Raritan Secure KVM Switch Series

Security Target

Version 0.7
December 13, 2017

Prepared for:
Raritan Inc.
400 Cottontail Lane, Somerset, NJ 08873, U.S.A

Prepared by:

leidos

Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive, Columbia, Maryland 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Raritan Secure KVM Switch Series provided by Raritan Inc.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – Raritan Secure KVM Switch Series Security Target

ST Version – Version 0.7

ST Date – December 13, 2017

TOE Identification –Raritan Secure KVM Switch Series

- Raritan 2-port Secure KVM Switch w/CAC (RSS-102C)
- Raritan 4-port Secure KVM Switch w/CAC (RSS-104C)
- Raritan 2-port Secure KVM Switch (RSS-102)
- Raritan 4-port Secure KVM Switch (RSS-104)

Each model includes firmware version v1.1.101.

TOE Developer – Raritan Inc.

Evaluation Sponsor – Raritan Inc.

CC Identification – *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012*

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- *Protection Profile for Peripheral Sharing Switch, Version 3.0, 13 February 2015* [PSS] including the following optional SFRs: FAU_GEN.1, FDP_RIP.1(2), FIA_UID.2, FIA_UAU.2, FMT_MOF.1, FMT_SMF.1, and FMT_SMR.1 and the following technical decisions:
  - TD0083 - Vulnerability Survey Assurance Component (AVA_VAN.1) in PSS PP v3.0, published date 02/29/2016
  - TD0136 – FDP_RIP.1.1 – Refinement, published date 12/16/2016
  - TD0144 - FDP_RIP.1.1 - Purge Memory and Restore Factory Defaults Optional
  - TD0251 - FMT_MOF.1.1 - Added Assignment

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012
    - Part 3 Conformant

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parentheses placed at the end of the component. For example, FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, (1) and (2).
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that 'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.
    - The [PSS] uses an additional convention – Text highlighted in **blue fonts** defines conditions for the following paragraph. Only the applicable conditions are identified in this ST and they are identified using **bold text**.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4 Technical Definitions, Abbreviations and Acronyms

See CC Part 1 Section 4 and [PSS] Section A.1 for definitions of common CC terms.

1.4.1 Technical Definitions

Administrator A person who administers (e.g. installs, configures, updates, maintains) a system of device(s) and connections.

Combiner A PSS switch with video integration functionality

Configurable Device Filtration (CDF) PSS function that qualifies (accepts or rejects) peripheral devices based on field configurable parameters.

Connected Computer A computing device (platform) connected to the PSS. May be a personal computer, server, tablet or any other computing device with user interaction interfaces.

Connection Enables devices to interact through respective interfaces. It may consist of one or more physical (e.g. a cable) and/or logical (e.g. a protocol) components.

Device An information technology product with which actors (persons or devices) interact.

Display A Human Interface Device (HID), such as a monitor or touch screen,

External Entity An entity outside the TOE evaluated system, its connected computers and its connected peripheral devices.

Fixed Device Filtration (FDF) PSS function that qualifies (accepts or rejects) peripheral devices based on fixed parameters.

Human Interface Device (HID) A device that allows for user input. For example, keyboard and mouse.

Interface Enables interactions between actors.

Isolator A PSS with single connected computer.

Keyboard A Human Interface Device (HID) such as a keyboard, keypad or other text entry device.

KM A PSS that switches only the keyboard and pointing device.

Non-Selected Computer A connected computer not currently selected by the PSS user.

Peripheral A device that exposes an actor's interface to another actor.

Peripheral Group An ordered set of peripherals.

Pointing Device A Human Interface Device (HID), such as a mouse, track ball or touch screen (including multi-touch). Selected Computer A connected computer currently selected by the PSS user.

User A person or device that interacts with devices and connections.

User Authentication Device A peripheral device used to authenticate the identity of the user, such as a smart-card reader, biometric authentication device or proximity card reader.

Video Wall Consists of multiple computer monitors, video projectors, or television sets tiled together contiguously or overlapped in order to form one large display.

1.4.2 Abbreviations and Acronyms

AUX	Display Port Auxiliary Channel
CAC	Common Access Card
CCTL	Common Criteria Test Lab
CDC	Communication Device Class
CODEC	Coder-Decoder
dBv	A measurement of voltages ratio – decibel volt
DC	Direct Current
DP	Display Port
DVI	Digital Visual Interface
EDID	Extended Display Identification Data
FDF	Fixed Device Filtration
FIPS	Federal Information Processing Standards
HD	High Definition
HDMI	High Definition Multimedia Interface
HID	Human Interface Device
IP	Internet Protocol
IT	Information Technology

USB Keep-Alive NAK transaction	USB 2.0 standard handshake PID (1010B) – Receiving device cannot accept data or transmitting device cannot send data.
KM	Keyboard, Mouse
KVM	Keyboard, Video and Mouse
LED	Light-Emitting Diode
LoS	Line-of-Sight
MCCS	Monitor Control Command Set
MHL	Mobile High-Definition Link
MSC	Mass Storage Class
mV	millivolt KVM/KM
OSD	On-Screen Display
PC	Personal Computer
PID	Device Product ID
PIN	Personal Identification Number
PP	Protection Profile
PSS	Peripheral Sharing Switch
S/PDIF	Sony/Philips Digital Interface Format
SP	Special Publication
SFP	Security Function Policy
SPF	Shared Peripheral Functions
TMDS	Transition-Minimized Differential Signalling
TSF	TOE Security Function
UART	Universal Asynchronous Receiver / Transmitter
USB	Universal Serial Bus
V	Volt
VESA	Video Electronics Standards Association
VID	Device Vender ID
VGA	Video Graphics Array

2. TOE Description

The TOE is the Raritan Secure KVM Switch Series. The RSS-102, RSS-102C, RSS-104, RSS-104C series are Peripheral Sharing Switch devices that permit a single set of devices such as keyboard, video display, mouse/pointing devices, and smart card readers to be shared securely among two or more connected computers.

2.1 TOE Overview

The Raritan Secure KVM Switches provide KVM (USB Keyboard/Mouse, DVI-I Video) switch functionality by combining a 2/4 port KVM switch, an audit output port with Speaker, and a Smartcard CCID/CAC port. The TOE is classified as a "Peripheral Sharing Switch" (KVM device) in the Common Criteria. Hardware and firmware components are included in the TOE.

2.2 TOE Architecture

Raritan Secure KVM Switch Series provides a secure medium to share a single set of peripheral components such as keyboard, video display and mouse/pointing devices among multiple computers over USB, and/or DVI.

Raritan Secure KVM port models include:

- 2-Port
- 2-Port with CAC
- 4-Port
- 4-Port with CAC

The Secure KVM Switch products allow for the connection of a mouse, keyboard, user authentication device such as smart card or CAC reader (optional), speaker, and a video display, which is then connected to 2, or up to 4 separate computers (depending on specific TOE device type). The user can then switch the connected peripherals between any of the connected computers using a push button on the front of the device. The selected device is always identifiable by a green LED associated with the applicable selection button.

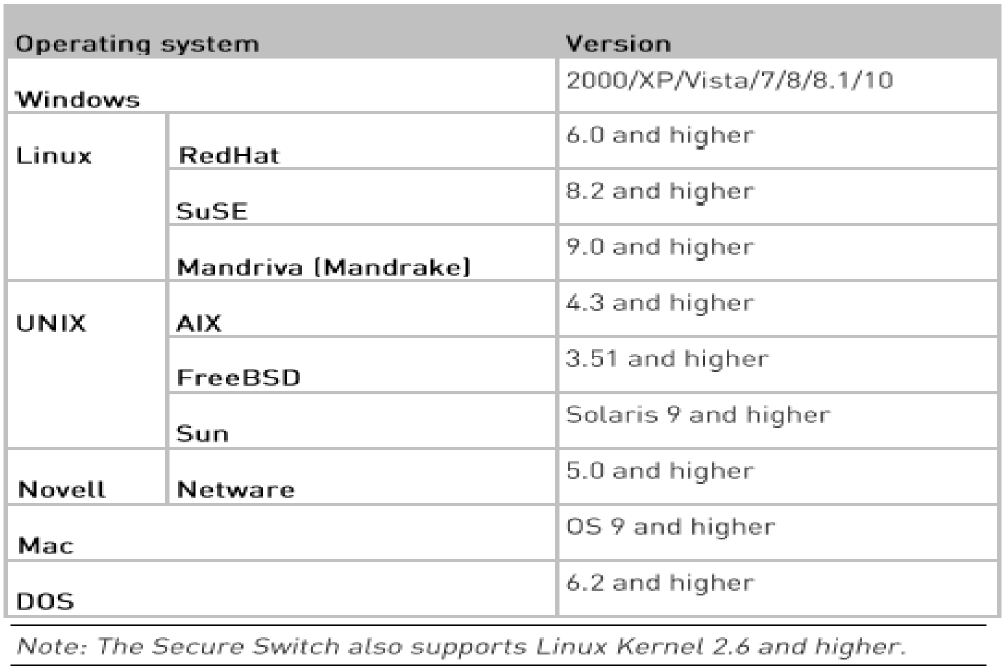
The Secure KVM Switch products support USB connections for the keyboard, mouse and user authentication device and DVI for the video display. Separate USB cables are used to connect the keyboard/mouse combination and the user authentication device to the connected computers. The Secure KVM Switch products support, DVI video connections from the connected computers and speaker connections. The use of an analog microphone or line-in audio device is prohibited.

The Raritan Secure KVM products implement a secure isolation design for all 2/4-Port models to share a single set of peripheral components. The Secure KVM Switch products support the following peripheral port types: USB keyboard; USB mouse; USB authentication device (CAC reader); audio output; and DVI video. Each peripheral has its own dedicated data path. USB keyboard and mouse peripherals are filtered and emulated. The USB authentication device connection is on a separate circuit from the keyboard and mouse and, after filtering for qualification, has a direct connection path to the selected computer. The TOE does not emulate the user authentication device function.

The Secure KVM Switch products are designed to enforce the allowed and disallowed data flows between user peripheral devices and connected computers as specified in [PSS]. Data leakage is prevented across the TOE to avoid compromise of the user's information. Modern Secure KVM security approaches address the risk of TOE local user data leakage through remote attacks to coupled networks in addition to protecting user information passing through the TOE. The Secure KVM Switch products automatically clear keyboard and mouse buffers.

The Port Authentication Utility tool is optionally used to initially define or modify user authentication device filter (whitelist and/or blacklist) on the Raritan Secure KVMs w/ CAC feature. The list can be configured or modified at any time. However the administrator must upload the list and power cycle the TOE for the new configuration to take effect. The Utility must be installed on a separate secure source computer using an installation wizard. The utility supports Microsoft Windows 7 and higher. The dedicated secure source computer must have its own monitor, keyboard, and mouse connected for installation and operation.

Raritan Secure PSS is compatible with standard personal/portable computers, servers or thin-clients. The supported operating systems are identified as follows:



Operating system		Version
Windows		2000/XP/Vista/7/8/8.1/10
Linux	RedHat	6.0 and higher
	SuSE	8.2 and higher
	Mandriva (Mandrake)	9.0 and higher
UNIX	AIX	4.3 and higher
	FreeBSD	3.51 and higher
	Sun	Solaris 9 and higher
Novell	Netware	5.0 and higher
Mac		OS 9 and higher
DOS		6.2 and higher

Note: The Secure Switch also supports Linux Kernel 2.6 and higher.

The following figure shows the data path design using a 2-Port KVM as an example.

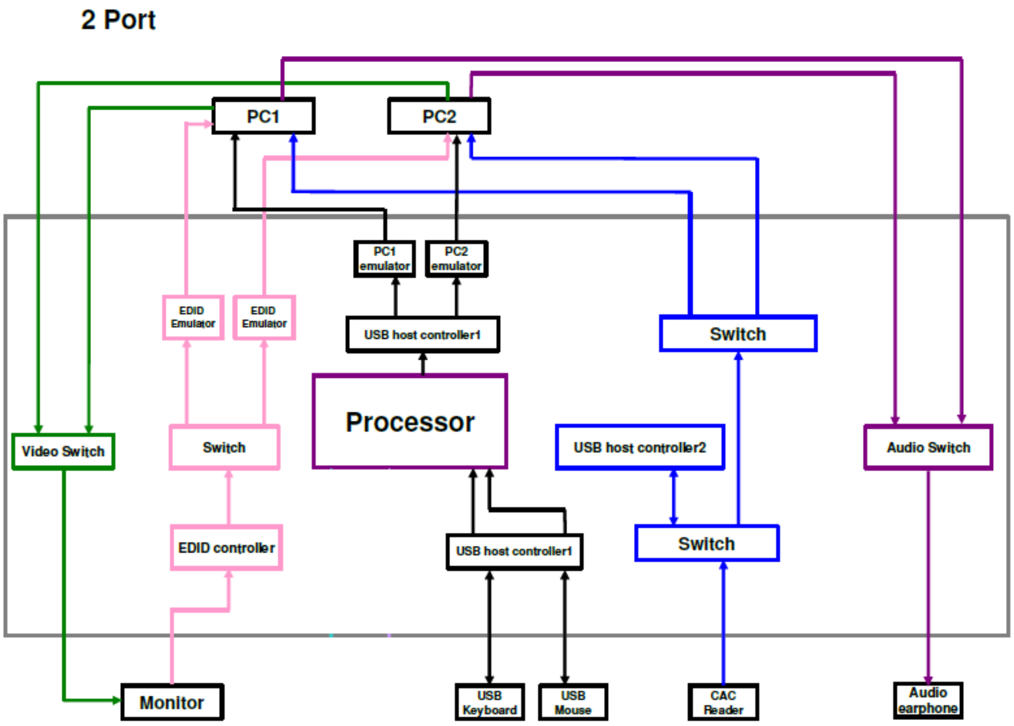


Figure 1 Simplified block diagram of a 2-Port KVM TOE

Tables 1 and 2 below provide a summary of the Raritan Secure KVM PSS security features. A detailed description of the TOE security features can be found in Section 6 (TOE Summary Specification) below.

2.2.1 Physical Boundaries

TOE Model	Ports	Interfaces
RSS-102	2	Dual Link DVI-I, USB Keyboard, USB mouse, Analog Audio output (ex: Speaker), Switch Buttons, LED indicators, Power Switch and Reset Button.
RSS-104	4	Dual Link DVI-I, USB Keyboard, USB mouse, Analog Audio output (ex: Speaker), Switch Buttons, LED indicators, Power Switch and Reset Button.
RSS-102C	2	Dual Link DVI-I, USB Keyboard, USB mouse, Analog Audio output (ex: Speaker), USB CID/CAC, Switch Buttons, LED indicators, Power Switch and Reset Button.
RSS-104C	4	Dual Link DVI-I, USB Keyboard, USB mouse, Analog Audio output (ex: Speaker), USB CID/CAC, Switch Buttons, LED indicators, Power Switch and Reset Button.

Table 1 TOE Models and Interfaces

The TOE includes the hardware models identified above along with their embedded firmware (version v1.1.101) and corresponding documentation identified in Section 2.3 below.

Console Port	Authorized Devices	Authorized Protocol
Keyboard	Wired keyboard and keypad without internal USB hub or composite device functions.	USB Type-A F
Display	Display, Video or KVM extender	DVI-I Dual Link F
Mouse/Point Device	Wired mouse or trackball without internal USB hub or composite device functions.	USB Type-A F
Audio Out	Analog amplified speakers	Mini Stereo Jack F
User Authentication Device	Smartcard, CAC reader	USB Type-B F

Table 2 TOE Security Functional Components

The peripheral devices: DVI-I Monitor, USB Keyboard, USB Mouse, Audio output (e.g. Speakers), smartcard/CAC reader and the Host Computers are in the operational environment.

2.2.2 Logical Boundaries

This Raritan Secure KVM Switch Series TOE allows an individual user to utilize a single set of peripherals to operate in an environment with several isolated computers. KVM switches keyboard, mouse, display, audio, and USB/CAC (on RSS-102C and RSS-104C models) from one isolated computer to another.

This section summarizes the security functions provided by Raritan Secure KVM Switch Series.

- Security Audit
- User Data Protection
- Identification and authentication
- Security Management
- Protection of the TSF
- TOE Access

2.2.2.1 Security Audit

The TOE generates audit records for the authorized administrator actions. Each audit record records a standard set of information such as date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event.

2.2.2.2 User Data Protection

The TOE controls and isolates information flowing between the peripheral device interfaces and a computer interface. The peripheral devices supported include keyboard, DVI-I, mouse, audio out, and CAC.

The TOE authorizes peripheral device connections with the TOE console ports based on the peripheral device type.

The TOE ensures that any previous information content of a resource is made unavailable upon the deallocation of the resource from a TOE computer interface immediately after TOE switch to another selected computer; and on start-up of the TOE

2.2.2.3 Identification and Authentication

The TOE provides an identification and authentication function for the administrative user to perform administrative functions such as configuring the user authentication (CDF) whitelist and blacklist. The authorized administrator must logon by providing a valid password. The logon function provides authentication failure handling.

2.2.2.4 Security Management

The TOE supports configurable device filtration. This function is restricted to the authorized administrator and allows the TOE to be configured to accept or reject specific USB devices using CDF whitelist and blacklist parameters. Additionally, the TOE provides security management functions to Reset to Factory Default and to change the administrator password.

2.2.2.5 Protection of the TSF

The TOE runs a suite of self-tests during initial startup and activating the reset button that includes a test of the basic TOE hardware and firmware integrity; a test of the basic computer-to-computer isolation; and a test of critical security functions (i.e., user control and anti-tampering). The TOE provides users with the capability to verify the integrity of the TSF and the TSF functionality.

The TOE resists physical attacks on the TOE enclosure for the purpose of gaining access to the internal components, or to damage the anti-tampering battery by becoming permanently disabled. The TOE preserves a secure state by disabling the TOE when there is a failure of the power on self-test, or a failure of the anti-tampering function.

The TOE provides unambiguous detection of physical tampering that might compromise the TSF. The TSF provides the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

2.2.2.6 TOE Access

The TOE displays a continuous visual indication of the computer to which the user is currently connected, including on power up, and on reset.

2.3 TOE Documentation

There are several documents that provide information and guidance for the deployment, administration, and usage of the TOE. In particular, the following guides reference the security-related guidance material for all devices in the evaluated configuration:

Guidance Documentation:

- *Raritan Secure KVM Switch Series Administrator Guide version 1.0, December, 2017*
- *Raritan Secure Switch User Guide Release 1.0, December 2017*
- *Raritan Secure KVM Switch Series Port Authentication Utility Guide 1.0, 2/4-Port USB DVI Secure KVM Switch with or without CAC Feature Port Authentication Utility Guide, Release 1.0, 15 December 2017*
- *Raritan PP3.0 Secure KVM Admin log audit code v1.0, 14 December 2017*
    - **Note:** The Admin Log Audit Code document is provided only to customers.

TOE Documentation:

- *Raritan PP3.0 Secure KVM Isolation Document v1.5, 28 November 2017*
    - **Note**: The Raritan PP3.0 Secure KVM Isolation Document is **proprietary** as permitted by protection profile Annex J Isolation Document and Assessment.
    - The isolation document supplements security target Section 6 TOE Summary Specification in order to demonstrate the TOE provides isolation between connected computers. In particular, the isolation document describes how the TOE mitigates the risk of each unauthorized data flow listed in protection profile Annex D Authorized and Unauthorized PP Data Flows.
- *PROPRIETARY: Letter of Volatility*, v4.4, 29 November 2017

3. Security Problem Definition

This security target includes by reference the Security Problem Definition from the [PSS]. The Security Problem Definition consists of threats that a conformant TOE is expected to address and assumptions about the operational environment of the TOE.

In general, the [PSS] has presented a Security Problem Definition appropriate for peripheral sharing switches. The Raritan Secure KVM Switch Series provide KVM (USB Keyboard/Mouse, DVI-I Video) switch functionality by combining a 2/4 port KVM switch, an audit output port, and a Smartcard/CAC port. As such, the [PSS] Security Problem Definition applies to the TOE.

4. Security Objectives

Like the Security Problem Definition, this security target includes by reference the Security Objectives from the [PSS] with all of the optional objectives included except:

- O.USER_AUTHENTICATION_TERMINATION

The [PSS]**Error! Reference source not found.** security objectives for the operational environment are reproduced below, since these objectives characterize technical and procedural measures each consumer must implement in their operational environment.

In general, the [PSS]**Error! Reference source not found.** has presented a Security Objectives statement appropriate for peripheral sharing switches. Consequently, the [PSS]**Error! Reference source not found.** security objectives are suitable for the TOE.

4.1 Security Objectives for the Environment

OE. NO_TEMPEST	The operational environment will not require the use of TEMPEST approved equipment.
OE. NO_SPECIAL_ANALOG_CAPABILITIES	The operational environment will not require special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.
OE.PHYSICAL	The operational environment will provide physical security, commensurate with the value of the TOE and the data it contains.
OE.TRUSTED_ADMIN	The operational environment will ensure that appropriately trained and trusted TOE Administrators and users are available to administer, configure and use the TOE.

5. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the Protection Profile: *Protection Profile for Peripheral Sharing Switch, Version 3.0, 13 February 2015 [PSS]* and include the following optional SFRs: FAU_GEN.1, FDP_RIP.1(2), FIA_UID.2, FIA_UAU.2, FMT_MOF.1, FMT_SMF.1, and FMT_SMR.1. As a result, refinements and operations already performed in that PP are not identified (e.g., highlighted) here, rather the requirements have been copied from that PP and any residual operations have been completed herein. Of particular note, the [PSS] made a number of refinements and completed some of the SFR operations defined in the CC and that PP should be consulted to identify those changes if necessary. Additionally, the [PSS] has a number of Conditional selections within certain SFRs that are to be selected only if supported in the TOE.

The SARs are the set of SARs specified in [PSS].

5.1 Extended Requirements

All of the extended requirements in this ST have been drawn from the [PSS]. The [PSS] defines the following extended SFRs and since they are not redefined in this ST, the [PSS] should be consulted for more information in regard to those CC extensions.

- FTA_CIN_EXT.1: Continuous Indications
- FTA_ATH_EXT.1: User Authentication Device Reset

5.2 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by either the TOE or the platform on which it runs.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
FDP: User Data Protection	FDP_IFC.1(1): Subset information flow control
	FDP_IFF.1(1): Simple security attributes
	FDP_IFC.1(2): Subset information flow control
	FDP_IFF.1(2): Simple security attributes
	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
	FDP_RIP.1(1): Subset Residual information protection
	FDP_RIP.1(2): Subset Residual information protection (Restore factory defaults)
FIA: Identity and authentication	FIA_UAU.2: User identification before any action
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MOF.1: Management of security functions behavior
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_PHP.1: Passive detection of a physical attack
	FPT_PHP.3: Resistance to physical attack
	FPT_FLS.1: Failure with preservation of secure state

Requirement Class	Requirement Component
	FPT_TST.1: TSF testing
FTA: TOE Access	FTA_ATH_EXT.1: User authentication device reset
	FTA_CIN_EXT.1: Extended: Continuous Indications

Table 3 TOE Security Functional Components

5.2.1 Security Audit (FAU)

5.2.1.1 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [not specified] level of audit; and
c) [administrator login, administrator logout, and [***Reset to Factory Default, change password***]].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no other information].

5.2.2 User Data Protection (FDP)

5.2.2.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the [peripheral device SFP] on

[Subjects: Peripheral devices

Objects: Console ports

Operations: allow connection, disallow connection].

5.2.2.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [peripheral device SFP] to objects based on the following:

[Subjects: Peripheral devices

Subject security attributes: peripheral device type

Objects: Console ports

Object security attributes: none].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [The TOE shall query the connected peripheral device upon initial connection or upon TOE power up and allow connection for authorized peripheral devices in accordance with the table in Annex C of ~~this~~ PP **PSS**].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none.].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [The TOE peripheral device interface (console) port shall reject any peripheral device with unauthorized values].

5.2.2.3 Subset information flow control (FDP_IFC.1(1)) (User Data Protection)

FDP_IFC.1.1(1) The TSF shall enforce the [User Data Protection SFP] on

[Subjects: TOE computer interfaces, TOE peripheral device interfaces

Information: User data transiting the TOE

Operations: Data flow between subjects].

5.2.2.4 Simple Security Attributes (FDP_IFF.1(1)) (User Data Protection)

FDP_IFF.1.1(1) The TSF shall enforce the [User Data Protection SFP] based on the following types of subject and information security attributes:
[Subject: TOE computer interfaces
Subject security attributes: user selected computer interface
Subject: TOE peripheral device interfaces
Subject security attributes: none
Information: User data transiting the TOE
Information security attributes: none].

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [The user makes a selection to establish a data flow connection between the peripheral device interfaces and one computer interface based on the following rules:

1. The attribute User Selected Computer determines the operation Allowed Data Flow such that the only permitted data flows are as listed in the table below:

Value of User Selected Computer	Allowed Data Flow
n	***User keyboard peripheral device interface data flowing from peripheral device interface to computer interface #n;*** ***User mouse peripheral device interface data flowing from peripheral device interface to computer interface #n;*** ***User display peripheral device interface data flowing from computer interface #1 to one or more user display peripheral device interfaces;*** ***User authentication peripheral device data flowing bidirectional between computer interface #n and user authentication device peripheral interface; and*** ***Analog audio output data flowing from computer interface #n to the audio peripheral device interface***;

2. When the user changes the attribute by selecting a different computer, this causes the TOE to change the data flow accordingly.

FDP_IFF.1.3(1) The TSF shall enforce the [the following additional information flow control SFP rules if the TOE supports user authentication devices [
1. The TOE user authentication device function is not emulated - following an event of the user changing the attribute by selecting a different computer, the TOE must reset the power to the connected user authentication device;
].

FDP_IFF.1.4(1) The TSF shall explicitly authorize an information flow based on the following rules: [no additional rules].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules:

[1. The TSF shall deny any information flow between TOE peripheral device interfaces and TOE non-selected computer interfaces.
2. The TSF shall deny any data flow between an external entity and the TOE computer interfaces.
3. The TSF shall deny any user data flow between the TOE and an external entity].

5.2.2.5 Subset information flow control (FDP_IFC.1(2)) (Data Isolation Requirements)

FDP_IFC.1.1(2) The TSF shall enforce the [Data Isolation SFP] on
[Subjects: TOE computer interfaces, TOE peripheral interfaces
Information: data transiting the TOE
Operations: data flows between computer interfaces].

5.2.2.6 Simple security attributes (FDP_IFF.1(2)) (Data Isolation Requirements)

FDP_IFF.1.1(2) The TSF shall enforce the [Data Isolation SFP] based on the following types of subject and information security attributes:
[Subject: TOE interfaces
Subject security attributes: Interface types (Allowed TOE interface types are listed in Annex C of ~~this~~ PP **PSS**. Power source and connected computer interfaces are also applicable interface types.)
Subject: TOE peripheral device interfaces
Subject security attributes: none
Information: data transiting the TOE
Information security attributes: data types. (The TSF shall enforce the data isolation SFP on the following data types:

a. User keyboard key codes;

b. User pointing device commands;

c. Video information (User display video data and display management data);

d. Audio output data; and

e. User authentication device data.)].

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
[1. During normal TOE operation, the TSF shall permit only user entered keyboard key codes, and user input mouse commands to flow between the TOE keyboard and mouse peripheral device interfaces and the TOE selected computer interface. No flow is permitted between the selected computer interface and the TOE keyboard and mouse peripheral device interfaces.
2. The TSF shall permit information flow and TSF resources sharing between two TOE user peripheral interfaces of the same Shared Peripheral group. Both functions may share the same interface].

FDP_IFF.1.3(2) The TSF shall enforce the [No additional rules].

FDP_IFF.1.4(2) The TSF shall explicitly authorize an information flow based on the following rules: [No additional rules].

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules:
[1. The TSF shall deny any information flow between TOE Computer Interfaces, except those allowed by the User Data Flow rules;

2. ***The TSF shall deny data flow other than keyboard entries and mouse reports between the TOE keyboard and mouse peripheral device interfaces and the TOE selected computer interface;***

3. ***The TSF shall deny power flow between the selected computer interface and TOE keyboard and mouse peripheral device interfaces;***

4. ***The TSF shall deny information flow from the TOE selected computer interface to the TOE keyboard and mouse peripheral device interface;***

5. ***The TSF shall deny data flow of user authentication device data transiting the TOE to non-selected TOE computer interfaces;***

6. ***The TSF shall assure that the user authentication device computer interfaces are not shared with any other TOE peripheral function interface (keyboard, mouse etc.);***

7. The TSF shall deny information flow between two TOE user peripheral interfaces in different Shared Peripheral groups;

8. ***The TSF shall deny analog audio information flow between the TOE selected computer audio interface and the user audio device peripheral interface when a microphone peripheral device is*** **intentionally or unintentionally connected to the** ***TOE audio peripheral device interface;***

9. ***The TSF shall enforce unidirectional information flow between the TOE selected computer audio interface and the user audio device peripheral interface. Bidirectional information flow shall be denied;***

11. ***The TSF shall deny any information flow from the TOE display peripheral device interface and the selected computer interface with the exception of EDID information that may be passed once at TOE power up or after recovery from TOE reset****;*

12. ***The TSF shall deny an information flow between the selected computer display interface and the TOE display peripheral device interface on the EDID channel****;*

13. The TSF shall recognize and enable only those peripherals with an authorized interface type as defined in Annex C of ~~this~~ PP **PSS**. Information flow to all other peripherals shall be denied; and

14. All denied information flows shall also be denied when the TOE's power source is removed].

5.2.2.7 Subset Residual information protection (FDP_RIP.1(1))

FDP_RIP.1.1(1)[1] Refinement: The TSF shall ensure that any previous information content of a resource is made unavailable [

• immediately after TOE switches to another selected computer;

• and on start-up of the TOE for

] the following objects: [a TOE computer interface].

5.2.2.8 Subset Residual information protection (FDP_RIP.1(2) Restore factory defaults)

FDP_RIP.1.1(2) The TOE shall have a purge memory or Restore Factory Defaults function accessible to the user to delete all TOE stored configuration and settings.

5.2.3 Identification and Authentication (FIA)

FIA_UAU.2.1 The TSF shall require each administrator to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2.1 The TSF shall require each administrator to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[1] This SFR has been modified by TD0136.

5.2.4 Security Management (FMT)

5.2.4.1 Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [perform] the functions [modify TOE user authentication device filtering (CDF) whitelist and blacklist, [***Reset to Factory Default, view audit logs, change password***]]to [the authorized administrators][2].

5.2.4.2 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TOE shall be capable of performing the following management functions:

a. The TOE shall provide authorized administrators the option to assign whitelist and blacklist definitions for the TOE user authentication device qualification function**,**
b. [**Reset to Factory Default, view audit records, change password**].

5.2.4.3 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [users, administrators].

5.2.5 Protection of the TSF (FPT)

5.2.5.1 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state by disabling the TOE when the following types of failures occur: [failure of the power on self-test, failure of the anti-tampering function].

5.2.5.2 Passive detection of a physical attack (FPT_PHP.1)

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.

5.2.5.3 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist [a physical attack on the TOE for the purpose of gaining access to the internal components, or to damage the anti-tampering battery] to the [TOE Enclosure] by becoming permanently disabled.

5.2.5.4 TSF testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self-tests that includes as minimum:

a. Test of the basic TOE hardware and firmware integrity; and

b. Test of the basic computer-to-computer isolation; and

c. Test of critical security functions (i.e., user control and anti-tampering).

[during initial startup, [upon reset button activation]] to demonstrate the correct operation of [the TSF].

FPT_TST.1.2 The TSF shall provide users with the capability to verify the integrity of [the TSF functionality].

FPT_TST.1.3 The TSF shall provide users with the capability to verify the integrity of [the TSF].

[2] TD0251 has modified this SFR.

5.2.6 TOE Access (FTA)

5.2.6.1 User authentication device reset (FTA_ATH_EXT.1)

FTA_ATH_EXT.1 The TSF shall reset the power supplied to the user authentication device for at least one second when the user switches the device from one computer to another.

5.2.6.2 Extended: Continuous Indications (FTA_CIN_EXT.1)

FTA_CIN_EXT.1 The TSF shall display a continuous visual indication of the computer to which the user is currently connected, including on power up, [***on reset***].

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are included by reference from the [PSS].

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Analysis

Table 4 Assurance Components

Consequently, the assurance activities specified in the [PSS] apply to the TOE evaluation.

6. TOE Summary Specification

This chapter describes the security functions:

- Security Audit
- User Data Protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE Access

6.1 Security Audit

The TOE logs security events such as start-up and shutdown of the audit functions; administrator actions (login, logout, blacklist/whitelist configuration, password changes, and Reset to Factory Default events); and the permanent disabling of the TOE. Start-up and shutdown of the audit functions occurs with startup and shutdown of the product. The audit function cannot be started or stopped separately from the product. After a successful Administrator Logon, the logs can be viewed in the text editor by entering the command [LIST].

The event logs are divided into two types: critical and general. The Log Data Area displays the critical and non-critical Log data. Each logged event is recorded with date, time, subject identity and includes special codes that indicate the type of event and the outcome (success or failure) of the event. The types of events recorded and identified in the special codes include Administrator Logon/Logoff events; Administrator password change events; Administrator configuration events: Reset to Factory Default and Device filter configuration events; power cycle events; and Self-test / Tampering events. Some special Log/Event data logs (such as KVM shut down due to tampering, KVM locked) can only be decoded by Raritan.

The logs are stored on EEPROM on the KVM PCBoard component of the TOE. The logs can be extracted by the authorized administrator by entering Administrator Logon mode; logging on; and then issuing the command [LIST]. The TOE extracts the log data and displays them using the text editor. The administrator can view the logs but cannot erase or delete any of the information The TOE stores the critical event logs only for the most recent occurrence of events. The logging feature can accommodate a maximum of thirty-two non-critical audit events. A new non-critical log entry will overwrite the oldest one (for example, the thirty-third log entry will overwrite the first log).

The Security Audit security function satisfies the following security functional requirements:

- FAU_GEN.1—audit records are generated for security relevant events and include the date and time of the event, type of event, subject identity, and outcome of the event.

6.2 User Data Protection

The TOE enforces data isolation and the User Data Protection SFP on TOE computer interfaces and TOE peripheral device interfaces by controlling the data flow and user data transiting the TOE.

The TOE supports the following types of devices: USB Keyboard and Mouse, DVI-I Video, analog audio out, and USB CAC. All other devices are rejected.

The TOE ensures that any previous information content of a resource is made unavailable upon the deallocation of the resource from the TOE computer interfaces immediately after a TOE switch to another selected computer; and on start-up of the TOE.

The detailed Letter of Volatility provides assurance that no user data remains in the TOE after power down.

6.2.1 Subset information flow control (FDP_IFC.1(1)) and Simple security attributes (FDP_IFF.1(1)) User Data Information Flow

The TOE enforces the User Data Protection SFP on TOE computer interfaces and TOE peripheral device interfaces by controlling the data flow and user data transiting the TOE.

The TOE supports USB keyboard and mouse, DVI-I, analog audio output, and user authentication devices peripheral and connected port types. The TOE does not allow any other user data transmission to or from external entities. Docking protocols and analog microphone or audio line inputs are not supported by the TOE.

User peripheral input device mechanism by micro controller ensures unidirectional data to each Device Controller per port to prevent data flow from Device Controller to host controller, that is, from selected computer to user peripheral input device. The TOE has individual circuitry for both output data flow (like video signal) and input data (like HID data).

USB keyboard and mouse peripherals are filtered and emulated. The USB authentication device connection is on a separate circuit/power source from the keyboard and mouse and, after filtering for qualification, has a direct connection path to the selected computer. The TOE does not emulate the user authentication device function.

Digital buffers are used to ensure uni-directional data flow from the connected computer to the user peripheral device. Audio data from the connected peripheral devices to the connected computer is controlled by a 4-to-1 audio switch. All audio signals will pass through the audio switch first, but only the selected channel will connect to a unidirectional buffer which is connected to the audio peripheral device. The use of unidirectional buffers ensures that the audio data could only travel from the selected computer to the audio device and prevents the use of microphones or audio line input devices.

Each connected computer has its own TOE isolated channel with its own EDID emulator and video input port. Data flows from the input video source through its respective emulator and out of the monitor display port. The video input interfaces are isolated from one another using different EDID ICs, power planes, ground planes, and electronic components in each independent channel. The TOE prevents MCCS write commands through independent, read only emulated EDID EEPROMs. The TOE processor reads the EDID data from the monitor and then individually writes this EDID data to each independent emulator during power up. All changes in display after the EDID read/write process are ignored. There are switches in the internal circuitry to prevent connected computers from writing to their respective EDID emulators. The TOE will reject invalid EDID display devices.

The proprietary *Raritan PP3.0 Secure KVM Isolation Document* contains detailed descriptions and dataflow figures supporting the data flow isolation descriptions above. This document was provided by Raritan for Common Criteria certification as assurance that the TOE can be relied upon to provide proper isolation between connected computers as defined by the PP Annex J.

6.2.2 Subset information flow control (FDP_IFC.1(2)) and Simple security attributes (FDP_IFF.1(2)) Data Isolation

The TOE supported peripheral and connected port types include USB keyboard and mouse, DVI-I, analog audio output, and user authentication devices only. The TOE does not allow any other user data transmission to or from any other external entities. The TOE only recognizes those peripherals with an authorized interface type as described in Section 6.2.3 Table 5. All other peripherals shall be denied.

The TOE enforces data isolation on the following data types:

a. User keyboard key codes;

b. User pointing device commands;

c. Video information (User display video data and display management data);

d. Audio output data; and

e. User authentication device data.

Keyboard, Mouse, Video, Audio, and USB CAC reader port are switched together.

During normal TOE operation, the TOE only permits user entered keyboard key codes, and user input mouse commands to flow between the TOE keyboard and mouse peripheral device interfaces and the TOE selected computer interface. No flow is permitted between the selected computer interface and the TOE keyboard and mouse peripheral device interfaces. This data separation is described in Section 6.2.1. The TSF denies data flow other than keyboard entries and mouse reports between the TOE keyboard and mouse peripheral device interfaces and the TOE selected computer interface.

The TOE denies power flow between the selected computer interface and TOE keyboard and mouse peripheral device interfaces; and denies information flow from the TOE selected computer interface to the TOE keyboard and mouse peripheral device interface.

The TOE denies analog audio information flow between the TOE selected computer audio interface and the user audio device peripheral interface when a microphone peripheral device is intentionally or unintentionally connected to the TOE audio peripheral device interface. The TOE enforces unidirectional information flow and denies bidirectional information flow between the TOE selected computer audio interface and the user audio device peripheral interface. This data separation is described further in Section 6.2.1.

The TOE denies any information flow from the TOE display peripheral device interface and the selected computer interface with the exception of EDID information that may be passed once at TOE power up or after recovery from TOE reset. The TOE denies an information flow between the selected computer display interface and the TOE display peripheral device interface on the EDID channel. This data separation is described further in Section 6.2.1.

The only way to control channel selection is via the TOE's internally illuminated push-buttons. This is to prevent unintended switching of the TOE or user confusion of the current TOE state. There are no other interfaces to control the TOE.

The TOE only supports user authentication devices switched by the TOE (such as Smartcard and CAC readers), but does not integrate or emulate any authentication device. The TOE's CAC USB controller uses SRAM memory to store USB device information (PID/VID) during CAC device identification. After the micro controller has read this information, the SRAM is erased. The SRAM is also erased if anti-tampering is triggered, or power is disconnected from the device. No flash ROM is dedicated to the CAC USB controller to save any data.

The TOE denies data flow of user authentication device data transiting the TOE to non-selected TOE computer interfaces; and does not share the user authentication device computer interfaces with any other TOE peripheral function interface (keyboard, mouse etc.). The TOE does not emulate the user authentication device function. The power source of USB card reader is provided by the TOE and is isolated from other circuitry. Switches are connected to each USB Device Controller and CAC Reader for micro-controllers to manipulate the power flow. Inserting a card reader at the CAC port will activate the verification process of the USB host controller's dedicated micro-controller. If the card reader is in the white list (i.e., pass the CAC authentication), the micro-controller will switch the CAC multiplexer to computer channel (Figure 1) and reboot the card reader; if not, the CAC multiplexer stays at micro-controller channel, so CAC data could not be passed to computers. When port switching, the TOE disables the power of the card reader for at least one second, and reboots the card reader when the port switching is done. The TOE has an electrically/logically isolated USB/CAC port for each connected computer that remains isolated when TOE is not powered. TOE rejects all unauthorized USB/CAC devices and provides USB/CAC LED indication when the port being used by an authorized device (light green indicator when authorized), unauthorized device (light red indicator), or unused (off).

6.2.3 Subset access control (FDP_ACC.1) and Security attribute based access control (FDP_ACF.1)

The TOE allows the following devices for each peripheral port type:

Console Port	Authorized Devices	Authorized Protocol
Keyboard	Wired keyboard and keypad without internal USB hub or composite device functions.	USB 1.1/2.0
Display	Display, Video or KVM extender	DVI-I
Mouse/Point Device	Wired mouse or trackball without internal USB hub or composite device functions.	USB 1.1/2.0
Audio Out	Analog amplified speakers Analog headphones	Analog audio output
User Authentication Device	Smartcard, CAC reader	USB 1.1/2.0

Table 5 Supported Authorized Devices/Protocols

As indicated by the table above, the TOE does not support PS/2 keyboard and mouse console ports.

The authorized authentication devices are identified using an administrator configured white list and the TOE allows black list configuration for user authentication device profiling (filtering).

Hub and composite devices are not supported. The TOE's USB keyboard and USB mouse console ports are interchangeable but cannot be combined into one port (composite USB device). Embedded Keyboard LEDs are not supported by the TOE.

Each CAC port contains its own dedicated and proprietary USB Hub chips or USB data re-generator ensuring data isolation between each CAC channel and corresponding computer.

The TOE's firmware is programmed to accept basic keyboard and mouse USB devices only. Wireless keyboard and mouse are not allowed by the TOE. Only USB host peripheral devices are allowed by TOE keyboard and mouse host emulators. Basic USB 1.1/2.0 devices are authorized as valid endpoints by the TOE. All other devices (including USB hubs) will be rejected by the TOE.

Inside the TOE, the keyboard and mouse peripherals are switched together from one isolated connected computer to the next isolated connected computer. There are no user interfaces/configuration that allows keyboard and mouse functionality to be split into separate serial data channels.

The TOE provides Administrator Functions that include CDF configuration. Administrators can use the Configuration Menu to Configure CAC filters. Configuration options are limited to allowing or blocking currently connected device on all ports; and resetting the Admin CAC Allow and Block lists. The blacklist and whitelist defined by this function always supersedes the filtering list created by the Port Authentication Utility.

The Port Authentication Utility tool is used to define or modify a whitelist and/or blacklist for the TOE. The Port Authentication Utility is installed on a secure source computer using an installation Wizard. This secure source computer is for management only, and has its own monitor, keyboard, and mouse connected for installation and operation.

The Port Authentication Utility has its own default password and like the password for the TOE Administrator Logon function should be changed after first logon. Guidance instructs the administrator not to use the same password as was used for the TOE Administrator Logon functions.

After the secure source computer is connected to the TOE and the authorized administrator has authenticated to the utility, the administrator uses the utility GUI commands to configure the filter list. A filtering rule is defined by USB (Base) Class ID, Sub-Class, Protocol, VID, and PID of a USB device. For example, a Base Class ID of a Smart Card device is 0Bh. By completing the Class ID, Sub-Class, Protocol, VID and PID field of a filtering rule, the administrator can assign this filtering rule to a Blacklist or to a Whitelist to block or allow a device.

After configuring the filter list, the administrator then logs onto the TOE and the filter list is uploaded to the Secure KVM TOE. The updated Filtering list will take effect after removing the Secure KVM from the installation and performing a power cycle the Secure KVM. The Secure KVM allows or blocks USB devices on the USB CAC Port based on the updated Blacklist/Whitelist.

6.2.4 Subset Residual information protection (FDP_RIP.1(1), FDP_RIP.1(2))

The TOE ensures that any previous information content of a resource is made unavailable upon the deallocation of the resource from the TOE computer interfaces immediately after a TOE switch to another selected computer; and on start-up of the TOE.

User data held in any TOE component with non-volatile memory is made unavailable to any TOE computer interface upon the next TOE power on. User keyboard and mouse buffers in any TOE component are automatically cleared and made unavailable to the next connected TOE computer interface when the TOE is switched to a different computer.

The TOE provides two functions to delete TOE stored configuration and settings.

After logging in, authorized administrators can use the Reset to Factory Default management function (not to be confused with the front panel reset button). When a successfully authenticated authorized Administrator performs Reset to Factory Default, all settings previously configured by the Administrator (such as USB device whitelist/blacklist) will be cleaned and reset to factory default settings. Once the Reset KVM to Default function has been completed, the Secure KVM will terminate the Administrator Logon mode, purge keyboard/mouse buffer, and power cycle the Secure KVM automatically. After a successful self-test, the KVM port focus will be switched to Port1, and the CAC function of each port will be set to factory default (enabled).

The TOE also provides non-administrative users a front panel Reset button allowing the user to delete TOE stored configuration and settings. When performing the reset function by pressing the Reset button for more than 5 seconds, purges the Keyboard/Mouse buffer is purged; the CAC enable/disable feature is restored to the factory default 'enabled' state; and the switch performs a self-test and switches to Port 1. CDF configured by Administrator, logs, Administrative tasks, or other secure functions are not affected by the front panel Reset function.

The proprietary Letter of Volatility is provided as a separate document. The document identifies the TOE components that have non-volatile memory and provides details of the memory and its use.

6.3 Identification and Authentication

Authentication is required to perform administrative functions such as configuring the user authentication device filtering (CDF) whitelist and blacklist. The authorized administrator is identified and authenticated through the logon function. The authorized administrator logs on by entering the Administrator Logon mode as described in the administrator guide and providing a valid password. The administrator guide states that the administrator must change the password after the first successful logon.

The logon function provides authentication failure handling. With 3 (three) failed attempts to logon, the Administrator Logon mode will be terminated automatically. Access to Administrator Logon mode will be blocked for 15 minutes. With 9 (nine) failed attempts to logon, the Secure KVM becomes permanently inoperable. Authentication failure handling is not evaluated.

The Identification and Authentication function satisfies the following security functional requirements:

- FIA_UAU.2—the TOE requires administrators to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
- FIA_UID.2—the TOE requires administrators to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.4 Security Management

The TOE provides management functions to configure the user authentication device filtering (CDF), to return the device to factory setting, and to change the administrator password; and restricts access to these management functions to the authorized administrator.

6.4.1 Management of security functions behavior (FMT_MOF.1)

The TOE restricts the management functions such as the ability to modify the user authentication device filtering (CDF) whitelist and blacklist to the authorized administrator. The authorized administrator must successfully authenticate by providing a valid password.

6.4.2 Specification of Management Functions (FMT_SMF.1)

The TOE provides security management functions to configure the user authentication device filtering (CDF), to return the device to factory setting, view audit records, and to change the administrator password.

The TOE provides the authorized administrator with the ability to view audit records and to assign whitelist and blacklist definitions for the TOE user authentication device qualification function. Once successfully authenticated, the Administrator can choose to add, edit, or remove a device to the Whitelist/Blacklist.

If a device is on the white list, the TOE considers the device as authorized. Otherwise, if the device is on the black list it is considered unauthorized. If a device has been added to both black list and white list, the USB device will be considered a blacklisted device.

The TOE provides a security management function to Reset to Factory Default (not to be confused with the front panel reset button). When a successfully authenticated authorized Administrator performs Reset to Factory Default, settings previously configured by the Administrator (such as USB device whitelist/blacklist) will be cleaned and reset to factory default settings. Once the Reset KVM to Default function has been completed, the Secure KVM will terminate the Administrator Logon mode, purge keyboard/mouse buffer, and power cycle the Secure KVM automatically. After a successful self-test, the KVM port focus will be switched to Port1, and the CAC function of each port will be set to factory default (enabled).

The Reset KVM to Default does not affect or erase Log data nor does it affect the previously changed Administrator password.

6.4.3 Security roles (FMT_SMR.1)

The TOE maintains a single administrator role. All other users are non-administrative users. A properly authenticated administrator has the ability to view audit records, Reset to factory defaults, change password, and configure whitelist and blacklist definitions for the TOE user authentication device qualification function. Users without an administrator role cannot use these function and are not required to authenticate.

6.5 Protection of the TSF

In order to mitigate potential tampering and replacement, the TOE is designed to ensure that any replacement may be detected, any physical modification is evident, and any logical modification may be prevented. Access to the TOE firmware, software, or its memory via its accessible ports is prevented. No access is available to modify the TOE or its memory. To mitigate the risk that a potential attacker will tamper with a TOE and then reprogram it with altered functionality, the TOE software is contained in one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly. The TOE's operational code is not upgradeable through any of the TOE external or internal ports.

The TOE has two tamper-evident labels attached to each side of the TOE. Each label is printed with the TOEs unique product serial number and the vendor's specific design. The labels are clearly visible to the user and any attempt to open the enclosure sufficient to gain access to internal components will change the labels to a tampered state.

6.5.1 Passive detection of a physical attack (FPT_PHP.1) and Resistance to physical attack (FPT_PHP.3)

Any attempt to open the TOE will trigger a Tamper Detection switch. The Tamper Detection switch inside the TOE is powered by a dedicated battery. This switch will be triggered once the enclosure cover of the TOE is opened. Once the Tamper Detection switch is triggered, the green LED lights on the front panel will continuously flash. All TOE functions and the TOE itself are disabled. Operations cannot be restored and since the ROM inside the TOE is OTP (One time programmable), there is no way for the user to reset or recover the system once the firmware runs into the disable loop after the switch is triggered. The TOE has to be returned to Raritan. Raritan will either change a new main board and then send back to the customer or exchange with new hardware.

6.5.2 Failure with preservation of secure state (FPT_FLS.1)

The TSF preserves a secure state by disabling the TOE when the following types of failures occur: failure of the power on self-tests, and failure of the anti-tampering function.

6.5.3 TSF testing (FPT_TST.1)

The TOE runs a suite of self-tests during initial startup and upon reset button activation that includes:

a) basic integrity test of the TOE hardware and firmware (memory testing and firmware checksum compare);

b) a test of the computer interfaces' isolation functionality (for example, generating data flow on one port and checking that it is not received on another port (port isolation test));

c) a test of the user interface – in particular tests of the user control mechanism (e.g. checking that the front panel push-buttons are not jammed (key stuck test)); and

d) a test of the anti-tampering mechanism - the TOE will verify if the tamper detection switch is triggered..

The TOE ensures a shutdown upon a self-test failure or a failed anti-tampering function. In case of a failed anti-tampering function or self-test failure, front panel LEDs will indicate the self-tests failure status, the firmware will ensure that connections of all interfaces are disabled, and the TOE will be permanently disabled.

A pre-defined combination of the Port and CAC LEDs indicate the cause to the failure. For a Button jam failure, the Port of the jammed button port will flash green. If any of the other self-tests fail; all Port LEDs continually flash green indicating that the unit is disabled. A button jam self-test failure may be recoverable if the button jam is temporary. Guidance documentation instructs the user to verify the KVM installation, pushbuttons, and power cycle the Secure KVM Switch in order to attempt to recover. This is the only self-test that may be recoverable. If the button jam is permanent (for example, the pushbutton is broken and truly stuck), the KVM remains disabled since it fails the button jam self-test. If the self-test failure remains, users are instructed to stop using the Raritan Secure KVM Switch immediately, remove it from service and contact their Raritan dealer. The TOE generates an audit record for each failed self-test.

Successful execution of the self-tests demonstrate the correct operation of the TSF. The TOE provides users with the capability to verify the integrity of the TSF functionality. During the self-tests, all Port LEDs will turn on and off. When the self-tests have been successfully executed the KVM focus will be switched to Port 1 (Port 1 Port LED lights GREEN) and the event will be logged.

The TOE's architecture ensures that when the TOE is powered off or if anti-tampering is triggered, the peripheral devices will no longer function. All video signals are isolated electrically and logically from the TOE. The emulated EDID EEPROMs are still powered by their respective computers, but cannot communicate with the TOE due to hardware component isolation. The TOE uses a relay to isolate the audio input ports from all internal TOE circuitry. The TOE contains an internal battery which is non-replaceable and cannot be accessed without opening the device enclosure. The TOE's anti-tampering function is triggered when the battery is damaged or exhausted, permanently disabling the switch.

6.6 TOE Access

6.6.1 User Authentication Device Reset and Termination (FTA_ATH_EXT.1)

The CAC functionality is not emulated; and the power source of USB card reader is provided by TOE and is isolated from other circuitry. External power sources are prohibited per applicable user guidance. When port switching, TOE will disable the power of the card reader for at least one second, and reboot the card reader when the port switching is done. The output capacitance of the TOE is about 10µF. For a typical user authentication device, voltage decreases from 5V to 2V in much less than 1s. The time is at the millisecond level.

6.6.2 Continuous Indications (FTA_CIN_EXT.1)

All push-buttons for selecting computer channels are internally illuminated via LEDs on the front panel of the TOE. There is one LED interface with two LED indicators (either white or green) located above each pushbutton. The white LED indicator of a specific port lights when there is a computer connected on that port and powered on. Once a specific computer is selected by the user which means the shared set of peripherals switches to that port of computer has been selected, the green LED indicator lights. On models that have SmartCard readers, there is a third LED which is red to indicate a warning and green during normal operation. During operation, the front panel LED indicators cannot be turned off by the user. The LED indicators illuminate upon TOE power up including after the reset function has been initiated. Each time the TOE powers up, Port 1 will always be selected and the LED of Port 1 will be illuminated.

7. Protection Profile Claims

This ST is conformant to the *Protection Profile for Peripheral Sharing Switch (PSS), Version 3.0, 13 February 2015* [PSS] and includes the following optional SFRs: FAU_GEN.1, FDP_RIP.1(2), FIA_UID.2, FIA_UAU.2, FMT_MOF.1, FMT_SMF.1, and FMT_SMR.1.

As explained in Section 3, Security Problem Definition, the Security Problem Definition of the [PSS] has been included in this ST by reference.

As explained in Section 4, Security Objectives, the Security Objectives of the [PSS] have been included by reference from the [PSS] in this ST including all of the optional objectives except: O.USER_AUTHENTICATION_TERMINATION.

The following table identifies all the Security Functional Requirements (SFRs) in this ST. Each SFR is drawn from the [PSS]. The only operations performed on the SFRs drawn from the [PSS] are assignment and selection operations.

The following table identifies the SFRs that are satisfied by the TOE.

Requirement Class	Requirement Component	Source
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	[PSS]
FDP: User Data Protection	FDP_IFC.1(1): Subset information flow control	[PSS]
	FDP_IFF.1(1): Simple security attributes	[PSS]
	FDP_IFC.1(2): Subset information flow control	[PSS]
	FDP_IFF.1(2): Simple security attributes	[PSS]
	FDP_ACC.1: Subset access control	[PSS]
	FDP_ACF.1: Security attribute based access control	[PSS]
	FDP_RIP.1(1): Subset Residual information protection	[PSS]
	FDP_RIP.1(2): Subset Residual information protection (Restore factory defaults)	[PSS]
FIA: Identity and	FIA_UAU.2: User identification before any action	[PSS]

Requirement Class	Requirement Component	Source
authentication	FIA_UID.2: User identification before any action	[PSS]
FMT: Security management	FMT_MOF.1: Management of security functions behavior	[PSS]
	FMT_SMF.1: Specification of Management Functions	[PSS]
	FMT_SMR.1: Security roles	[PSS]
FPT: Protection of the TSF	FPT_PHP.1: Passive detection of a physical attack	[PSS]
	FPT_PHP.3: Resistance to physical attack	[PSS]
	FPT_FLS.1: Failure with preservation of secure state	[PSS]
	FPT_TST.1: TSF testing	[PSS]
FTA: TOE Access	FTA_ATH_EXT.1: User authentication device reset	[PSS]
	FTA_CIN_EXT.1: Extended: Continuous Indications	[PSS]

Table 6 SFR Protection Profile Sources

8. Rationale

This security target includes by reference the [PSS] Security Problem Definition, Security Objectives, and Security Assurance Requirements. The security target makes no additions to the [PSS] assumptions. [PSS] security functional requirements have been reproduced with the Protection Profile operations completed. Operations on the security requirements follow [PSS] application notes and assurance activities. Consequently, [PSS] rationale applies but is incomplete. The TOE Summary Specification rationale below serves to complete the rationale required for the security target.

8.1 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 7 Table 7 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security Audit	**User Data Protection**	**Identification and Authentication**	**Security Management**	**Protection of the TSF**	**TOE Access**

	Security Audit	User Data Protection	Identification and Authentication	Security Management	Protection of the TSF	TOE Access
FAU_GEN.1	X					
FDP_IFC.1(1)		X				
FDP_IFF.1(1)		X				
FDP_IFC.1(2)		X				
FDP_IFF.1(2)		X				
FDP_ACC.1		X				
FDP_ACF.1		X				
FDP_RIP.1(1)		X				
FDP_RIP.1(2)		X				
FIA_UAU.2			X			
FIA_UID.2			X			
FMT_MOF.1				X		
FMT_SMF.1				X		
FMT_SMR.1				X		
FPT_PHP.1					X	
FPT_PHP.3					X	
FPT_FLS.1					X	
FPT_TST.1					X	
FTA_ATH_EXT.1						X
FTA_CIN_EXT.1						X

Table 7 Security Functions vs. Requirements Mapping