National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

ATEN Secure KVM Switch Series of Peripheral Sharing Switches

Report Number: CCEVS-VR-10830-2018

Dated: January 29, 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

Stelios Melachrinoudis
Daniel Faigin
John Butterworth

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) [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 ATEN 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 ATEN 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 January 2018. 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). Leidos determined Technical Decisions TD0083, TD0086, TD0136, TD0141, TD0144, and TD0251 applied to this evaluation. 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 ATEN 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 publicly available Assurance Activities Report (AAR) [7] and the associated proprietary test report [8] produced by the Leidos evaluation team.

Each device in the ATEN 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

[1] See section 14 Bibliography.

mouse, keyboard, user authentication device (for example, CAC reader), speaker, and one or two video displays to a Secure KVM Switch. The user may switch the set of peripherals between connected computers. The maximum number of connected computers is two, four, or eight depending on model. 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 ATEN Secure KVM Switch Series.

Table 1 ATEN Secure KVM Switch Series TOE Models

Configuration		2-Port	4-Port	8-Port
DisplayPort	Single Head	CS1182DP	CS1184DP	CS1188DP
	Dual Head	CS1142DP	CS1144DP	CS1148DP
HDMI	Single Head	CS1182H	CS1184H	CS1188H
	Dual Head	CS1142H	CS1144H	CS1148H
DVI	Single Head	CS1182D	CS1184D	CS1188D
	Dual Head	CS1142D	CS1144D	CS1148D

In Table 1, DisplayPort and HDMI configurations support HDMI monitor peripherals. DVI configurations support DVI monitors. All TOE devices support both USB and PS/2 keyboards and mice.

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 ATEN Secure KVM Switch Security Target.

Item	Identifier
Evaluated Product	ATEN Secure KVM Switches Series devices identified in Table 1

Item	Identifier
Sponsor & Developer	ATEN 3F, No. 125, Section 2, Datung Road, Sijhih District, New Taipei City, 221 Taiwan
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 ATEN Secure KVM Switch Series by any agency of the U.S. Government and no warranty of the ATEN Secure KVM Switch Series is either expressed or implied.
Evaluation Personnel	Gregory Beaver Cody Cummins Gary Grainger Kevin Steiner
Validation Personnel	Stelios Melachrinoudis, Lead Validator Daniel Faigin, Senior Validator John Butterworth, ECR Team

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	ATEN Secure KVM Switch Series Security Target
ST Version	V1.0
Publication Date	January 19, 2018
Vendor and ST Author	ATEN International Co., Ltd.
TOE Reference	ATEN Secure KVM Switch Series 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 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.
- 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.
- 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.

2.2 Organizational Security Policies

There are no Organizational Security Policies for the *Protection Profile for Peripheral Sharing Switch* [10].

3 Architectural Information

The ATEN Secure KVM Switch series are keyboard, video, mouse (KVM) switches with the following characteristics:

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

ATEN Secure KVM Switch series devices allow for the connection of a mouse, keyboard, user authentication device such as smart card or CAC reader (optional), speaker (optional), 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. The selected computer is always identifiable by a bright orange LED associated with the applicable selection button.

ATEN Secure KVM Switch series devices support USB connections for the keyboard, mouse and user authentication device and DVI or HDMI connections for the video display(s). ATEN Secure KVM Switch series devices additionally support PS/2 keyboard and mouse connections. Separate USB cables are used to connect the keyboard/mouse combination and the user authentication device to the connected computers. ATEN Secure KVM Switch series devices support, depending on device type, the following video connections from the connected computers: DisplayPort; HDMI; and DVI. ATEN Secure KVM Switch series devices supporting DisplayPort convert the DisplayPort video signal to HDMI for output to the connected video display(s). ATEN Secure KVM Switch series devices 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.

ATEN Secure KVM Switch series devices implement a secure isolation design for all 2/4/8-Port and DVI/HDMI/DisplayPort models to share a single set of peripheral components. ATEN Secure KVM Switch series devices support the following peripheral port types:

- USB keyboard,
- USB mouse,
- PS/2 keyboard,
- PS/2 mouse,
- USB authentication device (CAC reader or smart card reader),
- Audio output, and
- DVI or HDMI video (depending on device type).

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 to HDMI for communication with the connected video display and the AUX channel is monitored and converted to video.

ATEN Secure KVM Switch series devices are designed to enforce the allowed and disallowed data flows between user peripheral devices and connected computers as specified in [10]. Data leakage is prevented across the TOE to avoid compromise of the user's information. Modern KVM security approaches address the risk of TOE local user data leakage through remote attacks to coupled networks in addition to protecting user information passing through the TOE. ATEN Secure KVM Switch series devices automatically clear the internal TOE keyboard and mouse buffers.

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

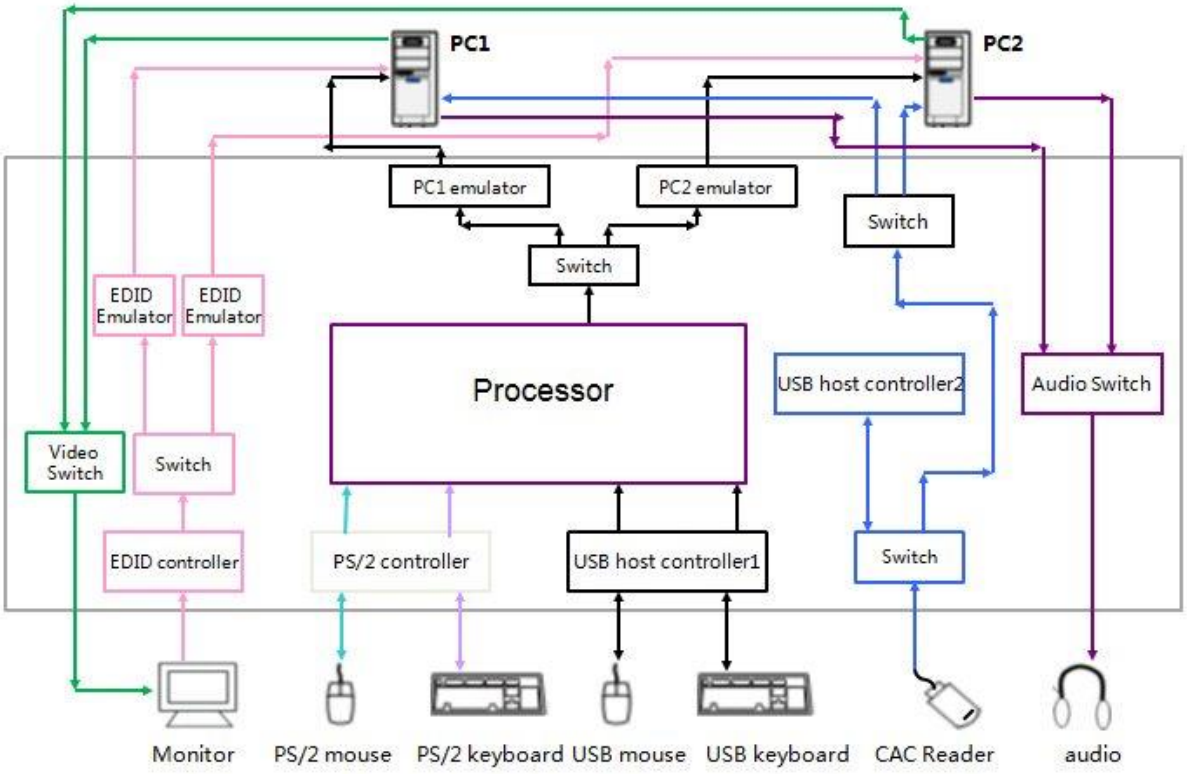

Figure 1 Simplified block diagram of a 2-Port KVM TOE

The data flow of USB and PS/2 keyboard/mouse is controlled by two types of host controller for console human interface device (HID) keyboard and pointing devices: USB host controller and PS/2 host controller. Details of the data flow architecture are provided in the proprietary ATEN Secure KVM Switch Isolation Document. All keyboard and mouse connections are filtered first, and only authorized devices will be allowed. The TOE emulates data from authorized USB or PS/2 keyboard and mouse to USB data for computer sources.

The TOE's proprietary design mitigates the possibility of data leakage from a user's peripheral output device to the input device and ensures that no unauthorized data flows from the monitor to a connected computer. 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 user peripheral input device 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 ATEN Secure KVM Switch series devices feature hardware security mechanisms including tamper-evident labels, always active chassis-intrusion detection, and tamper-proof hardware construction. Software security includes restricted USB connectivity (non-HID 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.

ATEN Secure KVM Switch series devices are compatible with standard personal/portable computers, servers or thin-clients. The ATEN Port Authentication Utility must be installed on a separate secure source computer using an installation wizard. The utility supports Microsoft Windows 7 and higher. 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:

- 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 [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

ATEN 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, 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,
- PS/2 keyboard,
- PS/2 mouse,
- USB authentication device (CAC reader or smart card reader),
- Audio output, and
- DVI or HDMI video (depending on device type).

Some TOE models accept DisplayPort signals at the computer interface and convert the signals to HDMI signals at the peripheral 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 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 device filtering whitelist and blacklist (configurable device filtration). 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 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 after activating the reset button. The suite includes:

- Test of the basic TOE hardware and firmware integrity,
- Test of the basic computer-to-computer isolation, and
- 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 when tampering is detected. 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:

- *ATEN 2/4/8-Port USB DVI/HDMI/DisplayPort Single/Dual Display Secure KVM Switch Administrator Guide,* Version 1.02, 29 September 2017
- *ATEN 2/4/8-Port USB DVI/HDMI/DisplayPort Single/Dual Display Secure KVM Switch User Manual,* Version 1.02, 29 September 2017
- *ATEN 2/4/8-Port USB DVI/HDMI/DisplayPort Single/Dual Display Secure KVM Switch Port Authentication Utility Guide,* Version 1.02, 29 September 2017
- *ATEN 2/4/8-Port USB DVI/HDMI/DisplayPort Single/Dual Display Secure KVM Switch Admin Log Audit Code,* Version 1.01, 29 September 2017 *(ATEN 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 www.aten.com.

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:

- *ATEN Secure KVM Switch Series Common Criteria Test Report and Procedures,* Version 1.0, December 18, 2017 [8]

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

- *Assurance Activities Report For ATEN Secure KVM Switch Series,* Version 1.1, January 19, 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 August 7, 2017 to October 20, 2017 with follow up testing through December 18, 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 ATEN 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

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices, 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.

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, TD0141, TD0144 and TD0251. (See https://www.niap-ccevs.org/Documents_and_Guidance/view_tds.cfm.) All six PSS-TRRT Technical Decisions applied to the ATEN Secure KVM Switch Series evaluation.

There was one TRRT decision made throughout the course of this evaluation. The TRRT decision was captured in TD0251.

Per deprecated TD0141, the Application Note of FMT_MOF.1.1 stated the following:

> *If there are additional management functions performed by the TOE (including those specified in Section 4.2.4, FMT_SMF), they should be added in the assignment.*

However, the SFR text was originally missing an assignment, thus not adequately reflecting the Application Note. As a result, the issue was raised to the PSS TRRT team. Upon review, the PSS Technical Community (PSS TC) agreed to modify the SFR to include the missing assignment, "[assignment: list of functions]".

In addition to the items mentioned above, some additional product administration and usability features are worth considering:

- If the product uses default passwords, the administrator should make sure these passwords are changed.
- An audit feature is supported, but is of a limited nature given the product.
- The PSS PP requires that for compliant TOEs, wireless keyboards cannot be used and that only authorized supported switched methods (e.g. push-buttons) can be used. This is consistent with the PE-5 access controls for Output Devices as documented in the DoD Joint Special Access Program (SAP) Implementation Guide (JSIG).

11 Annexes

Not applicable.

12 Security Target

Table 4 Security Target Identification

Name	Description
ST Title	ATEN Secure KVM Switch Series Security Target
ST Version	V1.0
Publication Date	January 19, 2018

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] *ATEN Secure KVM Switch Series Security Target,* version 1.0, January 19, 2018

[7] *Assurance Activities Report For ATEN Secure KVM Switch Series,* Version 1.1, January 19, 2018

[8] *ATEN Secure KVM Switch Series Common Criteria Test Report and Procedures,* Version 1.0, December 18, 2017

[9] *Evaluation Technical Report for ATEN Secure KVM Switch,* Version 1.0, January 19, 2018

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