National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

Belkin® Secure DVI-I KVM Switch

Report Number: CCEVS-VR-VID10455-2011
Dated: August 1, 2011
Version: 1.2

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

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Belkin® Secure DVI-I KVM Switch, the target of evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation of the Belkin® Secure DVI-I KVM Switch product was performed by InfoGard Laboratories, Inc., in San Luis Obispo, CA in the United States and was completed in June, 2011. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and the functional testing report. The ST was written by InfoGard Laboratories. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1r.3 July 2009, Evaluation Assurance Level 2 (EAL 2) and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1 r.3, July 2009.

The Belkin® Secure DVI-I KVM Switch allows the sharing of a single set of peripheral components such as keyboard, DVI video monitor, audio output signals, and mouse/pointer devices among multiple computers through a standard USB interface. The Secure DVI-I KVM offers isolation among the switchable channels to ensure that computers are thoroughly isolated within the Belkin Secure KVM and ensures that only a single computer can access the shared peripheral resource set at one time. Dedicated manual switches with LED “switched state” indicators for each channel assure that the channel selection is unambiguously indicated. The Belkin® Secure DVI-I KVM Switch requests the connected peripherals for “plug and play” settings and stores this data internal to the KVM switch, to assure the host computer can quickly access the needed configuration data. In addition, an on-board keyboard/mouse emulator assures that connected computers boot uninterrupted regardless of switched status. The KVM Switch is available in 2 or 4 port models offering switchable connections to 2 or 4 computers through a USB connection. The Belkin® Secure DVI-I KVM Switch conforms to the Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile Version 2.1 dated 7 September 2010.

The Belkin® Secure DVI-I KVM Switch product consists of the following hardware components:

TOE or Environment	**Component**	**Description**
TOE	Belkin Secure 2-port DVI-I KVM w/audio Part Number F1DN102B <or> Belkin Secure 4-port DVI-I KVM w/audio Part Number F1DN104B <or> Belkin Secure 2-port DVI-I KVM w/audio Plus Part Number F1DN102C <or> Belkin Secure 4-port DVI-I KVM w/audio Plus Part Number F1DN104C <or> Belkin Secure 4-port DVI-I Dual-Head KVM w/audio Part Number F1DN104E <or> Belkin Secure 4-port DVI-I Dual-Head KVM w/audio Plus Part Number F1DN104F	TOE Hardware

2 Identification of the TOE

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) for EAL 1 through EAL 4 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 NIAP Validated Products List.

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

- The Target of Evaluation (TOE), the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Belkin Secure 2-port DVI-I KVM w/audio Part Number F1DN102B Belkin Secure 4-port DVI-I KVM w/audio Part Number F1DN104B Belkin Secure 2-port DVI-I KVM w/audio Plus Part Number F1DN102C Belkin Secure 4-port DVI-I KVM w/audio Plus Part Number F1DN104C Belkin Secure 4-port DVI-I Dual-Head KVM w/audio Part Number F1DN104E Belkin Secure 4-port DVI-I Dual-Head KVM w/audio Plus Part Number F1DN104F
Protection Profile	Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile Version 2.1, 7 September 2010
Security Target	Belkin® Secure DVI-I KVM Switch Security Target EAL2 augmented ALC_FLR.3, Version 1.0, July 18, 2011
Dates of Evaluation	April 2011 – June 2011
Conformance Result	EAL 2 augmented ALC_FLR.3
Common Criteria Version	Common Criteria for Information Technology Security Evaluation Version 3.1, August 2007
Common Evaluation Methodology (CEM) Version	CEM Version 3.1, September 2007
Evaluation Technical Report (ETR)	11-2098-R-0049 V1.1
Sponsor/Developer	Belkin International, Inc.
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc.
CCTL Evaluators	Annie Browne, Victor Mendoza, Kenji Yoshino
CCEVS Validators	Franklin Haskell, Olin Sibert

Table 1: Product Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that the TOE is also compliant with all International interpretations with effective dates on or before April 20, 2011.

4 Security Policy

The Belkin® Secure DVI-I KVM Switch supports the following Security Function Policy to assure data is effectively isolated through the device:

Data Separation Security Function Policy (SFP):
The TOE shall allow PERIPHERAL DATA and STATE INFORMATION to be transferred only between PERIPHERAL PORT GROUPS with the same ID.

Any User who has access to the TOE is considered an Authorized User as stated in the secure usage assumption section of the Security Target.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

A.ACCESS An AUTHORIZED USER possesses the necessary privileges to access the information transferred by the TOE.

USERS are AUTHORIZED USERS.

A.MANAGE The TOE is installed and managed in accordance with the manufacturer’s directions.

A.NOEVIL The AUTHORIZED USER is non-hostile and follows all usage guidance.

A.PHYSICAL The TOE is physically secure.

5.2 Threats Countered and Not Countered

The TOE is designed to fully or partially counter the following threats:

T.INVALIDUSB The AUTHORIZED USER will connect unauthorized USB devices to the peripheral switch.

T.RESIDUAL RESIDUAL DATA may be transferred between PERIPHERAL PORT GROUPS with different IDs.

T.ROM_PROG The TSF may be modified by an attacker such that code embedded in reprogrammable ROMs is overwritten; thus, leading to a compromise of the separation-enforcing components of the code and subsequent compromise of the data flowing through the TOE.

T.SPOOF Via intentional or unintentional actions, a USER may think the set of SHARED PERIPHERALS are CONNECTED to one COMPUTER when in fact they are connected to a different one.

T.STATE STATE INFORMATION may be transferred to a PERIPHERAL PORT GROUP with an ID other than the selected one.

T.TRANSFER A CONNECTION, via the TOE, between COMPUTERS may allow information transfer.

T.PHYSICAL The TOE may be physically tampered or modified, allowing unauthorized information flows.

5.3 Organizational Security Policies

There are no applicable organizational security policies.

6 Architectural Information

The TOE Secure KVM system can be divided into 8 subsystems:

- The power supply subsystem.
- The anti-tampering and security subsystem.
- The system controller subsystem.
- The front panel subsystem.
- The video switching and EDID emulation subsystem.
- The audio switching subsystem.
- The keyboard and mouse peripheral switching subsystem.
- The dedicated peripheral port subsystem (optional – model specific).

6.1.1 Power Supply Subsystem

The power supply sub-system uses AC main voltage to generate low DC voltages needed for TOE Secure KVM internal circuitry and various external devices (such as user keyboard, mouse and Common Access Card (CAC) reader).

The power supply sub-system is responsible for the following:

- Voltage reduction from 90-240 VAC to various low voltage DC planes
- Line and load regulation
- Power up and down timing
- Current limiting for external loads (such as console USB ports)
- Filtration to prevent radiated and conducted emissions on power lines
- ESD and over current protection of power planes

6.1.2 Anti-tampering and security subsystem

The anti-tampering and security subsystem design goals are:

1. To detect potential physical intrusion attempt.
2. To permanently prevent any use of the TOE in case that tampering event has been detected.
3. To provide clear and unambiguous user indications after TOE has been tampered.

6.1.3 System Controller Subsystem

The System Controller Subsystem is responsible for Secure KVM TOE device management, user interaction and monitoring. It communicates with the front panel subsystem to receive user inputs and provide proper user indications. The System Controller Subsystem drives the Secure KVM TOE channel select lines that controls the various switching circuitries in the TOE. In case of tampering event detected by the anti-tampering and security subsystem, the system controller subsystem permanently changes its behavior to disable use and to provide proper user indications.

6.1.4 Front Panel Subsystem

The Front Panel Subsystem provides an array of manually actuated push-buttons and switches by which the user can select which Host Computer resource is connected to the Peripheral Port Group (Keyboard, Mouse, Monitor, and CAC). The number of these switches correlates directly to the number of available ports for the applicable model 2 or 4 port versions. Also included within the Front Panel Subsystem are the LED indicators which display to the user which Host Computer is currently attached to the Peripheral Port Group through the TOE. The number of LEDs also correlates to the number of ports for the applicable model 2 or 4 port.
In some models equipped with CAC switching subsystem, the front panel subsystem also includes CAC enable disable switches and CAC status indicators for each channel (Peripheral Port Group).

6.1.5 Video Switching and EDID Emulation Subsystem

The Video switching and EDID emulation subsystem primary function is to switch a single selected Host Computer video output into the user display. As modern operating systems and software applications require Plug and Play (EDID) information from the user display to operate normally, the TOE replicates the user display EDID content into 4 isolated EDID emulators during TOE boot. After TOE boot all coupled hosts may access through read-only cycles the EDID replicated information stored at the EDID emulators.

6.1.6 Audio Switching Subsystem

Audio switching Subsystem allows users to receive audio output from one of the coupled computer hosts based on the channel selected.

6.1.7 Keyboard and Mouse Peripheral Switching Subsystem

The Keyboard and Mouse Peripheral Switching Subsystem is responsible for the qualification of the user keyboard and mouse devices and for the switching operation inside the Secure KVM TOE device.

6.1.8 Dedicated Peripheral Port Switching Subsystem

The product on which the TOE is based includes the capability of port switching for USB-connected user authentication devices (e.g., Common Access Card (CAC) readers). This subsystem is excluded from the TOE and is disabled through use of tamper-evident seals applied to the associated ports.

6.2 TOE Boundaries

The entire Belkin® Secure DVI-I KVM Switch is included in the TOE boundary. Components other than the Belkin® Secure DVI-I KVM Switch product (i.e., Switched Peripheral Port Group and Host Computers), are not part of the TOE.

The TSF consists of all subsystems except the dedicated peripheral port subsystem (i.e. port for other USB device types). This subsystem is excluded though the use of a tamper-evident seal covering the USB port. The seven subsystems that compose the TSF perform the SFR-supporting or SFR-enforcing roles below:

Data Separation TOE Security Function:

- The Data Separation security function assures that the TOE is connected to only a single computer at one time.
- Each connected computer has a discrete switch and hub on the TOE (Switch Subsystem: Multiplexer module) assigned to its USB port and each switched computer has its own logical ID within the TOE through this switch arrangement.

The design of these switches and associated circuitry assure that only a single computer can be engaged by the Peripheral Port Group resources.

Switch Management TOE Security Function:

- The switch management security function supports the switching rule that specifies that Data can flow to a Peripheral Port Group only if it was received from the same switched computer.
- The switching mechanism used precludes activating two switched computer members at once or partial activation of more than a single Peripheral Port Group member.

The TOE supports domain separation through the switch management security function and ensures that TSP functions are successful prior to allowing data to travel through the TOE from the Peripheral Port Group to the switch computer resource.

Protection of the TOE Security Function:

- Tamper switches ensure that security is maintained in the event of a physical attack.

If tamper is detected, the TOE will be disabled and all LEDs will flash.

Visual Indication of Selected Computers:

- LEDs on the front panel indicate which computer is selected.

USB Connection:

- The TOE will query the device for its USB class.
- The TOE will only communicate with devices claiming a class of “03h” corresponding to the HID USB class.

Read-Only Memory:

- The memory of the TOE is a form of ROM located within the flash of an internal [to the TOE] microcontroller.

7 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Belkin® Secure DVI-I KVM Switch.[1] Note that not all evidence is available to customers. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is *not* delivered is shown in a normal typeface.
- Documentation that is delivered as part of the product but was not used as evaluation is shown with a bold title, but a hashed background.

The TOE is physically delivered to the End-User. The guidance is part of the TOE components and is delivered with the TOE as a supplement.

7.1 Design Documentation

Document	Revision	Date
EAL 2 augmented ALC_FLR.3 Design Documentation Belkin® Secure DVI-I KVM Switch Models: Belkin Secure 2-port DVI-I KVM w/audio - Part Number F1DN102B, Belkin Secure 4-port DVI-I KVM w/audio - Part Number F1DN104B, Belkin Secure 2-port DVI-I KVM w/audio Plus - Part Number F1DN102C, Belkin Secure 4-port DVI-I KVM w/audio Plus - Part Number F1DN104C, Belkin Secure 4-port DVI-I Dual-Head KVM w/audio - Part Number F1DN104E, Belkin Secure 4-port DVI-I Dual-Head KVM w/audio Plus - Part Number F1DN104F	1.0	June 28, 2011

7.2 Guidance Documentation

Document	Revision	Date
Belkin® Secure DVI-I KVM Common Criteria Supplement	1.0	June 28, 2011
Belkin® Secure DVI-I KVM Dual-Head Switch with Audio User Manual	8820-00764 Rev. A00	2011
Belkin® Secure DVI-I KVM Switch with Audio User Manual	8820-00762 Rev. A00	2011

[1] This documentation list is based on the lists provided in the Evaluation Technical Report developed by InfoGard.

7.3 Configuration Management and Lifecycle

Document	Revision	Date
EAL 2 Life Cycle Support Documentation Belkin® DVI-I Secure KVM Switch Models: Belkin Secure 2-port DVI-I KVM w/audio - Part Number F1DN102B, Belkin Secure 4-port DVI-I KVM w/audio - Part Number F1DN104B, Belkin Secure 2-port DVI-I KVM w/audio Plus - Part Number F1DN102C, Belkin Secure 4-port DVI-I KVM w/audio Plus - Part Number F1DN104C, Belkin Secure 4-port DVI-I Dual-Head KVM w/audio - Part Number F1DN104E, Belkin Secure 4-port DVI-I Dual-Head KVM w/audio Plus - Part Number F1DN104F	1.0	June 2, 2011
Belkin ® Systematic Flaw Remediation	1.0	June 2, 2011

7.4 Test Documentation

Document	Revision	Date
EAL 2 + ALC_FLR.3 Tests Activity ATE Belkin® Secure DVI-I KVM Switch	1.0	June 6, 2011
Belkin® Secure DVI-I Dual-Link KVM EAL 2 Independent Test Plan (ATE_IND.2)	1.0	June 28, 2011

7.5 Vulnerability Assessment Documentation

Document	Revision	Date
Common Criteria Vulnerability Analysis AVA_VAN.3 EAL2	1.0	June 2, 2011

7.6 Security Target

Document	Revision	Date
Belkin® Secure DVI-I KVM Switch Security Target EAL2 augmented ALC_FLR.3	1.0	July 18, 2011

8 IT Product Testing

This section describes the testing efforts of the Developer and the evaluation team.

8.1 Developer Testing

The test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces.

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results (ATRs) are also included in the TOE Test Plan. Each test case was identified by a number that correlates to the expected test results in the TOE Test Plan.

The evaluation team analyzed the Developer's testing to ensure adequate coverage for EAL 2. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

8.2 Evaluation Team Independent Testing

The evaluation team conducted independent testing at the CCTL. The evaluation team installed the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2-2. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation
- Security functions not tested adequately in the vendor's test plan and procedures

The evaluation team repeated 6 of the 10 Sponsor test cases and specified additional tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

Each TOE Security Function was exercised at least once, and the evaluation team verified that each test passed.

8.3 Vulnerability Analysis

The evaluation team devised penetration testing to confirm that the TOE was resistant to penetration attacks performed by an attacker with an expertise level of unsophisticated. The evaluation team conducted testing using the same test configuration that was used for the independent team testing. In addition to the documentation review used in the independent testing, the team used the knowledge gained during independent testing to devise the penetration testing. This resulted in a set of four penetration tests.

8.4 Vulnerability Search

The evaluation team performed a thorough search of public vulnerability databases in order to identify potential vulnerabilities that could affect the evaluated TOE. No vulnerabilities were found related to the evaluated TOE or similar products.

9 Evaluated Configuration

The evaluated configuration of the Belkin® Secure DVI-I KVM Switch, as defined in the Security Target, consists of one hardware component and one firmware component (please refer to Table 1).

The Belkin® Secure DVI-I KVM Switch is delivered to the end user with an instructional supplement describing the actions necessary to configure the TOE to be in the Common Criteria evaluated configuration.

10 Results of the Evaluation

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

InfoGard has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in June of 2011.

11 Validator Comments

The product on which the evaluated TOE is based includes the additional capability of switching access to USB-connected user authentication devices (e.g., Common Access Card (CAC) readers). Because of the requirements of the Peripheral Sharing Switch Protection Profile and CCEVS PD-0165 (effective 19 May 2011), the associated ports in the evaluated TOE are disabled by application of a tamper-evident seal. Administrative guidance describes the purpose of the seal.

In compliance with CCEVS PD-0166 (effective 19 May 2011), the evaluated TOE does include the capability of switching (non-USB) audio output devices. No capability exists in the product for switching audio input devices.

The TOE provides secure operation when powered off: no data is passed between any ports in the TOE when power is not supplied. Although this function was not explicitly tested by the evaluation, it was repeatedly exercised during the evaluation team’s activities and found to operate as described.

12 Annexes

N/A

13 Security Target

Belkin® Secure DVI-I KVM Switch Security Target EAL2 augmented ALC_FLR.3, Version 1.0, July 18, 2011.

14 Glossary

Keep-Alive Feature This feature of the Belkin Secure KVM switch stores data within the hubs in the device to provide keyboard/mouse emulation to the connected computers to assure boot up processes are not interrupted if a computer is not switched to the peripheral port group.

KVM Switch Keyboard, Video, Mouse - A KVM (keyboard, video, mouse) switch allows a single keyboard, video monitor and mouse to be switched to any of a number of computers when typically a single person interacts with all the computers but only one at a time.

Peripheral Data Refers to data entered via a member of a peripheral port group i.e.: data entered by the mouse or keyboard and displayed through the monitor.

Peripheral Port Group A collection of device ports treated as a single entity by the TOE.

Plug and Play A standardized interface for the automatic recognition and installation of interface cards and devices on a PC.

Switched Computers Refers to the computers connected to the TOE and connected to the Peripheral port group upon the switching function of the TOE.

State Information The current or last known status or condition, of a process, transaction, or setting. “Maintaining state” means keeping track of such data over time.

User The human operator of the TOE.

15 Bibliography

Common Criteria Project Sponsoring Organizations. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and General Model, July 2009, Version 3.1, Revision 3, CCMB-2009-07-001.

Common Criteria Project Sponsoring Organizations. Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.

Common Criteria Project Sponsoring Organizations. Common Criteria for Information Technology Security Evaluation - Part 3: Security Assurance Components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.

Common Criteria Project Sponsoring Organizations. Common Criteria Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.

Common Criteria, Evaluation and Validation Scheme, Publication #3, Guidance to Validators, Version 2.0, 8 September 2008.

InfoGard Laboratories, Inc. Belkin® Secure DVI-I KVM Switch Security Target EAL2 augmented ALC_FLR.3, Version 1.0, July 18, 2011.

InfoGard Laboratories, Inc. Evaluation Technical Report Belkin® Secure DVI KVM Switch Version 1.1, June 28, 2011.