National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Sekuryx Secure KVM Switch (CAC Models)

Report Number: **CCEVS-VR-11168-2021**

Dated: **September 3, 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 George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

John Butterworth
Jenn Dotson
Ted Farnsworth
Lisa Mitchell
Linda Morrison
Chris Thorpe
MITRE Corporation

Common Criteria Testing Laboratory

Leidos
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Sekuryx Secure KVM Switch (CAC Models) Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the 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 Sekuryx Secure KVM Switch (CAC Models) was performed by Leidos Common Criteria Testing Laboratory (CCTL) at the manufacturing facility in North Las Vegas, Nevada, with some test activities performed at the CCTL in Columbia, Maryland, and was completed in September 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]

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 Sekuryx Secure KVM Switch (CAC Models) is conformant to the *PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, User Authentication Devices,* and *Video/Display Devices (CFG_PSD-AO-KM-UA-VI_V1.0),* Version: 1.0, July 19, 2019 and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfied all of the security functional requirements stated in the Security Target (ST). The information in this VR is largely derived from the publicly available Assurance Activities Report (AAR) and the associated proprietary test report produced by the Leidos evaluation team.

The 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 the product satisfies all the functional requirements and assurance requirements 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 products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the *Sekuryx Secure KVM Switch Security Target (CAC Models),* Revision 1.07, August 20, 2021. The technical information included in this report was obtained from the ST and analysis performed by the Validation Team.

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) using the Common Evaluation Methodology (CEM) 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 Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile (PP) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Sekuryx Secure KVM Switch (CAC Models) as defined in Section 3
ST	*Sekuryx Secure KVM Switch Security Target (CAC Models)*, Revision 1.07, August 20, 2021
Sponsor & Developer	Steven Barash Sekuryx, Inc. 12437 Huston St Valley Village, CA 91607
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	September 3, 2021
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 5, April 2015
Conformance Result	CC Part 2 extended and CC Part 3 conformant

Item	Identifier
Protection Profile	*PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices*, version 1.0, 19 July 2019, 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
Evaluation Personnel	Justin Fisher Shreyansh Kansara Madhav Nakar Pascal Patin Allen Sant Furukh Siddique Sindhu Veerabhadru
Validation Personnel	John Butterworth Jenn Dotson Ted Farnsworth Lisa Mitchell Linda Morrison Chris Thorpe

Table 1: ST and TOE Details

3 Architectural Information

The Sekuryx Secure KVM Switch (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.

Sekuryx Secure KVM port models:

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

Sekuryx 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.

The TOE is a family of hardware appliances that consists of the following models:

Model Name	Description and NIAP Certification Version	Version
CK4-P102C	2-Port SH Secure Pro DP KVM w/audio and CAC	4.31.001
CK4-P202C	2-Port DH Secure Pro DP KVM w/audio and CAC	4.31.001
CK4-D102C	2-Port SH Secure Pro DVI-I KVM w/audio and CAC	4.31.010
CK4-D202C	2-Port DH Secure Pro DVI-I KVM w/audio and CAC	4.31.010
CK4-HP102C	2-Port SH Secure DP/HDMI KVM w/audio and CAC	4.31.202
CK4-HP202C	2-Port DH Secure DP/HDMI KVM w/audio and CAC	4.31.202

CK4-PM102C	2-Port SH DP to 2xHDMI Secure KVM w/audio and CAC	4.31.003
CK4-PM202C	2-Port DH DP to 2xHDMI Secure KVM w/audio and CAC	4.31.003

Table 2: Sekuryx 2-Port TOE Models Identification

Model Name	Description and NIAP Certification Version	Version
CK4-P104C	4-Port SH Secure Pro DP KVM w/audio and CAC	4.31.001
CK4-P204C	4-Port DH Secure Pro DP KVM w/audio and CAC	4.31.001
CK4-P404C	4-Port QH Secure Pro DP KVM w/audio and CAC	4.31.001
CK4-D104C	4-Port SH Secure Pro DVI-I KVM w/audio and CAC	4.31.010
CK4-D204C	4-Port DH Secure Pro DVI-I KVM w/audio and CAC	4.31.010
CK4-D404C	4-Port QH Secure Pro DVI-I KVM w/audio and CAC	4.31.010
CK4-HP104C	4-Port SH Secure DP/HDMI KVM w/audio and CAC	4.31.202
CK4-HP204C	4-Port DH Secure DP/HDMI KVM w/audio and CAC	4.31.202
CK4-HPD404C	4-Port QH Secure SH DVI, SH HDMI, and DH DP KVM w/audio and CAC	4.31.111
CK4-PM104C	4-Port SH DP to 2xHDMI Secure KVM w/audio and CAC	4.31.003
CK4-PM204C	4-Port DH DP to 2xHDMI Secure KVM w/audio and CAC	4.31.003
CK4-PS104C	4-Port SH Secure DP KVM w/audio, CAC and preview screen	4.31.004

Table 3: Sekuryx 4-Port TOE Models Identification

Model Name	Description and NIAP Certification Version	Version
CK4-P108C	8-Port SH Secure Pro DP KVM w/audio and CAC	4.31.001
CK4-P208C	8-Port DH Secure Pro DP KVM w/audio and CAC	4.31.001
CK4-D108C	8-Port SH Secure Pro DVI-I KVM w/ audio and CAC	4.31.010
CK4-D208C	8-Port DH Secure Pro DVI-I KVM w/ audio and CAC	4.31.010
CK4-D116C	16-Port DH Secure Pro DVI-I KVM w/ audio and CAC	4.31.010

Table 4: Sekuryx 8/16-Port TOE Models Identification

4 Assumptions

The Security Problem Definition, including the assumptions, may be found the *Sekuryx Secure KVM Switch Security Target (CAC Models)*, Revision, 1.07, August 20, 2021. That information has not been reproduced here and the ST should be consulted if there is interest in that material.

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 (in accordance with the evaluation activities specified in the PP and PP-Modules associated with the claimed PP-Configuration 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 in the PP and PP-Modules associated with the claimed PP-Configuration and applicable Technical Decisions. 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 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 KVM switches in its evaluation boundary.

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. 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. 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.

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 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 the 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).

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:

- *User Manual Sekuryx Secure DP/HDMI KVM Switch with CAC Port and 4K Ultra-HD Support*, Revision 1.0, July 21, 2021
- *User Manual Sekuryx Secure 4 Port Single Head DP KVM Switch with CAC Port, Preview Screen and 4K Ultra-HD Support*, Revision 1.0, July 21, 2021
- *User Manual Sekuryx Secure DP MST KVM Switch with CAC Port and 4K Ultra-HD Support*, Revision 1.0, July 21, 2021
- *User Manual Sekuryx Secure 4 Port COMBO KVM Switch with CAC Port and 4K Ultra-HD Support*, Revision 1.0, July 21, 2021
- *User Manual Sekuryx Secure DVI KVM Switch with CAC Port*, Revision 1.0, July 21, 2021
- *User Manual Sekuryx Secure DP KVM Switch with CAC Port and 4K Ultra-HD Support*, Revision 1.0, July 21, 2021
- *Sekuryx Secure KVM Administration and Security Management Tool Guide (CAC)*, Version 1.0, April 6, 2021

The above documents are considered to be part of the evaluated TOE. The documentation is delivered with the product and is also available by download from: https://sekuryx.com/documentation/NIAP4.

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:

- *Sekuryx Secure KVM Switch Security Target (CAC Models)*, Version 1.07, August 20, 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:

- *Sekuryx PSD PP 4.0 Common Criteria Test Report and Procedures*, Version 1.2, September 1, 2021

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

- *Assurance Activities Report for Sekuryx Secure KVM Switch (CAC Models)*, Version 1.1, September 1, 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 the *PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices*, version 1.0, July 19, 2019, which consists of [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 manufacturer site in North Las Vegas, NV by Leidos personnel from July 26, 2021 to August 3, 2021. Additional supplemental evidence was collected at the Leidos facility between August 18 and September 1, 2021.

Testing performed at the vendor site was performed in accordance with NIAP Labgram #078/Valgram #098. The Leidos CCTL Quality System specifies an on-site checklist that identify the evaluator(s) sent to the vendor site and the following elements:

- Personnel access control to vendor facility (receptionist, visitor sign-in, escort)
- Physical access control to test environment within vendor facility (mechanism of isolation from general facility, personnel present in test environment)
- Logical isolation of devices under test (non-networked devices or devices deployed in isolated network)
- Verification of test equipment (serial number match, preservation of tamper-evident labels, baseline oscilloscope readings)

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.

CCTL personnel completed the checklist and included it as a supplement to the test evidence.

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 was conducted in May 2021, repeated in June, and a final search was performed on 20 August 2021 which did not reveal any known vulnerabilities. The vulnerability analysis is documented in the Vulnerability Survey documented by the evaluation team. The evaluation team searched the National Vulnerability Database (https://nvd.nist.gov/) for vulnerabilities related to the TOE series and used NVD's Basic and Advanced search features (https://nvd.nist.gov/vuln/search). The terms used for the search were as follows:

- Aten
- Belkin
- black box, blackbox
- logear
- Ipgard
- Kvm, kvm switch, peripheral switch
- Raritan
- smartavi
- tripplite
- Sekuryx

The evaluator conducted penetration testing based on the threat model defined in the claimed PP-Configuration which consists of [PSD PP], [AO Module], [KM Module], [UA Module], and [VI Module]. The testing did not exploit any vulnerability.

8 Evaluated Configuration

The evaluated version of the TOE consists of the Sekuryx Secure KVM Peripheral Sharing Devices identified in Tables 2 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 (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)

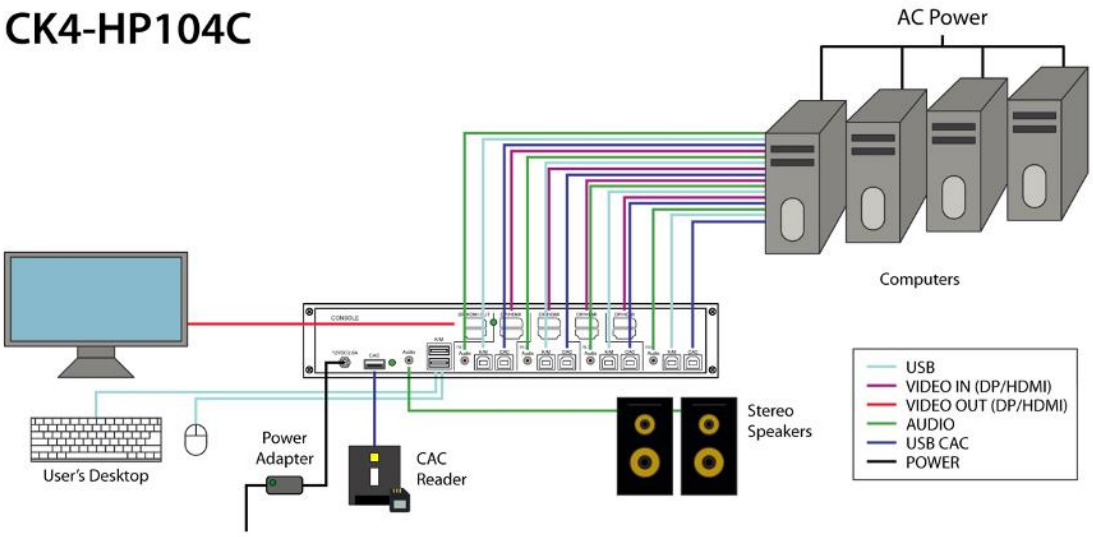

Figure 1: Setup of 4-Port TOE Installation

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 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 5: TOE Security Assurance Requirements

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 requirements 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.

This product does not use encryption. Therefore, a certificate review and entropy analysis were 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 ten 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. Note however that the purpose of TD0583 was to address FPT_PHP.3 with respect to TOE models that have a wired remote control. The TOE does not have a wired remote control, but the TD was still applied as it modifies SFR and test activity wording regardless of whether or not the TOE has a wired remote control.

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.

11 Annexes

Not applicable.

12 Security Target

Name	Description
ST Title	Sekuryx Secure KVM Switch Security Target (CAC Models)
ST Version	1.07
Publication Date	August 20, 2021

13 Abbreviations and Acronyms

Acronym	Full Definition
CAC	Common Access Card
CEM	Common Evaluation Methodology
DP	DisplayPort
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. *Assurance Activities Report for Sekuryx Secure KVM Switch (CAC Models)*, Version 1.1, September 1, 2021
2. *Common Criteria for Information Technology Security Evaluation Part 1: Introduction*, Version 3.1, Revision 5, April 2015.
3. *Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements*, Version 3.1 Revision 5, April 2015.
4. *Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components*, Version 3.1 Revision 5, April 2015.
5. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, Version 3.1, Revision 5, April 2015.
6. *Evaluation Technical Report for Sekuryx Secure KVM Switch (CAC Models)*, Version 1.1, September 1, 2021
7. *Sekuryx Secure KVM Switch Security Target (CAC Models)*, Version 1.07, August 20, 2021
8. *User Manual Sekuryx Secure DP/HDMI KVM Switch with CAC Port and 4K Ultra-HD Support*, Revision 1.0, July 21, 2021
9. *User Manual Sekuryx Secure 4 Port Single Head DP KVM Switch with CAC Port, Preview Screen and 4K Ultra-HD Support*, Revision 1.0, July 21, 2021
10. *User Manual Sekuryx Secure DP MST KVM Switch with CAC Port and 4K Ultra-HD Support*, Revision 1.0, July 21, 2021
11. *User Manual Sekuryx Secure 4 Port COMBO KVM Switch with CAC Port and 4K Ultra-HD Support*, Revision 1.0, July 21, 2021
12. *User Manual Sekuryx Secure DVI KVM Switch with CAC Port*, Revision 1.0, July 21, 2021
13. *User Manual Sekuryx Secure DP KVM Switch with CAC Port and 4K Ultra-HD Support*, Revision 1.0, July 21, 2021
14. *Sekuryx Secure KVM Administration and Security Management Tool Guide (CAC)*, Version 1.0, April 6, 2021
15. *Sekuryx PSD PP 4.0 Common Criteria Test Report and Procedures*, Version 1.2, September 1, 2021
16. *SmartAVI Vulnerability Survey*, Version 1.4, August 20, 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