National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Raritan Secure KVM Switch Series of Peripheral Sharing Switches

Report Number: CCEVS-VR-10865-2018

Dated: February 13, 2018

Version: 1.0

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Sheldon Durrant
Joanne Fitzpatrick
The MITRE Corporation

Common Criteria Testing Laboratory

Gregory Beaver
Gary Grainger
Thibaut Marconnet
Kevin Steiner
Leidos
Columbia, MD

Table of Contents

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) [6][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 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 of peripheral sharing switches was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in Feburary 2108. 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 4 [4] and the assurance activities specified in the *Protection Profile for Peripheral Sharing Switch*, Version 3.0 [10]. Leidos performed an analysis of the NIAP Technical Decisions (https://www.niap-ccevs.org/Documents_and_Guidance/view_tds.cfm). 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 Leidos evaluation team determined that the Raritan Secure KVM Switch Series 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 of the security functional requirements stated in the ST. The information in this VR is largely derived from the publically available Assurance Activities Report (AAR) [7] and the associated proprietary test report [8] produced by the Leidos evaluation team.

Each device in the Raritan Secure KVM Switch series is a peripheral sharing switch that allows for securely sharing one set of peripherals between multiple computers. A user may connect a mouse, keyboard, user authentication device such as smart card or CAC reader (optional),

[1] See section 14 Bibliography.

speaker, and a video display, which is then connected to 2, or up to 4 separate computers (depending on specific TOE 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. The selected device is always identifiable by a green 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.

Table 1 Raritan Secure KVM Switch Series TOE Models

TOE Model	Ports	Interfaces
RSS-102	2	Dual Link DVI-I, USB Keyboard, USB mouse, Analog Audio output (ex: Speaker), Switch Buttons, LED indicators, Power Switch and Reset Button.
RSS-104	4	Dual Link DVI-I, USB Keyboard, USB mouse, Analog Audio output (ex: Speaker), Switch Buttons, LED indicators, Power Switch and Reset Button.
RSS-102C	2	Dual Link DVI-I, USB Keyboard, USB mouse, Analog Audio output (ex: Speaker), USB CID/CAC, Switch Buttons, LED indicators, Power Switch and Reset Button.
RSS-104C	4	Dual Link DVI-I, USB Keyboard, USB mouse, Analog Audio output (ex: Speaker), USB CID/CAC, Switch Buttons, LED indicators, Power Switch and Reset Button.

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 Raritan Secure KVM Switch Security Target.

Item	Identifier
Evaluated Product	Raritan Secure KVM Switches Series devices identified in Table 1
Sponsor & Developer	Raritan Inc. 400 Cottontail Lane Somerset, NJ 08873, U.S.A

Item	Identifier
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	January 2018
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	Protection Profile for Peripheral Sharing Switch, Version 3.0
Disclaimer	The information contained in this Validation Report is not an endorsement of the Raritan Secure KVM Switch Series by any agency of the U.S. Government and no warranty of the Raritan Secure KVM Switch Series is either expressed or implied.
Evaluation Personnel	Gregory Beaver Thibaut Marconnet Gary Grainger Kevin Steiner
Validation Personnel	Paul Bicknell: Senior Validator Sheldon Durrant: Lead Validator Joanne Fitzpatrick: Validator Trainee

Table 2: Evaluation Details

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 Security Target
ST Version	V0.7
Publication Date	December 13, 2017
Vendor and ST Author	Raritan, Inc.
TOE Reference	Raritan Secure KVM Switch Series identified in Table 1
TOE Software Version	Firmware version v1.1.101
Keywords	KVM Switch, Peripheral Sharing Switch

3 Architectural Information

Raritan Secure KVM Switch Series provides a secure medium to share a single set of peripheral components such as keyboard, video display and mouse/pointing devices among multiple computers over USB, and/or DVI.

It provides KVM (USB Keyboard/Mouse, DVI-I Video) switch functionality by combining a 2/4 port KVM switch, an audit output port with Speaker, and a Smartcard CCID/CAC port. The TOE is classified as a "Peripheral Sharing Switch" (KVM device) in the Common Criteria. Hardware and firmware components are included in the TOE.

Raritan Secure KVM port models include:

- 2-Port
- 2-Port with CAC
- 4-Port
- 4-Port with CAC

Further architectural information can be found in the Security Target.

4 Assumptions, Threats & Clarifications of Scope

4.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in Protection Profile for Peripheral Sharing Switch, Version 3.0.

4.2 Threats

The Security Problem Definition, including the threats, may also be found in Protection Profile for Peripheral Sharing Switch, Version 3.0.

4.3 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 [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 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, subject identity (if applicable), 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 keyboard, DVI-I, mouse, audio out, and CAC.

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 TOE switch to another selected computer; and on start-up of the TOE.

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 (CDF) whitelist and blacklist. The authorized administrator must logon by providing a valid password. The logon function provides authentication failure handling.

5.4 Security Management

The TOE supports configurable device filtration. This function is restricted to the authorized administrator and allows the TOE to be configured to accept or reject specific USB devices using CDF whitelist and blacklist parameters. Additionally, the TOE provides security management functions to 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 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 TOE 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 course of the evaluation and delivered with the TOE is as follows:

- *Raritan Secure Switch Administrator Guide,* Release 1.0, January 2018
- *Raritan Secure Switch User Guide,* Release 1.0, December 2017
- *2/4-Port USB DVI Secure KVM Switch with or without CAC Feature Port Authentication Utility Guide,* Release 1.0, 15 December 2017
- *Raritan PP3.0 Secure KVM Admin log audit code,* v1.0, 14 December 2017 *(Raritan Proprietary)*
    - **Note:** The Admin Log Audit Code document is provided only to registered customers.

The above documents are considered to be part of the evaluated TOE. The documentation is available by download from https://Raritan.com/support/product/Raritan-secure-switch.

Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration.

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 Switch Series Common Criteria Test Report and Procedures,* Version 1.1, November 1, 2017 [8]

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

- *Assurance Activities Report For Raritan Secure KVM Switches,* Version 0.8, January 25, 2018 [7]

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 Switch* [10].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Protection Profile for Peripheral Sharing Switch,* [10]. 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 September 25, 2017 to October 31, 2017.

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 Switch* [10] were fulfilled.

7.2 Vulnerability Survey

A search of public domain sources for potential vulnerabilities in the TOE did not reveal any known vulnerabilities.

The evaluator conducted penetration testing, based on the potential vulnerabilities identified in the general KVM switch technologies. The testing did not exploit any vulnerability.

8 Evaluated Configuration

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

The TOE must be deployed as described in section 4 Assumptions of this document and 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 Switch* [10] in conjunction with version 3.1 revision 4 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) [9], which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 3: TOE Security Assurance Requirements

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

10 Validator Comments/Recommendations

NIAP established a Peripheral Sharing Switch Technical Rapid Response Team (PSS-TRRT) to address questions and concerns related to evaluations claiming conformance to *Protection Profile for Peripheral Sharing Switch.* A Technical Decision is an issue resolution statement that clarifies or interprets protection profile requirements and assurance activities. PSS-TRRT has formally posted five Technical Decisions related to *Protection Profile for Peripheral Sharing Switch*, namely TD0083, TD0086, TD0136, TD0144 and TD0251. (See https://www.niap-ccevs.org/Documents_and_Guidance/view_tds.cfm.) All PSS-TRRT Technical Decisions with the exception of TD0086 have applied to the Raritan Secure KVM Switch Series evaluation. TOE does not support DisplayPort and therefore TD0086 is not applicable.

11 Annexes

Not applicable.

12 Security Target

Table 4 Security Target Identification

Name	Description
ST Title	Raritan Secure KVM Switch Series Security Target
ST Version	V0.7
Publication Date	December 13, 2017

13 Abbreviations and Acronyms

AAR	Assurance Activity Report
AUX	Auxiliary (Channel)
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
HD	High Definition
HDMI	High Definition Multimedia Interface
HID	Human Interface Device
IT	Information Technology
KVM	Keyboard, Video and Mouse
LED	Light-Emitting Diode
MCCS	Monitor Control Command Set
MCU	Microcontroller Unit
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

PSS	Peripheral Sharing Switch
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 4, September 2012.

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements,* Version 3.1 Revision 4, September 2012.

[3] *Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components,* Version 3.1 Revision 4, September 2012.

[4] *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology,* Version 3.1, Revision 4, September 2012.

[5] *Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories,* Version 2.0, 8 Sep 2008.

[6] *Raritan Secure KVM Switch Series Security Target,* version 0.7, December 13, 2017

[7] *Assurance Activities Report For Raritan Secure KVM Switches, Version 0.8, January 25, 2018*

[8] *Raritan Secure KVM Switch Series Common Criteria Test Report and Procedures,* Version 1.1, November 1, 2017

[9] *Evaluation Technical Report for Raritan Secure KVM Switch,* Version 1.1, January 29, 2018

[10] *Protection Profile for Peripheral Sharing Switch (PSS),* Version 3.0, 13 February 2015