National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Tripp Lite B002a Secure KVM Switch Series

Report Number: **CCEVS-VR-11062-20209**

Dated: **July 9, 2020**

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 (Senior Validator)
Linda Morrison (Lead Validator)

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), (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 Tripp Lite B002a Secure KVM Switch Series. 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 Tripp Lite B002a Secure KVM Switch Series was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in July 2020. 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 and the assurance activities specified in the Protection Profile for Peripheral Sharing Switch, Version 3.0, February 13, 2015 (PSS PP).

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 Tripp Lite B002a Secure KVM Switch Series 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 publicly available Assurance Activities Report (AAR) and the associated proprietary test report produced by the Leidos evaluation team.

The Tripp Lite B002a Secure KVM Switch Series provide a secure medium to share peripheral components such as keyboard, video display and mouse/pointing devices among multiple computers over USB and either DisplayPort or HDMI, depending on model. The TOE is a hardware and firmware solution that consists of the following Secure KVM Switch models:

#	Model Name	Description and NIAP Certification Version	Version
1	B002A-DP2A2	2-Port DH Secure DP KVM w/audio, PP 3.0	285.213
2	B002A-DP2AC2	2-Port DH Secure Pro DP KVM w/audio and CAC, PP 3.0	285.113
3	B002A-UH2A2	2-Port DH Secure HDMI KVM w/audio, PP 3.0	285.212
4	B002A-UH2AC2	2-Port DH Secure Pro HDMI KVM w/audio and CAC, PP 3.0	285.112

Table 1: Tripp Lite 2-Port TOE Models Identification

#	Model Name	Description and NIAP Certification Version	Version
1	B002A-UH2A4	4-Port DH Secure HDMI KVM w/audio, PP 3.0	285.222
2	B002A-UH2AC4	4-Port DH Secure Pro HDMI KVM w/audio and CAC, PP 3.0	285.122

Table 2: Tripp Lite 4-Port TOE Models Identification

#	Model Name	Description and NIAP Certification Version	Version
1	B002A-DP1AC8	8-Port SH Secure Pro DP KVM w/ audio and CAC, PP 3.0	285.133

Table 3: Tripp Lite 8-Port TOE Models Identification

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 the security functional requirements stated in the Tripp Lite B002a Secure KVM Switch Series Security Target, Version 1.04, June 8, 2020.

Item	Identifier
Evaluated Product	Tripp Lite B002a Secure KVM Switch Series consisting of the following hardware models: - B002A-DP2A2 - B002A-DP2Ac2 - B002A-UH2A2 - B002A-UH2AC2 - B002A-UH2A4 - B002A-UH2AC4 - B002A-DP1AC8
Sponsor & Developer	David Posner Tripp Lite Network Services 1111 W 35th St Chicago, IL 60609
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	July 2020
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012

Item	Identifier
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, February 13, 2015
Disclaimer	The information contained in this Validation Report is not an endorsement of the Tripp Lite B002a Secure KVM Switch Series by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
Evaluation Personnel	Justin Fisher Allen Sant Furukh Siddique Kevin Steiner
Validation Personnel	Paul Bicknell, MITRE Linda Morrison, MITRE

Table 4: 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).

The following table identifies the evaluated Security Target and TOE.

Name	**Description**
ST Title	Tripp Lite B002a Secure KVM Switch Series Security Target
ST Version	1.04
Publication Date	June 8, 2020
Vendor and ST Author	Tripp Lite, Inc.
TOE Reference	Tripp Lite Secure KVM Switch models identified in Tables 1-3 [of this VR]
TOE Software Version	Tripp Lite Secure KVM Switch models identified in Tables 1-3 [of this VR]
Keywords	Secure KVM, Tripp Lite, Protection Profile 3.0, February 13, 2105

2.1 Threats

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

- A connection via the PSS between computers may allow unauthorized data flow through the PSS or its connected peripherals.
- A connection via the PSS between computers may allow unauthorized data flow through bit-by-bit signaling.
- A PSS may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer. More specifically, a PSS may leak user keyboard entries to a PSS-connected computer other than the selected computer in real-time or at a later time.
- A threat in which the user is connected to a computer other than the one to which they intended to be connected.

- The use of an unauthorized peripheral device with a specific PSS peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers.
- The use of an authorized peripheral device with the PSS may still cause unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers. Such threats are possible due to known or unknown device vulnerabilities or due to additional functions within the authorized peripheral device.
- Microphone connected to the TOE used for audio eavesdropping or to transfer data across an air-gap through audio signaling.
- Audio output device used by an attacker as a low-gain microphone for audio eavesdropping. This threat is an abuse of the computer and TOE audio output path to reverse the analog data flow from the headphones to the computer. The computer then amplifies and filters the weak signal, and then digitizes and streams it to another location.
- An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code embedded in the TOE's volatile or non-volatile memory to allow unauthorized information flows between connected devices.
- A malicious human agent could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.
- A malicious human agent could replace the TOE during shipping, storage, or use with an alternate device that does not enforce the TOE security policies.
- Detectable failure of a PSS may cause an unauthorized information flow, weakening of PSS security functions, or unintended switching.

2.2 Organizational Security Policies

There are no Organizational Security Policies for the Protection Profile for Peripheral Sharing Switch.

3 Architectural Information

The Tripp Lite Secure KVM Switch provides a secure medium to share a single set or more of peripheral components such as keyboard, video display and mouse/pointing devices among multiple computers over USB and DisplayPort or HDMI (depending on model).

The Tripp Lite Secure KVM Switch utilizes multiple isolated microcontrollers to emulate the connected peripherals in order to prevent a multitude of threats. The TOE is also equipped with numerous unidirectional data flow forcing devices to guarantee isolation of connected computer data channels.

Tripp Lite Secure KVM port models:

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

Tripp Lite Secure KVM video outputs (displays):

- Single-head
- Dual-head

The Tripp Lite Secure KVM Switch is compatible with standard personal/portable computers, servers or thin-clients. Connected computers are assumed to run off-the-shelf general-purpose operating systems such as Windows or Linux. The TOE includes ports for the following interfaces:

- USB keyboard
- USB mouse
- DisplayPort 1.2 Video Input/Output (computer and peripheral ports) (depending on TOE model)
    - DisplayPort TOE models are single-head or dual-head, depending on model
- HDMI 1.4 Video Input/Output (computer and peripheral ports) (depending on TOE model)
    - All HDMI TOE models are dual-head
- 3.5mm Audio Input (computer ports)
- 3.5mm Audio Output (peripheral port)
- USB Smart-card reader, PIV/CAC reader, Token or Biometric reader – supported models only

Computers of varying sensitivities are connected to a single TOE that is intended to restrict peripheral connectivity to one computer at a time. Data leakage is prevented across the TOE to avoid severe compromise of the user's information.

4 Assumptions

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

- It is assumed that the computers and peripheral devices connected to the TOE are not TEMPEST approved.
- It is assumed that 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, and analog video capture function.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators and users are trusted to follow and apply all guidance in a trusted manner.
- Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

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 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

The TOE implements the User Data Protection and Data Isolation security function policies of the *Protection Profile for Peripheral Sharing Switch* as specified in the ST.

The TOE allows an individual user to utilize a single set of peripherals to operate in an environment with several isolated computers. All TOE models switch keyboard/mouse input and audio output from one isolated computer to another. KVM models additionally switch display output. Some models (those with C as the second to last character in the model name) additionally switch USB/CAC authentication devices. Consequently, the TOE security policy consists of data isolation policies for the traffic that is transmitted to/from peripherals that are connected to the TOE and computers that are connected to the TOE along with supporting audit, authentication, management and self-protection policies.

5.1 Keyboard and Mouse Subsystem

The keyboard and mouse processor is programmed in firmware only to accept basic keyboard and mouse USB devices (standard 108-key keyboard and 3-button mouse). Wireless keyboard and mouse are not allowed by the TOE. Only USB host peripheral devices are allowed by TOE keyboard and mouse host emulators. A secure peripheral switch (multiplexer) is used to assure the selection of just one tied keyboard and mouse serial data stream during TOE operation. The secure multiplexer has a third position, isolation, which is activated when the TOE has been tampered with or self-test has failed to disable the keyboard and mouse stream.

5.2 TOE External Interfaces

The TOE only supports AC/DC power, USB keyboard and mouse, video out (DP 1.2 in/DP 1.2 out or HDMI 1.4 in/HDMI 1.4 out), analog audio output, and USB authentication devices on supported models. Docking protocols are not supported by the TOE. Analog microphone or audio line inputs are not supported by the TOE. Unidirectional audio diodes are placed in parallel on both right and left stereo channels to ensure unidirectional data flow from the connected computer to the user peripheral device. Audio data from the connected peripheral devices to the connected computer is blocked by the audio data diodes.

5.3 Audio Subsystem

Electrical isolation of the audio subsystem from all other TOE interfaces prevents data leakage to and from the audio paths. The use of microphones or audio line input devices is prohibited. All TOE devices support analog audio out switching and all TOE devices will prevent the use of microphone devices. These microphones are stopped through the use of unidirectional audio diodes on both left and right stereo channels (which force data flow from only the computer to the connected audio device) and the analog output amplifier which enforces unidirectional audio data flow. The TOE audio subsystem does not delay, store, or convert audio data flows. This prevents any audio overflow during switching between isolated audio channels.

5.4 Video Subsystem

Each connected computer has its own TOE isolated channel with its own Extended Display Identification Data (EDID) emulator and video input port. Data flows from the input video source through its respective EDID emulator and out of the monitor display port. Each video input interface is isolated from one another using different EDID ICs, power planes, ground planes, and electronic components in each independent channel. The TOE supports HDMI/DP 1.2 video input, and HDMI/DP 1.4 video output (depending on the TOE model). DP models include both single-head and dual-head designs, while all HDMI models are dual-head.

5.5 TOE Administration and Security Management

Each TOE is equipped with an Administration and Security Management Tool that can be initiated by running an executable file on a computer with keyboard connected to the same computer via the TOE. The tool requires administrator or a user to be successfully identified and authenticated by the TOE in order to gain access to any supported feature. Some features are restricted to the Administrator role only, while other features can be performed by either the Administrator or User role.

5.6 User Authentication Device Subsystem

TOE models that support USB authentication devices are shipped with default Device Filtration for the CAC port. The filter is set at default to allow only standard smart-card reader, PIV/CAC USB 1.1/2.0 token, or biometric reader. All devices must be bus powered only (no external power source allowed). The TOE default settings accept standard smart-card reader, PIV/CAC USB 1.1/2.0 token or biometric reader. Authenticated users and administrator can register (whitelist) other USB devices. All other USB devices are prohibited (blacklisted).

5.7 User Control and Monitoring Security

User monitoring and control of the TOE is performed through the TOE front panel LED illuminated push-buttons. These buttons are tied to the TOE system controller functionality. All push-buttons for selecting computer channels are internally illuminated via LEDs. The current selected channel is indicated by the illumination of the current channel push-button LED (the other channel LEDs remain off). During operation, all front panel LED indications cannot be turned off or dimmed by the user in any way including after Restore Factory Default (reset).

All features of the TOE front panel are tested during power up self-testing. From power up until the termination of the TOE self-test, no channel is selected.

5.8 Tampering Protection

In order to mitigate potential tampering and replacement, the TOE is devised to ensure that any replacement may be detected, any physical modification is evident, and any logical modification may be prevented. The TOE is designed so that access to the TOE firmware, software, or its memory via its accessible ports is prevented. The TOE is designed to prevent any physical or logical access its internal memory. There is a mechanical switch on the inside of the TOE that triggers the anti-tampering state when the enclosure is manually opened. Once the anti-tampering state is triggered, the TOE is permanently disabled.

5.9 Self-Testing and Security Audit

The TOE has a self-testing function that executes immediately after power is supplied including Restore Factory Default (reset) and power reset. Self-testing must complete successfully before normal operational access is granted to the TSF. The self-test function includes the following activities:

- Basic integrity test of the TOE hardware (no front panel push buttons are jammed).
- Basic integrity test of the TOE firmware.
- Integrity test of the anti-tampering system and control function.
- Test the data traffic isolation between ports.

The TOE has a non-volatile memory event log which records all abnormal security events that occur within TOE operation. This log can be accessed by the identified and authorized administrator and dumped into a .txt file using a connected computer and the Administration and Security Management tool that is provided by the TOE vendor.

6 Documentation

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- Tripp Lite B002a Secure KVM Switch Series Administration and Security Management Tool Guide, Version 2.1, June 8, 2020
- Owner's Manual Secure KVM Switches, NIAP Protection Profile Version 3.0, 18-06-260 93-3845_RevB, 2018

The above documents are considered to be part of the evaluated TOE. The documentation is delivered with the product and is also available by download from: https://www.tripplite.com/pages/niap-secure-kvm/.

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.

The Security Target used is:

- Tripp Lite B002a Secure KVM Switch Series Security Target, Version 1.04, June 8, 2020

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 documents:

- *Tripp Lite B002a Secure KVM Switch Series Common Criteria Test Report and Procedures,* Version 1.0, June 15, 2020

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

- Assurance Activities Report for Tripp Lite B002a Secure KVM Switch Series, Version 1.0, June 12, 2020

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,* Version 3.0.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Protection Profile for Peripheral Sharing Switch,* Version 3.0. 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 May 11, 2020 to June 5, 2020.

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,* Version 3.0 were fulfilled.

7.2 Vulnerability analysis

A search of public domain sources for potential vulnerabilities in the TOE conducted in January 2020 and again in June 2020 did not reveal any known vulnerabilities.

None of the vulnerabilities identified in the search of public sources are related to the TOE. Therefore, no testing is required to verify that an identified potential vulnerability has been mitigated.

This is further supported by the fact that the functional testing activities prescribed by the PSS PP include several tests that could be categorized as penetration testing since they represent likely areas of attack from the perspective of a threat agent or security researcher. Specifically, the functional testing demonstrates that the TOE cannot be switched to multiple computers at once, that audio leakage does not occur, that the TOE chassis cannot be physically compromised without detection and response, and that the TOE will not accept data flows to/from unauthorized peripherals and peripheral types.

8 Evaluated Configuration

The evaluated version of the TOE consists of the Tripp Lite Secure KVM Peripheral Sharing Switches identified in Tables 1 through 3.

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. The figure below identifies a sample evaluated configuration for a 2-port model. The only differences between the TOE models are:

- The number of computers that can be connected to the TOE (2, 4, 8)
- Whether a CAC reader is supported
- Whether the display protocol is DisplayPort or HDMI
- Whether one (single-head) or up to two (dual-head) peripheral displays are supported

The same configuration is applied to the 2, 4, and 8 port models.

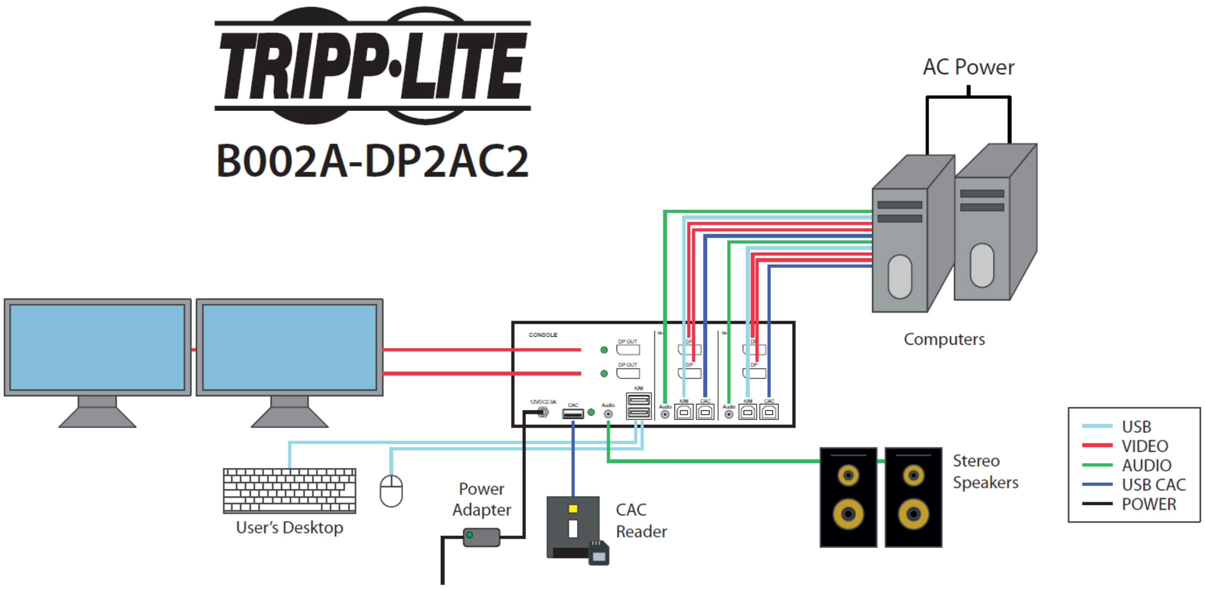

Figure 1: Setup of 2-Port TOE Installation

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Protection Profile for Peripheral Sharing Switch*, Version 3.0, in conjunction with version 3.1, revision 4 of the CC and the CEM, and all applicable NIAP Technical Decisions, scheme policies, scheme publications, and official responses to Technical Queries. 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 it demonstrates that 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), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 5: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic Functional 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 – Sample
AVA_VAN.1	Vulnerability Survey

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Tripp Lite B002a Secure KVM Switch Series Administration and Security Management Tool Guide, Version 2.1, June 8, 2020.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation.

11 Annexes

Not applicable.

12 Security Target

Name	Description
ST Title	Tripp Lite B002a Secure KVM Switch Series Security Target
ST Version	1.04
Publication Date	June 8, 2020

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 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. *Tripp Lite B002a Secure KVM Switch Series Security Target*, Version 1.04, June 8, 2020
6. *Evaluation Technical Report for Tripp Lite B002a Secure KVM Switch Series*, Version 1.0, June 12, 2020
7. *Tripp Lite B002a Secure KVM Switch Series Common Criteria Test Report and Procedures*, Version 1.0, June 15, 2020
8. *Tripp Lite B002a Secure KVM Switch Series Vulnerability Survey*, Version 1.0, June 5, 2020
9. *Assurance Activities Report for Tripp Lite B002a Secure KVM Switch Series*, Version 1.0, June 12, 2020