National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Belkin® OmniView Secure KVM Switch
(F1DN102U, F1DN104U, F1DN108U)

Report Number: CCEVS-VR-07-0036
Dated: 8 June 2007
Version: V1.1

National Institute of Standards and Technology ..... *National Security Agency*
Information Technology Laboratory ..... *Information Assurance Directorate*
100 Bureau Drive ..... *9800 Savage Road, STE 6757*
Gaithersburg, MD 20899 ..... *Fort George G. Meade, MD 20755-6757*

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® OmniView™ Secure 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® OmniView™ Secure KVM Switch product was performed by InfoGard Laboratories, Inc., in San Luis Obispo, CA in the United States and was completed on April 30th, 2007. 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 2.3, August 2005 Evaluation Assurance Level 4 (EAL 4) and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.3, January 2004.

The Belkin® OmniView™ Secure KVM Switch allows the sharing of a single set of peripheral components such as keyboard, Video Monitor and Mouse/Pointer devices among multiple computers through a standard USB interface. The OmniView Secure 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 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, 4 or 8 port models offering switchable connections to 2, 4 or 8 computers through a USB connection. The Belkin OmniView Secure KVM Switch conforms to the Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile Version 1.0 dated 8 August 2000.

The Belkin® OmniView™ Secure KVM Switch product consists of the following hardware and software components:

TOE or Environment	Component	Description
TOE	Belkin Secure KVM Switch 2 Port PN # F1DN102U (or) Belkin Secure KVM Switch 4 Port PN # F1DN104U (or) Belkin Secure KVM Switch 8 Port PN # F1DN108U	TOE Hardware

Table 1: Hardware Components

TOE or Environment	Component	Description
TOE	Firmware 2050-161-1-0-0-1-0-2.s19	Embedded Firmware software component Version 3.1.6

Table 2: Software Components

It is important to note that there are no aspects of the TOE that are excluded from the CC Evaluated Configuration.

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 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 KVM Switch 2 Port PN # F1DN102U (or) Belkin Secure KVM Switch 4 Port PN # F1DN104U (or) Belkin Secure KVM Switch 8 Port PN # F1DN108U
Protection Profile	N/A
Security Target	Belkin® OmniView™ Secure KVM Models: F1DN102U, F1DN104U, F1DN108U, May 2, 2007, Version 1.0
Dates of evaluation	August 11, 2006 – May 2, 2007
Conformance result	EAL 4
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 2.3, August 2005
Common Evaluation Methodology (CEM) version	CEM version 2.3, January 2005
Evaluation Technical Report (ETR)	07-1131-R-0046 V1.1
Sponsor/Developer	Belkin International, Inc.
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories
CCTL Evaluators	Albert Chang, Clyde Sy
CCEVS Validators	Noblis, The Aerospace Corporation

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) identified below were applicable to this evaluation.

The TOE is also compliant with all International interpretations with effective dates on or before August 11, 2006.

4 Security Policy

The Belkin® OmniView™ Secure 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

The Belkin® OmniView™ Secure KVM Switch performs the following security functionality:

- Data Separation
- Switch Management

Any User who has access to the TOE is considered as 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.EMISSION	The TOE meets the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions. [In the United States, Part 15 of the FCC Rules for Class B digital devices.]
A.ISOLATE	Only the selected COMPUTER'S video channel will be visible on the shared MONITOR.
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.
A.SCENARIO	Vulnerabilities associated with attached DEVICES (SHARED PERIPHERALS or SWITCHED COMPUTERS), or their CONNECTION to the TOE, are a concern of the application scenario and not of the TOE.

5.2 Threats Countered and Not Countered

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

T.BYPASS	The TOE may be bypassed, circumventing nominal SWITCH functionality.
T.INSTALL	The TOE may be delivered and installed in a manner which violates the security policy.
T.LOGICAL	The functionality of the TOE may be changed by reprogramming in such a way as to violate the security policy.
T.PHYSICAL	A physical attack on the TOE may violate the security policy.
T.RESIDUAL	RESIDUAL DATA may be transferred between PERIPHERAL PORTGROUPS with different IDs.
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.

It should be noted that use of peripheral devices with bi-directional communication and storage capabilities introduces a new threat that the TOE does not protect against. It is possible for data to leak from the TOE through peripheral devices, specifically those with storage capabilities. Please see Section 11 for additional guidance.

5.3 Organizational Security Policies

There are no applicable organizational security policies

6 Architectural Information

The Belkin® OmniView™ Secure KVM Switch architecture is divided into the following sections in the ST:

- Data Separation
- Switch Management

The TOE itself is not concerned with the User's information flowing between the shared peripherals and the switched computers. It is only providing a connection between the human interface devices and a selected computer at any given instant.

6.1.1 Data Separation

The Data Separation security function assures that the TOE is connected to only a single computer at one time. Manual switches allow the operator to select which computer is connected to the Peripheral Port Group at any given time. Each connected computer has a discrete switch and hub on the TOE assigned to its USB port and each switched computer has its own logical ID within the TOE through this switch arrangement. Through this dedicated switching mechanism, the connection between the Peripheral port group and the selected computer is activated. The design of these switches and associated circuitry assure that only a single computer can be engaged by the keyboard, mouse and video monitor resources. Through this data separation security function, the TOE precludes the sharing or transfer of data between computers by the TOE.

6.1.2 Switch Management

The TOE provides a LED indicator light above the push button switch that indicates to the User which computer is activated to the Peripheral port group. The switch management security function also 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 is strictly manual and 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.

6.2 TOE Boundaries

Figure 5 illustrates the Belkin® OmniView™ Secure KVM Switch and its intended environment. Components other than the Belkin® OmniView™ Secure KVM Switch product (i.e. Switched Peripheral Port Group and Host Computers), are not part of the TOE.

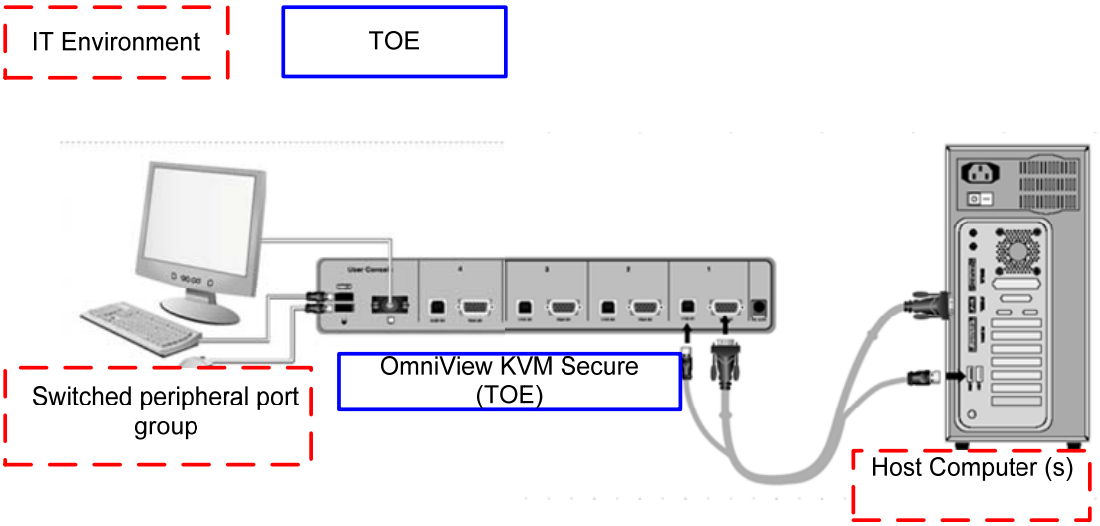

Figure 5: Physical Boundaries

In terms of logical boundaries, the following table enumerates the division between services provided *by* the TOE. The TOE itself does not rely on any services provided by the Operating Environment:

Functional Area	Services Provided *By* The TOE	Services Provided *To* The TOE By The Operating Environment
Data Separation	The Data Separation security function assures that the TOE is connected to only a single computer at one time. Manual switches allow the operator to select which computer is connected to the Peripheral Port Group at any given time. Each connected computer has a discrete switch and hub on the TOE assigned to its USB port and each switched computer has its own logical ID within the TOE through this switch arrangement. Through this dedicated switching mechanism, the connection between the Peripheral port group and the selected computer is activated. The design of these switches and associated circuitry assure that only a single computer can be engaged by the keyboard, mouse and video monitor resources. Through this data separation security function, the TOE precludes the sharing or transfer of data between computers by the TOE.	None
Switch Management	The TOE provides a LED indicator light above the push button switch that indicates to the User which computer is activated to the Peripheral port group. The switch management security function also supports the switching rule that specifies that Data can flow to a Peripheral Port Group only if it was	None

	received from the same switched computer. The switching mechanism used is strictly manual and 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.	

Table 3: TOE Security Functions

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® OmniView™ Secure 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 on a CD labeled "Documentation CD".

7.1 Design documentation

Document	Revision	Date
EAL 4 Design Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U	1.0	May 2, 2007
Belkin Schematic Sheet 1	5.0.1	October 5, 2006
Belkin Schematic Sheet 2	5.0.1	October 5, 2006

7.2 Guidance documentation

Document	Revision	Date
Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Supplement EAL 4	1.0	May 2, 2007
Belkin® OmniView™ Secure KVM Switch User Manual F1DN102U F1DN104U F1DN108U	P75209-A	2006

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

Document	Revision	Date
Belkin® OmniView™ Secure KVM Switch Quick Installation Guide F1DN102U F1DN104U F1DN108U	P75210	2006

7.3 Configuration Management and Lifecycle

Document	Revision	Date
EAL 4 Life Cycle Support Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U	1.0	April 30, 2007

7.4 Delivery and Operation documentation

Document	Revision	Date
Common Criteria Supplement EAL4 Secure Delivery Document Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U	1.0	April 30, 2007
EAL 4 Configuration Management Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U	1.0	May 2, 2007

7.5 Test documentation

Document	Revision	Date
EAL 4 Tests Activity ATE Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U	1.0	May 2, 2007
Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U EAL 4 Independent Test Plan	1.0	May 2, 2007

7.6 Vulnerability Assessment documentation

Document	Revision	Date
Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Vulnerability Analysis AVA_VLA.2 EAL4	1.0	April 30, 2007
EAL 4 Design Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U	1.0	May 2, 2007
Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Supplement EAL 4	1.0	May 2, 2007

7.7 Security Target

Document	Revision	Date
Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Security Target	1.0	May 2, 2007

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. During the evaluation of the ATE_FUN.1, the evaluation team identified inconsistencies in the test cases and worked with the Developer to create accurate test cases.

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 4. 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 reran 100% of the Sponsor's 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 ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the Developer Vulnerability Analysis, the evaluation team's Vulnerability Analysis, and the evaluation team's performance of penetration tests.

The Developer performed a Vulnerability Analysis of the TOE to identify any obvious vulnerabilities in the product and to show that they are not exploitable in the intended environment for the TOE operation. In addition, the evaluation team conducted a sampling of the vulnerability sites claimed by the Sponsor to determine the thoroughness of the analysis.

Based on the results of the Developer's 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 two penetration tests.

9 Evaluated Configuration

The evaluated configuration of the Belkin® OmniView™ Secure KVM Switch, as defined in the Security Target, consists of one hardware component and one firmware component (Please refer to Table 1 and 2).

The Belkin® OmniView™ Secure KVM Switch is already configured when they are shipped to the customers. No additional instructions are necessary for the secure installation and startup of the TOE.

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 2.3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3.

InfoGard Laboratories has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 4. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed on April 30, 2007.

11 Validator Comments/Recommendations

It should be noted that Precedent Decision -138 affects the Protection Profile that this TOE conforms with. The customer is urged to review PD-138 (http://www.niap-ccevs.org/cc-scheme/PD/0138.html) as products compliant with this profile may not include mechanisms to ensure that all peripheral memory is cleared when the device is switched between computers. Switching functionality for the Belkin OmniView Secure KVM switch includes complete disconnect of the active Host during switching, resulting in the requisite USB reset upon reconnection to the new Host. Through USB enumeration rules, this reset activity eliminates any data stored in a volatile USB buffer within a peripheral device. Any commercially available peripheral (as defined in the referenced Protection Profile) without non volatile memory is assumed to conform to the USB standard.

It is the responsibility of integrators of the switch to assess the risk of information transfer with compliant switches.

12 Annexes

N/A

13 Security Target

Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Security Target, Version 1.0, May 2, 2007.

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

1.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 2.3, August 2005. CCMB-2005-08-001 .

2.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 2.3, August 2005.CCMB-2005-08-002

3.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 2.3, August 2005. CCMB-2005-08-003.

4.) Common Criteria Project Sponsoring Organisations. Common Criteria Common Methodology for Information Technology Security Evaluation. Version 2.3, August 2005. CCMB-2005-08-004.

5.) Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

6.) InfoGard Laboratories, Inc. *Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Security Target,* Version 1.0, May 2, 2007.

7.) InfoGard Laboratories. *Evaluation Technical Report Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U*, Version 1.1, May 2, 2007.