

Belkin® OmniView™ Secure DVI Dual-Link KVM Switch

Models: F1DN102D, F1DN104D

Security Target EAL 4 augmented ALC_FLR.3



Release Date: January 29, 2009

Document ID: 07-1602-R-0109

Version: 1.1

Prepared By: InfoGard Laboratories, Inc.

Prepared For: Belkin Corporation
501 West Walnut Street
Compton, CA 90220

Table of Contents

DOCUMENT HISTORY	4
1 INTRODUCTION.....	5
1.1 IDENTIFICATION	5
1.2 OVERVIEW	5
1.3 DOCUMENT ORGANIZATION	7
1.4 DOCUMENT CONVENTIONS	8
1.5 DOCUMENT TERMINOLOGY	8
1.5.1 <i>ST Specific Terminology</i>	8
1.5.2 <i>Acronyms</i>	9
1.6 COMMON CRITERIA PRODUCT TYPE	10
1.7 TOE ARCHITECTURE OVERVIEW	10
1.8 ARCHITECTURE DESCRIPTION	10
1.8.1 <i>Front Panel Subsystem</i>	11
1.8.2 <i>Control Subsystem</i>	11
1.8.3 <i>Switch Subsystem</i>	11
1.9 PHYSICAL BOUNDARIES	12
1.9.1 <i>Hardware Components</i>	13
1.9.2 <i>Software Components</i>	14
1.9.3 <i>Guidance Documents</i>	14
1.10 LOGICAL BOUNDARIES	14
1.10.1 <i>Data Separation</i>	15
1.10.2 <i>Switch Management</i>	15
1.11 ITEMS EXCLUDED FROM THE TOE	15
2 CONFORMANCE CLAIMS	16
2.1 CONFORMANCE CLAIMS: COMMON CRITERIA	16
2.2 PROTECTION PROFILE REFERENCE	16
3 SECURITY PROBLEM DEFINITION.....	17
3.1 SECURE USAGE ASSUMPTIONS	17
3.2 THREATS	17
3.3 ORGANIZATIONAL SECURITY POLICIES	18
4 SECURITY OBJECTIVES.....	19
4.1 SECURITY OBJECTIVES FOR THE TOE.....	19
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT	20
4.3 MAPPING OF SECURITY ENVIRONMENT TO SECURITY OBJECTIVES	21
4.4 SECURITY OBJECTIVES RATIONALE	22
4.5 SECURITY OBJECTIVES RATIONALE FOR THE OPERATIONAL ENVIRONMENT	24
4.6 RATIONALE FOR ORGANIZATIONAL POLICY COVERAGE.....	24
5 EXTENDED COMPONENTS DEFINITION.....	25
5.1 TOE EXTENDED FUNCTIONAL REQUIREMENTS.....	25
5.2 EXTENDED REQUIREMENTS (EXT).....	25
5.2.1 <i>EXT_VIR.1 Visual indication rule</i>	25
5.3 RATIONALE FOR EXPLICITLY STATED SECURITY REQUIREMENTS.....	25

6	SECURITY REQUIREMENTS	27
6.1	TOE SECURITY FUNCTIONAL REQUIREMENTS	27
6.1.1	<i>User Data Protection (FDP)</i>	27
6.1.2	<i>Security Management (FMT)</i>	28
6.1.3	<i>Protection of the TSF (FPT)</i>	29
6.2	RATIONALE FOR TOE SECURITY REQUIREMENTS.....	30
6.2.1	<i>TOE Security Functional Requirements Tracing & Rationale</i>	30
6.3	RATIONALE FOR IT SECURITY REQUIREMENT DEPENDENCIES	32
6.4	DEPENDENCIES NOT MET.....	33
6.5	SECURITY ASSURANCE MEASURES	33
6.6	RATIONALE FOR SECURITY ASSURANCE	35
6.6.1	<i>TOE Security Assurance Requirements selection criteria</i>	35
6.7	RATIONALE FOR TOE SECURITY FUNCTIONS	35
7	TOE SUMMARY SPECIFICATION	37
7.1	TOE SECURITY FUNCTIONS	37
7.1.1	<i>Data Separation</i>	37
7.1.2	<i>Switch Management</i>	38

List of Tables

Table 1:	Hardware Components	13
Table 2:	Software Components.....	14
Table 3:	TOE Security Objectives	20
Table 4:	Operational Environment Security Objectives	20
Table 5:	Threats & IT Security Objectives Mappings	22
Table 6:	Extended SFR Components.....	25
Table 7:	Explicitly Stated SFR Rationale	26
Table 8:	Functional Requirements	27
Table 9:	SFR and Security Objectives Mapping.....	30
Table 10:	SFR Dependencies.....	33
Table 12:	Security Assurance Measures	34
Table 14:	TOE Security Function to SFR Mapping	36

List of Figures

Figure 1: TOE Architecture Overview	10
Figure 2: Belkin OmniView Secure DVI KVM internal architecture	11
Figure 3: TOE Physical Boundaries	12

Document History

Document Version	Date	Author	Comments
1.1	01/29/09	Mike McAlister	Updated based on FVOR verdicts

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 Identification

TOE Identification: Belkin® OmniView™ Secure DVI Dual-Link 2-port KVM Switch
Part Number F1DN102D

<or>

Belkin® OmniView™ Secure DVI Dual-Link 4-port KVM Switch
Part Number F1DN104D

ST Identification: Belkin® OmniView™ Secure DVI Dual-Link KVM Switch Models:
F1DN102D, F1DN104D Security Target

ST Version: 1.1

ST Publish Date: January 29, 2009

ST Author: M McAlister, InfoGard

PP Identification: Validated Protection Profile - Peripheral Sharing Switch for Human
Interface Devices Protection Profile, Version 1.2, 21 August 2008

1.2 Overview

The TOE is a Belkin® OmniView™ Secure DVI Dual-Link KVM Switch available in 2 or 4 port versions. The Switch allows the sharing of a single keyboard, audio devices (ie: speakers, microphone), video monitor and mouse pointing device among host computers. These devices comprise the shared Peripheral Port Group. These peripherals may be switched between connected computers solely upon activation of a manual switch on the front of the unit. The design of the unit precludes the connection of peripherals to more than 1 host computer at once and does not allow host computers to communicate with each other through the unit. In addition,

the TOE does not store user data in any form and ensures that no data transfers from one computer to an adjacent computer during the switching process, including computer state data.

The dedicated manual switches on the front panel include LED “switched state” indicators for each channel and assure that the current channel selection is unambiguously indicated to the user. The TOE during initialization polls 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 when connected. In addition, an on-board keyboard/mouse emulator assures that connected host computers boot uninterrupted regardless of active switched status.

The TOE consists of both hardware and firmware in a single component assembly. The firmware contained in the device is non-volatile and cannot be modified to assure secure operation and is identical for 2 or 4 port versions of the TOE.

This Security Target and the TOE conforms to the Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile Version 1.2, 21 August 2008. The TOE 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 switched PERIPHERAL PORT GROUPS with the same ID.

1.3 Document Organization

Security Target Introduction (Section 1)

Provides identification of the TOE and ST, an overview of the TOE, an overview of the content of the ST, document conventions, and relevant terminology. The introduction also provides a description of the TOE security functions as well as the physical and logical boundaries for the TOE, the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE.

Conformance Claims (Section 2)

Provides applicable Common Criteria (CC) conformance claims, Product Profile (PP) conformance claims and Assurance Package conformance claims.

Security Problem Definition (Section 3)

Describes the threats, organizational security policies, and assumptions pertaining to the TOE and the TOE environment.

Security Objectives (Section 4)

Identifies the security objectives for the TOE and its supporting environment as well as a rationale that objectives are sufficient to counter the threats identified for the TOE.

Extended Components Definition (Section 5)

Presents components needed for the ST but not present in Part II or Part III of the Common Criteria Standard.

Security Requirements (Section 6)

Presents the Security Functional Requirements (SFRs) met by the TOE and the security functional requirements rationale. In addition this section presents Security Assurance Requirements (SARs) met by the TOE as well as the assurance requirements rationale. Provides pointers to all other rationale sections, to include the rationale for the selection of IT security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability

Summary Specification (Section 7)

Describes the security functions provided by the TOE that satisfy the security functional requirements, provides the rationale for the security functions. It also describes the security assurance measures for the TOE as well as the rationales for the assurance measures.

1.4 Document Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify these operations. When NIAP interpretations are included in requirements, the additions from the interpretations are displayed as refinements.

Assignment: indicated with bold text

Selection: indicated with underlined text

Refinement: *additions indicated with bold text and italics*

deletions indicated with strike-through ~~bold text and italics~~

Iteration: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MSA.1a)

Extended: indicated as per the applicable PP (e.g. EXT_VIR.1)

The explicitly stated requirements claimed in this ST are denoted by the “EXT” extension in the unique short name for the explicit security requirement.

1.5 Document Terminology

Please refer to CC Part 1 Section 4 for definitions of commonly used CC terms.

1.5.1 ST Specific Terminology

Keep-Alive Feature	This feature of the Belkin Secure DVI 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 shared 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 the shared peripheral port group i.e.: data entered by the mouse or keyboard and displayed through the monitor.
Shared Peripheral port group	A collection of device ports for peripherals shared among Host Computers via the TOE and 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 shared Peripheral port group upon the switching function of the TOE. aka Switched Peripheral Port Group
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.

1.5.2 Acronyms

CCIB	Common Criteria Implementation Board
CCIMB	Common Criteria Interpretations Management Board
CM	Configuration Management
DVI	Digital Video Interface
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read-Only Memory
FCC	Federal Communications Commission
ID	Identification
ISO	International Standards Organization
ISSE	Information Systems Security Engineer[ing]
ISSO	Information Systems Security Organization
IT	Information Technology
KVM	Keyboard-Video-Mouse
LCD	Liquid Crystal Display
LED	Light-Emitting Diode
MAC	Mandatory Access Control
PP	Protection Profile
PSS	Peripheral Sharing Switch
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
VDT	Video Display Terminal

1.6 Common Criteria Product type

The TOE is a KVM switch device classified as a “Peripheral Sharing Switch” for Common Criteria. The TOE includes both hardware and firmware components.

1.7 TOE Architecture Overview

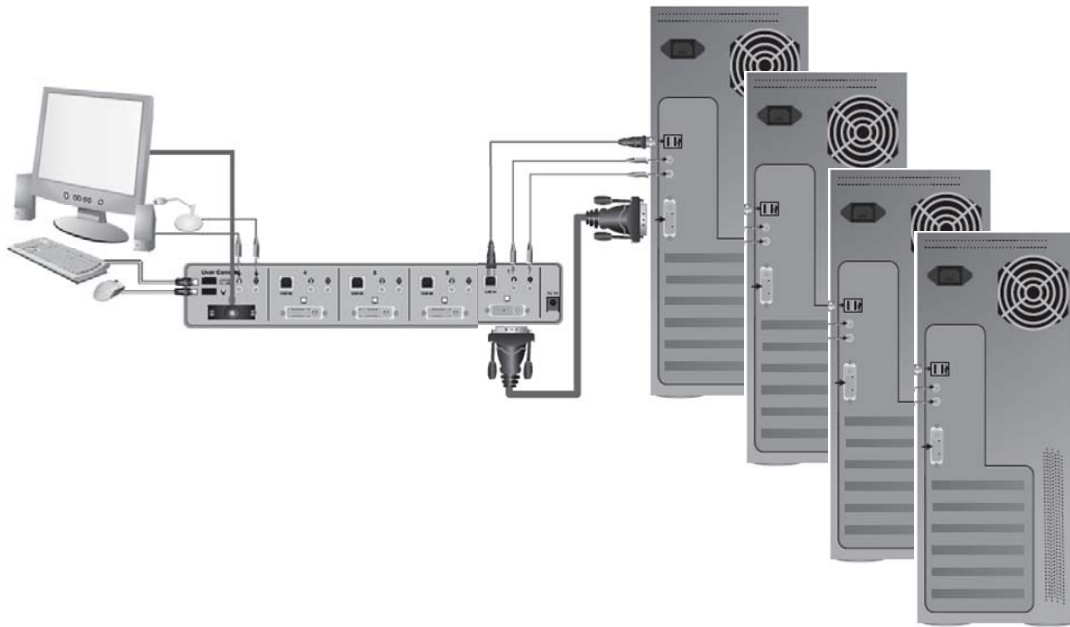


Figure 1: TOE Architecture Overview

1.8 Architecture Description

The TOE is made up of hardware components and a firmware component integrated into a single electronic component chassis.

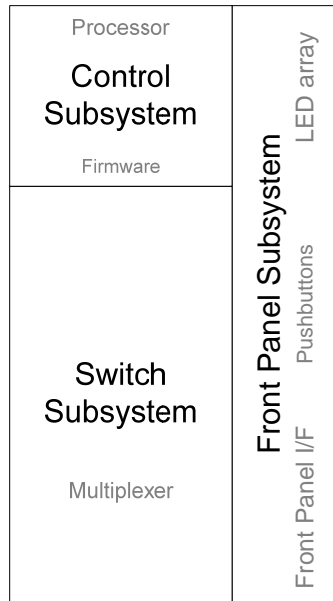


Figure 2: Belkin OmniView Secure DVI KVM internal architecture

1.8.1 Front Panel Subsystem

The Front Panel Subsystem consists of the front panel interface circuit board, associated manual pushbutton switches and the LED array. This subsystem sends and receives signals from the Control subsystem to specify when a button is pushed and then energize the appropriate LED to indicate the switching action has succeeded.

1.8.2 Control Subsystem

The Control Subsystem consists of a Processor Module and integrated Firmware module. The Control Subsystem contains the switching logic that generates commands to the switch subsystem to execute a switch from one Host Computer to another based on a front panel button push.

1.8.3 Switch Subsystem

The Switch Subsystem consists of the signal path circuitry between the shared Peripheral Port Group and the Host Computers and a Multiplexer Module that translates Control Subsystem signals into switching actions. The Switch Subsystem provides discrete circuitry (Hub modules) for each Host Computer.

1.9 Physical Boundaries

This section lists the hardware and software components of the product and denotes which are in the TOE and which are in the environment.

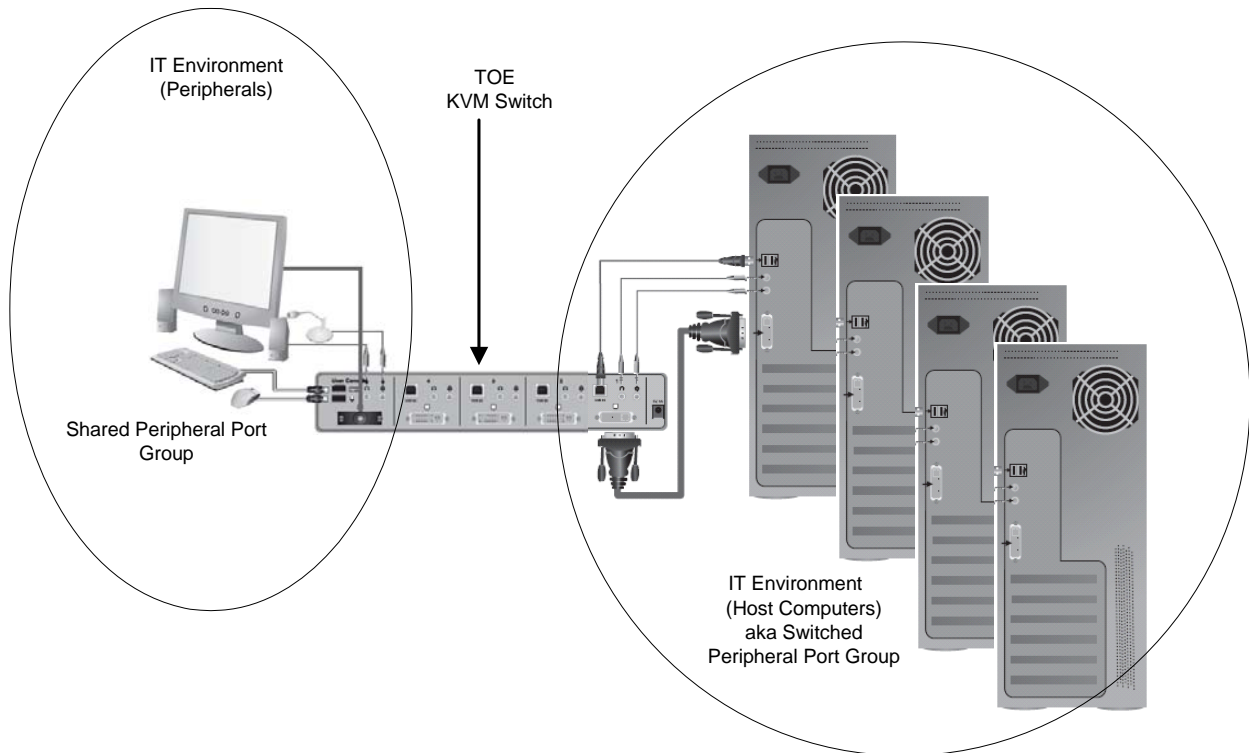


Figure 3: TOE Physical Boundaries

1.9.1 Hardware Components

This table identifies hardware components and indicates whether or not each component is in the TOE.

TOE or Environment	Component	Description
TOE	Belkin Secure DVI KVM Switch 2 Port PN # F1DN102D (or) Belkin Secure DVI KVM Switch 4 Port PN # F1DN104D	TOE Hardware
Environment	USB Mouse	Shared Peripheral Port Group Member
Environment	USB Keyboard	Shared Peripheral Port Group Member
Environment	Monitor – DVI-D (video) DVI dual-link Monitors Including, but not limited to: Apple Cinema HD display up to 30-inch Dell Widescreen up to 30-inch HP Widescreen (LP3065) up to 30-inch (video resolution of up to 2560x1600)	Shared Peripheral Port Group Member
Environment	Belkin DVI/USB KVM Cables (one per KVM): F1D9201-06 – 6 ft. (1.8m) or F1D9201-10 – 10 ft. (3m) or F1D9201-15 – 15 ft. (4.6m)	Cables for connection of Host Computers to Peripheral Port Group
Environment	Audio Device 1 as applicable (i.e.: Speakers (supports 3.5mm connector))	Shared Peripheral Group Member
Environment	Audio Device 2 as applicable (i.e.: Microphone (supports 3.5mm connector))	Shared Peripheral Group Member
Environment	Host Computers Qty 2 or 4 based on KVM used Any hardware platform able to support the following Operating Systems: Windows® 2000, XP, Server 2003, Vista Mac OS® X v10.3 and above Red Hat® Linux Desktop®, Red Hat Enterprise Linux WS	Operational Environment Host Computer resources

Table 1: Hardware Components

1.9.2 Software Components

This table identifies software components and indicates whether or not each component is in the TOE.

TOE or Environment	Component	Description
TOE	Firmware 2050-211-1-0-0-1-0-1 (Master) 2050-212-1-0-0-1-0-1 (Slave)	Embedded Firmware software component Version 1.01
Environment	Host Computer Operating Systems	All versions/releases of the following OS types: Windows® 2000, XP, Server 2003, Vista™ Mac OS® X v10.3 and above Red Hat® Linux Desktop®, Red Hat Enterprise Linux WS

Table 2: Software Components

1.9.3 Guidance Documents

The following guidance documents are provided with the TOE upon delivery in accordance with EAL 4 requirements:

1. Belkin® OmniView™ Secure DVI Dual-Link KVM Switch Models: F1DN102D F1DN104D Common Criteria Supplement EAL 4
2. Belkin® OmniView® Secure DVI Dual-Link KVM Switch User Manual, PM00507
3. Belkin® OmniView® Secure DVI Dual-Link KVM Switch Quick Installation Guide, PM00506

All documentation delivered with the product is germane to and within the scope of the TOE.

1.10 Logical Boundaries

This section contains the product features and denotes which are in the TOE.

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.

1.10.1 Data Separation

The Data Separation security function assures that the TOE is connected to only a single computer at one time. Manual switches within the Front Panel Subsystem allow the operator to select which computer is connected to the shared Peripheral Port Group at any given 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. Through this dedicated switching mechanism, the connection between the shared 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 shared peripheral port group resources. Through this data separation security function, the TOE precludes the sharing or transfer of data between computers through the TOE.

1.10.2 Switch Management

The TOE provides a series of LED indicators above the push button switches that indicates to the User which computer is activated to the shared Peripheral port group. The switch management security function also supports the switching rule that specifies that Data can flow to a shared 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 host computer to the shared Peripheral Port Group. This is enforced by the manual pushbutton switches within the Front Panel Subsystem, the logic controls within the Control Subsystem and the circuit path switches within the Switch Subsystem. External enclosure mating surfaces are sealed with tamper labels prior to delivery to provide a method of detecting if the TOE packaging has been compromised. 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 shared peripheral port group to the switch computer resource.

1.11 Items Excluded from the TOE

This section identifies any items that are specifically excluded from the TOE.

- None

2 Conformance Claims

The following Conformance Claims apply the Belkin OmniView Secure DVI KVM:

2.1 Conformance Claims: Common Criteria

The TOE is Common Criteria (CC) Version 3.1 Part 2 Extended.

The TOE is Common Criteria (CC) Version 3.1 Part 3 conformant at EAL 4 (+ALC_FLR.3).

The TOE is compliant with all International interpretations with effective dates on or before 02/14/08.

This TOE is conformant to the following Protection Profile: Validated Protection Profile - Peripheral Sharing Switch for Human Interface Devices Protection Profile, Version 1.2, 21 August 2008 (note: the ALC_FLR.2 requirement is met by ALC_FLR.3 which is an augmentation to the PP requirement)

2.2 Protection Profile Reference

This Security Target claims conformance to the following Protection Profile:

- a. Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile Version 1.2, 21 August 2008.
- b. This Security Target has maintained the Assumptions, Threats, Security Objectives, and Security Functional Requirement of the Protection Profile without modification.
- c. This Security Target conforms to EAL 4 + ALC_FLR.2 as indicated in the referenced Protection Profile except that the ALC_FLR.3 has been claimed in lieu of ALC_FLR.2.

3 Security Problem Definition

The TOE is intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is equivalent.

This section contains assumptions regarding the security environment and the intended usage of the TOE and threats on the TOE and the Operational Environment.

3.1 Secure Usage Assumptions

- 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.

3.2 Threats

The asset under attack is the information transiting the TOE. In general, the threat agent is most likely (but not limited to) people with TOE access (who are expected to possess "average" expertise, few resources, and moderate motivation) or failure of the TOE or PERIPHERALS.

- 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 and remain undetected during use.
T.RESIDUAL	RESIDUAL DATA may be transferred between (Switched) PERIPHERAL PORT GROUPS 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 (Switched) PERIPHERAL PORT GROUP with an ID other than the selected one.
T.TRANSFER	A CONNECTION, via the TOE, between COMPUTERS may allow information transfer.

3.3 Organizational Security Policies

There are no Organizational Security Policies for this TOE.

4 Security Objectives

This chapter describes the security objectives for the TOE and the Operational Environment. The security objectives are divided between TOE Security Objectives (for example, security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (for example, security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 Security Objectives For The TOE

This section defines the IT security objectives that are to be addressed by the TOE.

Security Objective	Description
O.CONF	The TOE shall not violate the confidentiality of information which it processes. Information generated within any PERIPHERAL GROUP COMPUTER CONNECTION shall not be accessible by any other PERIPHERAL GROUP-COMPUTER CONNECTION.
O.CONNECT	No information shall be shared between SWITCHED COMPUTERS via the TOE. This includes STATE INFORMATION, if such is maintained within the TOE.
O.INDICATE	The AUTHORIZED USER shall receive an unambiguous indication of which SWITCHED COMPUTER has been selected.
O.INVOKE	Upon switch selection, the TOE is invoked.
O.NOPROG	Logic contained within the TOE shall be protected against unauthorized modification. Embedded logic must not be stored in programmable or re-programmable components.
O.ROM	TOE software/firmware shall be protected against unauthorized modification. Embedded software must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.
O.SELECT	An explicit action by the AUTHORIZED USER shall be used to select the COMPUTER to which the shared set of PERIPHERAL DEVICES is CONNECTED. Single push button, multiple push button, or rotary selection methods are used by most (if not all) current market products. Automatic switching based on

	scanning shall not be used as a selection mechanism
O.SWITCH	All DEVICES in a SHARED PERIPHERAL GROUP shall be CONNECTED to at most one SWITCHED COMPUTER at a time.
O.TAMPER	The TOE Device provides unambiguous detection of physical tampering to determine whether physical tampering with the TSF's devices or TSF's enclosure has occurred.

Table 3: TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The following IT security objectives for the environment are to be addressed by the Operational Environment by technical means.

Environment Security Objective	Description
OE.ACCESS	The AUTHORIZED USER shall possess the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.
OE.EMISSION	The TOE shall meet 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.]*
OE.ISOLATE	Only the selected COMPUTER'S video channel shall be visible on the shared MONITOR.
OE.MANAGE	The TOE shall be installed and managed in accordance with the manufacturer's directions.
OE.NOEVIL	The AUTHORIZED USER shall be non-hostile and follow all usage guidance.
OE.PHYSICAL	The TOE shall be physically secure.
OE.SCENARIO	Vulnerabilities associated with attached DEVICES (SHARED PERIPHERALS or SWITCHED COMPUTERS), or their CONNECTION to the TOE, shall be a concern of the application scenario and not of the TOE.

Table 4: Operational Environment Security Objectives

Belkin claims the TOE is designed to conform to the following:

Global regulatory, safety and certification requirements

- Common Criteria EAL 4: Peripheral Sharing Switch (PSS) for Human Interface Devices*
- FCC class B*
- CE*
- Canadian ICES-003*
- Australian , C-Tick*
- cUL (Power supply only)

*Certification and testing performed in the USA

Industry Certification

- WHQL (Windows Hardware Quality Labs testing) for MS Windows XP
- USB IF - USB Implementers Forum

*Certification and testing performed in the USA

Global environmental requirements

- RoHS - Restriction of Hazardous Substances Directive
- WEEE - Waste Electrical and Electronic Equipment

Note: Testing and verification of compliance to the above certifications is outside the scope of the Common Criteria Evaluation process and were not verified as part of this evaluation.

4.3 Mapping of Security Environment to Security Objectives

The following table represents a mapping of the threats and assumptions to the security objectives defined in this ST.

	O.CONF	O.CONNECT	O.INDICATE	O.INVOKE	O.NOPROG	O.ROM	O.SELECT	O.SWITCH	O.TAMPER	OE.MANAGE
T.BYPASS				X						
T.INSTALL										X
T.LOGICAL					X	X				
T.PHYSICAL	X				X	X			X	
T.RESIDUAL	X	X								
T.SPOOF			X				X			
T.STATE	X	X								
T.TRANSFER	X	X						X		

Table 5: Threats & IT Security Objectives Mappings

4.4 Security Objectives Rationale

All of the Security Objectives for the Operational Environment are considered to be Secure Usage Assumptions. These sections are taken directly from the applicable Protection Profile reference, including comments.

O.CONF Threats countered: T.PHYSICAL, T.RESIDUAL, T.STATE, T.TRANSFER

If the PERIPHERALS can be CONNECTED to more than one COMPUTER at any given instant, then a channel may exist which would allow transfer of information from one to the other. This is particularly important for DEVICES with bi-directional communications channels such as KEYBOARD and POINTING DEVICES.

(PP Excerpt) Since many PERIPHERALS now have embedded microprocessors or microcontrollers, significant amounts of information may be transferred from one COMPUTER system to another, resulting in compromise of sensitive information. An example of this is transfer via the buffering mechanism in many KEYBOARDS.) *excerpt from the applicable Protection Profile.

- O.CONNECT Threats countered: T.RESIDUAL, T.STATE, T.TRANSFER
- The purpose of the TOE is to share a set of PERIPHERALS among multiple COMPUTERS. Information transferred to/from one SWITCHED COMPUTER is not to be shared with any other COMPUTER.
- O.INDICATE Threats countered: T.SPOOF
- The USER must receive positive confirmation of SWITCHED COMPUTER selection.
- O.INVOKE Threats countered: T.BYPASS
- The TOE must be invoked whenever a switch selection is made.
- O.NOPROG Threats countered: T.LOGICAL, T.PHYSICAL
- The functional capabilities of the TOE are finalized during manufacturing. The configuration of the TOE (operating parameters and other control information) may change.
- O.ROM Threats countered: T.LOGICAL, T.PHYSICAL
- Any software/firmware affecting the basic functionality of the TOE must be stored in a medium which prevents its modification.
- O.SELECT Threats countered: T.SPOOF

The USER must take positive action to select the current SWITCHED COMPUTER.

O.SWITCH Threats countered: T.TRANSFER

The purpose of the TOE is to share a set of PERIPHERALS among multiple COMPUTERS. It makes no sense to have, for example, video CONNECTED to one COMPUTER while a POINTING DEVICE is CONNECTED to another COMPUTER.

O.TAMPER Threats countered: T.PHYSICAL

The TOE provides mechanisms that provide unambiguous indication of a physical tampering attempt that might compromise the TSF.

4.5 Security Objectives Rationale for the Operational Environment

OE.MANAGE Threats countered: T.INSTALL

The security objective OE. MANAGE addresses the threat T.INSTALL by specifying that the TOE shall be installed and managed in accordance with the manufacturer's directions.

Since the rest of the security objectives for the Operational Environment are a restatement of the security assumptions, those security objectives trace to all aspects of the assumptions.

4.6 Rationale For Organizational Policy Coverage

There are no Organizational Policies for this TOE.

5 Extended Components Definition

Extended Security Functional Requirements (Explicit)	
EXT_VIR.1	Visual indication rule

Table 6: Extended SFR Components

5.1 TOE Extended Functional Requirements

The security requirements listed in this section are explicitly stated as they have not been obtained from Section 2 of the Common Criteria Standard. The explicit requirements for EXT_VIR.1 are taken directly from the applicable Protection Profile.

5.2 Extended Requirements (EXT)

Hierarchical to: No other components.

Dependencies: No dependencies.

5.2.1 EXT_VIR.1 Visual indication rule

EXT_VIR.1.1 A visual method of indicating which COMPUTER is CONNECTED to the shared set of PERIPHERAL DEVICES shall be provided.

(PP reference) Application Note: Does not require tactile indicators, but does not preclude their presence. The indication shall persist for the duration of the CONNECTION.

5.3 Rationale for Explicitly Stated Security Requirements

Table 7 below presents the rationale for the inclusion of the explicit requirements found in this Security Target.

Explicit Requirement	Identifier	Rationale
EXT_VIR.1	Visual Indication Rule	<p>There must be some positive feedback from the TOE to the USER to indicate which SWITCHED COMPUTER is currently CONNECTED.</p> <p>Part 2 of the Common Criteria does not provide a component appropriate to express the requirement for visual indication.</p>

Table 7: Explicitly Stated SFR Rationale

6 Security Requirements

The security requirements that are levied on the TOE are specified in this section of the ST.

TOE Security Functional Requirements (from CC Part 2)	
FDP_ETC.1	Export of User Data Without Security Attributes
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple Security Attributes
FDP_ITC.1	Import of User Data Without Security Attributes
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FPT_PHP.1	Passive detection of physical attack

Table 8: Functional Requirements

6.1 TOE Security Functional Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

6.1.1 User Data Protection (FDP)

6.1.1.1 FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the **Data Separation SFP** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

6.1.1.2 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **Data Separation SFP** on the set of (Switched) **PERIPHERAL PORT GROUPS**, and the bi-directional flow of **PERIPHERAL DATA** and **STATE INFORMATION** between the **SHARED PERIPHERALS** and the **SWITCHED COMPUTERS**.

6.1.1.3 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **Data Separation SFP** based on the following types of subject and information security attributes:

(Switched) PERIPHERAL PORT GROUPS (SUBJECTS), PERIPHERAL DATA and STATE INFORMATION (OBJECTS), PERIPHERAL PORT GROUP IDs (ATTRIBUTES).

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

Switching Rule:
PERIPHERAL DATA can flow to a (Switched) PERIPHERAL PORT GROUP with a given ID only if it was received from a (Switched) PERIPHERAL PORT GROUP with the same ID.

FDP_IFF.1.3 The TSF shall enforce the **No additional information flow control SFP rules.**

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: **No additional rules.**

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **No additional rules.**

6.1.1.4 FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the **Data Separation SFP** when importing user data, controlled under the SFP, from outside the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **No additional rules.**

6.1.2 Security Management (FMT)

6.1.2.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **Data Separation SFP** to restrict the ability to modify the security attributes (Switched) **PERIPHERAL PORT GROUP IDs** to the **USER**.

Application Note: An AUTHORIZED USER shall perform an explicit action to select the COMPUTER to which the shared set of PERIPHERAL devices is CONNECTED.

*excerpt from the applicable Protection Profile.

6.1.2.2 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **Data Separation SFP** to provide restrictive default values for security attributes that are used to enforce the SFP.

Application Note: On start-up, one and only one attached COMPUTER shall be selected.

*excerpt from the applicable Protection Profile.

FMT_MSA.3.2 The TSF shall allow the **None** to specify alternative initial values to override the default values when an object or information is created.

6.1.2.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **None**.

6.1.3 Protection of the TSF (FPT)

6.1.3.1 FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

6.2 Rationale For TOE Security Requirements

The section below demonstrates the tracing of Security Functional Requirements to Security Objectives and describes the applicable rationale based on direct reference from the applicable Protection Profile.

6.2.1 TOE Security Functional Requirements Tracing & Rationale

	O.CONF	O.CONNECT	O.INDICATE	O.INVOKE	O.ROM	O.SELECT	O.SWITCH	O.TAMPER	O.NOPROG
FDP_ETC.1	X	X							
FDP_IFC.1	X	X							
FDP_IFF.1	X	X					X		
FDP_ITC.1	X	X							
FMT_MSA.1						X			
FMT_MSA.3							X		
FPT_PHP.1								X	
EXT_VIR.1			X						
ADV_ARC.1				X	X				X

Table 9: SFR and Security Objectives Mapping

FDP_ETC.1 (Export of User Data Without Security Attributes)

In typical TOE applications, USER data consists of HUMAN INTERFACE DEVICE control information. Also included is configuration information such as KEYBOARD settings that must be reestablished each time the TOE switches between COMPUTERS. These DEVICES neither expect nor require any security

ATTRIBUTE information. The information content of the data passed through a CONNECTION is ignored.

Objectives addressed: O.CONF, O.CONNECT

FDP_IFC.1 (Subset Information Flow Control)

This captures the policy that no information flows between different (Switched) PERIPHERAL PORT GROUP IDS.

This requirement is a dependency of FDP_ETC.1, FDP_IFF.1, FDP_ITC.1 and FMT_MSA.1.

Objectives addressed: O.CONF, O.CONNECT

FDP_IFF.1 (Simple Security Attributes)

This requirement identifies the security ATTRIBUTES needed to detail the operation of a switch and the rules allowing information transfer.

This requirement is a dependency of FDP_IFC.1.

Objectives addressed: O.CONF, O.CONNECT, O.SWITCH

FDP_ITC.1 (Import of User Data Without Security Attributes)

In typical TOE applications, USER data consists of HUMAN INTERFACE DEVICE control information. These DEVICES neither expect nor require any security ATTRIBUTE information.

Objectives addressed: O.CONF, O.CONNECT

FMT_MSA.1 (Management of Security Attributes)

This restricts the ability to change selected (Switched) PERIPHERAL PORT GROUP IDS to the AUTHORIZED USER.

This requirement is a dependency of FMT_MSA.3.

Objectives addressed: O.SELECT

FMT_MSA.3 (Static Attribute Initialization)

The TOE assumes a default (Switched) PERIPHERAL PORT GROUP selection based on a physical switch position or a manufacturer's specified sequence for choosing among the CONNECTED COMPUTERS (CONNECTED here implies powered on).

This requirement is a dependency of FDP_IFF.1 and FDP_ITC.1.

Objectives addressed: O.SWITCH

FPT_PHP.1 (Passive detection of physical attack)

Mechanisms are provided that provide the ability to detect a physical attack on the TOE hardware component, where the enclosure is opened and internal components are potentially modified.

Objectives addressed: O.TAMPER

EXT_VIR.1 (Visual Indication Rule)

There must be some positive feedback from the TOE to the USER to indicate which SWITCHED COMPUTER is currently CONNECTED.

Part 2 of the Common Criteria does not provide a component appropriate to express the requirement for visual indication.

Objectives addressed: O.INDICATE

ADV_ARC.1 Design/Development Assurance Measure

The following Security Objectives are either partially or completely satisfied through the TOE's design and are verified through the ADV Development Series assurance measure:

- O.NOPROG
- O.INVOKE
- O.ROM

This mapping and reference is provided in the applicable PP reference:

**Validated Protection Profile - Peripheral Sharing Switch for Human Interface Devices
Protection Profile, Version 1.2, 21 August 2008**

6.3 Rationale For IT Security Requirement Dependencies

This section includes a table of all the security functional requirements and their dependencies and a rationale for any dependencies that are not satisfied.

Functional Component	Dependency	Included/Rationale
FDP_ETC.1	FDP_IFC.1 Subset information flow control	Yes
FDP_IFC.1	FDP_IFF.1 Simple security attributes	Yes
FDP_IFF.1	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Yes
FDP_ITC.1	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Yes
FMT_MSA.1	FDP_IFC.1 Subset information flow control FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	No (FMT_SMR.1) *FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	No *FMT_SMR.1
FPT_PHP.1	None	Yes
EXT_VIR.1	None	Yes

Table 10: SFR Dependencies

6.4 Dependencies Not Met

FMT_SMR.1 (Security Roles) dependency of FMT_MSA.1 and FMT_MSA.3

The TOE is not required to associate USERS with roles; hence, there is only one “role”, that of USER. This deleted requirement, a dependency of FMT_MSA.1 and FMT_MSA.3, allows the TOE to operate normally in the absence of any formal roles.

6.5 Security Assurance Measures

The assurance measures provided for this Security Target are described in detail in evidence documentation to be provided to the evaluation team during the course of the evaluation of this TOE.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.3 Systematic Flaw Remediation
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing: security enforcing modules
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Table 11: Security Assurance Measures

6.6 Rationale for Security Assurance

6.6.1 TOE Security Assurance Requirements selection criteria

EAL 4 + ALC_FLR.3 was chosen to provide a moderate level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws.

EAL 4 was selected because it challenges vendors to use best (rather than average) commercial practices, permits economically feasible retrofit of security-enhancing techniques, and avoids the non-trivial expense and rigor of formal methods.

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 4 as defined by the CC.

6.7 Rationale for TOE Security Functions

This section provides a table demonstrating the tracing of TOE security functions back to aspects of the security functional requirements (SFRs).

A justification that the security functions are suitable to cover the SFRs can be found in Section 7.1.

	Data Separation	Switch Management
FDP_ETC.1	X	
FDP_IFC.1	X	
FDP_IFF.1	X	X
FDP_ITC.1	X	

	Data Separation	Switch Management
FMT_MSA.1	X	
FMT_MSA.3	X	
EXT_VIR.1		X
FPT_PHP.1		X

Table 12: TOE Security Function to SFR Mapping

7 TOE Summary Specification

7.1 TOE Security Functions

The TOE consists of 2 Security Functions:

- Data Separation
- Switch Management

7.1.1 Data Separation

The Belkin® OmniView™ Secure DVI Dual-Link KVM Switch provides the ability to switch a single keyboard, mouse (pointing device), two audio circuits that may be used for connecting speakers/microphone and video monitor (constituting the peripheral device group) among a group of computer resources. The TOE includes models that feature either 2 or 4 port versions that can switch among 2 or 4 computer resources, respectively. Firmware used by the TOE is stored in a One Time Programmable (OTP) device to assure programming cannot be altered to result in an insecure state. In addition, the integrated circuit that houses the firmware is directly soldered to the circuit board to prevent removal or tampering with the firmware device.

The TOE features a design and utilizes circuitry that assures that user data, including keystrokes traveling through the device, are not stored or buffered within the unit. The Belkin Secure DVI KVM simply activates a circuit to pass data through the device based on the selection of a button push/host selection. Data entered or displayed through the shared Peripheral Port Group is directly associated with the active host computer selected. The dedicated front panel buttons each correspond to a specific host computer attached to an associated port. The design utilizes separate processors and switching mechanisms within the Multiplexer module for each port that, in conjunction with the firmware, controls data flow by port and assures data, including state information, cannot flow from one computer resource to another computer.

A USB reset command is executed as part of USB initialization during each switch, resulting in the resetting and re-enumeration of the USB connection, thereby deleting the old address information/settings and requiring that this data be re-established for each switch between host computers. (FDP_IFC.1, FDP_IFF.1)

User related attribute and state data is not transferred upon switching of host computers. This assures isolation of all data from computer to computer during the switching process and,

through design of discrete circuit paths, while a given channel is activated. During operation, switching from one host computer to another can only be executed by manual activation through the front panel buttons by the user of the TOE. (FDP_ITC.1, FMT_MSA.1, FDP_ETC.1)

Upon startup of the TOE or power cycle, the switching status of the TOE is forced to a default channel (channel 1) and enacts all data separation functions. The TOE provides restrictive default values for access to switched computer resources by requiring manual activation of the switching mechanism to engage a specific computer resource connected to the Belkin Secure DVI KVM Switch. The TOE maintains a security domain within the device and enforces separation between subjects within the TOE's Scope of Control (TSC) through the Data Separation security function. (FMT_MSA.3)

7.1.2 Switch Management

The Switch Management security function provides visual indicators through LEDs on the front panel of the TOE that are clearly illuminated, indicating which computer port is switched and active at a given instant. In addition, separate switch circuitry is provided within the Switch Subsystem: Multiplexer module for each computer connected to a USB port on the Secure KVM device to provide direct selection and isolation on a port by port basis. The Data Separation SFP is fully engaged and all security functionality is effective upon startup of the Secure KVM or upon activation of the manual switch. (EXT_VIR.1, FDP_IFF.1)

The Belkin Secure DVI KVM switch stores “plug and play” information for the connected DVI monitor within the shared peripheral port group in a serial EEPROM to enable the attached computers to directly access this information whenever they request it.

The TOE also features a “Keep-Alive” switch management function within the dedicated hubs for each port that provides a keyboard/mouse emulator function to assure that connected host computers are not interrupted during the boot process. This assures that even if the host computers are not set to the active channel, they will still detect the required keyboard and mouse presence to allow the boot to succeed.

The TOE enclosure is sealed with anti-tamper labels on the time of manufacture. Any attempts to open the enclosure after manufacturing will result in alteration of the tamper seal and make it obvious that the tamper label has been disturbed, possibly due to an access attempt. This assures that TOE physical integrity can be verified when received as well as during use. (FPT_PHP.1)