National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

IPGARD Secure KVM Switch/Isolator (CAC Models)

Report Number: **CCEVS-VR-11133-2021**

Dated: **July 9, 2021**

Version: **1.0**

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

John Butterworth

The MITRE Corporation

Matt Downey

National Information Assurance Partnership (NIAP)

Daniel Faigin

The Aerospace Corporation

Anne Gugel

Peter Kruus

Johns Hopkins Applied Physics Laboratory

Common Criteria Testing Laboratory

Leidos

Columbia, MD

Table of Contents

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 Secure KVM Switch/Isolator (CAC Models). 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 Secure KVM Switch/Isolator (CAC Models) was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in July 2021. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 5 and the evaluation activities specified in the following materials:

- Protection Profile for Peripheral Sharing Device, Version 4.0, 19 July 2019 [PSD PP]
- PP-Module for Analog Audio Output Devices, Version 1.0, 19 July 2019 [AO Module]
- PP-Module for Keyboard/Mouse Devices, Version 1.0, 19 July 2019 [KM Module]
- PP-Module for User Authentication Devices, Version 1.0, 19 July 2019 [UA Module]
- PP-Module for Video/Display Devices, Version 1.0, 19 July 2019 [VI Module]

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:

- TD0506
- TD0507
- TD0514
- TD0539 – note this TD applies to switch models only; it does not apply to isolators because it references a selection in FDP_CDS_EXT.1.1 that the isolator models do not claim
- TD0557
- TD0584
- TD0585
- TD0586
- TD0593

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 Switch/Isolator (CAC Models) is conformant to the claimed Protection Profile (PP) and PP-Modules and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfied all of the security functional requirements stated in the STs. The information in this VR is largely derived from the publically available Assurance Activities Report (AAR) and the associated proprietary test report produced by the Leidos evaluation team.

The IPGARD Secure KVM Switch/Isolator (CAC Models) provide a secure medium to share peripheral components such as keyboard, video display and mouse/pointing devices among one or more computers over USB, 3.5mm analog audio, and various video protocols. The TOE also includes isolator models, which are functionally identical to their switch counterparts except that only a single computer is supported. In this case the TOE acts as a secure medium between the connected computer and its end user peripherals. Different TOE models support one or more of DisplayPort 1.2, HDMI 1.4, or DVI-I video. The TOE is a family of hardware appliances that consists of the following models:

Model Name	Description and NIAP Certification Version	Version
SA-DVN-1S-P	1-Port SH Secure DVI-I KVM w/audio and CAC	4.01.010
SA-DPN-1S-P	1-Port SH Secure DP KVM w/audio and CAC	4.01.001
SA-UHN-1S-P	1-Port SH Secure HDMI KVM w/audio and CAC	4.01.100

Table 1: IPGARD 1-Port TOE Models Identification

Model Name	Description and NIAP Certification Version	Version
SA-DPN-2S-P	2-Port SH Secure Pro DP KVM w/audio and CAC	4.01.001
SA-DPN-2D-P	2-Port DH Secure Pro DP KVM w/audio and CAC	4.01.001
SA-DVN-2S-P	2-Port SH Secure Pro DVI-I KVM w/audio and CAC	4.01.010
SA-DVN-2D-P	2-Port DH Secure Pro DVI-I KVM w/audio and CAC	4.01.010
SA-HDN-2S-P	2-Port SH Secure DP/HDMI KVM w/audio and CAC	4.01.202
SA-HDN-2D-P	2-Port DH Secure DP/HDMI KVM w/audio and CAC	4.01.202
SA-DPMST-2S-P	2-Port SH DP to 2xHDMI Secure KVM w/audio and CAC	4.01.003
SA-DPMST-2D-P	2-Port DH DP to 2xHDMI Secure KVM w/audio and CAC	4.01.003

Table 2: IPGARD 2-Port TOE Models Identification

Model Name	Description and NIAP Certification Version	Version
SA-DPN-4S-P	4-Port SH Secure Pro DP KVM w/audio and CAC	4.01.001
SA-DPN-4D-P	4-Port DH Secure Pro DP KVM w/audio and CAC	4.01.001
SA-DPN-4Q-P	4-Port QH Secure Pro DP KVM w/audio and CAC	4.01.001
SA-DVN-4S-P	4-Port SH Secure Pro DVI-I KVM w/audio and CAC	4.01.010
SA-DVN-4D-P	4-Port DH Secure Pro DVI-I KVM w/audio and CAC	4.01.010
SA-DVN-4Q-P	4-Port QH Secure Pro DVI-I KVM w/audio and CAC	4.01.010
SA-HDN-4S-P	4-Port SH Secure DP/HDMI KVM w/audio and CAC	4.01.202
SA-HDN-4D-P	4-Port DH Secure DP/HDMI KVM w/audio and CAC	4.01.202
SA-DPH-4Q-P	4-Port QH Secure DH DVI, SH HDMI, and DH DP KVM w/ audio and CAC	4.01.111

SA-DPMST-4S-P	4-Port SH DP to 2xHDMI Secure KVM w/audio and CAC	4.01.003
SA-DPMST-4D-P	4-Port DH DP to 2xHDMI Secure KVM w/audio and CAC	4.01.003
SA-DMN-DP-P	4-Port SH Secure DP KVM w/audio, CAC and preview screen	4.01.004

Table 3: IPGARD 4-Port TOE Models Identification

Model Name	Description and NIAP Certification Version	Version
SA-DPN-8S-P	8-Port SH Secure Pro DP KVM w/audio and CAC	4.01.001
SA-DPN-8D-P	8-Port DH Secure Pro DP KVM w/audio and CAC	4.01.001
SA-DVN-8S-P	8-Port SH Secure Pro DVI-I KVM w/ audio and CAC	4.01.010
SA-DVN-8D-P	8-Port DH Secure Pro DVI-I KVM w/ audio and CAC	4.01.010
SA-DVN-16S-P	16-Port DH Secure Pro DVI-I KVM w/ audio and CAC	4.01.010

Table 4: IPGARD 8-Port and 16-Port TOE Models Identification

Because of the fact that isolators and switches have different SFR claims, the TOE was separated into two STs. Within each ST, different video-related SFR claims are made since different TOE models support different protocols. For example, the selection-based SFR FDP_SPR_EXT.1/HDMI in [VI Module] is applicable to the TOE but only for TOE models that support at least one HDMI source video feed.

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 evaluation activities specified in the claimed PP and PP-Modules had been completed successfully and that the product satisfied all of the security functional and assurance requirements as stated in the STs.

From this, 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 Switch Security Target (CAC Models) and IPGARD Secure KVM Isolator Security Target (CAC Models), depending on the specific TOE model.

Item	Identifier
Evaluated Product	IPGARD Secure KVM Switch/Isolator (CAC Models) consisting of various models within the SA-DVN, SA-DPN, SA-UHN, SA-HDN, SA-DPMST, SA-DPH, and SA-DMN model families. In particular all TOE models are those with –P at the end of the model name, which designates IPGARD devices with support for USB authentication (CAC) peripherals.
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	July 9, 2021
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2015
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 5, April 2015
PP	PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, version 1.0, which includes the following PP and PP-Modules: • Protection Profile for Peripheral Sharing Device, Version 4.0, 19 July 2019 • PP-Module for Analog Audio Output Devices, Version 1.0, 19 July 2019 • PP-Module for Keyboard/Mouse Devices, Version 1.0, 19 July 2019 • PP-Module for User Authentication Devices, Version 1.0, 19 July 2019 • PP-Module for Video/Display Devices, Version 1.0, 19 July 2019
Disclaimer	The information contained in this Validation Report is not an endorsement of IPGARD Secure KVM Switch/Isolator (CAC Models) by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
Evaluation Personnel	Justin Fisher Shreyansh Kansara Madhav Nakar Pascal Patin Allen Sant Furukh Siddique Sindhu Veerabhadru
Validation Personnel	John Butterworth, Matt Downey, Daniel Faigin, Anne Gugel, Peter Kruus

Table 5: 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 Switch Security Target (CAC Models) [Switch ST] IPGARD Secure KVM Isolator Security Target (CAC Models) [Isolator ST]
ST Version	1.07 [Switch ST] 1.02 [Isolator ST]
Publication Date	June 25, 2021
Vendor and ST Author	IPGARD, Inc.
TOE Reference	Devices identified in Table 1 through Table 4 [of this VR]
TOE Software Version	Firmware versions of devices identified in Table 1 through Table 4 [of this VR]
Keywords	KVM Switch, KVM Isolator, Peripheral Sharing

Table 6: ST and TOE Details

2.1 Threats

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

- A connection via the PSD between one or more computers may allow unauthorized data flow through the PSD or its connected peripherals.
- A connection via the PSD between one or more computers may allow unauthorized data flow through bit-by-bit signaling.
- A PSD may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer.
- A PSD may connect the user to a computer other than the one to which the user intended to connect.

- The use of an unauthorized peripheral device with a specific PSD peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSD or its connected computers.
- An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code or data stored in the PSD's volatile or non-volatile memory to allow unauthorized information flows.
- A malicious user or human agent could physically modify the PSD to allow unauthorized information flows.
- A malicious human agent could replace the PSD during shipping, storage, or use with an alternate device that does not enforce the PSD security policies.
- Detectable failure of a PSD may cause an unauthorized information flow or weakening of PSD security functions.

2.2 Organizational Security Policies

There are no Organizational Security Policies for the Protection Profile for Peripheral Sharing Device or the claimed PP-Modules.

3 Architectural Information

The IPGARD Secure KVM Switch (CAC Models) and IPGARD Secure KVM Isolator (CAC Models), collectively referred to as the TOE, provide 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, analog audio, and, depending on TOE model, one or more of DisplayPort, HDMI, and DVI-I.

The TOE 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:

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

IPGARD Secure KVM video outputs (displays):

- Single head
- Dual head
- Quad head
- Preview Screen (single head switch with a secondary monitor that functions as a multi-viewer)

The TOE 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. All TOE models include ports for the following interfaces:

- USB keyboard
- USB mouse
- 3.5mm Audio Input (computer ports)
- 3.5mm Audio Output (peripheral port)
- USB Smart-card reader, PIV/CAC reader, Token or Biometric reader

All TOE models support video as well. Depending on the specific TOE model, different numbers and types of video inputs are supported. The permutations of this are listed in section 5.4 below.

4 Assumptions

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

- Computers and peripheral devices connected to the PSD are not TEMPEST approved.

  (Added from [KM Module]) The TSF may or may not isolate the ground of the keyboard and mouse computer interfaces (the USB ground). The Operational Environment is assumed not to support TEMPEST red-black ground isolation.

- The environment provides physical security commensurate with the value of the TOE and the data it processes and contains.
- The environment includes no wireless peripheral devices.
- PSD Administrators and users are trusted to follow and apply all guidance in a trusted manner.
- Personnel configuring the PSD and its operational environment will follow the applicable security configuration guidance.
- All PSD users are allowed to interact with all connected computers. It is not the role of the PSD to prevent or otherwise control user access to connected computers. Computers or their connected network shall have the required means to authenticate the user and to control access to their various resources.
- Users are trained not to connect a microphone to the TOE audio output interface.
- 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, or analog video capture function.

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 evaluation activities specified in the claimed PP and PP-Modules 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 PP and PP-Modules. 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 STs, 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 Device. This PP defines a peripheral sharing device as "a PSD is an IT product for connecting one or more peripheral devices to one or more computers such that data cannot flow between computers by way of the peripherals or the PSD. Examples of PSDs that can claim compliance to this PP include Keyboard, Video, Mouse (KVM) switches; Keyboard, Mouse (KM) switches; and Isolators." The TOE includes both KVM switches and isolators in its evaluation boundary.

Aside from behavior specifically relating to port switching, both switches and isolators function in the manner described below.

5.1 Keyboard and Mouse Subsystem

The keyboard and mouse processor is programmed in firmware only to accept 108-key keyboard and 3-button mouse USB devices. Unauthorized peripheral devices will be rejected by the TOE's keyboard and mouse ports. Wireless keyboard and mouse are special USB composite devices; when this type of device is recognized by the TOE, all front LED's of the TOE will blink and the user will need to disconnect and reboot the TOE. The only USB host peripheral devices that are allowed by the TOE are keyboard and mouse host emulators. Basic USB 1.1/2.0 HID-class devices are authorized as valid endpoints by the TOE. Note that devices having integrated USB hub and composite devices will only be supported if the connected device has at least one endpoint which is a keyboard or mouse HID class. All other non-keyboard/mouse HID class endpoints will be disabled in this scenario. Both keyboard and mouse TOE ports are interchangeable. It is assumed based on the claimed PP that all standard peripheral devices are untrusted; therefore, the TOE protects the system from attacks that may be executed to exploit such devices and enable unauthorized data flows. By creating uni-directional isolated keyboard and mouse TOE channels that are tied to the two USB 1.1/2.0 ports on the TOE, unauthorized data flows are eliminated.

5.2 TOE External Interfaces

The TOE only supports AC/DC power, USB keyboard and mouse, user authentication devices, and video, which includes one or more of the following depending on TOE model:

- DVI-I in/DVI-I out
- DP 1.2 in/DP 1.2 out
- HDMI 1.4 in/HDMI 1.4 out
- HDMI 1.4 or DP 1.2 in/HDMI 1.4 or DP 1.2 out (interchangeable DP/HDMI ports)
- DP 1.2 in/HDMI 1.4 out

The user authentication device filter is set by default to allow only standard smart-card reader USB 1.1/2.0 token or biometric reader but when user or administrator registers new CAC

devices, the TOE will start to support these registered devices. All other peripheral types are rejected, either physically (because the TOE does not support the required physical interface) or logically (because the TOE does not recognize the connected peripheral as authorized).

5.3 Audio Subsystem

The use of microphones as input devices is prohibited. All TOE devices support analog audio out switching and all TOE devices will prevent microphone devices. These microphones are stopped through the use of uni-directional audio diodes on both left and right stereo channels (forces data flow from only the computer to the connected audio device) and the LM4880 Boomer analog output amplifier which enforces uni-directional audio data flow. All audio signals are filtered in accordance with the Audio Filtration Specifications table defined in the PP-Module for Analog Audio Output.

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. Depending on the specific TOE model, the following numbers and types of video inputs are supported:

- 1x DVI-I in to DVI-I out
- 2x DVI-I in to DVI-I out
- 4x DVI-I in to DVI-I out
- 1x DisplayPort in to DisplayPort out
- 2x DisplayPort in to DisplayPort out
- 4x DisplayPort in to DisplayPort out
- 1x HDMI in to HDMI out
- 1x DisplayPort or HDMI in to DisplayPort or HDMI out (interchangeable port)
- 2x DisplayPort or HDMI in to DisplayPort or HDMI out (interchangeable port)
- 1x DisplayPort in to 2x HDMI out (DisplayPort Multi-Stream Transport)
- 2x DisplayPort in to 4x HDMI out (DisplayPort Multi-Stream Transport)
- 1x DisplayPort in to 2x DisplayPort out (one normal peripheral monitor and one ‘preview screen’ multi-viewer monitor)
- “Combo” (4x total supported displays with 2x DisplayPort in to 2x DisplayPort out, 1x DVI-I in to 1x DVI-I out, and 1x HDMI in to 1x HDMI out)

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

The TOE is 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 (allowlist) individual USB devices. All other USB devices are prohibited (denylisted).

5.7 User Control and Monitoring Security

User monitoring and control of the TOE is performed through the TOE front panel push buttons. These buttons are tied to the TOE system controller functionality. The TOE chassis has port selection LEDs that correspond to the push buttons. When a given computer is selected, its corresponding port selection LED is illuminated (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). There are two exceptions to this:

- Isolator models do not have a switching capability because they only support a single connected computer, and there is therefore no mechanism to switch computers or indicate which computer is selected
- The TOE ‘preview screen’ model includes a secondary set of push-button controls for controlling the display layout and active computers on the secondary multi-viewer display window. This window uses on-screen display to indicate the active video feed for each region of the display (e.g. if this monitor is configured for picture-in-picture viewing, both the inner and outer picture are labeled with the video feed they each represent)

The USB authentication device interface may be independently enabled or disabled using push-button controls. Whether or not the port selection button is illuminated indicates the status of this interface.

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:

- IPGARD Secure KVM Administration and Security Management Tool Guide (CAC), Version 1.1, February 11, 2021
- IPGARD Advanced Single Port KVM User Manual, Revision 1.12, June 22, 2020
- IPGARD Advanced 2/4/8/16-Port DVI-I Secure KVM User Manual, Revision 1.12, June 22, 2020
- IPGARD Advanced 2/4-Port DP/HDMI to DP/HDMI Secure KVM User Manual, Revision 1.12, June 22, 2020
- IPGARD Advanced 2/4/8-Port DisplayPort Secure KVM Switch User Manual, Revision 1.12, June 22, 2020
- IPGARD 2/4 Port Secure KVM DP MST with Dual or Quad 4K HDMI Out and CAC support User Manual, Revision 1.12, June 22, 2020
- IPGARD Advanced 4-Port DVI, HDMI, DP Secure KVM Switch User Manual, Version 1.12, June 22, 2020
- IPGARD Advanced 4-Port DisplayPort Secure KVM Switch User Manual, Version 1.12, June 22, 2020

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 Targets used are:

- IPGARD Secure KVM Switch Security Target (CAC Models), Version 1.07, June 25, 2021
- IPGARD Secure KVM Isolator Security Target (CAC Models), Version 1.02, June 25, 2021

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 PSD PP 4.0 Common Criteria Test Report and Procedures, Version 1.1, June 25, 2021

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

- Assurance Activities Report for IPGARD KVM Switch/Isolator (CAC Models), Version 1.1, June 25, 2021

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the STs for a product claiming conformance to [PSD PP], [AO Module], [KM Module], [UA Module], and [VI Module].

The evaluation team devised a Test Plan based on the Testing Evaluation Activities specified in the materials referenced above. 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 January 11, 2021 to May 26, 2021, with additional supplemental evidence collected as needed through June 30, 2021.

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 the claimed security functionality were fulfilled.

7.2 Vulnerability Analysis

A search of public domain sources for potential vulnerabilities in the TOE conducted in May 2021 and repeated on June 25, 2021 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 Devices identified in Tables 1 through 4.

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 model. The only differences between the TOE models are:

- The maximum number of computers that can be connected to the TOE (1, 2, 4, 8, 16)
- The number and type of input video ports (1, 2, 4; DVI-I, DisplayPort, HDMI)
- The number and type of output video ports (1, 2, 4; DVI-I, DisplayPort, HDMI)
- Whether or not the TOE has a secondary peripheral monitor that has "preview screen" (also known as multi-viewer) functionality

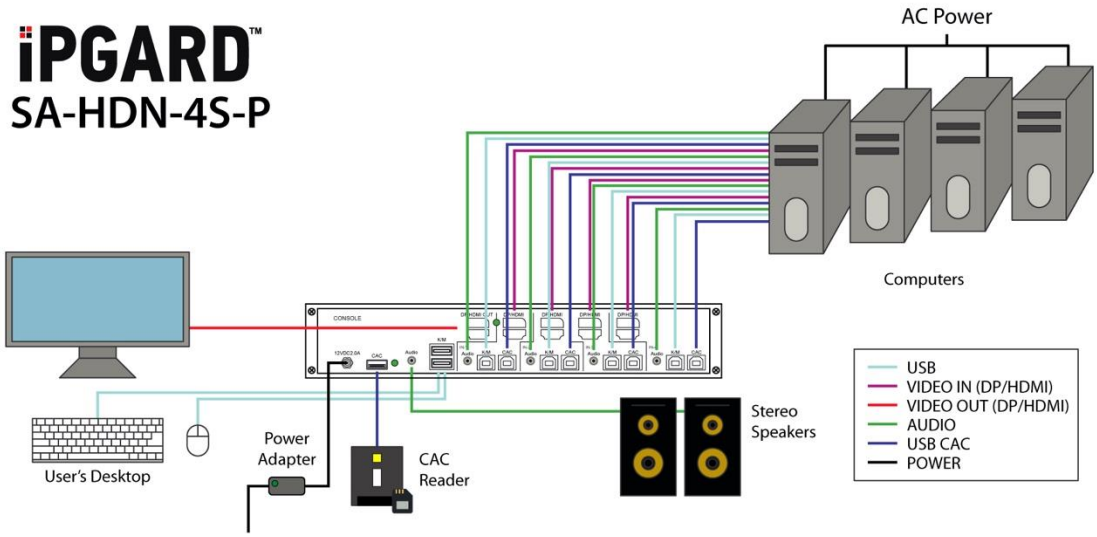

Figure 1: Setup of 4-Port TOE Installation

9 Results of the Evaluation

The evaluation was conducted based upon the evaluation activities specified in the following materials:

- Protection Profile for Peripheral Sharing Device, Version 4.0, July 19, 2019
- PP-Module for Analog Audio Output Devices, Version 1.0, July 19, 2019
- PP-Module for Keyboard/Mouse Devices, Version 1.0, July 19, 2019
- PP-Module for User Authentication Devices, Version 1.0, July 19, 2019
- PP-Module for Video/Display Devices, Version 1.0, July 19, 2019

These evaluation activities were performed in conjunction with version 3.1, revision 5 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 evaluation 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 ETR provided evidence that all work units associated with the assurance requirements were performed and passed. The security assurance requirements are listed in the following table.

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

Table 7: TOE Security Assurance Requirements

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the IPGARD Secure KVM (CAC version) meets the claims stated in the Security Target.

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.

Consumers employing the devices must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

The validators point out that this product does not use encryption. Therefore, certificate review and entropy analysis was not required for this evaluation.

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 evaluation activities. PSS-TRRT has formally posted eleven Technical Decisions related to the claimed PP and PP-Modules: TD0506, TD0507, TD0514, TD0518, TD0539, TD0557, TD0583, TD0584, TD0585, TD0586, and TD0593 (see https://www.niap-ccevs.org/Documents_and_Guidance/view_tds.cfm). All Technical Decisions applied to this evaluation except for TD0518, which corrects a typographical error in the PSD PP, and TD0583, which applies to functionality that the TOE does not claim (specifically, the TD affects devices that include a wired remote controller, which the TOE lacks).

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.
- Different TOE models have different firmware versions. These versions are used to indicate the specific physical interfaces that are supported (e.g. the versioning for a TOE model with DVI-I support differs from one with DisplayPort support). They do not refer to a sequential versioning system such that a higher number indicates a newer release. The first digit of 4 is common to all firmware versions and is used to indicate that the firmware for that device meets the requirements of PSD PP 4.0 and the associated PP-Modules.

10.1 Validation Approach

This was a re-evaluation of IPGARD models were previously evaluated (e.g. VIDs 11064, 10997, and 10894). They were split up into separate VIDs to comply with the PP-Configurations introduced in PP PSD v4.0 to ensure each model was evaluated against the specific PP-Configuration to which it applies.

To minimize documentation and test, the CCTL and the validation team agreed that a single test plan could be shared across all three VIDs 11133, 11134, and 11135, as long as it is clear which tests apply to which VID.

Additional equivalencies were accepted by the validation team:

- The validation team accepted the vendor assertion of equivalency between different video protocols not affecting the performance of other types. For example, DVI vs HDMI vs DisplayPort does not affect the behavior of mouse/keyboard, or audio inputs.
- The validation team accepted the port isolation equivalency in cases where the TOE has a different numbers of ports (e.g. 2 vs 4 vs 8 vs 16). Thus, testing for data path isolation on a model with the highest number of ports will be performed and the validation team accepted that a model with fewer ports will meet the same isolation requirements.
- The validation team agreed that testing of a given video protocol on a multi-head model is sufficient to assume that all handling of sub-protocols, data flow isolation, and other relevant video testing will pass on a single-head model.
- The validation team agreed that DMPST multiplexed output on one monitor is the equivalent of the other because they both originate from the same video source and are processed by the same hardware and firmware.
- The validation team agreed that , in cases where the TSF is blocking unauthorized sub-protocols from coming into the TOE, (e.g. from two HDMI ports), that both ports will be tested to ensure they are both doing appropriate filtration.

- The validation team agreed that, for tests that do not require a specific port to be tested, the CCTL may perform the required testing on up to four arbitrary ports, and, if the intended results are achieved on those ports, equivalent functionality is accepted for the others.

11 Annexes

Not applicable.

12 Security Target

Name	Description
ST Title	IPGARD Secure KVM Switch Security Target (CAC Models) [Switch ST] IPGARD Secure KVM Isolator Security Target (CAC Models) [Isolator ST]
ST Version	1.07 [Switch ST] 1.02 [Isolator ST]
Publication Date	June 25, 2021

13 Abbreviations and Acronyms

Acronym	Full Definition
CAC	Common Access Card
CEM	Common Evaluation Methodology
DP	DisplayPort
DPMST	DisplayPort Multi-Stream Transport
EDID	Extended Display Identification Data
HDMI	High Definition Multimedia Interface
IC	Integrated Circuit
KVM	Keyboard, Video and Mouse
LED	Light-Emitting Diode
NIAP	National Information Assurance Partnership
NVLAP	National Voluntary Laboratory Accreditation Program
PCL	Product Compliant List
PSD	Peripheral Sharing Device
ST	Security Target
TOE	Target of Evaluation
USB	Universal Serial Bus
VR	Validation Report

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2015.
2. Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 5, April 2015.
3. Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1 Revision 5, April 2015.
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2015.
5. IPGARD Secure KVM Switch Security Target (CAC Models), Version 1.07, June 25, 2021
6. IPGARD Secure KVM Isolator Security Target (CAC Models), Version 1.02, June 25, 2021
7. IPGARD Secure KVM Administration and Security Management Tool Guide (CAC), Version 1.1, February 11, 2021
8. IPGARD Advanced Single Port KVM User Manual, Revision 1.12, June 22, 2020
9. IPGARD Advanced 2/4/8/16-Port DVI-I Secure KVM User Manual, Revision 1.12, June 22, 2020
10. IPGARD Advanced 2/4-Port DP/HDMI to DP/HDMI Secure KVM User Manual, Revision 1.12, June 22, 2020
11. IPGARD Advanced 2/4/8-Port DisplayPort Secure KVM Switch User Manual, Revision 1.12, June 22, 2020
12. IPGARD 2/4 Port Secure KVM DP MST with Dual or Quad 4K HDMI Out and CAC support User Manual, Revision 1.12, June 22, 2020
13. IPGARD Advanced 4-Port DVI, HDMI, DP Secure KVM Switch User Manual, Version 1.12, June 22, 2020
14. IPGARD Advanced 4-Port DisplayPort Secure KVM Switch User Manual, Version 1.12, June 22, 2020
15. IPGARD PSD PP 4.0 Common Criteria Test Report and Procedures, Version 1.1, June 25, 2021
16. SmartAVI Vulnerability Survey, Version 1.2, June 25, 2021
17. Protection Profile for Peripheral Sharing Device, Version 4.0, July 19, 2019
18. PP-Module for Analog Audio Output Devices, Version 1.0, July 19, 2019

19. PP-Module for Keyboard/Mouse Devices, Version 1.0, July 19, 2019
20. PP-Module for User Authentication Devices, Version 1.0, July 19, 2019
21. PP-Module for Video/Display Devices, Version 1.0, July 19, 2019