Belkin® OmniView™ Secure KVM Models:

F1DN102U

F1DN104U

F1DN108U

Security Target

Release Date:	May 2, 2007
Document ID:	06-1131-R-0029
Version:	1.0

Prepared By:	InfoGard Laboratories, Inc.
Prepared For:	Belkin International, Inc. 501 West Walnut Street Compton, CA 90220

Table of Contents

List of Tables

List of Figures

Document History

Document Version	Date	Author	Comments
1.0	05/02/07	IGL	Final release version

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 2-port KVM Switch PN F1DN102U Or Belkin® OmniView™ Secure 4-port KVM Switch PN F1DN104U Or Belkin® OmniView™ Secure 8-port KVM Switch PN F1DN108U
ST Identification:	Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Security Target
ST Version:	1.0
ST Publish Date:	May 2, 2007
ST Authors:	MMcAlister, InfoGard
PP Identification:	Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile Version 1.0, 8 August 2000

1.2 CC Conformance Claim

The TOE is Common Criteria (CC) Version 2.3[1] Part 2, conformant.

The TOE is Common Criteria (CC) Version 2.3 Part 3 conformant at EAL4.

The TOE is compliant with all International interpretations with effective dates on or before 8/11/06.

This TOE is conformant to the following Protection Profile: Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile Version 1.0, 8 August 2000

[1] Common Criteria (CC) for Information Technology Security Evaluation (ISO/IEC 15408:2005;) – August 2005, Version 2.3.

1.3 Overview

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;

1.4 Organization

Section	Title	Description
1	Introduction	Provides an overview of the security target.
2	TOE Description	Defines the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE.
3	TOE Security Environment	Contains the threats, assumptions and organizational security policies that affect the TOE.
4	Security Objectives	Contains the security objectives the TOE is attempting to meet.
5	IT Security Requirements	Contains the functional and assurance requirements for this TOE.
6	TOE Summary Specification	A description of the security functions and assurances that this TOE provides.
7	PP Claims	Protection Profile Conformance Claims
8	Rationale	Contains pointers to the rationales contained throughout the document.

Table 1: ST Organization and Description

1.5 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 ".EXP" extension in the unique short name for the explicit security requirement.

1.6 Document Terminology

Please refer to CC Part 1 Section 3 for definitions of commonly used CC terms.

1.6.1 ST Specific Terminology

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.

1.6.2 Acronyms

CCIB	Common Criteria Implementation Board
CCIMB	Common Criteria Interpretations Management Board
CM	Configuration Management
CRT	Cathode Ray Tube
EAL	Evaluation Assurance Level
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

1.7 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.

2 TOE Description

2.1 Overview

The TOE is a Belkin OmniView Secure KVM switch available in 2, 4 or 8 port versions. The Switch allows the sharing of a keyboard, video monitor and mouse pointing device through USB and VGA connections. 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, 4 or 8 port versions of the TOE. The TOE provides assured isolation among connected computers through the KVM components and switching mechanism. The Switch allows only 1 computer to access the shared peripheral set of devices at one time and disallows any attempt to connect the peripheral set to more than 1 computer resource at once. The TOE also ensures that no data transfers from one computer to an adjacent computer during the switching process, including computer state data. This Security Target and the TOE conforms to the Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile Version 1.0, 8 August 2000. 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 PERIPHERAL PORT GROUPS with the same ID.

2.2 Architecture Description

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

2.3 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.

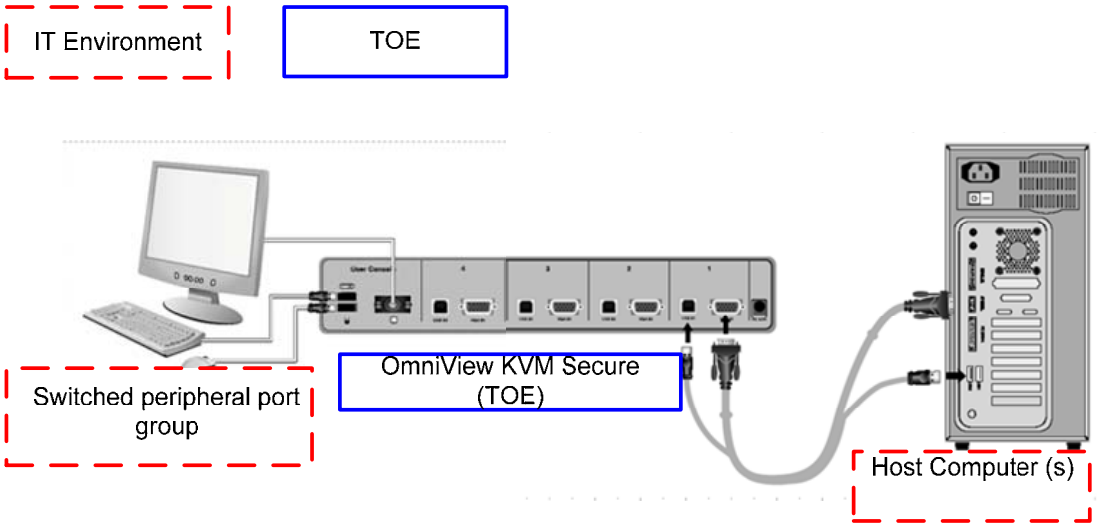

Figure 1: TOE Physical Boundaries

2.3.1 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 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
Environment	USB Mouse	Peripheral Group Member
Environment	USB Keyboard	Peripheral Group Member
Environment	Monitor – VGA connector	Peripheral Group Member
Environment	Host Computers Qty 2, 4 or 8 based on KVM used	IT Environment Computer resources

Table 2: Hardware Components

2.3.2 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 2050-176-5-0-3-3-1-6	Embedded Firmware software component Version 3.16

Table 3: Software Components

2.3.3 Guidance Documents

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

- AGD_USR –User Guidance – Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Supplement EAL4
- AGD_ADM - Administrator Guidance – Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Supplement EAL4
- ADO_IGS – Installation Guidance - Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Supplement EAL4

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

2.4 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.

2.4.1 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 it's 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.

2.4.2 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.

2.5 Items Excluded from the TOE

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

- None

3 TOE Security Environment

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 IT 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.

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.

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 IT 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.

Table 4: TOE Security Objectives

4.2 Security Objectives for the IT Environment

The following IT security objectives for the environment are to be addressed by the IT 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 5: OE Security Objectives

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	OE.MANAGE
T.BYPASS				X					
T.INSTALL									X
T.LOGICAL					X	X			
T.PHYSICAL	X				X	X			
T.RESIDUAL	X	X							
T.SPOOF			X				X		
T.STATE	X	X							
T.TRANSFER	X	X						X	

Table 6: Threats & IT Security Objectives Mappings

4.4 Security Objectives Rationale

All of the Security Objectives for the IT Environment are considered to be Secure Usage Assumptions.

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.

(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.)

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.

4.5 Rationale For Organizational Policy Coverage

There are no Organizational Policies for this TOE.

5 IT 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_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
Explicitly Stated TOE Security Functional Requirements	
EXT_VIR.1	Visual Indication Rule

Table 7: Functional Requirements

5.1 TOE Security Functional Requirements

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

5.1.1 User Data Protection (FDP)

5.1.1.1 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 TSC.

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

5.1.1.2 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **Data Separation SFP** on **the set of PERIPHERAL PORT GROUPS, and the bi-directional flow of**

PERIPHERAL DATA and STATE INFORMATION between the SHARED PERIPHERALS and the SWITCHED COMPUTERS.

5.1.1.3 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:

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 PERIPHERAL PORT GROUP with a given ID only if it was received from a 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 provide the following: **No additional SFP capabilities**.

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

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: **No additional rules**.

5.1.1.4 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 TSC.

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

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

5.1.2 Security Management (FMT)

5.1.2.1 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 **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.

5.1.2.2 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.

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.

5.1.3 Protection of the TOE security functions (FPT)

5.1.3.1 FPT_RVM.1

FPT_RVM.1.1 The TSF shall ensure that TSP functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.3.2 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.2 Extended Requirements (EXT)

5.2.1.1 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.

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 TOE Strength of Function Claim

None of the requirements imply probabilistic or permutational mechanisms; therefore, no strength of function claims are necessary.

5.4 TOE Security Assurance Requirements

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.

Assurance Component	Component ID	Component title
Configuration management - ACM	ACM_AUT.1	Partial CM Automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and operation – ADO	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development – ADV	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE Security Policy Model
Guidance documents –AGD	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support – ALC	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well defined development tools
Tests – ATE	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: High-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment - AVA	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

Table 8: Assurance Requirements: EAL4

5.4.1 ACM_AUT.1 Partial CM Automation

Developer action elements:

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

Content and presentation of evidence elements:

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

Evaluator action elements:

ACM_AUT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.2 ACM_CAP.4 Generation support and acceptance procedures

Developer action elements:

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labeled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.4.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.6C The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

ACM_CAP.4.7C The CM system shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.4.8C The CM plan shall describe how the CM system is used.

ACM_CAP.4.9C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.10C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.11C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.4.12C The CM system shall support the generation of the TOE.

ACM_CAP.4.13C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements:

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.3 ACM_SCP.2 Problem tracking CM coverage

Developer action elements:

ACM_SCP.2.1D The developer shall provide a list of configuration items for the TOE.

Content and presentation of evidence elements:

ACM_SCP.2.1C The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.

Evaluator action elements:

ACM_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.4 ADO_DEL.2 Detection of Modification

Developer action elements:

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts

of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

Evaluator action elements:

ADO_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.5 ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.4.6 ADV_FSP.2 Fully defined external interfaces

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements:

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.4.7 ADV_HLD.2 Security enforcing high-level design

Developer action elements:

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP enforcing and other subsystems.

Evaluator action elements:

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.4.8 ADV_IMP.1 Subset of implementation of the TSF

Developer action elements:

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

Content and presentation of evidence elements:

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be internally consistent.

Evaluator action elements:

ADV_IMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_IMP.1.2E The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

5.4.9 ADV_LLD.1 Descriptive low-level design

Developer action elements:

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

Content and presentation of evidence elements:

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

Evaluator action elements:

ADV_LLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.4.10 ADV_RCR.1 Informal correspondence demonstration

Developer action elements

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.11 ADV_SPM.1 Informal TOE Security Policy Model

Developer action elements:

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.12 AGD_ADM.1 Administrator guidance

Developer action elements

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.13 AGD_USR.1 User guidance

Developer action elements

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.14 ALC_DVS.1 Identification of security measures

Developer action elements

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

5.4.15 ALC_LCD.1 Developer defined life-cycle model

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation of evidence elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.16 ALC_TAT.1 Well defined development tools

Developer action elements:

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

Content and presentation of evidence elements:

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.17 ATE_COV.2 Analysis of coverage

Developer action elements

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action elements

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.18 ATE_DPT.1 Testing: high-level design

Developer action elements

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action elements

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.19 ATE_FUN.1 Functional testing

Developer action elements

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.20 ATE_IND.2 Independent testing - sample

Developer action elements

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.4.21 AVA_MSU.2 Validation of Analysis

Developer action elements:

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements:

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

5.4.22 AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.4.23 AVA_VLA.2 Independent vulnerability analysis

Developer action elements:

AVA_VLA.2.1D The developer shall perform a vulnerability analysis.

AVA_VLA.2.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:

AVA_VLA.2.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.2.2C The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.2.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.2.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

Evaluator action elements:

AVA_VLA.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.2.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.2.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.2.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.2.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

5.5 Rationale For TOE Security Requirements

5.5.1 TOE Security Functional Requirements

	O.CONF	O.CONNECT	O.INDICATE	O.INVOKE	O.NOPROG	O.ROM	O.SELECT	O.SWITCH
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_RVM.1				X				
FPT_SEP.1					X	X		
EXT_VIR.1			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 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 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 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_RVM.1 (Non-bypassability of the TSP)
The Data Separation SFP must be enforced at all times during TOE operation. This requires that the TSP functions always be invoked.
Objectives addressed: O.INVOKE

FPT_SEP.1 (TSF Domain Separation)
The TSF needs to ensure that it protects itself against changes which might compromise its security functionality.
Objectives addressed: O.NOPROG, O.ROM

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

5.5.2 TOE Security Assurance Requirements

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.

5.6 Rationale for Explicitly Stated Security Requirements

Table 10 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	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.

Table 10: Explicitly Stated SFR Rationale

5.7 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_SMF.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	No *FMT_SMR.1
FPT_RVM.1	None	Yes
FPT_SEP.1	None	Yes

Functional Component	Dependency	Included/Rationale
EXT_VIR.1	None	Yes

Table 11: SFR Dependencies

5.8 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.

FMT_SMF.1 (Specification of Management Functions) dependency of FMT_MSA.1

The TOE enforces a fixed state to enforce the Data Separation SFP and does not allow any settings or altering of the state of the device with the exception of manual selection of the applicable computer to the peripheral data group. Since no settings are available, there are no Security Management Functions within the device. Therefore, FMT_SMF.1 does not apply to this TOE.

5.9 Rationale For Internal Consistency and Mutually Supportive

The selected requirements are internally consistent. The ST includes all the SFRs provided by the TOE. All operations performed on the security requirements comply with the rules and intent required by the operation in the CC. The requirements defined in the ST are not contradictory.

The selected requirements together form a mutually supportive whole by:

- satisfying all dependencies as demonstrated in **Table 11: SFR Dependencies**
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.5
- including the SFRs FPT_RVM.1 and FPT_SEP.1 to protect the TSF

6 TOE Summary Specification

6.1 TOE Security Functions

The TOE consists of 2 Security Functions:

- Data Separation
- Switch Management

6.1.1 Data Separation

The Belkin OmniView Secure KVM provides the ability to switch a single keyboard, mouse (pointing device) and video monitor (constituting the peripheral device group) among a group of computer resources. The TOE includes models that feature either 2, 4 or 8 port versions that can switch among 2, 4 or 8 computer resources, respectively. The TOE utilizes firmware within the device that is stored in non-modifiable form to assure operation cannot be altered to an insecure state. The integrated circuits that house the firmware are directly soldered to the circuit board to prevent 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. Data entered or displayed through the Peripheral port group is directly associated with the computer resource selected through the dedicated front panel buttons that correspond to the specific computer attached to the associated port. The design utilizes separate processors and switching mechanisms 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. (FDP_IFC.1, FDP_IFF.1)

User related attribute and state information is not transferred upon the switching of resources to assure isolation of all data from computer to computer during the switching process and while a given channel is activated. Switching from one computer resource 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, the switching status of the TOE is forced to a default channel and fully provides all data separation functions. The TOE provides restrictive default values for access to switched computer resource by requiring manual activation of the switching mechanism to engage a specific computer resource connected to the Belkin Secure KVM Switch. The TOE maintains a security domain within the device and enforces separation between subjects within the TOE's Scope of control through the Data Separation security function. (FMT_MSA.3, FPT_SEP.1)

6.1.2 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 switches and hubs are provided (within the TOE) 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 effective upon startup of the Secure KVM switch or upon activation of the manual switch, implemented by the Switch Management security function, for the applicable port. (FPT_RVM.1, EXT_VIR.1, FDP_IFF.1)

The Belkin Secure KVM switch stores “plug and play” information for the connected monitor within the 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 computer resources are not interrupted during the boot process in the event they are not switched to the active channel containing a direct connection to the peripheral port group.

6.2 Security Assurance Measures

The documentation titles in the table below will be updated with new titles and version numbers during the course of the evaluation.

Assurance Requirement	Assurance Components
ACM_AUT.1	The description of automated means in the CM system is provided in EAL 4 Configuration Management Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
ACM_CAP.4	The description of the configuration items is provided in EAL 4 Configuration Management Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U.
ACM_SCP.2	The description of the tracking of specified items in the CM system and the methods used for tracking are provided in EAL 4 Configuration Management Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
ADO_DEL.2	The description of the delivery procedures is provided in Common Criteria Supplement EAL2 Secure Delivery Document Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
ADO_IGS.1	The installation, generation, and start-up procedures are provided in Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Supplement EAL4.
ADV_FSP.2	The informal functional specification is provided in EAL 4 Design Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U.
ADV_HLD.2	The descriptive high-level design is provided in EAL 4 Design Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U.
ADV_IMP.1	The implementation representation is provided in EAL 4 Design Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U.
ADV_LLD.1	The low level design description is provided in EAL 4 Design Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U.
ADV_RCR.1	The informal correspondence demonstration is provided in EAL 4 Design Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U.

Assurance Requirement	Assurance Components
ADV_SPM.1	The informal TOE security policy model is provided in EAL 4 Design Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U.
AGD_ADM.1	The administrator guidance is provided in the following documents: Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Supplement EAL4.
AGD_USR.1	The user guidance is provided in the following documents: Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Supplement EAL4.
ALC_DVS.1	The development security documentation is provided in EAL 4 Life Cycle Support Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U.
ALC_LCD.1	The life cycle model document is provided in EAL 4 Life Cycle Support Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U.
ALC_TAT.1	The development tools are described and defined in EAL 4 Life Cycle Support Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U.
ATE_COV.2	The evidence of coverage is provided in EAL 2 Tests Activity ATE Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U.
ATE_DPT.1	The high level design depth analysis is provided in EAL 2 Tests Activity ATE Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U.
ATE_FUN.1	The functional testing description is provided in EAL 2 Tests Activity ATE Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U.
ATE_IND.2	The TOE and testing documentation were made available to the CC testing laboratory for independent testing. EAL 2 Tests Activity ATE Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U.
AVA_MSU.2	The guidance analysis documentation is provided in Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Supplement EAL4
AVA_SOF.1	The strength of function analysis performed is Not Applicable
AVA_VLA.2	The vulnerability analysis performed is provided in Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Vulnerability Analysis AVA_VLA.2 EAL 4

Table 12: Assurance Requirements: EAL4

6.3 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 5.5.

	Data Separation	Switch Management
FDP_ETC.1	X	
FDP_IFC.1	X	
FDP_IFF.1	X	X
FDP_ITC.1	X	
FMT_MSA.1	X	
FMT_MSA.3	X	
FPT_RVM.1		X
FPT_SEP.1	X	
EXT_VIR.1		X

Table 13: TOE Security Function to SFR Mapping

6.4 Rationale for Security Assurance Measures

The assurance documents listed below were developed to meet the developer action and content and presentation of evidence elements for each assurance required defined in the CC.

The documentation titles in the table below will be updated with new titles and version numbers during the course of the evaluation.

ACM_AUT.1	EAL 4 Configuration Management Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
The partial configuration management automation document describes the automated methodologies, tools and processes used in the development environment to make authorized changes to the implementation representation.	
ACM_CAP.4	EAL 4 Configuration Management Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
The configuration management documents defines the configuration items and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE. It will demonstrate the CM system is operating in accordance with the CM plan, providing measures that only authorized changes are made to configuration items and that it supports generation of the TOE.	
ACM_SCP.2	EAL 4 Configuration Management Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
This problem tracking CM coverage document defines the minimum scope of the configuration items to be maintained under the CM system.	
ADO_DEL.2	Common Criteria Supplement EAL2 Secure Delivery Document Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
The delivery document describes the steps performed to deliver the TOE. It describes the process used to create distribution copies of the TOE software and the steps taken to ensure consistent, dependable delivery of the TOE to the customer. The document describes how the procedures and technical measures provide for detection of modifications for or attempts to masquerade as the developer to ensure integrity of the TOE.	
ADO_IGS.1	Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Supplement EAL4
The installation, documents describe the steps necessary for secure installation, generation, and start-up of the TOE.	
ADV_FSP.2	EAL 4 Design Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
The fully defined external interface document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It	

also describes the effects, exceptions, error messages for each of the external TSF interfaces and includes rationale that the TSF is completely represented.	
ADV_HLD.2	EAL 4 Design Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
The security enforcing high-level design describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified. The purpose and method of use of all interfaces to the subsystems of the TSF are provided and it describes the separation of the TOE into TSP-enforcing and other subsystems.	
ADV_IMP.1	EAL 4 Design Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
This document is a subset of the TSF implementation representation that is defined to a level of detail such that the TSF can be generated without further design decisions.	
ADV_LLD.1	EAL 4 Design Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
The informal descriptive low-level design document decomposes each subsystem into modules and defines the purpose of each module. It defines the interrelationship between modules, dependency on other modules and describes how each TSP – enforcing function is provided. The document identifies all interfaces to the modules of the TSF and those that are externally visible.	
ADV_RCR.1	EAL 4 Design Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
The informal correspondence document maps the security functionality as described in the Security Target TOE Security Summary section to the functional specification, from the functional specification to the high-level design, from the high-level design to the low-level design and from the low-level design to the Implementation.	
ADV_SPM.1	EAL 4 Design Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
The informal Toe security policy model describes the rules and characteristics of all policies of the TOE Security Policy that can be modeled including a rationale. The document describes the correspondence between the TSP model and the functional specification.	
AGD_ADM.1	Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Supplement EAL4
The administrator guidance documents provide complete administrative guidance for the TOE, including all security features and configuration items.	
AGD_USR.1	Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Supplement EAL4
The user guidance describes the security functions and interfaces in a way that allows a user to interact with the TOE securely.	
ALC_DVS.1	EAL 4 Life Cycle Support Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
The Identification of Security Measures document describes all physical, procedural, personnel	

and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	
ALC_LCD.1	EAL 4 Life Cycle Support Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
The life-cycle model document describes the necessary controls used during development and maintenance of the TOE.	
ALC_TAT.1	EAL 4 Life Cycle Support Documentation Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
The development tools document unambiguously defines the tools used for implementation and defines the meaning of all implementation – dependent options.	
ATE_COV.2	EAL 2 Tests Activity ATE Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
The test coverage document provides a complete mapping of the test cases performed against the TSF as described in the functional specification.	
ATE_FUN.1	EAL 2 Tests Activity ATE Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort. The tests identify the security functions to be tested and include any ordering dependencies. The document includes the expected and actual test results.	
ATE_IND.2	EAL 2 Tests Activity ATE Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U
The TOE hardware, software, guidance, and testing documentation were made available to the CC testing laboratory for independent testing.	
AVA_MSU.2	Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Supplement EAL4
The developer provided guidance (User and Administrator) documentation will identify all modes of operation of the TOE, their consequences and implications for maintaining the secure operation. The document will include all requirements for external security measures.	
AVA_SOF.1	Not Applicable
The strength of function analysis document provides the SOF argument for the biometric mechanism.	
AVA_VLA.2	Belkin® OmniView™ Secure KVM Models: F1DN102U F1DN104U F1DN108U Common Criteria Vulnerability Analysis AVA_VLA.2 EAL 4
The vulnerability analysis document identifies and describes the process used to discover obvious vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified obvious vulnerability. The document will provide justification that the TOE, with identified vulnerabilities, is resistant to obvious penetration attacks.	

Table 14: Rationale for Security Assurance Measures

7 Protection Profile Claims

7.1 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 1.0, 8 August 2000.

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 as indicated in the referenced Protection Profile.

7.2 Protection Profile Modifications

The following changes were made to content added to this ST from the applicable Protection Profile:

a. EAL 4 Assurance Measures were updated in this ST to reflect CC Part 3 Version 2.3 (PP was written to CC Version 2.1) as follows:

(**bold** text indicates additions, ~~**strikethrough**~~ text indicates deletions from the reference PP written against CC version 2.1)

ACM_CAP.4.4C The configuration list shall ~~**describe the**~~ **uniquely identify all** configuration items that comprise the TOE.

ACM_CAP.4.5C The ~~**CM documentation**~~ **configuration list** shall describe the ~~**method used to uniquely identify the configuration items**~~ configuration items that comprise the TOE.

ACM_CAP.4.6C The CM ~~**system**~~ **documentation shall describe the method used to** uniquely identify ~~**all**~~ the configuration items **that comprise the TOE**.

ACM_CAP.4.7C **The CM system shall uniquely identify all configuration items that comprise the TOE.**

ACM_SCP.2.1D The developer shall provide ~~**CM documentation**~~ **a list of configuration items for the TOE.**

ACM_SCP.2.1C **The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.**

~~**ACM_SCP.2.1C**~~ ~~**The CM documentation shall show that the CM system, as**~~

~~**a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.**~~

~~**ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.**~~

ADO_IGS.1.1C **The installation, generation and start-up documentation** ~~**The documentation**~~ shall describe **all** the steps necessary for secure installation, generation, and start-up of the TOE.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavio~~u~~r that are relevant to secure operation of the TOE.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavio~~u~~r found in the statement of TOE security environment.

~~**AVA_VLA.2.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.**~~

~~**AVA_VLA.2.2D The developer shall document the disposition of identified vulnerabilities.**~~

AVA_VLA.2.1D The developer shall perform a vulnerability analysis.

AVA_VLA.2.2D The developer shall ~~**document the disposition of identified vulnerabilities**~~ **provide vulnerability analysis documentation**.

~~**AVA_VLA.2.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.**~~

AVA_VLA.2.1C **The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.**

AVA_VLA.2.2C **The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.**

b. FMT_MSA.1 “modify” is underlined vs. italics to match ST convention.

c. FMT_MSA.3 “restriction” is underlined vs. italics to match ST convention.

7.3 Protection Profile Additions

Only additions are those related to Assurance Measures as listed above.

8 Rationale

8.1 Security Objectives Rationale

Section 4.4 provides the security objectives rationale.

8.2 Security Requirements Rationale

Section 5.5 provides the security requirements rationale.

8.3 TOE Summary Specification Rationale

Section 6.3 provides the TOE summary specification rationale.

8.4 Protection Profile Claims Rationale

The Protection Profile claims and rationale is contained in Section 7.