National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

IPGARD Secure KVM/KM Peripheral Sharing Switches

Report Number:	**CCEVS-VR-10997-2019**
Dated:	**October 18, 2019**
Version:	**1.1**

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

John Butterworth
Daniel Faigin

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 IPGARD KVM/KM 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 IPGARD KVM/KM Peripheral Sharing Switches was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in October 2019. 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 (PSS PP). Leidos performed an analysis of the NIAP Technical Decisions (https://www.niap-ccevs.org/Documents_and_Guidance/view_tds.cfm). Leidos determined that the following NIAP Technical Decisions applied to this evaluation:

- TD0083
- TD0086
- TD0136
- TD0144
- TD0251
- TD0298
- TD0421

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 IPGARD Secure KVM/KM 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) and the associated proprietary test report produced by the Leidos evaluation team.

IPGARD Secure KVM/KM Peripheral Sharing Switches provide a secure medium to share peripheral components such as keyboard, video display and mouse/pointing devices among multiple computers over USB, DVI, and DisplayPort. The TOE is a hardware and firmware solution.

The below tables contain the full list of products covered by this evaluation. All TOE models that have the same type of video interfaces run the same firmware; the "Eval. Version" columns of the tables below identify the configuration for each model, which is based on the number of ports of that model.

#	Model Name	P/N	Description and NIAP Certification Version	Eval. Version
1	SDVN-2S	1872-IPG-1001	2-Port SH Secure DVI-I KVM w/audio, PP 3.0	111.111
2	SDVN-2S-P	1872-IPG-1002	2-Port SH Secure Pro DVI-I KVM w/audio and CAC, PP 3.0	111.111
3	SDVN-2D	1872-IPG-1003	2-Port DH Secure DVI-I KVM w/audio, PP 3.0	111.111
4	SDVN-2D-P	1872-IPG-1004	2-Port DH Secure Pro DVI-I KVM w/audio and CAC , PP 3.0	111.111
5	SDPN-2S	1872-IPG-1005	2-Port SH Secure DP KVM w/audio, PP 3.0	121.212
6	SDPN-2S-P	1872-IPG-1006	2-Port SH Secure Pro DP KVM w/audio and CAC, PP 3.0	121.212
7	SDPN-2D	1872-IPG-1007	2-Port DH Secure DP KVM w/audio, PP 3.0	121.212
8	SDPN-2D-P	1872-IPG-1008	2-Port DH Secure Pro DP KVM w/audio and CAC, PP 3.0	121.212
9	SDHN-2S-P	1872-IPG-1009	2-Port SH Secure Pro DP to HDMI KVM w/audio and CAC, PP 3.0	131.313
10	SDHN-2D-P	1872-IPG-1010	2-Port DH Secure Pro DP to HDMI KVM w/audio and CAC, PP 3.0	131.313

Table 1: IPGARD 2-Port Secure TOE Identification

#	Model Name	P/N	Description and NIAP Certification Version	Eval. Version
1	SDVN-4S	1872-IPG-1011	4-Port SH Secure DVI-I KVM w/audio, PP 3.0	242.414
2	SDVN-4S-P	1872-IPG-1012	4-Port SH Secure Pro DVI-I KVM w/audio and CAC, PP 3.0	242.414
3	SDVN-4D	1872-IPG-1013	4-Port DH Secure DVI-I KVM w/audio, PP 3.0	242.414
4	SDVN-4D-P	1872-IPG-1014	4-Port DH Secure Pro DVI-I KVM w/audio and CAC, PP 3.0	242.414
5	SDPN-4S	1872-IPG-1015	4-Port SH Secure DP KVM w/audio, PP 3.0	252.515
6	SDPN-4S-P	1872-IPG-1016	4-Port SH Secure Pro DP KVM w/audio and CAC, PP 3.0	252.515
7	SDPN-4D	1872-IPG-1017	4-Port DH Secure DP KVM w/audio, PP 3.0	252.515
8	SDPN-4D-P	1872-IPG-1018	4-Port DH Secure Pro DP KVM w/audio and CAC, PP 3.0	252.515
9	SDHN-4S-P	1872-IPG-1019	4-Port SH Secure Pro DP to HDMI KVM w/audio and CAC, PP 3.0	262.616
10	SDHN-4D-P	1872-IPG-1020	4-Port DH Secure Pro DP to HDMI KVM w/audio and CAC, PP 3.0	262.616
11	SDVN-4Q-P	1872-IPG-1021	4-Port QH Secure Pro DVI-I KVM w/audio and CAC, PP 3.0	242.414
12	SDPN-4Q-P	1872-IPG-1022	4-Port QH Secure Pro DP KVM w/audio and CAC, PP 3.0	252.515

13	SDHN-4Q-P	1872-IPG-1023	4-Port QH Secure Pro DP to HDMI KVM w/audio and CAC, PP 3.0	262.616
14	SKMN-4S	1872-IPG-1030	4-Port Secure KM w/audio, PP 3.0	202.410
15	SKMN-4S-P	1872-IPG-1031	4-Port Secure Pro KM w/audio and CAC, PP 3.0	202.410

Table 2: IPGARD 4-Port Secure TOE Identification

#	Model Name	P/N	Description and NIAP Certification Version	Eval. Version
1	SDVN-8S	1872-IPG-1024	8-Port SH Secure DVI-I KVM w/audio, PP 3.0	373.717
2	SDVN-8S-P	1872-IPG-1025	8-Port SH Secure Pro DVI-I KVM w/ audio and CAC, PP 3.0	373.717
3	SDVN-8D	1872-IPG-1026	8-Port DH Secure DVI-I KVM w/ audio, PP 3.0	373.717
4	SDVN-8D-P	1872-IPG-1027	8-Port DH Secure Pro DVI-I KVM w/ audio and CAC, PP 3.0	373.717
5	SKMN-8S	1872-IPG-1032	8-Port Secure KM w/ audio, PP 3.0	303.710
6	SKMN-8S-P	1872-IPG-1033	8-Port Secure Pro KM w/ audio and CAC, PP 3.0	303.710
7	SDVN-16S	1872-IPG-1028	16-Port SH Secure DVI-I KVM w/ audio, PP 3.0	484.818
8	SDVN-16S-P	1872-IPG-1029	16-Port SH Secure Pro DVI-I KVM w/ audio and CAC, PP 3.0	484.818

Table 3: IPGARD 8-Port and 16-Port Secure TOE 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 all of the security functional requirements stated in the IPGARD Secure KVM/KM Switch Security Target.

Item	Identifier
Evaluated Product	IPGARD Secure KVM/KM Peripheral Sharing Switches identified in Table 1, Table 2, and Table 3
Sponsor & Developer	Albert Cohen IPGARD, Inc. 2455 W Cheyenne Ave Ste 112 North Las Vegas, NV 89032

Item	**Identifier**
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	October 2019
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 IPGARD Secure KVM/KM Peripheral Sharing Switches by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
Evaluation Personnel	Dawn Campbell Justin Fisher Allen Sant Kevin Steiner
Validation Personnel	John Butterworth, The MITRE Corporation Daniel Faigin, The Aerospace Corporation

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	IPGARD Secure KVM/KM Switch Security Target
ST Version	4.11
Publication Date	October 7, 2019
Vendor and ST Author	IPGARD, Inc.
TOE Reference	IPGARD KVM/KM Peripheral Sharing Switches identified in Table 1, Table 2, and Table 3 [of this VR]
TOE Software Version	IPGARD KVM/KM Peripheral Sharing Switches identified in Table 1, Table 2, and Table 3 [of this VR]
Keywords	KVM/KM, Secure, IPGARD, Protection Profile 3.0

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 IPGARD Secure Peripheral Sharing Switches (PSS) provide 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, DVI, HDMI, and DisplayPort.

The IPGARD Secure PSS product 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.

IPGARD Secure KVM port models:

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

IPGARD Secure KVM video outputs (displays):

- Single head
- Dual-head
- Quad-head

IPGARD Secure KM port models:

- 4-Port
- 8-Port

The IPGARD Secure KVM/KM switches are 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 PSS includes ports for the following interfaces:

- USB keyboard
- USB mouse
- DVI, HDMI 1.4 and DisplayPort 1.2 Video Input (computer ports) – specific port depends on model
- DVI, HDMI 1.4 and DisplayPort 1.2 Video Output (peripheral port) – specific port depends on model
- 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 -P 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 (DVI in/DVI out, DP 1.2 in/DP 1.2 out, DP 1.2 in/HDMI 1.4 out, or VGA in/VGA out via adapter), 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 (KVM Models Only)

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 DVI/DP 1.2 video input, and DVI/HDMI 1.4 video output (depending on the TOE model).

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.

KVM models of the TOE can also be configured to be in KM mode, which permits cursor control of selected channel. This identifies the selected computer by visual position of the mouse cursor. In the evaluated configuration, the TOE is configured to use “multi-head mode display switching” when this functionality is active. This configuration enforces a guard by requiring the administrator to press the middle mouse button (scroll wheel button) twice before the cursor control mechanism can be engaged.

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:

- IPGard Secure KVM Administration and Security Management Tool Guide (KVM/KM), Version 3.1, July 15, 2019 (ADG-0S0-ALL)
- IPGARD Advanced 2/4 Port DisplayPort to HDMI Secure KVM, Document ID USM-0S0-1M4, Version 1.11, July 3, 2018
- IPGARD Advanced 2/4/8-Port DisplayPort Secure KVM Switch User Manual, Document ID USM-0S0-MM3, Version 1.11, July 3, 2018
- IPGARD Advanced 2/4/8/16-Port DVI-I Secure KVM User Manual, Document ID USM-0S0-MM1, Version 2.10, July 3, 2018
- IPGARD Advanced 4/8-Port Secure KM Switch User Manual, Document ID USM-0S0-MM0, Version 1.11, July 3, 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: http://ipgard.com/documentation/.

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:

- IPGARD Secure KVM/KM Switch Security Target, Document ID: DOC-IPG-2001, Revision: 4.11, Publication Date: October 7, 2019

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:

- *IPGARD Secure KVM/KM Switch Security Common Criteria Test Report and Procedures,* Version 1.0, August 8, 2019

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

- Assurance Activities Report For IPGARD Secure KVM/KM Switches, Version 1.0, August 9, 2019

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 vendor facility in North Las Vegas, Nevada from June 25, 2019 to June 27, 2019.

Prior to testing, the evaluation team performed an onsite evaluation per NIAP Labgram #078/Valgram #098: CCTL Evaluation Test Requirements. The vendor site controlled access to the test facility. Only the employees who were involved in testing were allowed in the testing facility. This ensured that testing was performed in an isolated environment to prevent tampering. All test equipment was verified to be functioning properly before being used as part of testing.

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 August of 2019 did not reveal any known vulnerabilities.

The evaluator conducted penetration testing based on the threat model defined in the claimed PP. The testing did not exploit any vulnerability.

8 Evaluated Configuration

The evaluated version of the TOE consists of the IPGARD Secure KVM Peripheral Sharing Switches identified in Table 1, Table 2, and Table 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 4-port KVM model. The only differences between the TOE models are:

- The number of computers that can be connected to the TOE (2, 4, 8, 16)
- The number of display peripherals that can be connected to the TOE (zero for KM models; one, two, or four for KVM models depending on whether they include single, dual, or quad-head support)
- For models that support at least one display peripheral, the specific display protocol that is supported (e.g., HDMI, DVI, DisplayPort)
- Whether a CAC reader is supported

The same configuration is applied to the 2, 4, 8, and 16 port models.

IPGARD Secure KVM port models:

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

IPGARD Secure KM port models:

- 4-Port
- 8-Port

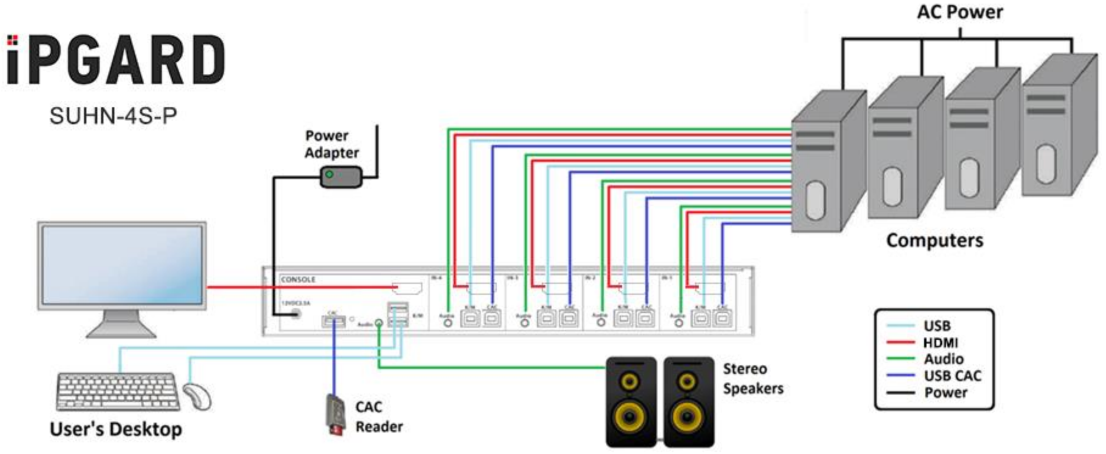

Figure 1: Setup of 4-Port KVM TOE Installation

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

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 six Technical Decisions related to *Protection Profile for Peripheral Sharing Switch*: TD0083, TD0086, TD0136, TD0144, TD0251, and TD0298 (see https://www.niap-ccevs.org/Documents_and_Guidance/view_tds.cfm). All six PSS-TRRT Technical Decisions applied to this evaluation.

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

- The vendor provides an administrative tool to configure the product. This tool is a software application that runs on a general-purpose Windows computer. The security of the application was not separately assessed as part of the evaluation of the product. Distribution of this tool should only be to systems that are required to perform administrative functions.
- The product provides administrative functionality but this is limited to role-based administration with administrative accounts defined on the product itself. The administrator must take care to ensure that the account credentials are provided to the necessary individuals over secure channels.
- The product provides default passwords for its management accounts. The administrator should ensure that these passwords are changed to secure values.
- An administrator mode is supported in the product, but its usability and features are limited. The administrator should make sure they enable multiple users and change default passwords.
- An audit feature is supported, but is of a limited nature given the product.
- Different TOE models provide support for different peripheral interfaces. Vendor guidance must be consulted to determine the interfaces that are supported for a given TOE model. There is no difference in the underlying security architecture for each TOE model so for those interfaces that are shared across multiple models, the required security functionality is implemented in the same manner.
- KM TOE models (and KVM TOE models if configured into “KM mode”) can use cursor control to select the active computer as an alternate switching mechanism from the standard toggle buttons on the TOE hardware. The following configuration changes must be made when using this functionality:
    - To ensure that there is no ambiguous control through having multiple supported switching methods, the administrator must configure the TOE into “KM (two-minute delay)” mode. This setting will prevent the other switching mechanism

from being used for a period of two minutes (e.g. if the user switches active computers using cursor control, they may immediately make another switch using the cursor but the toggle buttons will be disabled for two minutes each time a cursor switch is made, and vice versa).

- To ensure that cursor control doesn't result from an unintended operation, the user or administrator must configure the TOE into "multi-head display switching" mode. This setting requires the user to press the middle mouse button twice before cursor control can be engaged to switch computers.

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 that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

Consumers employing the devices must follow the configuration instructions provided in the Configuration Guidance documentation to ensure the evaluated configuration is established and maintained.

11 Annexes

Not applicable.

12 Security Target

Name	Description
ST Title	IPGARD Secure KVM/KM Switch Security Target
ST Version	4.11
Publication Date	August 8, 2019

13 Abbreviations and Acronyms

Acronym	Full Definition
AUX	DisplayPort Auxiliary Channel
CAC	Common Access Card
CCTL	Common Criteria Test Lab
CDC	Communication Device Class
CODEC	Coder-Decoder
dBv	A measurement of voltages ratio – decibel volt
DC	Direct Current
DP	DisplayPort
DVI	Digital Visual Interface
EDID	Extended Display Identification Data
FDF	Fixed Device Filtration
HD	High Definition
HDMI	High Definition Multimedia Interface
HEAC	HDMI Ethernet Audio Control
HID	Human Interface Device
IP	Internet Protocol
USB Keep-Alive NAK transaction	USB 2.0 standard handshake PID (1010B) – Receiving device cannot accept data or transmitting device cannot send data.
KM	Keyboard, Mouse
KVM	Keyboard, Video and Mouse
LED	Light-Emitting Diode
LoS	Line-of-Sight
MCU	Microcontroller Unit
MCCS	Monitor Control Command Set
MSC	Mass Storage Class
mV	millivolt
OSD	On-Screen Display
PC	Personal Computer
PIN	Personal Identification Number
PSS	Peripheral Sharing Switch
S/PDIF	Sony/Philips Digital Interface Format

SP	Special Publication
SPF	Shared Peripheral Functions
TMDS	Transition-Minimized Differential Signalling
UART	Universal Asynchronous Receiver / Transmitter
USB	Universal Serial Bus
V	Volt
VESA	Video Electronics Standards Association
VGA	Video Graphics Array

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. *IPGARD Secure KVM/KM Switch Security Target*, Document ID: DOC-IPG-2001, Revision: 4.11, Release Date: August 9, 2019
6. *Evaluation Technical Report for IPGARD Secure KVM/KM Switch*, Version 1.0, August 9, 2019
7. *IPGARD Secure KVM/KM Switch Security Common Criteria Test Report and Procedures*, Version 1.0, August 8, 2019
8. *IPGARD Secure KVM/KM Switch Vulnerability Survey*, Version 1.0, August 8, 2019
9. *Assurance Activities Report For IPGARD Secure KVM/KM Switches*, Version 1.0, August 9, 2019