

**National Information Assurance Partnership**  
**Common Criteria Evaluation and Validation Scheme**



**Validation Report**  
**for**  
**Black Box Secure KM Switch (CAC Models)**

**Report Number:** CCEVS-VR-11242-2021  
**Dated:** December 10, 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**

Daniel Faigin

Alex Korobchuk

Seada Mohammed

*The Aerospace Corporation*

Matt Downey

*National Information Assurance Partnership (NIAP)*

John Butterworth

*The MITRE Corporation*

### **Common Criteria Testing Laboratory**

Leidos

Columbia, MD

# Table of Contents

1	Executive Summary .....	1
2	Identification .....	4
2.1	Threats.....	4
2.2	Organizational Security Policies.....	5
3	Architectural Information .....	6
4	Assumptions.....	7
4.1	Clarification of Scope .....	7
5	Security Policy .....	9
5.1	Keyboard and Mouse Subsystem.....	9
5.2	TOE External Interfaces .....	9
5.3	Audio Subsystem .....	9
5.4	TOE Administration and Security Management.....	10
5.5	User Authentication Device Subsystem.....	10
5.6	User Control and Monitoring Security .....	10
5.7	Tampering Protection.....	10
5.8	Self-Testing and Security Audit.....	11
6	Documentation .....	12
7	Independent Testing.....	13
7.1	Evaluation Team Independent Testing .....	13
7.2	Vulnerability Analysis .....	14
8	Evaluated Configuration .....	15
9	Results of the Evaluation .....	16
10	Validator Comments/Recommendations .....	17
11	Annexes.....	19
12	Security Target.....	20
13	Abbreviations and Acronyms .....	21
14	Bibliography .....	22

# 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 Black Box Secure KM Switch (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 Black Box Secure KM Switch (CAC Models) was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in December 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]

Leidos performed an analysis of the NIAP Technical Decisions ([https://www.niap-cccevs.org/Documents\\_and\\_Guidance/view\\_tds.cfm](https://www.niap-cccevs.org/Documents_and_Guidance/view_tds.cfm)). Leidos determined that the following NIAP Technical Decisions applied to this evaluation:

- TD0507
- TD0518
- TD0557
- TD0583
- TD0585
- 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-cccevs.org](http://www.niap-cccevs.org)).

The Leidos evaluation team determined that the Black Box Secure KM Switch (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 publicly available Assurance Activities Report (AAR) and the associated proprietary test report produced by the Leidos evaluation team.

The Black Box Secure KM Switch (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 and 3.5mm analog audio. The TOE is a family of hardware appliances that consists of the following models:

Model Name	Description and NIAP Certification Version	Version
KVS4-1004KX	4-Port Secure KM w/ audio and CAC	4.01.000

**Table 1: Black Box 4-Port TOE Models Identification**

Model Name	Description and NIAP Certification Version	Version
KVS4-1008KX	8-Port Secure KM w/ audio and CAC	4.01.000

**Table 2: Black Box 8-Port TOE Models Identification**

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all 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 Black Box Secure KM Switch Security Target (CAC Models).

Item	Identifier
Evaluated Product	Black Box Secure KM Switch (CAC Models) consisting of the KVS4-1004KX and KVS4-1008KX models.
Sponsor & Developer	David Isola Black Box, Inc. George’s Quay Limerick, V94 CK06 Republic of Ireland
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	December 10, 2021

Item	Identifier
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	<p>PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, and User Authentication Devices, version 1.0, which includes the following PP and PP-Modules:</p> <ul style="list-style-type: none"> <li>• Protection Profile for Peripheral Sharing Device, Version 4.0, 19 July 2019</li> <li>• PP-Module for Analog Audio Output Devices, Version 1.0, 19 July 2019</li> <li>• PP-Module for Keyboard/Mouse Devices, Version 1.0, 19 July 2019</li> <li>• PP-Module for User Authentication Devices, Version 1.0, 19 July 2019</li> </ul>
Disclaimer	The information contained in this Validation Report is not an endorsement of Black Box Secure KM Switch (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	Daniel Faigin, Matt Downey, John Butterworth, Alex Korobchuk, Seada Mohammed

**Table 3: 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	Black Box Secure KM Switch Security Target (CAC Models)
ST Version	1.07
Publication Date	November 3, 2021
Vendor and ST Author	Black Box, Inc.
TOE Reference	Devices identified in Table 1 and 2 [of this VR]
TOE Software Version	4.01.000
Keywords	KM Switch, Peripheral Sharing

**Table 4: 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 Black Box Secure KM 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, mouse/pointing devices, and speakers among multiple computers over USB and analog audio.

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.

Black Box Secure KM port models:

- 4-Port
- 8-Port

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

## 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.

### 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 KM switches.

### **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, analog audio output, and user authentication devices. The filter is set at 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 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.

## **5.5 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).

## **5.6 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).

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.

## **5.7 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.

## **5.8 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:

- Black Box Secure KVM Administration and Security Management Tool Guide (CAC), Version 1.2, November 1, 2021
- Black Box Advanced 4/8-Port Secure KM Switch User Guide, Revision 2.0B, October 25, 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://www.blackbox.com/NIAP4/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:

- Black Box Secure KM Switch Security Target (CAC Models), Version 1.07, November 3, 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:

- Black Box PSD PP 4.0 Common Criteria Test Report and Procedures, Version 1.4, November 30, 2021

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

- Assurance Activities Report for Black Box KM Switch (CAC Models), Version 1.4, November 30, 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], and [UA 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 July 19, 2021 to July 26, 2021, at the vendor facility in North Las Vegas, Nevada from July 26, 2021 to August 3, 2021, with additional supplemental evidence conducted as needed at the Leidos facility through November 30, 2021. For collection of supplemental evidence, devices used for testing at the vendor site were shipped to the Leidos facility.

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.



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 several times, most recently in November 30, 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 Black Box Secure KM Peripheral Sharing Devices identified in Tables 1 and 2.

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 difference between the TOE models are the maximum number of computers that can be connected to the TOE (4, 8).

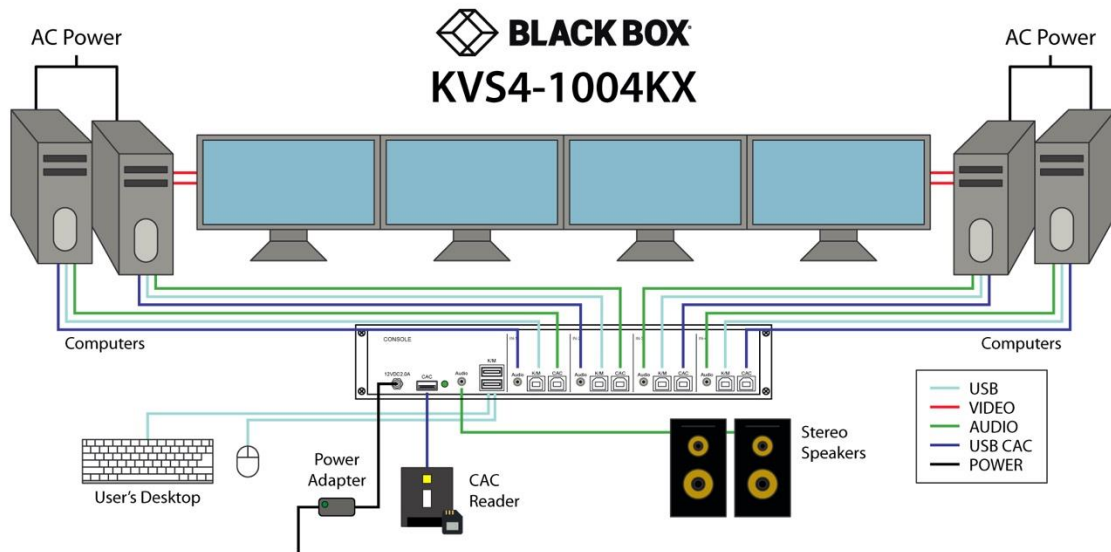


Figure 1: Setup of 4-Port TOE Installation

## 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

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 validation team's observations support the evaluation team's conclusion that the Black Box Secure KM Switch (CAC Models) meet 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 five Technical Decisions related to the claimed PP and PP-Modules: TD0507, TD0518, TD0557, TD0583, TD0585, and TD0593 (see [https://www.niap-ccevs.org/Documents\\_and\\_Guidance/view\\_tds.cfm](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 TOE provides a Cursor Control technology that allows the user to switch the active computer by pressing the middle mouse button (scroll wheel button) twice and then 'swipe' in a given direction to change the channel. In the evaluated configuration, the default configuration is used. However, other configurations that change the relationship between the mouse swipe direction and the channel switching behavior are available. It is recommended that the user be aware of this feature.
- 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.
- The administrative tool guide references KVM models despite the TOE being a family of KM devices. KVM devices from the same vendor have been evaluated separately and the administrative tool guide is shared across all models because none of the functionality described in this guide relates to behavior of a video interface.

## **10.1 Validation Approach**

These evaluations were split up into separate VIDs (11240, 11241, and 11242) 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 11240, 11241, and 11242, as long as it was made clear which tests apply to which VID.

## **11 Annexes**

Not applicable.

## 12 Security Target

Name	Description
ST Title	Black Box Secure KM Switch Security Target (CAC Models)
ST Version	1.07
Publication Date	November 3, 2021

## 13 Abbreviations and Acronyms

<b>Acronym</b>	<b>Full Definition</b>
<b>CAC</b>	Common Access Card
<b>CEM</b>	Common Evaluation Methodology
<b>IC</b>	Integrated Circuit
<b>KM</b>	Keyboard and Mouse
<b>KVM</b>	Keyboard, Video and Mouse
<b>LED</b>	Light-Emitting Diode
<b>NIAP</b>	National Information Assurance Partnership
<b>NVLAP</b>	National Voluntary Laboratory Accreditation Program
<b>PCL</b>	Product Compliant List
<b>PSD</b>	Peripheral Sharing Device
<b>ST</b>	Security Target
<b>TOE</b>	Target of Evaluation
<b>USB</b>	Universal Serial Bus
<b>VR</b>	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. Black Box Secure KM Switch Security Target (CAC Models), Version 1.07, November 3, 2021
6. Black Box Secure KVM Administration and Security Management Tool Guide (CAC), Version 1.2, November 1, 2021
7. Black Box Advanced 4/8-Port Secure KM Switch User Guide, Revision 2.0B, October 25, 2021
8. Black Box PSD PP 4.0 Common Criteria Test Report and Procedures, Version 1.4, November 30, 2021
9. SmartAVI Vulnerability Survey, Version 1.7, November 30, 2021
10. Protection Profile for Peripheral Sharing Device, Version 4.0, July 19, 2019
11. PP-Module for Analog Audio Output Devices, Version 1.0, July 19, 2019
12. PP-Module for Keyboard/Mouse Devices, Version 1.0, July 19, 2019
13. PP-Module for User Authentication Devices, Version 1.0, July 19, 2019