs: FDP_FIL_EXT.1/KM, FDP_RIP.1/KM, and FDP_SWI_EXT.3.
- PP-Module: PP-Module for User Authentication Devices, Version 1.0, 19 July 2019

[1] See section 14 Bibliography.

  - including the following selection-based SFRs: FDP_TER_EXT.2 and FDP_TER_EXT.3.

- PP-Module: PP-Module for Video/Display Devices, Version 1.0, 19 July 2019
  - *including the following selection-based SFRs: FDP_CDS_EXT.1, FDP_IPC_EXT.1, FDP_SPR_EXT.1/DP(DP), FDP_SPR_EXT.1/DVI-I(D), and FDP_SPR_EXT.1/HDMI(H).*

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

- TD0686 – DisplayPort CEC Testing
- TD0681 – PSD purging of EDID data upon disconnect
- TD0620 – EDID Read Requirements
- TD0619 – Test EAs internal UA devices
- TD0593 – Equivalency Arguments for PSD
- TD0586 – DisplayPort and HDMI Interfaces in FDP_IPC_EXT.1
- TD0585 – Update to FDP_APC_EXT.1 Audio Output Tests
- TD0584 – Update to FDP APC_EXT.1 Video Tests
- TD0583 – FPT_PHP.3 modified for PSD remote controllers
- TD0557 – Correction to Audio Filtration Specification Table in FDP_AFL_EXT.1
- TD0539 – Incorrect Selection Trigger in FTA_CIN_EXT.1 in MOD_VI_V1.0
  - The TOE does not fit the Combiner Use Case and so the specific assignment required by the VI Module does not apply.
- 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 Leidos evaluation team determined that the Raritan Secure KVM Switch Series with CAC of peripheral sharing switches is conformant to the claimed Protection Profile (PP) and, when installed, configured, and operated as specified in the evaluated guidance documentation, satisfied all the security functional requirements stated in the ST. The information in this VR is largely derived from the publicly available Assurance Activities Report (AAR) **Error! Reference source not found.** and the associated proprietary test report **Error! Reference source not found.** produced by the Leidos evaluation team.

The Raritan Secure KVM Switch Series with CAC products allow for the connection of a mouse, keyboard, user authentication device (such as smart card or CAC reader), speaker, and one or two video displays (depending on specific device type) to the Secure KVM Switch, which is then connected to 2, up to 4, or up to 8 separate computers (again depending on specific device type). The user can then switch the connected peripherals between any of the connected computers using a push button on the front of the device or on the RPS. The selected device is always identifiable by a bright orange LED associated with the applicable selection button. The user can switch the peripherals between any of the connected computers while preventing unauthorized data flows or leakage between computers.

The TOE is the following models of the Raritan Secure KVM Switch Series with CAC. The firmware version for all models is v1.1.101.

Table 1: Raritan Secure KVM Switch Series with CAC TOE Models

Configuration (with CAC function)		2-Port	4-Port	8-Port
DisplayPort	Single Head	RSS4-102-DP	RSS4-104-DP	RSS4-108-DP
	Dual Head	RSS4-102-DUAL-DP	RSS4-104-DUAL-DP	RSS4-108-DUAL-DP
HDMI	Single Head	RSS4-102	RSS4-104	N/A
	Dual Head	RSS4-102-DUAL	RSS4-104-DUAL	N/A

The Raritan Secure KVM Switch Series with CAC implement a secure isolation design for all models to share a single set of peripheral components. Each peripheral has its own dedicated data path. USB keyboard and mouse peripherals are filtered and emulated. The USB authentication device connection is on a separate circuit from the keyboard and mouse and, after filtering for qualification, has a direct connection path to the selected computer. The TOE does not emulate the user authentication device function. DisplayPort video from the selected computer is converted internally to HDMI, then back to DisplayPort for communication with the connected video display and the AUX channel is monitored and converted to EDID.

The Raritan Secure KVM Switch Series with CAC are 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 products automatically clear the internal TOE keyboard and mouse buffers.

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 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 the security functional requirements stated in the Raritan Secure KVM Switch Series with CAC Security Target.

Table 2: Evaluation Details

Item	Identifier
Evaluated Product	Raritan Secure KVM Switch Series with CAC devices identified in Table 1
Sponsor & Developer	Legrand DPC LLC d.b.a Raritan 400 Cottontail Lane, Somerset, NJ 08873, U.S.A
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	April 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	PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/MouseDevices, User Authentication Devices, and Video/Display Devices, 19 July 2019 including the following components: Base-PP: Protection Profile for Peripheral Sharing Device, Version 4.0 • PP-Module: PP-Module for Analog Audio Output Devices, Version 1.0, 19 July 2019 • PP-Module: PP-Module for Keyboard/Mouse Devices, Version 1.0, 19 July 2019 • PP-Module: PP-Module for User Authentication Devices, Version 1.0, 19 July 2019 • PP-Module: PP-Module for Video/Display Devices, Version 1.0, 19 July 2019
Disclaimer	The information contained in this Validation Report is not an endorsement of the Raritan Secure KVM Switch Series with CAC by any agency of the U.S. Government and no warranty of Raritan Secure KVM Switch Series with CAC is either expressed or implied.

Item	Identifier
Evaluation Personnel	Justin Fisher Greg Beaver Allen Sant Josh Marciante Armin Najafabadi
Validation Personnel	Daniel Faigin Fernando Guzman Meredith Martinez

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/).

The following table identifies the evaluated Security Target and TOE.

Name	Description
ST Title	Raritan Secure KVM Switch Series with CAC Security Target
ST Version	V1.1
Publication Date	April 10, 2023
Vendor and ST Author	Raritan
TOE Reference	Raritan Secure KVM Switch Series with CAC identified in Table 1
TOE Software Version	Firmware version v1.1.101
Keywords	KVM Switch, Peripheral Sharing Switch

2.1 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.
- A malicious agent could use an unauthorized peripheral device such as a microphone, connected to the TOE audio out peripheral device interface to eavesdrop or transfer data across an air-gap through audio signaling.
- A malicious agent could repurpose an authorized audio output peripheral device by converting it to a low-gain microphone to eavesdrop on the surrounding audio or transfer data across an air-gap through audio signaling.

2.2 Organizational Security Policies

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

3 Architectural Information

The Raritan Secure KVM Switch Series with CAC series are KVM switches with the following characteristics:

- 2/4/8 port USB DisplayPort single and dual display for DisplayPort (6 devices)
- 2/4 port USB HDMI single and dual display for HDMI (4 devices)

The Secure KVM Switch products allow for the connection of a mouse, keyboard, user authentication device (such as smart card or CAC reader), speaker, and one or two video displays (depending on specific device type) to the Secure KVM Switch, which is then connected to 2, up to 4, or up to 8 separate computers (again depending on specific device type). The user can then switch the connected peripherals between any of the connected computers using a push button on the front of the device or on the RPS. The selected device is always identifiable by a bright orange LED associated with the applicable selection button.

To interface with connected computers, the Secure KVM Switch products support analog audio output and USB connections for the keyboard, mouse, and user authentication device. Depending on model, they support DisplayPort or HDMI for the computer video display interface. The switched peripherals on the console side are analog audio output, USB keyboard and mouse, USB user authentication device, and DisplayPort or HDMI video output (depending on model).

Separate USB cables are used to connect the keyboard/mouse combination and the user authentication device to the connected computers. The Secure KVM Switch products supporting DisplayPort convert the DisplayPort video signal to HDMI. The HDMI signal inside the KVM will be converted again to DisplayPort signal for output to the connected video display(s) and the AUX channel is monitored and converted to EDID. The Secure KVM Switch products also support audio output connections from the computers to a connected audio output device. Only speaker connections are supported, and the use of an analog microphone or line-in audio device is prohibited. The tables below identify the interfaces of the Secure KVM console and computer ports according to model number.

Table 3: Raritan Secure KVM Switch Console Interfaces and TOE Models

	Console Video Output		**Console Keyboard**	**Console Mouse**	**Console Audio output**	**Console CAC Reader**
	DisplayPort	**HDMI**	**USB 1.1/2.0**	**USB 1.1/2.0**	**Analog Audio output (Speaker)**	**USB 1.1/2.0**
RSS4-102-DP	•		•	•	•	•
RSS4-102-DUAL-DP	•		•	•	•	•

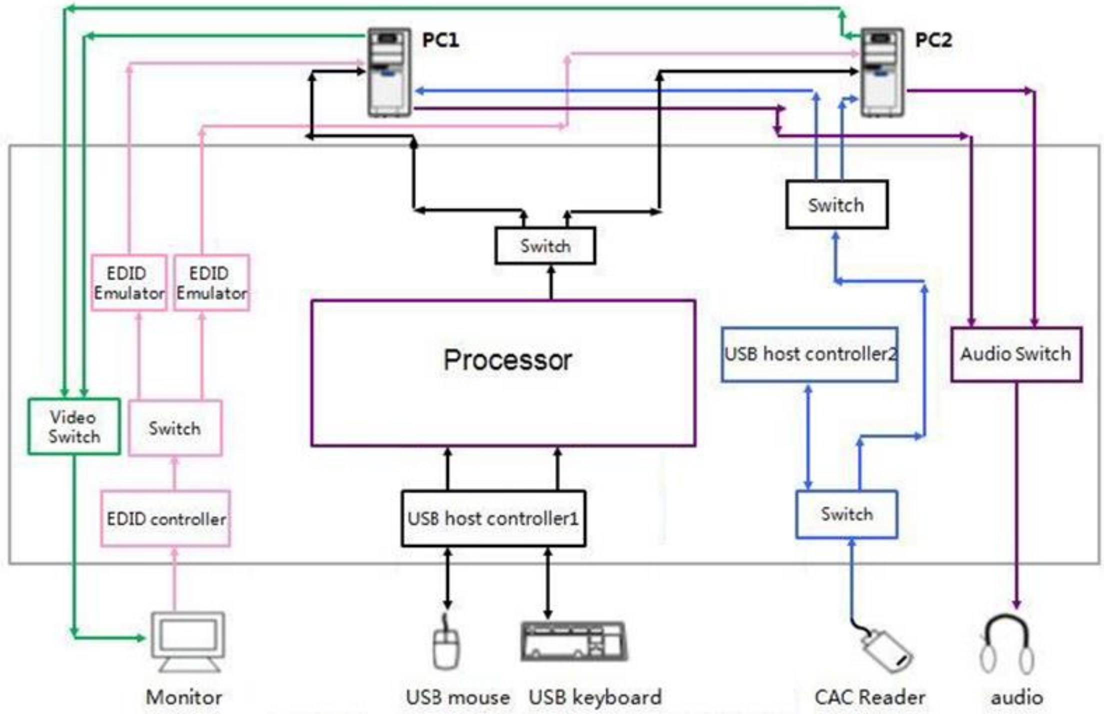
	Console Video Output		Console Keyboard	Console Mouse	Console Audio output	Console CAC Reader
	DisplayPort	HDMI	USB 1.1/2.0	USB 1.1/2.0	Analog Audio output (Speaker)	USB 1.1/2.0
RSS4-102		•	•	•	•	•
RSS4-102-DUAL		•	•	•	•	•
RSS4-104-DP	•		•	•	•	•
RSS4-104-DUAL-DP	•		•	•	•	•
RSS4-104		•	•	•	•	•
RSS4-104-DUAL		•	•	•	•	•
RSS4-108-DP	•		•	•	•	•
RSS4-108-DUAL-DP	•		•	•	•	•

Table 4: Raritan Secure KVM Switch Computer Interfaces and TOE Models

	Computer Video Input Interface		Console Keyboard	Console Mouse	Console Audio output	Console CAC Reader
	DisplayPort	HDMI	USB 1.1/2.0	USB 1.1/2.0	Analog Audio output (Speaker)	USB 1.1/2.0
RSS4-102-DP	•		•	•	•	•
RSS4-102-DUAL-DP	•		•	•	•	•
RSS4-102		•	•	•	•	•
RSS4-102-DUAL		•	•	•	•	•
RSS4-104-DP	•		•	•	•	•
RSS4-104-DUAL-DP	•		•	•	•	•
RSS4-104		•	•	•	•	•
RSS4-104-DUAL		•	•	•	•	•
RSS4-108-DP	•		•	•	•	•
RSS4-108-DUAL-DP	•		•	•	•	•

The following figure shows the data path design using a 2-Port KVM as an example.

Figure 1: Simplified block diagram of a 2-Port KVM TOE



As shown in Figure 1 above, the internal components of the KVM consist of switches, emulators, USB host controllers, processors, and embedded with non-updateable firmware v1.1.101. The internal hardware components are identified in Appendix A and include the manufacturer and the part number. The data flow of USB keyboard/mouse is controlled by the host controller for console HID keyboard and pointing devices. Details of the data flow architecture are provided in the proprietary Secure KVM Isolation Document. All keyboard and mouse connections are filtered first, and only authorized devices will be allowed. The TOE emulates data from authorized USB keyboard and mouse to USB data for computer sources.

The TOEs proprietary design ensures there is no possibility of data leakage from a user's peripheral output device to the input device; ensures that no unauthorized data flows from the monitor to a connected computer; and unidirectional buffers ensure that the audio data can travel only from the selected computer to the audio device. 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 has its own independent Device Controller, power circuit, and EEPROM. Additionally, keyboard and mouse are always switched together.

All Secure KVM Switch components, including the RPS, feature hardware security mechanisms including tamper-evident labels, always active chassis-intrusion detection, and tamper-proof hardware construction, while software security includes restricted USB connectivity (non-Human Interface Devices (HIDs) are ignored when switching), an isolated channel per port that makes it impossible for data to be communicated between computers, and automatic clearing of the keyboard and mouse buffer.

The Raritan Port Authentication Utility must be installed on a separate secure source computer using an installation wizard. The utility supports Microsoft Windows 8 and higher. The Port Authentication Utility computer connects to the TOE via USB connection to Computer Port 1. The dedicated secure source computer must have its own monitor, keyboard, and mouse connected for installation and operation.

4 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.
- PSD Administrators and 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.

4.1 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 [4] defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.

5 Security Policy

Raritan Secure KVM Switch Series with CAC series devices enforce the following TOE security functional policies as specified in the ST.

5.1 Security Audit

The TOE generates audit records for the authorized administrator actions. Each audit record records a standard set of information such as date and time of the event, type of event, and the outcome (success or failure) of the event.

5.2 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 mouse; USB authentication device (CAC reader and smart card); audio output; and (depending on device type) DisplayPort or HDMI video. Some TOE models accept DisplayPort signals at the computer interface and internally convert the signals to HDMI signals and then convert back to DisplayPort for output to the console interface.

The TOE authorizes peripheral device connections with the TOE console ports based on the peripheral device type.

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 immediately after the TOE switches to another selected computer and on start-up of the TOE.

The TOE provides a Reset to Factory Default function allowing authenticated authorized Administrators to remove all settings previously configured by the Administrator (such as USB device Allowlist/Blocklist). Once the Reset to Factory Default function has been completed, the Secure KVM will terminate the Administrator Logon mode, purge keyboard/mouse buffer, and power cycle the Secure KVM automatically.

5.3 Identification and Authentication

The TOE provides an identification and authentication function for the administrative user to perform administrative functions such as configuring the user authentication device filtering Allowlist and Blocklist. The authorized administrator must logon by providing a valid password.

5.4 Security Management

The TOE supports configurable device filtration (CDF). This function is restricted to the authorized administrator and allows the TOE to be configured to accept or reject specific USB devices using CDF Allowlist and Blocklist parameters. Additionally, the TOE provides security management functions to configure the keyboard/mouse device filtration, Reset to Factory Default and to change the administrator password.

5.5 Protection of the TSF

The TOE runs a suite of self-tests during initial startup and after activating the reset button that includes a test of the basic TOE hardware and firmware integrity; a test of the basic computer-to-computer isolation; and a test of critical security functions (i.e., user control and anti-tampering). The TOE provides users with the capability to verify the integrity of the TSF and the TSF functionality.

The TOE resists physical attacks on the main TOE enclosure as well as the RPS enclosure for the purpose of gaining access to the internal components or to damage the anti-tampering battery by becoming permanently disabled. The TOE preserves a secure state by disabling the TOE when there is a failure of the power on self-test, or a failure of the anti-tampering function.

The TOE provides unambiguous detection of physical tampering that might compromise the TSF. The TSF provides the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

5.6 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 guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- *Raritan Secure Switch Administrator Guide,* Release 1.0, August 2022
- *Raritan Secure Switch User Guide,* Release 1.1, August 2022

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. Consumers are encouraged to download these listed guidance documents from the NIAP website.

7 Independent Testing

7.1 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:

- *Raritan Secure KVM PSD PP 4.0 Common Criteria Test Report and Procedures, Version 1.2, April 18, 2023*, **Error! Reference source not found.**

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

- *Assurance Activities Report For Raritan Secure KVM Switch Series with CAC Version 1.2, 2023-04-18*, **Error! Reference source not found.**

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.

Independent testing took place at the Leidos facility in Columbia, Maryland from August 18, 2022, to April 14, 2023.

The evaluators received the TOE in the form that normal customers would receive it, installed, and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

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] were fulfilled.

8 Evaluated Configuration

The evaluated version of the TOE consists of the Raritan Secure KVM Switch Series with CAC devices identified in Table 1.

The TOE must be deployed as described in Section 4 Assumptions of this document and must be configured in accordance with the documentation identified in Section 6.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Protection Profile for Peripheral Sharing Device* [5] in conjunction with version 3.1 revision 5 of the CC and the CEM ([1], [2], [3], and [4]). 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.

Table 5: TOE Security Assurance Requirements

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)
Vulnerability Assessment (AVA)	Vulnerability Survey (AVA_VAN.1)

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the TOE that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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.

9.2 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 and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the claimed PP and PP-Modules related to the examination of the information contained in the TSS.

The validator 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.

9.3 Evaluation of the Guidance Documents (AGD)

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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator 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 Life Cycle Support Activities (ALC)

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

The validator 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 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 assurance activities in the claimed PP and PP-Modules and recorded the results in a Test Report, summarized in the AAR.

The validator 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.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

Searches of public domain sources for potential vulnerabilities in the TOE were conducted periodically throughout the evaluation, most recently on April 11, 2023. During each search, no known vulnerabilities were revealed.

Vulnerability searches were performed using the terms listed below for the rationale listed below:

Search Term	Search Type	Rationale
aten	Advanced: Vendor	TOE vendor
belkin	Advanced: Vendor	Comparable vendor
black box	Advanced: Vendor	Comparable vendor
blackbox	Advanced: Vendor	Comparable vendor
iogear	Advanced: Vendor	Comparable vendor
ipgard	Advanced: Vendor	Comparable vendor
kvm	Basic: Keyword	General type
kvm switch	Basic: Keyword	TOE type
peripheral switch	Basic: Keyword	TOE type
raritan	Advanced: Vendor	Comparable vendor
smartavi	Advanced: Vendor	Comparable vendor (OEM)
tripplite	Advanced: Vendor	Comparable vendor
sekuryx	Advanced: Vendor	Comparable vendor
SICG8021A	Basic: Keyword	Raritan: System Controller Host Controller
SICG8022A	Basic: Keyword	Raritan: Host Controller Device Emulators
AT24C512	Basic: Keyword	Raritan: System EEPROM ATMEL
EN29LV040A	Basic: Keyword	Raritan: System Flash EON

Search Term	Search Type	Rationale
BR24G02-3	Basic: Keyword	Raritan: EDID Emulator ROHM
MX25L4006E	Basic: Keyword	Raritan: DP Video Controller Flash MXIC
ITE IT66354	Basic: Keyword	Raritan: HDMI2.0 Switch

The search of public domain sources for potential vulnerabilities in the TOE did not reveal any known vulnerabilities. More detail on the vulnerability assessment can be found in the *Assurance Activities Report For Raritan Secure KVM Switch Series with CAC Version 1.2, 2023-04-18*, **Error! Reference source not found.**, Section 7.8.

The validator 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.

10 Validator Comments/Recommendations

All validator comments have been addressed in section 4 of this document.

11 Annexes

Not applicable.

12 Security Target

Table 6: Security Target Identification

Name	Description
ST Title	Raritan Secure KVM Switch Series with CAC Security Target
ST Version	v1.1
Publication Date	April 10, 2023

13 Abbreviations and Acronyms

AAR	Assurance Activity Report
CAC	Common Access Card
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Test Lab
CDF	Configurable Device Filtration
CEM	Common Evaluation Methodology
DP	DisplayPort
DVI	Digital Visual Interface
EEPROM	Electrically Erasable Programmable Read-Only Memory
ETR	Evaluation Technical Report
HDMI	High Definition Multimedia Interface
HID	Human Interface Device
IT	Information Technology
KVM	Keyboard, Video and Mouse
LED	Light-Emitting Diode
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PC	Personal Computer
PCL	Product Compliant List
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
USB	Universal Serial Bus

VR	Validation Report

14 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

[6] *Raritan Secure KVM Switch Series with CAC Security Target,* Version 1.1, April 10, 2023

[7] *Assurance Activities Report For Raritan Secure KVM Switch Series with CAC,* Version 1.2, April 18, 2023

[8] *Raritan Secure KVM PSD PP 4.0 Common Criteria Test Report and Procedures, Version 1.2, April 18, 2023*

[9] *Evaluation Technical Report For Raritan Secure KVM Switch Series with CAC (Leidos Proprietary) ETR,* Version 1.2, April 18, 2023