National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report for the

I O INTERCONNECT LTD

Secure KVM

Report Number: **CCEVS-VR-VID10878-2018**
Dated: **May 11, 2018**
Version: **1.0**

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Panel

Paul Bicknell
Michelle Carlson
Jenn Dotson
Stelios Melachrinoudis
The MITRE Corporation

Common Criteria Testing Laboratory

Michael C. Baron
Ryan Day
UL Verification Services Inc.
San Luis Obispo, CA

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 9, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the I O INTERCONNECT LTD Secure KVM Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This 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 documented in the ST.

The evaluation was completed by UL Verification Services Inc. in May 2018. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by UL Verification Services Inc. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the collaborative Protection Profile for Peripheral Sharing Switch (PSS).

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory (CCTL) using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the Protection Profile for Peripheral Sharing Switch. This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, 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 ETR are consistent with the evidence produced.

2 Identification

The Common Criteria Evaluation and Validation Scheme (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 CCTLs. CCTLs evaluate products against one or more Protection Profiles (PP) containing Assurance Activities, which are an interpretation of CEM work units specific to the technology described by the PP.

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 Compliance List (PCL).

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

- The Target of Evaluation: the fully qualified identifier of the product as evaluated.
- The Security Target: document describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The PP(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Target of Evaluation	Secure KVM v1.0
Protection Profile	Protection Profile for Peripheral Sharing Switch, February 13, 2015, Version 3.0
Security Target	I O INTERCONNECT Secure KVM Security Target v1.2, May 10, 2018
Evaluation Technical Report (ETR)	Common Criteria Evaluation Technical Report VID 10878 17-3912-R-0036 Version 1.4, May 10, 2018
Common Criteria Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor/Developer	I O INTERCONNECT LTD.
Common Criteria Testing Lab (CCTL)	UL Verification Services Inc.
CCTL Evaluators	Michael C. Baron, Ryan Day
CCEVS Validators	Paul Bicknell, Michelle Carlson, Jenn Dotson, Stelios Melachrinoudis

Table 1: Evaluation Identifiers

3 Architectural Information

I O INTERCONNECT Secure KVM is a device that allows a user to use a single set of peripherals (Keyboard, Mouse, CAC Reader, Speakers, and/or video devices) with multiple computers. The TOE allows the user to easily switch which computer the peripherals are connected to by pressing a button on the TOE. The TOE ensures the peripherals are only connected to a single computer at a time and prevents the computers from communicating with each other through the TOE. The TOE consists of a stand-alone KVM (Keyboard, Video, Mouse) switching unit or a KVM with a Desktop Control Unit (DCU). The DCU is a small device that provides channel switching buttons and selection channel indicators allowing the user to save even more desk space.

The following peripheral devices from the operational environment may be connected to the TOE in the evaluated configuration:

- PS/2 Keyboard
- PS/2 Mouse
- USB Mouse
- USB Keyboard
- USB CAC Reader
- Analog Audio Speakers or Headphones
- Video device(s) supporting DVI-D, DisplayPort, or HDMI.

The following computer interfaces from the operational environment may be connected to the TOE in the evaluated configuration:

- USB 2.0 (for Mouse and Keyboard Input)
- USB 2.0 (for CAC input)
- Analog Audio Out
- Video output supporting DVI, DisplayPort, or HDMI. See the Computer Video Interface column in Table 1 of the ST to determine which interfaces are compatible with each model of the TOE.

The TOE will switch all compatible and authorized devices attached; however, it does not require all peripheral or computer interfaces to be populated.

3.1 TOE Hardware

The TOE consists of the following hardware model identifiers:

- KVM Hardware:
  - SV141D1
  - SV141D0
  - SV241D1
  - SV241D0
  - SV121D1

    - SV121D0
    - SV142H1
    - SV142H0
    - SV242H1
    - SV242H0
    - SV142P1
    - SV142P0
    - SV122P1
    - SV122P0
    - SV242P1
    - SV242P0
    - SV222P1
    - SV222P0

- DCU Hardware:
    - AR000010

3.2 TOE Software

The TOE consists of the following firmware identifiers:

- KVM Firmware:
    - Firmware Version 26B-29B
- DCU Firmware:
    - Firmware Version 288

4 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

- User Data Protection and Data Isolation
- Protection of the TSF
- TOE Access

4.1 User Data Protection and Data Isolation

The TOE switches one peripheral group between two or four (depending on model) computer port groups. The TOE filters USB devices to ensure that only Human Interface Devices (HID) and CAC Readers are allowed. The TOE ensures the peripheral group is only connected to a single computer port group at a time and prevents the computer port groups to communicate with each other through the TOE.

The TOE indicates which computer port group is selected using LEDs on the front of the KVM or DCU and only changes the selected computer port group when the user presses the button for a different channel.

4.2 Protection of the TSF

The TOE utilizes tamper labels and tamper switches to indicate and respond to the enclosure being opened. If the KVM or DCU enclosure is opened, the TOE overwrites a portion of its firmware to permanently disable the TOE.

The TOE runs a suite of self-tests to check the integrity of the hardware and firmware. The self-tests also check to see if one of the selector buttons is stuck. If any self-tests fail, the TOE enters a warning mode and will not connect the peripheral group to any computer group.

4.3 TOE Access

When the TOE powers-up, it defaults to selecting computer group 1. The TOE also removes power from the CAC reader when the selected computer is changed to ensure the any authentication sessions are cleared.

5 Assumptions, Threats, & Clarifications of Scope

5.1 Secure Usage Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Peripheral Sharing Switch, Version 3.0, 13 February 2015 [PSS].

That information has not been reproduced here.

5.2 Threats Countered by the TOE

The Security Problem Definition, including the threats, may also be found in the [PSS]. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

5.3 Clarifications of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the [PSS].
- 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.
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, 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.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PP. Any additional security related functional capabilities included in 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.

6 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the I O INTERCONNECT LTD TOE.

The guidance documents are provided to the product consumer via download from a web-based customer portal provided by the vendor. These documents apply to the CC Evaluated configuration:

6.1 Guidance Documentation

Document	Revision	Date
IOI Administrative Guide	A1	October 19, 2017
Administrator Guide for Secure Desktop Controller Unit (DCU)	A1	October 19, 2017

6.2 Test Documentation

Document	Revision	Date
17-3912-R-0031 V1.6 IOI SV241D1 PSS Test Report	1.6	May 10, 2018
17-3912-R-0032 V1.5 IOI SV142P1 PSS Test Report	1.5	May 10, 2018
17-3912-R-0034 V1.6 IOI SV242H1 PSS Test Report	1.6	May 10, 2018

6.3 Vulnerability Assessment Documentation

Document	Revision	Date
17-3912-R-0031 V1.6 IOI SV241D1 PSS Test Report	1.6	May 10, 2018
17-3912-R-0032 V1.5 IOI SV142P1 PSS Test Report	1.5	May 10, 2018
17-3912-R-0034 V1.6 IOI SV242H1 PSS Test Report	1.6	May 10, 2018

6.4 Security Target

Document	Revision	Date
I O INTERCONNECT Secure KVM Security Target	1.2	May 10, 2018

7 IT Product Testing

This section details the testing conducted during the evaluation.

7.1 Developer Testing

No testing was performed by the developer.

7.2 Evaluation Team Independent Testing

The evaluation team performed the independent testing activities to confirm the TOE operates to the TOE security functional requirements as specified in the ST for a product claiming conformance to the PSS. The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in PSS.

Independent testing was performed at the UL facility in San Luis Obispo, CA and the Vendor facility in Santa Ana, CA.

7.3 Vulnerability Analysis

The evaluation team performed a vulnerability assessment of the TOE. A search of publically available sources for vulnerabilities (known and/or potential) in the TOE did not yield known nor viable vulnerabilities of which to test for successful exploitation of the TOE. General vulnerabilities applicable to the KVM device type where researched and all public knowledge attack vectors identified are covered in functional testing prescribed by the PP; thus, additional penetration testing using publicly gained knowledge was unnecessary.

8 Results of the Evaluation

The evaluation was carried out in accordance with CCEVS processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.

UL has determined that the TOE meets the security criteria in the ST. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in May 2018.

The Validation Team verified the correctness and completeness of the results and documentation stemming from the Assurance Activities of Security Functional Requirements (SFRs). Additionally, the Validation Team examined the ETR and the Detailed Test Reports (DTRs) corresponding to three TOE models: SV241D1, SV142P1, and SV242H1, all referenced in Section 6.2. It was determined that all evaluator activities stemming from the required Security Assurance Requirement (SAR) work units were performed and resulted in passing verdicts. Also, the equivalency argument of the three models referenced in Section 6.2 to other models included in the TOE in Section 3.1 was valid. In examining the ETR and DTRs, ATE_IND.1 and AVA_VAN.1 verdicts are called out by reference in the ETR, with passing verdicts included in each of the DTRs. All other SAR verdicts were explicitly included in the ETR with passing verdicts.

9 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices, to include software, firmware, or hardware that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

NIAP established a Peripheral Sharing Switch Technical Rapid Response Team (PSS-TRRT) to address questions and concerns related to evaluations claiming conformance to Protection Profile for Peripheral Sharing Switch. A Technical Decision is an issue resolution statement that clarifies or interprets protection profile requirements and assurance activities. PSS-TRRT has formally posted seven Technical Decisions related to Protection Profile for Peripheral Sharing Switch, namely TD0083, TD0086, TD0136, TD0141, TD0144, TD0251, and TD0298. (See https://www.niap-ccevs.org/Documents_and_Guidance/view_tds.cfm). Five of the seven PSS-TRRT Technical Decisions applied to the I O INTERCONNECT Secure KVM evaluation.

There was one TRRT decision made throughout the course of this evaluation, which was captured in TD0298. The issue refers to Test 4.4, Part 2, Step 25 of FDP_IFF.1.5(2), which requires the evaluator to place the DisplayPort AUX Channel sniffer between the display peripheral and the TOE video output. Doing so is insufficient to address the spirit of the test as it does not consider the signals between the TOE and connected computer.

Upon review, the PSS Technical Community (PSS TC) agreed to modify steps 25-32 of the Test Assurance Activity for Test 4.4, Part 2 of FDP_IFF.1.5(2) to ensure the issue was addressed.

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

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

10 Security Target

I O INTERCONNECT Secure KVM Security Target, Version 1.2, May 10, 2018.

11 Terms

AAR	Assurance Activity Report
CAC	Common Access Card
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCLT	Common Criteria Testing Laboratory
DCU	Desktop Control Unit
DTR	Detailed Test Report
ETR	Evaluation Technical Report
HID	Human Interface Device
I/O	Input/Output
IT	Information Technology
KVM	Keyboard, Video, Mouse
NIAP	National Information Assurance Program
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PCL	Product Compliance List
PP	Protection Profile
PSS	Preliberal Sharing Switch
SF	Security Functions
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
UL	United Laboratories
USB	Universal Serial Bus
VR	Validation Report

12 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, Version 3.1 Revision 4, CCMB-2009-07-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, September 2012, Version 3.1, Revision 4, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, September 2012, Version 3.1, Revision 4, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, September 2012, Version 3.1, Revision 4, CCMB-2009-07-004.