Emerson®-Cybex® Secure DVI KVM Switch, Secure KM Switch and Secure Windowing KVM Security Target EAL 4 augmented ALC_FLR.3

Release Date: July 3, 2012

Document ID: HDC08462

Revision: 1.14

Prepared By: Erica Gomez, Emerson Network Power

Contents

Document Revisions

Rev.	Date	Author	Changes
1.14	July 3, 2012	Erica Gomez, Emerson	Updated products list

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.

An ST principally defines:

- A security problem expressed as a set of assumptions about the security aspects of the environment; a list of threats which the product is intended to counter; and any known rules with which the product must comply (in Chapter 3, Security Problem Definition).
- A set of security objectives and a set of security requirements to address that problem (in Chapters 4 and 5, Security Objectives and IT Security Requirements, respectively).
- The IT security functions provided by the Target of Evaluation (TOE) that meet the set of requirements (in Chapter 6, TOE Summary Specification).

The structure and content of this ST complies with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 6.

1.1 ST and TOE Identification

This section provides information needed to identify and control this ST and its Target of Evaluation (TOE), the TOE Name. This ST targets an Evaluation Assurance Level (EAL) 4 (augmented with ALC_FLR.3) level of assurance.

ST Title: Emerson-Cybex Secure DVI KVM Switch, Secure KM Switch and Secure Windowing KVM Security Target EAL 4 augmented ALC_FLR.3

ST Evaluation: EWA, Canada

Revision Number: 1.14

ST Publish Date: July 3, 2012

ST Authors: Erica Gomez, Emerson Network Power

TOE Identification:

Emerson - Cybex Secure 2-port DVI-I KVM Switch w/audio - Model SC 820, Part number 520-933-501, Ver. 33303-C3C3

Or

Emerson - Cybex Secure 4-port DVI-I KVM Switch w/audio - Model SC 840, Part number 520-935-501, Ver. 33303-C3C3

Or

–Emerson - Cybex Secure 4-port DVI-I KVM Switch w/audio and DPP - Model SC 845, Part number 520-956-501, Ver. 33333-C3C3

Or

Emerson - Cybex Secure 8-port DVI-I KVM Switch w/audio and DPP - Model SC 885, Part number 520-961-501, Ver. 33333-C3C3

Or

Emerson - Cybex Secure 4-port DVI-I Dual-Head KVM Switch w/audio and DPP - Model SC 945, Part number 520-958-501, Ver. 33333-C3C3

Or

Emerson - Cybex Secure 8-port DVI-I Dual-Head KVM Switch w/audio and DPP - Model SC SC 985, Part number 520-958-501, Ver. 33303-C3C3

Or

Emerson - Cybex Secure 16-port DVI-I KVM Switch w/audio and DPP - Model SC 1165, Part number 520-963-501, Ver. 33333-C3C3

Or

Emerson - Cybex Secure 4-port KM Switch w/audio - Model SC KM 140, Part number 520-926-501, Ver. 33303-C3C3

Or

Emerson - Cybex Secure 4-port KM Switch w/audio and DPP - Model SC KM 145, Part number 520-959-501, Ver. 33333-C3C3

Or

Emerson - Cybex Secure 8-port KM Switch w/audio - Model SC KM 180, Part number 520-927-501, Ver. 33303-C3C3

And

Emerson - Cybex Secure Remote Control Unit (RCU) w/ 4 push-buttons - Model SC RCU 100, Part number 520-944-501, Ver. 4-A3

PP Identification:

Validated Protection Profile – NIAP Peripheral Sharing Switch for Human Interface Devices Protection Profile, Version 2.1, September 7, 2010

1.2 TOE Overview

The Emerson - Cybex Secure KVM Switch allows the secure sharing of a single set of peripheral components such as keyboard, Video Display and Mouse/Pointing devices among multiple computers through standard USB, DVI, HDMI and DisplayPort interfaces.

The Emerson - Cybex Secure KVM product uses multiple microcontrollers to emulate the connected peripherals in order to prevent various methods of attacks such as: display signaling, keyboard signaling, power signaling etc. The product is also equipped with multiple unidirectional flow forcing devices to assure adherence to the organizational confidentiality policy and flow between coupled computers.

The Emerson - Cybex Secure KVM line products are available in 2, 4, 8 or 16 port models with single or dual-head (displays). Products include traditional KVM switching devices, Remote Control Unit (RCU), direct display connection products (KM), Windowing KVM to allow secure interaction with multiple connected computers.

The Emerson - Cybex Secure KVM works with standard Personal Computers running operating systems such as Windows or Linux and have ports for USB keyboard, USB mouse, DVI-I video, DVI-D video, HDMI video, DisplayPort video, audio (input and output), and USB Common Access Card (CAC) or Smart-Card reader.

The TOE is intended to be used in a range of security settings (i.e. computers coupled to a single TOE can vary from non-classified Internet connected to those protected in accordance with national security policy). Any data leakage across the TOE may cause severe damage to the organization and therefore must be prevented.

Unlike older Secure KVM security schemes that mostly protected user information transitioning through the TOE, the modern approach primarily addresses the risk of TOE compromise through remote attacks to coupled networks which could leak local user information.

A summary of the Emerson - Cybex Secure KVM security features can be found in Section 1.4. A detailed description of the TOE security features can be found in Section 6, TOE Summary Specification.

1.3 TOE Description

This section provides context for the TOE evaluation by identifying the logical and physical scope of the TOE, as well as its evaluated configuration.

1.3.1 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.

It should be noted that modern Secure KVM devices do not allow any electrical interface peripheral sharing in order to prevent certain attacks, and therefore they are no longer simple switching devices.

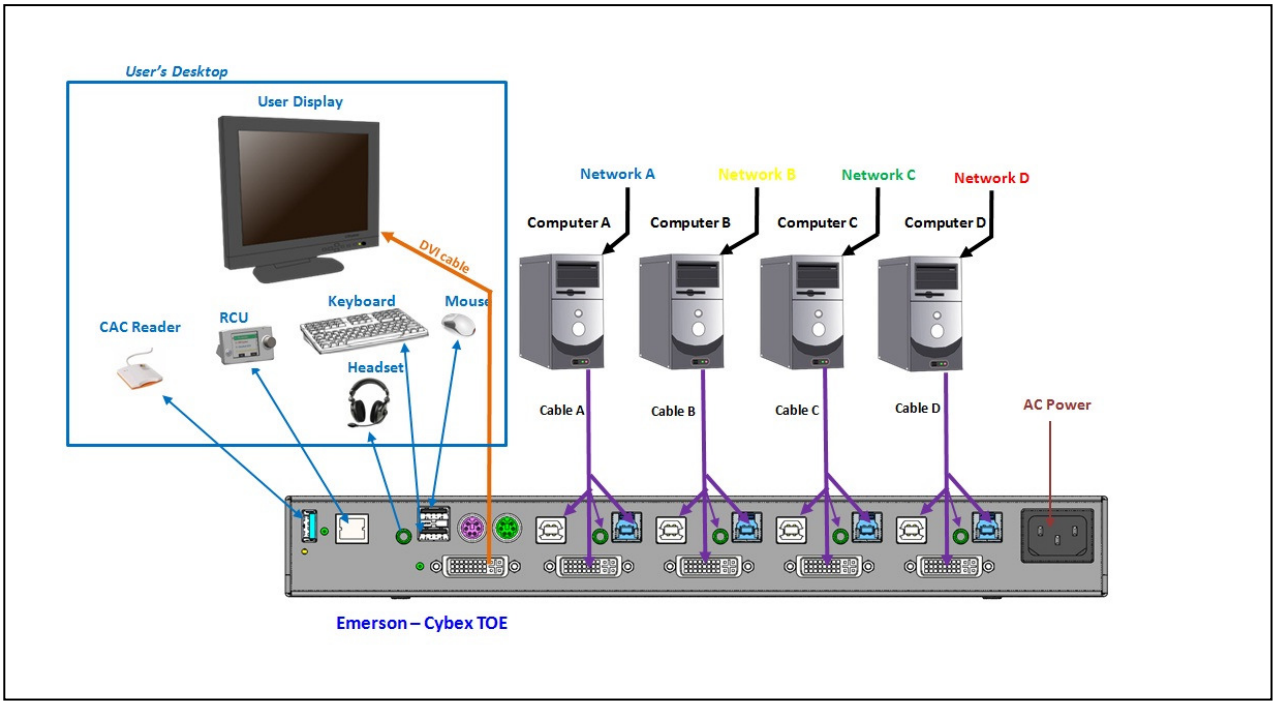

Figure 1 – Typical example of TOE installation

1.3.2 Physical Scope and Boundary

The TOE is a peripheral sharing switch.

The physical boundary of the TOE consists of (refer to figure 1 below):

- One Emerson - Cybex Secure KVM Switch, KM switch, or Windowing KVM;
- The firmware embedded inside the TOE that is permanently programmed into the TOE multiple microcontrollers;
- The TOE power supply that is shipped with the product (some model have internal power supply);
- The TOE COMPUTER interface cables that are shipped with the product;
- The optional Remote Control Unit (RCU) or Basic Remote Controller (BRC) accessory; and

- The accompanying User Guidance. Updated User Guidance can be downloaded from the Emerson - Avocent website at any time.

The evaluated TOE configuration does not include any peripherals or computer components, but do include supplied computer interface cables and a Remote Control Unit attached to the TOE. The following figure depicts the TOE and its environment.

It should be noted that some TOE models support the operation of multiple user displays.

1.3.3 Evaluated Environment

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

TOE / Environment	Component	Description
TOE	Emerson - Cybex Secure 2-port DVI-I KVM Switch w/audio - Model SC 820 Or Emerson - Cybex Secure 4-port DVI-I KVM Switch w/audio - Model SC 840 Or Emerson - Cybex Secure 4-port DVI-I KVM Switch w/audio and DPP - Model SC 845 Or Emerson - Cybex Secure 8-port DVI-I KVM Switch w/audio and DPP - Model SC 885 Or Emerson - Cybex Secure 4-port DVI-I Dual-Head KVM Switch w/audio and DPP - Model SC 945 Or Emerson - Cybex Secure 8-port DVI-I Dual-Head KVM Switch w/audio and DPP - Model SC 985 Or Emerson - Cybex Secure 16-port DVI-I KVM Switch w/audio and DPP - Model SC 1165 Or Emerson - Cybex Secure 4-port KM Switch w/audio - Model SC KM 140 Or Emerson - Cybex Secure 4-port KM Switch w/audio and DPP - Model SC KM 145	TOE Hardware

TOE	Or Emerson - Cybex Secure 8-port KM Switch w/audio - Model SC KM 180 And Emerson - Cybex Secure Remote Control Unit (RCU) w/ 4 push-buttons - Model SC RCU 100	TOE Hardware
Environment	USB Mouse and keyboard compatible with: Logitech mouse MX518 Logitech mouse M-UV96 Microsoft mouse 1.1A Logitech mouse G500 Logitech mouse M-V0007 Teac mouse M52 Microsoft IntelliMouse Explorer 2.0 and 3.0 Logitech Comfort Mouse and Keyboard Dell USB mouse models: 0CJ3339, CU036 Dell Keyboard models: SK-8115, 0N242F, L100, TH826 Microsoft keyboard 2000, Model 1047, KU-0459 Microsoft keyboard RT9450 Lenovo keyboard SK-8825 (L)	Shared Peripheral Port Group Member
Environment	USB User Authentication Device compatible with: Precise - 200 MC SCM - SCR 335 Gemalto - PC USB-TR	Shared Peripheral Port Group Member

Environment	Monitor – DVI-I (video) DVI dual-link displays Including, but not limited to: Apple Cinema HD display 30-inch Dell Widescreen 30-inch HP Widescreen (LP3065) 30-inch Gateway XHD3000 30-inch Samsung 30-inch (305T) Dell Ultra sharp 2007FP, 20” , Analog and Digital connections Dell Ultra sharp E190S, 19” , Analog and Digital connections Dell Ultra sharp E228WFP, Analog and Digital connections Samsung 2343BWX 23” , Analog and Digital connections Samsung SyncMaster 712n Analog only monitor Monitor – DisplayPort Including, but not limited to: Asus VE248Q 24-Inch LED Monitor Dell UltraSharp U2412M 24" LED LCD Monitor Apple LED Cinema Display - 27" IPS LED-backlit LCD monitor	Shared Peripheral Port Group Member

<table>
<tr>
<td>TOE</td>
<td>Secure KVM Cables (as needed):
<table>
<tr><th>P/N</th><th>Description</th></tr>
<tr><td>CWR05117</td><td>KVM Cable short (1.8 m), USB Type-A to USB Type-B, Black</td></tr>
<tr><td>CWR05116</td><td>KVM Cable short (1.8 m), Audio out, DPP, Black</td></tr>
<tr><td>CWR05205</td><td>KVM Cable short (1.8 m), DVI-A to VGA, USB, Black</td></tr>
<tr><td>CWR05114</td><td>KVM Cable short (1.8 m), DVI-D to DVI-D Single-Link, USB, Black</td></tr>
<tr><td>CWR05115</td><td>KVM Cable short (1.8 m), DVI-D to DVI-D Dual-Link, USB, Black</td></tr>
<tr><td>HWR08154</td><td>KVM Cable short (1.8m), HDMI to HDMI, USB, Black</td></tr>
<tr><td>CWR05113</td><td>KVM Cable short (1.8 m), DVI-D to DVI-D Single-Link, USB, Audio out, DPP, Black</td></tr>
<tr><td>CWR06011</td><td>Cable Ethernet CAT 5-E, Blue, 1.8m</td></tr>
<tr><td>CWR06246</td><td>KVM Cable short (1.8 m), DP to DP, USB A to USB B, Black</td></tr>
</table>
</td>
<td>Cables for connection of Host Computers to Peripheral Port Group</td>
</tr>
<tr>
<td>Environment</td>
<td>Audio Device (Speakers: supports 3.5mm connector)</td>
<td>Shared Peripheral Group Member</td>
</tr>
</table>

Environment	**Host Computers Qty 2,4,8 or 16 based on KVM model used** Any hardware platform supporting the following Operating Systems: Windows 2000 Professional –service pack 4 MS Windows XP (Home/Pro) –service pack 3 MS Windows 2003 Server – latest released service pack MS Windows Vista – 32/64bit MS Windows 7 / 8 – 32/64bit Apple OS X v10.4 and higher Red Hat Linux Desktop – latest released version Red Hat Enterprise Linux WS – latest released version Ubuntu 9.10 Linux – latest released version with USB HID support and single or dual DVI or DP monitor output support.	Operational Environment Host Computer resources

Table 1: Evaluated TOE and Environment Components

1.3.4 Guidance Documents

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

Product user's manual

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

Latest documentation may be found at Emerson web-site.

1.3.5 TOE Features Outside of Evaluation Scope

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

- Pointing device driver (software) used with KM models TOE to support multiple display COMPUTERS.
- Configuration utility software used with the KM models for initial product setup.
- Remote Fiber or Copper extender that may be used to extend the user console and RCU.

1.3.6 Logical Scope of the TOE

The TOE logical scope and boundary consists of the security functions/features provided/controlled by the TOE.

The TOE provides the following security features:

- Data Separation (TSF_DSP),
- Security Management (TSF_MGT),
- Protection of the TSF (TSF_TMP),
- Visual Indication Rule (EXT_VIR),
- Invalid USB Connection (EXT_IUC),
- Read-Only ROMs (EXT_ROM)

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 2 of the claimed Protection Profile. In operation, the TOE is not concerned with the user information flowing between the shared peripherals and the switched computers. Using emulation techniques and optical data diodes, the TOE enforces unidirectional data flow from shared peripherals to the coupled computers. The TOE only provides a single logical connection between the shared peripheral group and the one selected computer (TSF_DSP). Data Separation is accomplished as explained in Section 7 of this ST.

The TOE uses individual device emulators for each computer channel. This design allows for the connected computers to be powered-up at any time. The colored LEDs in the TOE front panel indicate the selected computer channel. The TOE provides the user with one or more of the following model dependant methods to select or switch a computer: push-buttons, mouse buttons, RCU rotary switches or keyboard shortcuts. These means allow the user to explicitly determine to which computer the shared set of peripherals is connected (TSF_MGT). This connection is visually displayed by a colored LED at the TOE front panel over the selected channel. Security Management and visual indication functions are accomplished as explained in Section 7 of this ST.

The TOE implements multiple always-on sensors to detect any attempt to open the TOE by removing the security screw. Once a tampering event is detected, normal use will be permanently disabled and the LEDs on the TOE front panel will blink to indicate tampered state. Special holographic Tampering Evident Labels are used as seals to provide additional visual indication in case of attempted physical tampering. Protection of the TSF through tampering detection is accomplished as explained in more detail in Section 7 of this ST.

The TOE implements strict filtering of connected USB devices at each peripheral port. Any connected device is enumerated and qualified based on a preprogrammed profile. A device will be accepted by the TOE only if it is qualified. A non-qualified (UNAUTHORIZED) USB device will be blocked by the TOE and cannot be used. Protection from invalid USB devices is accomplished as explained in more detail in Section 7 of this ST.

The TOE design uses read only non-volatile memory components to prevent any possibility of a remote tampering attack intended to modify TOE security functionality. Read Only Memory protection is accomplished as explained in more detail in Section 7 of this ST.

1.4 Organization

Security Target Introduction (Section 1)

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)

Section 2 provides applicable Common Criteria (CC) conformance claims, Protection Profile (PP) conformance claims and Assurance Package conformance claims.

Security Problem Definition (Section 3)

Section 3 describes the threats, organizational security policies, and assumptions pertaining to the TOE and the TOE environment.

Security Objectives (Section 4)

Section 4 identifies the security objectives for the TOE and its supporting environment as well as a rationale describing how objectives are sufficient to counter the threats identified for the TOE.

Extended Components Definition (Section 5)

Section 5 presents the components needed for the ST but not present in Part II or Part III of the Common Criteria Standard.

Security Requirements (Section 6)

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.

Summary Specification (Section 7)

This section describes the security functions provided by the TOE and how they satisfy the security functional requirements. It also describes the security assurance measures for the TOE and the rationale for the assurance measures.

1.5 Document Conventions

The CC defines four operations on security functional requirements. The descriptions 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)

1.6 Document Terminology

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

1.6.1 ST Specific Terminology

Attribute	(See Peripheral Port Group ID)
Authorized User	A USER who has been granted permission to interact with the TOE and all of its CONNECTED PERIPHERALS.
Computer	A programmable machine. The two principal characteristics of a computer are: it responds to a specific set of instructions in a well-defined manner, and it can execute a prerecorded list of instructions (a software program). For the purposes of this

	document, any electronic DEVICE controlling the MONITOR, and accepting signals from the KEYBOARD and POINTING DEVICE (if any) will qualify. Examples of computers under this definition are IBM-class personal computers (and so-called clones), desktop workstations, thin-clients and control console INTERFACES into "mainframe" computers.
Dedicated Peripheral Port	A KVM port intended for connection of specific pre-defined peripheral device. Typically used for user authentication device or more specifically for Common Access Card (CAC) reader.
Device	A unit of hardware, outside or inside the case or housing for the essential COMPUTER that is capable of providing INPUT to the essential COMPUTER or of receiving OUTPUT or both. The term PERIPHERAL is sometimes used as a synonym for device or any INPUT/OUTPUT unit.
Display	A COMPUTER OUTPUT surface and projecting mechanism that show text and other graphic images from a COMPUTER system to a user, using a Cathode Ray Tube (CRT), Liquid Crystal Display (LCD), Light-Emitting Diode (LED), gas plasma, active matrix, or other image projection technology. The display (the terms monitor and display are often used interchangeably) is usually considered to include the screen or projection surface and the DEVICE that produces the information on the screen. In some COMPUTERS, the display is packaged in a separate unit called a monitor. Displays (and monitors) are also sometimes called Video Display Terminals (VDTs). Also included in this category are tactile braille OUTPUT DEVICES.
Dual Head	Computer with two video outputs used to drive simultaneously two user displays.
Group	(See Peripheral Port Group)
Human Interface Devices	Those PERIPHERALS which primarily allow a USER to directly observe and/or modify the operation/status of a COMPUTER. Examples include a keyboard, video MONITOR, mouse, and an optical head tracker. Modems, printers, hard drives, and scanners are not such devices.
Interface	The CONNECTION and interaction between hardware, software, and the USER.
Input Device	Any machine that feeds data into a COMPUTER. This includes scanners, touch screens, and voice response systems.

Keyboard A DEVICE which converts the physical action of a USER such as the depressing of one or more buttons into electronic signals corresponding to the bitwise symbol for a character in some form of electronic alphabet. The most common example is the typewriter-like keyboard found on most home COMPUTERS, but the definition also includes braille keypads among other DEVICES.

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.

Windowing KVM A special KVM (keyboard, video and mouse) device that allows a single keyboard, video monitor and mouse to be switched to any of a number of computers while the user can interact with multiple video outputs presented *simultaneously* on a single display.

KM Switch Keyboard and Mouse switch - A switch allows a single set of use keyboard 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.

Network A collection of computers and devices interconnected by communications channels that facilitate communications and allows sharing of resources and information among interconnected devices. For the purposes of this document, any wired or wireless communication means coupled to the COMPUTER connected to the TOE.

Object (See Peripheral Data and State Information)

Optical Data Diode An optical hardware component used to enforce data flow in one direction only.

Peripheral Data Information, including [buffered] STATE INFORMATION, sent from or to a PERIPHERAL.

Peripheral Port Group ("Group")/ Peripheral Port Group ID
A collection of HUMAN INTERFACE DEVICE PORTS treated as a single entity by the SWITCH. There is one Group for the set of SHARED PERIPHERALS and one Group for each SWITCHED COMPUTER directly CONNECTED to the SWITCH. Each SWITCHED COMPUTER Group has a unique logical ID. The shared Group ID is the same as that of the SWITCHED COMPUTER Group currently selected by the SWITCH.

Plug and Play	A standardized interface for the automatic recognition and installation of interface cards and devices on a PC.
Pointing Device	A DEVICE, which convert relative positioning motion from a human operator into positioning information on a MONITOR. Examples of Pointing Devices include a mouse, trackball, joystick, and touchpad.
Port	An external socket for plugging in communications lines and/or PERIPHERALS.
QUALIFIED USB device	A USB device having a complete set of characteristics that should allow it to operate while connected to the TOE console device port. (see Section 7.4)
Residual Data	Any PERIPHERAL DATA stored in a SWITCH.
Switched Computers	Refers to the computers connected to the TOE and connected to the Peripheral port group upon the switching function of the TOE.
Shared Peripheral	(See Peripheral Port Group)
Subject	(See Peripheral Port Group)
Switched Computer	(See Peripheral Port Group)
UNAUTHORIZED USB device	A USB device having one or more characteristics that should prevent it from operation while connected to the TOE console device port. (See Section 7.4)
User	The human operator of the TOE.

1.6.2 Acronyms

CAC	Common Access Card
CM	Configuration Management
DP	DisplayPort
DPP	Dedicated Peripheral Port
DVI	Display Visual Interface (VESA Standard)
EAL	Evaluation Assurance Level
EDID	Extended Display Identification Data (VESA Standard)
EEPROM	Electrically Erasable Programmed Read Only Memory
HDMI	High-Definition Multimedia Interface
ID	Identification
IT	Information Technology
KVM	Keyboard-Video-Mouse
LCD	Liquid Crystal Display
LED	Light-Emitting Diode
MAC	Mandatory Access Control
PSS	Peripheral Sharing Switch
PS/2	IBM Personal System 2 peripheral interface
PP	Protection Profile
PPG	Peripheral Port Group
PSS	Peripheral Sharing Switch
RCU	Remote Control Unit
ROM	Read Only Memory
RSU	Remote Switching Unit
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
USB	Universal Serial Bus

VESA	Video Electronics Standards Association
VGA	Video Graphics Array (VESA Standard)

2 Conformance Claims

This section describes the conformance claims of this Security Target.

2.1 Common Criteria Conformance Claims

The Security Target is based upon:

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3, dated July 2009.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Assurance Components; Version 3.1, Revision 3, dated July 2009.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance components conformant at EAL4 (+ALC_FLR.3); Version 3.1, Revision 3, dated July 2009.
4. All International interpretations with effective dates on or before September 19, 2011.

referenced hereafter as [CC].

This Security Target claims the following CC conformance:

- Part 2 extended
- Part 3 conformant
- Evaluation Assurance Level (EAL) 4+

2.2 Protection Profile (PP) Claims

This ST claims demonstrable compliance to the following PP:

Protection Profile: Peripheral Sharing Switch (PSS) for Human Interface Devices. Assurance Level: EAL 2 augmented with ALC_FLR.2 PP Version: 2.1, 7 September 2010. The ALC_FLR.2 requirement of the PP is met through ALC_FLR.3 conformance.

2.3 Package Claims

This Security Target claims conformance to the EAL 4 package augmented with ALC_FLR.3.

3 Security Problem Definition

This section describes assumptions about the operational environment in which the TOE is intended to be used and represents the conditions for the secure operation of the TOE.

Note: The content in this section is appears in the Security Problem Definition of the claimed PSS PP and is copied here for completeness.

3.1 Secure Usage Assumptions

The Security Objectives and Security Functional Requirements defined in subsequent sections of this Security Target are based on the condition that all of the assumptions described in this section are satisfied.

Assumption	Definition
A.ACCESS	An AUTHORIZED USER possesses the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.
A.MANAGE	The TOE is installed and managed in accordance with the manufacturer's directions.
A.NOEVIL	The AUTHORIZED USER is non-hostile and follows all usage guidance.
A.PHYSICAL	The TOE is physically secure.

Table 2 – Secure usage assumptions

3.2 Threats

The assets under attack are one or more of the following:

1. The information that is transiting the TOE (e.g. information typed by the user on user keyboard).
2. The information that is residing in networks connected to the COMPUTERS that are coupled to the TOE (e.g. the risk of data leakages across the TOE between coupled isolated networks).
3. The integrity of the networks coupled to the COMPUTERS that are coupled to the TOE (e.g. the risk of network attacks or DoS on coupled networks from TOE).

In general, the threat agent may be one or more of:

1. People with TOE access (who are expected to possess "average" expertise, few resources, and moderate motivation).
2. Failure of the TOE or PERIPHERALS.
3. Infected COMPUTERS or NETWORKS coupled to the TOE.

4. An unidentified threat agent attacking the TOE and/or its coupled PERIPHERALS.

3.2.1 Threats Addressed by the TOE

"Threats to Security" Section 3.2 of the claimed Protection Profile identifies the following threats to the assets against which specific protection within the TOE is required:

Threat	Definition
T.INVALIDUSB	The AUTHORIZED USER will connect UNAUTHORIZED USB devices to the peripheral switch.
T.RESIDUAL	RESIDUAL DATA may be transferred between PERIPHERAL PORT GROUPS with different IDs.
T.ROM_PROG	The TSF may be modified by an attacker such that code embedded in reprogrammable ROMs is overwritten, thus leading to a compromise of the separation-enforcing components of the code and subsequent compromise of the data flowing through the TOE or the NETWORKS connected to its coupled COMPUTERS.
T.SPOOF	Via intentional or unintentional actions, a USER may think the set of SHARED PERIPHERALS are currently CONNECTED to one COMPUTER when in fact they are connected to a different one.
T.TRANSFER	A CONNECTION, via the TOE, between COMPUTERS may allow information transfer.
T.TAMPER	An unidentified threat agent could physically tamper with or modify the TOE, allowing unauthorized information flows.
T.INFECTED	TOE may be attacked by a coupled COMPUTER that was infected by malicious code that causes the TOE to change its functionality and compromise the data flowing through the TOE to the NETWORKS connected to its coupled COMPUTERS.
T.PERIP	A USER may connect to the TOE a qualified PERIPHERAL DEVICE that has a security vulnerability which allows the transfer of USER or NETWORK information through the coupled TOE, thereby violating the confidentiality of information.

Table 3 – Threats addressed by the TOE

3.2.2 **Threats addressed by the IT Operating Environment**

The Protection Profile claimed identifies no threats to the assets against which specific protection within the TOE environment is required.

3.3 Organizational Security Policies

The Protection Profile claimed identifies no Organizational Security Policies (OSPs) to which the TOE must comply.

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	Definition
O.CONF	The TOE shall not violate the confidentiality of information which it processes or exposed to. Information generated within any PERIPHERAL GROUP COMPUTER CONNECTION shall not be accessible by any other PERIPHERAL GROUP with a different GROUP ID.
O.INDICATE	The AUTHORIZED USER shall receive an unambiguous indication of which SWITCHED COMPUTER has been selected.
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 or fuse protected flash 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 user inputs are routed to; Single push button, multiple push buttons, rotary selection or mouse button methods are used by most current market products. Automatic switching based on scanning shall not be used as a selection mechanism.
O.SWITCH	All DEVICES except for User Authentication Device in a SHARED PERIPHERAL GROUP shall be CONNECTED to at most one SWITCHED COMPUTER at a time[1].
O.USBDETECT	The TOE shall detect any USB connection that is not a pointing device, keyboard, user authentication device or display and will perform no interaction with that device after the initial identification.
O.UNIDIR	TOE circuitry shall assure that USER KEYBOARD, USER POINTING DEVICE

[1] This objective differs slightly from the O.SWITCH objective in the PP. The user authentication device port may be switched independently of other PERIPHERAL GROUPS.

	and EDID data will flow only from PERIPHERAL DEVICES to the SWITCHED COUPLED COMPUTER.
O.TAMPER	The TOE Device provides unambiguous detection of physical tampering of the TSF's devices or TSF's enclosure, and permanently disables TOE normal functionality after such an event.

Table 4: TOE Security Objectives definitions

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	Definition
OE.ACCESS	The AUTHORIZED USER shall possess the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.
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 applicable guidance.
OE.PHYSICAL	The TOE shall be physically secure.

Table 5: Operational Environment Security Objectives

4.3 Rationale

This section demonstrates that each threat, organizational security policy, and assumption are mitigated by at least one security objective for the TOE, and that those security objectives counter the threats, enforce the policies, and uphold the assumptions.

Threats, Policies, Assumptions	O.CONF	O.INDICATE	O.ROM	O.SELECT	O.SWITCH	O.USBDETECT	O.UNIDIR	O.TAMPER	OE.ACCESS	OE.MANAGE	OE.NOEVIL	OE.PHYSICAL
T.INVALIDUSB						●	●					
T.RESIDUAL	●											
T.ROM_PROG			●									
T.TAMPER								●				
T.INFECTED			●				●					
T.SPOOF		●		●								
T.PERIP			●				●					
T.TRANSFER	●				●		●	●				
A.ACCESS									●			
A.MANAGE										●		
A.NOEVIL											●	
A. PHYSICAL												●

Table 6: Sufficiency of Security Objectives

4.3.1 TOE Security Objectives Rationale

Threats, Policies, and Assumptions	Summary	Objectives and rationale
T.INVALIDUSB The AUTHORIZED USER will connect UNAUTHORIZED USB devices to the peripheral switch.	**O.USBDETECT** This objective will ensure detection of the connection of an UNAUTHORIZED USB device to the TOE Console USB port. Information from this port would be ignored and not be passed on to a connected computer. Invalid connections are recognized on the keyboard, pointing device, and User Authentication device. **O.UNIDIR** This objective will ensure that console KEYBOARD and POINTING DEVICE data will only flow through the TOE in one direction from PERIPHERAL DEVICES to the SWITCHED COUPLED COMPUTER.	**O.USBDETECT** This objective will detect the UNAUTHORIZED device connection to the TOE Console USB port. Once such a device is detected, any information from it will be ignored and will not be coupled to the connected COMPUTERs. This objective will be valid for the TOE KEYBOARD, POINTING DEVICE, and User Authentication device. Connection of an invalid USB device to an USB hub or as part of a composite device will result in the TOE ignoring the information from that device and the device will be isolated from the coupled COMPUTERs. **O.UNIDIR** This objective prevents a connected mass storage device from infecting a COUPLED COMPUTER with malicious code or from exporting user data.
T.RESIDUAL RESIDUAL DATA may be transferred between PERIPHERAL PORT GROUPS with different IDs	**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 with a different	**O.CONF**: If the PERIPHERALS can be shared 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

	GROUP ID.	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. Further, 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.
T.ROM_PROG The TSF may be modified by an attacker such that code embedded in reprogrammable ROMs is overwritten, thus leading to a compromise of the separation-enforcing components of the code and subsequent compromise of the data flowing through the TOE.	**O.ROM** This Objective assures that TOE software/firmware will be protected against unauthorized modification. Embedded software must be contained in mask-programmed, fuse protected flash or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.	**O.ROM** The threat of software (firmware) embedded in reprogrammable ROMs is mitigated by ensuring that the ROMs used in the TSF to hold embedded TSF data are not physically able to be re-programmed. Thus, even if an interface does exist to the ROM containing the embedded TSF code, high confidence can be obtained that that code (stored in the ROM) will remain unchanged together with the TOE security functions.

T.INFECTED TOE may be attacked by a coupled COMPUTER that was infected by a malicious code inserted by an unidentified threat agent causes the TOE to change its functionality and subsequent compromise of the data flowing through the TOE or the NETWORKS connected to its coupled COMPUTERS.	**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 or fuse protected flash permanently attached (non-socketed) to a circuit assembly. **O.USBDETECT** The TOE shall detect any USB connection that is not a pointing device, keyboard, user authentication device or display and will perform no interaction with that device after the initial identification.	**O.ROM** This Objective assures that TOE software/firmware will be protected against unauthorized modification. Embedded software must be contained in mask-programmed, fuse protected flash or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly. **O.USBDETECT** This objective will ensure detection of the connection of an unauthorized device to the TOE Console USB port. Information from this port would be ignored and not be passed on to a connected computer. This objective also ensures that invalid connections are recognized on the keyboard, pointing device, User Authentication device and display console ports.
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.	**O.INDICATE** The AUTHORIZED USER shall receive an unambiguous indication of which SWITCHED COMPUTER has been selected. **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	**O.INDICATE**: The USER must receive positive confirmation of SWITCHED COMPUTER selection. **O.SELECT**: The USER must take positive action to select the current SWITCHED COMPUTER.

	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.	
T.PERIP A USER may connect to the TOE a qualified PERIPHERAL DEVICE that has a security vulnerability which allows the transfer of USER or NETWORK information through the coupled TOE, thereby violating the confidentiality of information.	**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 or fuse protected flash permanently attached (non-socketed) to a circuit assembly. **O.UNIDIR** The TOE circuitry shall assure that USER KEYBOARD, USER POINTING DEVICE and EDID data will flow only from PERIPHERAL DEVICES to the SWITCHED COUPLED COMPUTER.	**O.ROM** This Objective assures that TOE software/firmware will be protected against unauthorized modification by ensuring that embedded software is contained in read-only memory. This ensures that any ROM used in the TSF to hold embedded TSF data may not be re-programmed. **O.UNIDIR** This objective will ensure that console KEYBOARD and POINTING DEVICE data will only flow through the TOE in one direction from PERIPHERAL DEVICES to the SWITCHED COUPLED COMPUTER, thereby preventing data transfer from connected COMPUTERS or NETWORKS to peripheral devices.
T.TRANSFER A CONNECTION, via the TOE, between COMPUTERS may allow information transfer.	**O.CONF** The TOE shall not violate the confidentiality of information, which it processes. Information generated within any PERIPHERAL GROUPCOMPUTER CONNECTION shall not be accessible by any other PERIPHERAL GROUP-COMPUTER CONNECTION.	**O.CONF** 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. Further, 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.SWITCH** 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. Still TOE may enable User Authentication Device switched to another COMPUTER to maintain user authentication session.
	O.SWITCH All DEVICES in a SHARED PERIPHERAL GROUP shall be CONNECTED to at most one SWITCHED COMPUTER at a time.	**O.UNIDIR** This objective mitigates the threat of unauthorized information transfer by providing assurance through hardware design that data may only flow from a PERPHERAL DEVICE to a COMPUTER preventing the possibility that the TOE will loop data from one COMPUTER to another even if the microcontroller in the TOE has

		been altered.
	O.UNIDIR TOE circuitry shall assure that USER KEYBOARD, USER POINTING DEVICE and EDID data will flow only from PERIPHERAL DEVICES to the SWITCHED COUPLED COMPUTER. **O.TAMPER** The TOE Device provides unambiguous detection of physical tampering of the TSF's devices or TSF's enclosure, and to permanently disables TOE normal functionality after such an event.	**O.UNIDIR** This objective will ensure that console KEYBOARD and POINTING DEVICE data will only flow through the TOE in one direction from PERIPHERAL DEVICES to the SWITCHED COUPLED COMPUTER, thereby preventing data transfer from connected COMPUTERS or NETWORKS to peripheral devices. **O.TAMPER** Tampering of the TOE may cause data to be transferred between COMPUTERS. Detection of a physical tampering attempt may prevent such an event, or will permanently disable the TOE after detection of such event.
T.TAMPER An unidentified threat agent could physically tamper with or modify the TOE, allowing unauthorized information flows.	**O.TAMPER** The TOE Device provides unambiguous detection of physical tampering of the TSF's devices or TSF's enclosure, and permanently disables TOE normal functionality after such an event.	**O.TAMPER** The TOE contains mechanisms that provide unambiguous indication of a physical tampering attempt that might compromise the TSF, and permanently disable the TOE after such an event.

Table 7 – TOE Security Objectives rationale

4.3.2 Security Objectives Rationale for the Operational Environment

Threats, Policies, and Assumptions	Summary	Objectives and rationale
A.ACCESS An AUTHORIZED USER possesses the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.	**OE.ACCESS** The AUTHORIZED USER shall possess the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.	All authorized users are trustworthy individuals, having background investigations commensurate with the level of data being protected, have undergone appropriate training, and follow all user guidance.
A.MANAGE The TOE is installed and managed in accordance with the manufacturer's directions.	**OE.MANAGE** The TOE shall be installed and managed in accordance with the manufacturer's directions.	Restates the assumption.
A.NOEVIL The AUTHORIZED USER is non-hostile and follows all usage guidance.	**OE.NOEVIL** The AUTHORIZED USER shall be non-hostile and follow all usage guidance.	Restates the assumption.
A.PHYSICAL The TOE is physically secure.	**OE.PHYSICAL** The TOE shall be physically secure.	The TOE is assumed to be held in a secure site protected from physical attack (e.g., theft or destruction) [2]. Physical attack could include unauthorized intruders into the TOE environment, but it does not include physical destructive actions that might be taken by an individual that is authorized to access the TOE environment.

Table 8 – Operational Environment Security Objectives rationale

[2] The objective and rational here differs slightly from the PP because the TOE provides addition protections that are attributed to the TOE environment in the PP. It should be also noted that although the operating environment assumed to be physically secure, the TOE may be exposed to tampering while in transit to its operation site.

4.4 Rationale for Organizational Policy Coverage

There are no Organizational Policies for this TOE.

5 Extended Components Definition

The Extended Components Definition describes components for security objectives which cannot be translated or could only be translated with great difficulty to existing requirements.

Extended Security Functional Requirements (Explicit)	
EXT_VIR.1	Visual Indication Rule
EXT_IUC.1	Invalid USB Connection
EXT_ROM.1	Read-Only ROMs

Table 9: Extended SFR Components

5.1 Class EXT: Extended Visual indications

Visual confirmation provides the user with important information regarding the current connection made through the TOE. This allows the user to confirm that the data is being securely transported to the proper computer.

5.1.1 Visual Indication Rule (EXT_VIR)

Family Behavior

This family defines requirements for providing means of determining which computer is connected to which set of peripheral devices.

Component Leveling

EXT_VIR.1 Visual Indication Rule provides a visual indication of the connections between the computer and a set of peripheral devices.

Management: EXT_VIR.1

There are no management activities foreseen.

Audit: EXT_VIR.1

There are no auditable events foreseen.

EXT_VIR.1 Visual Indication Rule

Hierarchical to:	No other components.
Dependencies:	No dependencies.

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

Application Note: Does not require tactile indicators, but does not preclude their presence.

5.2 Class EXT: Extended - Invalid USB Connection (EXT_IUC)

Invalid USB connection protects the TOE and the coupled COMPUTERS from inadvertent connection of an UNAUTHORIZED USB device.

5.2.1 Invalid USB Connection (EXT_IUC)

Family Behavior

This family defines requirements for providing a means to qualify connected peripherals based on pre-defined profiles. The TOE must terminate all interaction with peripheral devices that are rejected.

Component Leveling

EXT_IUC.1 Invalid USB connection, provides a requirement to qualify each peripheral device connected to the TOE and to isolated such a device if it is not a qualified device.

Management: EXT_IUC.1

There are no management activities foreseen.

Audit: EXT_IUC.1

There are no auditable events foreseen.

EXT_IUC.1	**Invalid USB Connection**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

EXT_IUC.1.1 All USB devices connected to the Peripheral switch shall be interrogated to ensure that they are valid (pointing device, keyboard, user authentication device, display). No further interaction with non-valid devices shall be performed.

5.3 Class EXT: Extended – ROM (EXT_ROM)

The ROM requirement protects the TOE from remote tampering by re-programming of programmable components in the TOE. The use of non-volatile memory with mask ROM, OTP (One Time Programming) or fused write protection assures that firmware may not be changed after TOE production. All non-volatile memory devices used must be soldered directly to the board (not attached with a socket).

Family Behavior

This family defines the read-only (write-protection) feature required to protect the firmware stored on all TOE non-volatile memory devices.

Component Leveling

EXT_ROM Read only ROM, requires that the TSF disable all attempts to re-write data to the TOE non-volatile memory.

Management: EXT_ROM.1

There are no management activities foreseen.

Audit: EXT_ROM.1

There are no auditable events foreseen.

EXT_ROM.1	**Read Only ROMs**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

EXT_ROM.1.1 TSF software embedded in TSF ROMs must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.

5.4 Rationale for Explicitly Stated Security Requirements

The Explicit SFRs in this Security Target are from the claimed Protection Profile.

6 Security Requirements

This section defines the IT security requirements that shall be satisfied by the TOE or its environment. The CC divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.

- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

These requirements are discussed separately within the following subsections.

6.1 Security Functional Requirements for the TOE

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

The TOE satisfies the SFRs delineated in "Target of Evaluation Security Requirements," Section 5.1, of the claimed Protection Profile. The SFRs have been reproduced here for convenience.

Functional Component ID	Functional Component Name
FDP_ETC.1	Export of User Data Without Security Attributes
FDP_IFC.1a	Subset Information Flow Control (Data Separation)
FDP_IFC.1b	Subset Information Flow Control (Unidirectional Data Flow)
FDP_IFF.1a	Simple Security Attributes (Data Separation)
FDP_IFF.1b	Simple Security Attributes (Unidirectional Data Flow)
FDP_ITC.1	Import of user data without security attributes
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FPT_PHP.1	Passive detection of physical attack
FPT_PHP.3	Resistance to physical attack
EXT_VIR.1	Visual indication rule
EXT_IUC.1	Invalid USB connection
EXT_ROM.1	Read-Only ROMs

Table 10: TOE Security Functional Requirements summary

6.1.1 Class FDP: User Data Protection

6.1.1.1 FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control, or

FDP_IFC.1a subset information flow control

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.1a Subset Information Flow Control (Data Separation)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1a Simple security attributes

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

Application Note: The data flow is uni-directional in the TOE. i.e. the TOE implementation is more conservative than claimed Protection Profile.

6.1.1.3 FDP_IFC.1b Subset information flow control (Unidirectional data flow)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1a Simple security attributes

FDP_IFC.1.1b The TSF shall enforce the **Unidirectional Forced Data Flow SFP** on **the POINTING DEVICE and on the KEYBOARD PERIPHERAL DATA to restrict data flow from SHARED PERIPHERALS to SWITCHED COMPUTERS only.**

6.1.1.4 FDP_IFF.1a Simple Security Attributes (Data Separation)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1a Subset information flow control

FMT_MSA.3 Static attribute initialization

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

- **PERIPHERAL PORT GROUPS (SUBJECTS);**
- ***KEYBOARD PERIPHERAL DATA*, *POINTING DEVICE PERIPHERAL DATA*, *EDID PERIPHERAL DATA*, *and USER AUTHENTICATION DEVICE* PERIPHERAL DATA (OBJECTS), and**
- **PERIPHERAL PORT GROUP IDs (ATTRIBUTES).**

FDP_IFF.1.2a 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:
***KEYBOARD PERIPHERAL DATA and POINTING DEVICE* 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.1.3a The TSF shall enforce the **No additional information flow control SFP rules**.

FDP_IFF.1.4a The TSF shall provide the following: **No additional SFP capabilities.**

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

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

6.1.1.5 FDP_IFF.1b Simple Security Attributes (Unidirectional Data Flow)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1b Subset information flow control

FMT_MSA.3 Static attribute initialization

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

- **PERIPHERAL PORT GROUPS (SUBJECTS);**
- **KEYBOARD PERIPHERAL DATA, POINTING DEVICE PERIPHERAL DATA, EDID PERIPHERAL DATA, and USER AUTHENTICATION DEVICE PERIPHERAL DATA (OBJECTS), and**
- **PERIPHERAL PORT GROUP IDs (ATTRIBUTES).**

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

Unidirectional flow Rule:

KEYBOARD PERIPHERAL DATA, POINTING DEVICE PERIPHERAL DATA and EDID PERIPHERAL DATA can flow only from the PERIPHERAL DEVICE to the CONNECTED COMPUTER. Flow in the reverse direction must be prevented by hardware.

Separation Rule:

USER AUTHENTICATION DEVICE DATA must be separated from all other PERIPHERAL DATA.

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

FDP_IFF.1.4b The TSF shall provide the following: **No additional SFP capabilities.**

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

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

6.1.1.6 FDP_ITC.1 Import of User Data Without Security Attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1a Subset information flow control] FMT_MSA.3 Static attribute initialization
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 Class FMT: Security Management

6.1.2.1 FMT_MSA.1 Management of Security Attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1a Subset information flow control] FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles
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, thus effectively modifying the GROUP IDs associated with the PERIPHERAL DEVICES.*

6.1.2.2 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of Security Attributes
FMT_SMR.1 Security roles

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.

6.1.3 Class FPT: Protection of the TSF

6.1.3.1 FPT_PHP.1 Passive detection of physical attack

Hierarchical to: No other components.

Dependencies: None

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.

6.1.3.2 FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: FPT_PHP.1

FPT_PHP.3.1 FPT_PHP.3.1 The TSF shall resist **physical interference, such as attempts to open the TOE enclosure** to the **TOE exterior** by responding automatically such that the SFRs are always enforced.

6.2 Explicitly Stated Requirements for the TOE

This ST contains the explicitly stated requirement for the TOE as specified in Section 5.1.3 of the claimed Protection Profile. It has been reproduced here:

EXT_VIR.1	**Visual Indication Rule**
Hierarchical to:	No other components.
Dependencies:	None
EXT_VIR.1.1	A visual method of indicating which COMPUTER is CONNECTED to the shared set of PERIPHERAL DEVICES shall be provided that is persistent for the duration of the CONNECTION.

Application Note: Does not require tactile indicators, but does not preclude their presence.

EXT_IUC.1	**Invalid USB Connection**
Hierarchical to:	No other components.
Dependencies:	None
EXT_IUC.1.1	All USB devices connected to the Peripheral switch shall be interrogated to ensure that they are valid (pointing device, keyboard, and user authentication device). No further interaction with non-valid devices shall be performed.

EXT_ROM.1	**Read Only ROMs**
Hierarchical to:	No other components.
Dependencies:	None
EXT_ROM.1.1	TSF software embedded in TSF ROMs must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.

6.3 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 claimed Protection Profile.

6.3.1 TOE Security Functional Requirements Tracing & Rationale

	Objectives							
SFRs	**O.CONF**	**O.INDICATE**	**O.ROM**	**O.SELECT**	**O.SWITCH**	**O.USBDETECT**	**O.UNIDIR**	**O.TAMPER**
FDP_ETC.1	●							
FDP_IFC.1a	●							
FDP_IFC.1b	●						●	
FDP_IFF.1a	●				●			
FDP_IFF.1b	●						●	
FDP_ITC.1	●							
FMT_MSA.1			●	●				
FMT_MSA.3				●	●			
FPT_PHP.1								●
FPT_PHP.3								●
EXT_ROM.1			●					
EXT_VIR.1		●						
EXT_IUC.1						●		

Table 11: SFR and Security Objectives Mapping

Objective	SFR Addressing the Objective	Rationale
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	**FDP_ETC.1** (Export of User Data Without Security Attributes)	**FDP_ETC.1:** 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. *Note that although this SFR appears in the claimed Protection Profile, it is not applicable specifically for the TOE as it does not handle HUMAN INTERFACE DEVICE control information or states.*
	FDP_IFC.1a (Subset Information Flow Control)	**FDP_IFC.1a:** This captures the policy that no information flows between different PERIPHERAL PORT GROUP IDS.
	FDP_IFC.1b (Subset Information Flow Control - Unidirectional Data Flow)	**FDP_IFC.1b:** This captures the policy that HUMAN INTERFACE DEVICE data can flow only from a device to a selected COMPUTER, thus preventing data from one COMPUTER flowing through the TOE to another COMPUTER.
	FDP_IFF.1a (Simple Security Attributes)	**FDP_IFF.1a:** 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.1a.
	FDP_IFF.1b (Simple Security Attributes - Unidirectional Data Flow)	**FDP_IFF.1b:** This requirement identifies the security ATTRIBUTES needed to detail the operation of a switch and the rules allowing only unidirectional information transfer between a keyboard, pointing device and EDID chip to a CONNECTED COMPUTER. Unidirectional peripheral data flow is critical to assure that data confidentiality is maintained as it prevents data from entering the TOE from one COMPUTER and exiting the TOE to another COMPUTER. This requirement is a dependency of FDP_IFC.1b.
	FDP_ITC.1 (Import of User Data Without Security Attributes)	**FDP_ITC.1:** In typical TOE applications, USER data consists of HUMAN INTERFACE DEVICE control information. These DEVICES neither expect nor require any security ATTRIBUTE information.
O.INDICATE The AUTHORIZED USER shall receive an unambiguous indication of which SWITCHED COMPUTER has been selected	**EXT_VIR.1** (Visual Indication Rule)	**EXT_VIR.1:** 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.

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.	**EXT_ROM.1** (Read-Only ROMs)	**EXT_ROM.1:** implements the O.ROM objective directly. While there might be other ways to protect embedded TSF code on a ROM (programmable or not), the requirement stipulates an easily-verifiable implementation that ensures that the TSF code will not be overwritten or modified.
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.	**FMT_MSA.1** (Management of Security Attributes) **FMT_MSA.3** (Static Attribute Initialization)	**FMT_MSA.1:** This restricts the ability to change selected PERIPHERAL PORT GROUP IDS to the AUTHORIZED USER. This requirement is a dependency of FMT_MSA.3. **FMT_MSA.3:** 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.1a and FDP_ITC.1.
O.SWITCH All DEVICES in a SHARED PERIPHERAL GROUP shall be CONNECTED to at most one SWITCHED COMPUTER at a time.	**FDP_IFF.1a** (Simple Security Attributes) **FMT_MSA.3** (Static Attribute Initialization)	**FDP_IFF.1a:** 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.1a. **FMT_MSA.3:** 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.1a and FDP_ITC.1.
O.USBDETECT The TOE shall detect any USB connection that is not a pointing device, keyboard, or user authentication device and disable that connection.	**EXT_IUC.1** (invalid USB Connection)	**EXT_IUC.1:** Upon detection of an invalid USB connection, the TOE will disable the connection and notify the user.
O.UNIDIR TOE circuitry shall assure that USER KEYBOARD, USER POINTING DEVICE and EDID data will flow only from PERIPHERAL DEVICES to the SWITCHED COUPLED COMPUTER.	**FDP_IFC.1b** (Subset Information Flow Control) **FDP_IFF.1b** (Simple Security Attributes)	**FDP_IFC.1b:** This captures the policy that KEYBOARD, POINTING DEVICE and EDID information MUST flow from devices to SWITCHED COMPUTERs only. Reverse flow must be blocked by hardware. **FDP_IFF.1b:** This requirement identifies the security ATTRIBUTES needed to detail the operation of a switch and the rules allowing only unidirectional information transfer between a keyboard, pointing device and EDID chip to a CONNECTED COMPUTER. This requirement is a dependency of FDP_IFC.1b.

O.TAMPER The TOE Device provides unambiguous detection of physical tampering of the TSF's devices or TSF's enclosure and permanently disables TOE normal functionality after such an event..	**FPT_PHP.1** (Passive detection of physical attack)	**FPT_PHP.1:** The TOE is required to provide unambiguous detection of any potential physical modification or unauthorized internal access to the TOE.
	FPT_PHP.3 (Automatic response upon detection of physical attack)	**FPT_PHP.3:** The TOE is required to provide an automatic response to physical attack that will permanently prevent normal USER operation of the TOE.

Table 12 - Objective to SFRs Rationale

6.4 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	Satisfied
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1(a)
FDP_IFC.1a	FDP_IFF.1a Simple security attributes	Yes
FDP_IFC.1b	FDP_IFF.1b Simple security attributes	Yes
FDP_IFF.1a	FDP_IFC.1a Subset information flow control	Yes
	FMT_MSA.3 Static attribute initialization	Yes
FDP_IFF.1b	FDP_IFC.1b Subset information flow control	Yes
	FMT_MSA.3 Static attribute initialization	Yes
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1a
	FMT_MSA.3	Yes
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1a and FDP_IFC.1b
	FMT_SMF.1 Specification of management functions	No
	FMT_SMR.1 Security roles	No
FMT_MSA.3	FMT_MSA.1 Management of security attributes	Yes
	FMT_SMR.1 Security roles	No
FPT_PHP.1	None	None
FPT_PHP.3	None	None
EXT_ROM.1	None	None
EXT_VIR.1	None	None
EXT_IUC.1	None	None

Table 13: SFR Dependencies satisfied

6.5 Dependencies Not Met

6.5.1 FMT_SMR.1 (Security roles) and FMT_SMF.1 (Specification of management functions)

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. Accordingly, no management of security functions of the TOE is required. Therefore, no management functions are specified.

6.6 Security Assurance Requirements

The table below is provides a list of claimed assurance components for each class.

Assurance Class	Assurance Component ID	Assurance Components Description
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
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life Cycle Support	ALC_CMC.4	Product 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_FLR.3	Systematic Flaw Remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.3	Focused vulnerability analysis

Table 14: SAR list

6.7 Rationale for Security Assurance

The EAL 4 + ALC_FLR.3 were chosen to provide an adequate level of independently assured security.

The chosen assurance level is consistent with the threat environment where an attacker may be assumed to have an attack potential of Enhanced-Basic. This has been augmented with ALC_FLR.3 in accordance with commercial requirements for this TOE type.

The assurance security requirements for this Security Target are taken from Part 3 of the CC.

7 TOE Summary Specification

This section presents an overview of the security functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

7.1 User Data Protection – Data Separation (TSF_DSP)

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 2 of the claimed Protection Profile. The Data Separation Security Function Policy implemented in the TOE is enhanced compared to the requirements that were defined by the claimed Protection Profile.

The TOE PERIPHERAL DATA flow path design is based on the following features:

- Isolated device emulators per coupled computer to prevent any direct interface between the TOE shared resources and connected computers.
- Host emulators to interface with connected peripherals, thus isolating external peripherals from TOE internal circuitry and from connected computers.
- Optical data diodes to enforce unidirectional data flow between host emulators and device emulators.
- Multiplexer (switch) to enable selection of just one data source at any given time.

This peripheral data path design provides higher assurance that data confidentiality will be maintained even when targeted attacks are launched against the TOE.

The TOE design does not mix PERIPHERAL DATA having different IDs or security attributes, and therefore internal TOE user data security attributes are neither generated nor used. This design therefore satisfies Functional Requirement FDP_ETC.1, that covers user data export and FDP_ITC.1 that covers user data import.

Unidirectional optical data diodes are used in the PERIPHERAL PORT GROUP traffic to assure that PERIPHERAL DATA can only flow from the SHARED PERIPHERAL DEVICEs to the COMPUTERs. This design prevents the COMPUTERS from interacting directly with the SHARED PERIPHERAL DEVICEs and therefore satisfies Functional Requirements FDP_IFC.1b and FDP_IFF.1b.

The TOE design uses a data multiplexer that only allows PERIPHERAL DATA to flow from the PERIPHERAL PORT GROUP to one COMPUTER at a time based on the selected ID. This is implemented through the switching mechanism of the TOE, and satisfies Functional Requirements FDP_IFC.1a and FDP_IFF.1a.

The Data Separation Security Functional Policy – “the TOE shall allow peripheral data and state information to be transferred only between peripheral port groups with the same ID” is assured through the use of a single unidirectional channel select control bus to drive all TOE switching functions simultaneously. This design further satisfies the Functional Requirements FDP_IFC.1a and FDP_IFF.1a.

It should be noted here that this TOE may switch the User Authentication Device PERIPHERAL DATA to a second COMPUTER based on user selection.

The TOE may contain up to seven separate types of switching modules (model specific): Keyboard and pointing device; Display EDID; Analog display; Digital display; DP display; Audio output; and User Authentication device.

The types of digital data and analog signals processed by the TOE are: keyboard data (USB or PS/2), pointing device data (USB or PS/2), Display Channel Plug & Play (EDID) information, analog video signals, Digital video signals, DisplayPort video signals, User Authentication device, USB data, and audio output analog signals. Specific models of the TOE accommodate subsets or supersets of the listed signals to support different deployment configurations. In all cases, the TOE ensures data separation for all signal paths using hardware only.

Each module is managed by an independent microcontroller. The microcontroller receives channel select commands from the TOE main system controller and invokes state changes to each module, as needed.

It should be noted that TOE switching functions are disabled in the following cases:

1. Before TOE self test and initialization process completed.
2. If the TOE anti-tampering system was triggered by an enclosure intrusion attempt.

The TOE will transition to normal TOE operation on default channel one following a passed self-test. The TOE does not recover after the anti-tampering system is triggered.

The basic arrangement of the microcontrollers used for shared peripheral data ensures data separation in hardware. It does this by physically separating the microcontrollers connected to the user's peripheral devices (the host emulators) from the microcontrollers connected to the attached computers (the device emulators). In TOE operation, the host emulator microcontrollers receive user inputs from the shared peripherals; the bi-directional USB stream is converted into a proprietary unidirectional stream that is switched to the appropriate channel and passed through an optical data diode. At the selected channel the device emulator converts the proprietary stream back into a standard USB format that is coupled to the selected COMPUTER. Separation is ensured in hardware by use of separate microcontrollers for each of the computers and for the shared user peripheral devices.

Functional Requirements Satisfied: FDP_ETC.1, FDP_IFC.1a, FDP_IFC.1b, FDP_IFF.1a, FDP_IFF.1b, FDP_ITC.1

7.2 Security Management (TSF_MGT)

The TOE accepts inputs from the AUTHORIZED USER to perform any switching through the front panel switching commands (push buttons), mouse keys, RCU rotary switch or keyboard shortcuts. The TOE does not store any data passing through it (PERIPHERAL DATA).

The TOE design provides clear and continuous visual indication of the selected channel through one or more of the following (model specific): front panel LEDs illuminated for each channel number selected, RCU display text highlighting, and windows frame colors (in Windowing KVM models).

The PERIPHERAL PORT GROUP is connected to COMPUTER #1 by default upon completion of the self-check. This static setting cannot be modified.

Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3, EXT_VIR.1

7.3 Protection of the TSF (TSF_TMP)

The TOE includes multiple tamper sensors connected to a microcontroller. When a sensor is activated, it signals the microcontroller to enter into a permanent tamper state, thereby disabling the TOE normal functionality permanently. The tampering sensors and microcontroller are powered by the TOE power system while the TOE is powered on. When TOE is powered off, the anti-tampering subsystem is powered by a coin battery to enable operation while the TOE is in transit or in storage. After a tampering event is detected, all LEDs flash to indicate an error state. While the TOE is in the error state, the user is unable to pass any information through the TOE to any COMPUTER, and user DISPLAYS are blank. Since the TOE becomes unusable, the user will require replacement of the TOE. This ensures that security is always maintained in the event of a physical attack.

The TOE is also protected by special holographic Tampering Evident Labels that are used as seals to provide additional visual indication of attempted physical tampering. In the case of a mechanical intrusion attempt, the label's location between enclosure parts assures that the label must be moved or peeled, permanently exposing the text "VOID".

Each Tampering Evident Label contains a unique identification number and several visible and invisible means to assist the operator in checking the authenticity of the label.

Functional Requirements Satisfied: FPT_PHP.1, FPT_PHP.3

7.4 USB Connection (TSF_IUC)

When a peripheral device is connected to the TOE, or when the TOE is being initialized, the TOE will query the device for its characteristics such as USB class, sub-class etc. In the event that the reported set of characteristics match the pre-defined profile, the TOE will start communicating with that device (device is QUALIFIED). In the event that the device reported characteristics do not match the pre-defined profile, the TOE will reject the device and will no longer communicate with it (device is rejected or UNAUTHORIZED).

Functional Requirements Satisfied: EXT_IUC.1

7.5 Read-Only Memory (TSF_ROM)

The non-volatile memory of the TOE functions as a ROM (Read Only Memory). The flash memory located within the microcontroller includes microscopic lock fuses that function as OTP (One Time Programmable) devices. During TOE production, following programming and testing, these lock fuses are activated (or burned) to protect the flash memory from further modification. Once the lock fuses are activated, the memory in that chip becomes Read Only Memory. It should be noted that this lock process also protects the device memory content from external reading attempts and therefore provides another layer of security against reverse engineering.

These protections are not able to be bypassed without de-soldering of the microcontroller chip, which requires a physical access to the system board. The anti-tamper system described in Section 7.3 assures that an attempt to access these memory chips is not possible without causing permanent damage to the TOE.

Functional Requirements Satisfied: EXT_ROM.1

7.6 Audio Output Switching Function Clarification

This paragraph provides additional information about the TOE Audio Output Switching Function as the PP to which this ST claims conformance does not include audio switching functionality.

The design of the TOE does not negatively affect the TOE SFR due to the following reasons:

1. The audio switching circuitry is electrically isolated from all other data transitioning the TOE.
2. Audio switching commands are received from the TOE System Controller function through a unidirectional link to prevent export of audio data into other TOE circuitry.
3. The TOE does not support microphone switching, and therefore it is not vulnerable to analog leakage between coupled computers.
4. NIAP has issued clarification to the claimed Protection Profile in the Precedent Database PD-0166 dated May 19, 2011 indicating that Peripheral Sharing Devices may support an audio switching function: “Resolution - Analog audio devices (those typically connected through a 3.5mm Stereo Mini Jack) MAY be switched through a peripheral sharing switch.”