IOGEAR Secure KVM Switch Series

Security Target

Version 1.0
January 19, 2018

Prepared for:

15365 Barranca Pkwy,
Irvine, CA 92618

Prepared by:

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 IOGEAR Secure KVM Switch Series provided by IOGEAR.

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 –IOGEAR Secure KVM Switch Series Security Target

ST Version – Version 1.0

ST Date – January 19, 2018

TOE Identification – IOGEAR Secure KVM Switch Series

The following table identifies the model numbers per configuration. The firmware version for all models is v1.1.101.

Configuration		2-Port	4-Port	8-Port
DisplayPort	Single Head	GCS1412TAA3	GCS1414TAA3	GCS1418TAA3
	Dual Head	GCS1422TAA3	GCS1424TAA3	GCS1428TAA3
HDMI	Single Head	GCS1312TAA3	GCS1314TAA3	GCS1318TAA3
	Dual Head	GCS1322TAA3	GCS1324TAA3	GCS1328TAA3
DVI	Single Head	GCS1212TAA3	GCS1214TAA3	GCS1218TAA3
	Dual Head	GCS1222TAA3	GCS1224TAA3	GCS1228TAA3

Table 1 IOGEAR Secure KVM Switch TOE Models

TOE Developer – IOGEAR

Evaluation Sponsor – IOGEAR

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, 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
  - TD0086 - DisplayPort to HDMI Conversion Functionality, published date 03/10/2016

- 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 the text in blue is removed in the ST. The applicable conditions are identified using the conventions identified above.
- 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.
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.
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.
KVM	A PSS that switches the Keyboard, Video and Mouse.
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 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.

1.4.2 Abbreviations and Acronyms

AUX	Display Port Auxiliary Channel
CAC	Common Access Card
CCTL	Common Criteria Test Lab
DP	Display Port
DVI	Digital Visual Interface
EDID	Extended Display Identification Data
EEPROM	Electrically erasable programmable read-only memory
FIPS	Federal Information Processing Standards
HD	High Definition
HDMI	High Definition Multimedia Interface
HEAC	HDMI Ethernet Audio Control

HID	Human Interface Device
IP	Internet Protocol
IT	Information Technology
KM	Keyboard, Mouse
KVM	Keyboard, Video and Mouse
LED	Light-Emitting Diode
PC	Personal Computer
PS/2	IBM Personal System/2 series
PSS	Peripheral Sharing Switch
SP	Special Publication
SFP	Security Function Policy
SPF	Shared Peripheral Functions
USB	Universal Serial Bus

2. TOE Description

The TOE is the IOGEAR Secure KVM Switch Series. Each of the eighteen models identified in Section 1.1 is a Peripheral Sharing Switch device that allows for the connection of a mouse, keyboard, user authentication device such as smart card or CAC reader (optional), speaker (optional), and one or two video displays (depending on specific device type) to the Secure KVM Switch, which is then connected to 2, or up to 8 separate computers (again depending on specific device type). The user can then securely switch the connected peripherals between any of the connected computers while preventing unauthorized data flows or leakage between computers. User switching is accomplished using a push button on the front of the device.

2.1 TOE Overview

The IOGEAR Secure KVM Switches provide KVM (USB Keyboard/Mouse, PS/2 Keyboard/Mouse, DVI-I, HDMI, or DisplayPort Video (depending on model)) switch functionality by combining a 2/4/8 port KVM switch, an audio output port with Speaker, and a smart card/CAC port. The TOE is classified as a "Peripheral Sharing Switch" (KVM device) in the Protection Profile. Hardware and firmware components are included in the TOE.

2.2 TOE Architecture

The IOGEAR Secure KVM series are KVM switches with the following characteristics:

- 2/4/8 port USB HDMI single and dual display for DisplayPort (6 devices)
- 2/4/8 port USB HDMI single and dual display for HDMI (6 devices)
- 2/4/8 port USB DVI single and dual display for DVI (6 devices).

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 (optional), and one or two video displays (depending on specific device type) to the Secure KVM Switch, which is then connected to 2, up to 4, or up to 8 separate computers (again depending on specific 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 bright orange 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 or HDMI for the video display(s). The Secure KVM Switch products additionally support PS/2 keyboard and mouse connections. 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, depending on device type, the following video connections from the connected computers: DisplayPort; HDMI; and DVI. The Secure KVM Switch products supporting DisplayPort convert the DisplayPort video signal to HDMI for output to the connected video display(s). The Secure KVM Switch products also support audio output connections from the computers to a connected audio output device. Only speaker connections are supported and the use of an analog microphone or line-in audio device is prohibited. The tables below identify the interfaces of the Secure KVM console and computer ports according to model number.

Item	Model No.	Console Video Output Interface			Console Keyboard		Console Mouse		Console Audio output	Console CAC Reader
		DisplayPort	HDMI	DVI-I	USB 1.1/2.0	PS/2	USB 1.1/2.0	PS/2	Analogue Audio output (Speaker)	USB 1.1/2.0
2-Port										
1	GCS1412TAA3		•		•	•	•	•	•	•
2	GCS1422TAA3		•		•	•	•	•	•	•
3	GCS1312TAA3		•		•	•	•	•	•	•

4	GCS1322TAA3		•		•	•	•	•	•	•
5	GCS1212TAA3			•	•	•	•	•	•	•
6	GCS1222TAA3			•	•	•	•	•	•	•
4-Port										
7	GCS1414TAA3		•		•	•	•	•	•	•
8	GCS1424TAA3		•		•	•	•	•	•	•
9	GCS1314TAA3		•		•	•	•	•	•	•
10	GCS1324TAA3		•		•	•	•	•	•	•
11	GCS1214TAA3			•	•	•	•	•	•	•
12	GCS1224TAA3			•	•	•	•	•	•	•
8-Port										
13	GCS1418TAA3		•		•	•	•	•	•	•
14	GCS1428TAA3		•		•	•	•	•	•	•
15	GCS1318TAA3		•		•	•	•	•	•	•
16	GCS1328TAA3		•		•	•	•	•	•	•
17	GCS1218TAA3			•	•	•	•	•	•	•
18	GCS1228TAA3			•	•	•	•	•	•	•

Table 2 IOGEAR Secure KVM Switch Console Interfaces and TOE Models

Item	Model No.	Computer Video Input Interface			Computer Keyboard / Mouse		Computer Audio Input	Computer CAC Input
		DisplayPort	HDMI	DVI-I	USB 1.1/2.0	PS/2	Analogue Audio Input (Speaker)	USB 1.1/2.0
2-Port								
1	GCS1412TAA3	•			•		•	•
2	GCS1422TAA3	•			•		•	•
3	GCS1312TAA3		•		•		•	•
4	GCS1322TAA3		•		•		•	•
5	GCS1212TAA3			•	•		•	•
6	GCS1222TAA3			•	•		•	•
4-Port								
7	GCS1414TAA3	•			•		•	•
8	GCS1424TAA3	•			•		•	•
9	GCS1314TAA3		•		•		•	•
10	GCS1324TAA3		•		•		•	•
11	GCS1214TAA3			•	•		•	•
12	GCS1224TAA3			•	•		•	•
8-Port								
13	GCS1418TAA3	•			•		•	•
14	GCS1428TAA3	•			•		•	•
15	GCS1318TAA3		•		•		•	•
16	GCS1328TAA3		•		•		•	•
17	GCS1218TAA3			•	•		•	•
18	GCS1228TAA3			•	•		•	•

Table 3 IOGEAR Secure KVM Switch TOE Models and Computer Interfaces

The IOGEAR Secure KVM products implement a secure isolation design for all 2/4/8-Port and DVI/HDMI/DisplayPort models to share a single set of peripheral components. The Secure KVM Switch products support the following peripheral port types: USB keyboard; USB mouse; PS/2 mouse and keyboard; USB authentication device (CAC reader, smart card); audio output; and (depending on device type) DVI, or HDMI video. Some TOE models accept DisplayPort signals at the computer interface and convert the signals to HDMI signals at the peripheral interface. 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. DisplayPort video from the selected computer is converted to HDMI for communication with the connected video display and the AUX channel is monitored and converted to video.

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 the internal TOE keyboard and mouse buffers.

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

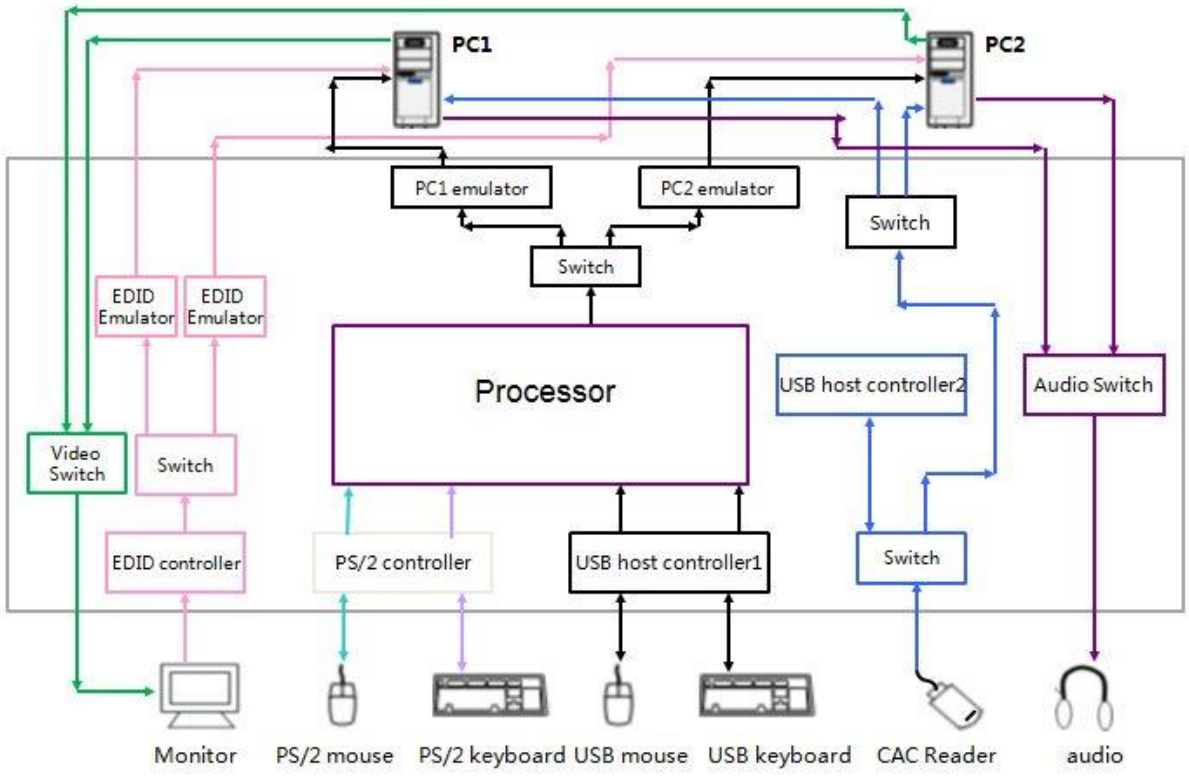

Figure 1 Simplified block diagram of a 2-Port KVM TOE

The data flow of USB and PS/2 Keyboard/Mouse is controlled by two types of host controller for console HID keyboard and pointing devices: USB host controller and PS/2 host controller. Details of the data flow architecture are provided in the proprietary Secure KVM Isolation Document. All Keyboard and Mouse connections are filtered first, and only authorized devices will be allowed. The TOE emulates data from authorized USB or PS/2 Keyboard and Mouse to USB data for computer sources.

The TOEs proprietary design ensures there is no possibility of data leakage from a user's peripheral output device to the input device; ensures that no unauthorized data flows from the monitor to a connected computer; and unidirectional buffers ensure that the audio data can travel only from the selected computer to the audio device. There is no possibility of data leakage between computers or from user peripheral input device to a non-selected computer. Each connected computer has its own independent Device Controller, power circuit, and EEPROM. Additionally, keyboard and mouse are always switched together.

All Secure KVM Switch products feature hardware security mechanisms including tamper-evident labels, always active chassis-intrusion detection, and tamper-proof hardware construction, while software security includes restricted USB connectivity (non-Human Interface Devices (HIDs) are ignored when switching), an isolated channel per port that makes it impossible for data to be communicated between computers, and automatic clearing of the keyboard and mouse buffer.

The IOGEAR Port Authentication 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.

A detailed description of the TOE security features can be found in Section 6 (TOE Summary Specification).

2.2.1 Physical Boundaries

The TOE includes the hardware models identified in Section 1.1 along with embedded firmware v1.1.101 and corresponding documentation identified in Section 2.3 below.

The peripheral devices: HDMI, DVI-I Monitor, USB Keyboard, USB Mouse, PS/2 Keyboard/Mouse, Audio output (e.g. Speakers), smart card/CAC reader and the Host Computers are in the operational environment.

2.2.2 Logical Boundaries

This section summarizes the security functions provided by IOGEAR 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, 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 USB keyboard; USB mouse; PS/2 mouse and keyboard; USB authentication device (CAC reader and smart card); audio output; and (depending on device type) DVI, or HDMI. video. Some TOE models accept DisplayPort signals at the computer interface and convert the signals to HDMI signals at the peripheral interface.

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 the 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 device filtering (CDF) whitelist and blacklist. The authorized administrator must logon by providing a valid password.

2.2.2.4 Security Management

The TOE supports configurable device filtration (CDF). 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 after 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 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:

- *IOGEAR 2/4/8-Port USB DVI/HDMI/DisplayPort, Single/Dual View Secure KVM Switch Administrator's Guide 2017*
- *IOGEAR 2/4/8-Port USB DVI/HDMI/DisplayPort, Single/Dual View Secure KVM Switch User Manual 2017*
- *IOGEAR 2/4/8-Port USB DVI/HDMI/DisplayPort, Single/Dual View Secure KVM Switch Port Authentication Utility Guide 2017*
- *IOGEAR 2/4/8-Port USB DVI/HDMI/DisplayPort, Single/Dual View Secure KVM Switch Admin Log Audit Code, IOGEAR Proprietary Document 2017*
    - **Note:** The Admin Log Audit Code document is provided only to registered customers.

TOE Documentation:

- *IOGEAR PP3.0 Secure KVM Isolation Document v1.3, 9/28/2017 (proprietary)*
    - **Note**: The IOGEAR 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.

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 IOGEAR Secure KVM Switch Series supports KVM (USB and PS/2 Keyboard/Mouse, DVI, HDMI or DisplayPort Video) switch functionality by combining a 2/4/8 port KVM switch, an audio output port, and a USB authentication device (CAC port and smart card). 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] 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] has presented a Security Objectives statement appropriate for peripheral sharing switches. Consequently, the [PSS] 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, 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 the TOE.

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

Requirement Class	Requirement Component
	FPT_FLS.1: Failure with preservation of secure state
	FPT_TST.1: TSF testing
FTA: TOE Access	FTA_ATH_EXT.1: User authentication device reset
	FTA_CIN_EXT.1: Continuous Indications

Table 4 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 [

- **assignment of whitelist and blacklist definitions for the TOE user authentication device qualification function,**
- **Reset to Factory Default, and**
- **password changes**.

].

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 [
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. ***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;***
10. ***The TSF shall deny all AUX Channel information flows other than link negotiation, link training and EDID reading;***
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) 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)

5.2.3.1 User authentication before any action (FIA_UAU.2)

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.

5.2.3.2 User identification before any action (FIA_UID.2)

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.

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 Security Administrators][1].

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 logs, 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:

[1] TD0251 has modified this SFR.

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].

5.2.6 TOE Access (FTA)

5.2.6.1 User authentication device reset (FTA_ATH_EXT.1)

FTA_ATH_EXT.1.1 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.1.1 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[2]

Table 5 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

[2] This AA is added per TD0083.

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). 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 non-critical. The Log Data Area displays the critical and non-critical Log data. Each logged event is recorded with Date, Time, a code that indicates the type of event and the outcome (success or failure) of the event. The types of events recorded and identified in the code include Administrator Logon/Logoff events; Administrator password change events; Administrator configuration events: Reset to Factory Default and Device filter configuration events; and power cycle events. During normal operation, the TOE provides administrator access to all audit records. IOGEAR's assistance is required to read audit records from an inoperable switch.

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 TOE stores a maximum of twelve critical events, one for each category code. 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).

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, PS/2 Keyboard/Mouse, HDMI, monitor, DVI-I Video, analog audio speakers, and USB smart card / CAC readers. The TOE accepts DisplayPort signals (monitors) at the computer interface and converts the signals to HDMI signals (monitors) at the peripheral interface. All other devices are rejected. . Refer to the two interface tables in Section 2.2 for details on TOE computer peripherals and connected computer port interfaces for each specific TOE model.

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 proprietary 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 Secure KVM Switch products support the following peripheral and connected port types: USB keyboard; USB mouse; PS/2 mouse and keyboard; USB authentication device (CAC reader and smart card); audio input/output; and (depending on device type) DVI, HDMI or DisplayPort video. The TOE converts DisplayPort signals at the computer interface to HDMI signals at the peripheral interface. Additionally, there are interfaces for AC power, reset (button) and LED indicators. The LEDs consist of Video, Num Lock, Cap Lock, Scroll Lock, power LEDs, and Port / CAC LEDs. The Video LED lights green when the video connection is up and running. The Video LED flashes when a non-qualified monitor is connected. The Num Lock, Cap Lock, and Scroll Lock are disabled. The Port / CAC LEDs indicate Port/CAC reader selection / connection status. All LEDs are located on the front panel except the Video LED that is located on the back panel. 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.

Each supported peripheral has its own dedicated data path. Both USB and PS/2 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.

DisplayPort video from the selected computer is converted to HDMI for communication with the connected video display and the AUX channel is monitored and converted to video. The data flow of USB and PS/2 Keyboard/Mouse is controlled by two types of host controller for console HID keyboard and pointing devices: USB host controller and PS/2 host controller. The USB host controller routes data by USB HID, while the PS/2 host controller routes data by PS/2-interfaced keyboard and mouse. All Keyboard and Mouse connections are filtered first, and only authorized devices will be allowed. The TOE emulates data from authorized USB or PS/2 Keyboard and Mouse to USB data for computer sources.

The TOE implements individual circuitry for both output data flow (e.g. video signals, user authentication device) and input data (e.g. HID data). This ensures there will be no possibility of data leakage from user peripheral output device to input device. The video EDID read procedure data flow path is only activated during EDID read transactions when the TOE boots and a connected monitor is detected. When the read/write transactions are finished, the micro-controller disables the EDID switch. This ensures there will be no unauthorized data flow from the monitor to a connected computer. For audio data output, the unidirectional buffers make sure that the audio data can travel only from the selected computer to the audio device. There is no possibility of data leakage between computers or from user peripheral input device to non-selected computer. Each connected computer has its own independent Device Controller, power circuit, and EEPROM. The keyboard, mouse, video, audio, and USB smart card /CAC reader ports are always switched together using a push button on the front of the device. As such, the keyboard and mouse are always switched together and there are no options to switch peripherals independently from the keyboard and mouse.

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

The TOE supported authorized devices and protocols for the PSS Console Ports are identified in the table below. Note that DisplayPort-interfaced TOE models convert DisplayPort supported protocols (version 1.1 or higher with filtration) to the HDMI protocol. Since the TOE converts DisplayPort signals at the computer interface to HDMI signals at the peripheral interface, DisplayPort is not identified as an authorized protocol for the PSS console port.

TOE models with HDMI source are capable of embedding digital audio into digital video data transmission. DisplayPort-interfaced TOEs support digital audio embedded in the video. The DisplayPort signal is converted to HDMI, and both digital audio and Video is allowed to monitor. Digital audio embedded in DisplayPort Video will be kept with HDMI video. DVI Secure KVM Models do not have the ability to embed digital audio into digital video data transmission.

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 below and all other peripherals will be denied. Specifically the TOE supports the following:

PSS Console Port	Authorized Devices	Authorized Protocol
Keyboard	Wired keyboard and keypad without internal USB hub or composite device functions.	USB 1.1/2.0, PS/2
Display	Display, Video or KVM extender	HDMI, DVI-I
Mouse/Point Device	Wired mouse or trackball without internal USB hub or composite device functions.	USB 1.1/2.0, PS/2
Audio Out	Analog amplified speakers, digital audio embedded inside the video	Analog audio output
User Authentication Device	Smartcard, CAC reader	USB 1.1/2.0

Table 6 Supported protocols by port

As previously stated, 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 power source of USB card reader is provided by the TOE and is isolated from other circuitry. Inserting a card reader at the smart card/CAC port will activate the filtering process of the USB host controller's dedicated micro-controller. If the card reader is in the whitelist (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 video auxiliary channel (AUX) path blocks information flows other than the minimal set required to establish the video link. Unauthorized DisplayPort transactions are prevented by disassembling the DisplayPort AUX channel transactions to block all unauthorized transactions. The TOE video function filters the AUX channel by converting it to EDID only. DisplayPort video is converted into HDMI video stream. Monitor's EDID is, through EDID channel, read, filtered, and sent to Port's EDID EEPROM for EDID emulation.

All AUX channel threats are mitigated through the conversion from DisplayPort to HDMI protocols. All types of traffic not authorized by the referenced PP including USB, Ethernet, MCCS and EDID write are blocked by this TOE function as the emulated EEPROM would only support valid EDID read requests from connected computers. Note that HEAC and CEC functions are not connected in these TOEs and therefore not supported.

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

See **Table 6 Supported protocols by port** for a description of the allowed devices for each peripheral port type. Composite USB devices are not supported. During KVM operation, non-standard keyboards with integrated USB hubs and/or other USB-integrated devices may not be fully supported due to the strict security standards and policy for the IOGEAR Secure KVM Switch. If supported, only basic (HID) keyboard operations will function. USB and PS/2 keyboard and mouse console ports are supported. The console USB keyboard and mouse ports are interchangeable, meaning you can connect a keyboard to the mouse port and vice versa. A user can mix and match USB and PS/2 keyboard/mouse peripherals. For example, a user can use PS/2 mouse + USB keyboard, or PS/2 keyboard + USB mouse. For optimal operation, the User Manual suggests connecting the USB keyboard to console's USB keyboard port and the USB mouse to console's USB mouse port. The authorized user authentication devices are identified using whitelist and the TOE allows blacklist configuration for user authentication device profiling (filtering). The KVM includes a built-in default whitelist for USB CAC Port, as to allow only authentication devices (eg. Smartcard/CAC reader). This built-in default whitelist cannot be deleted or revised.

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 (Vendor ID), and PID (Product ID) 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. Four digit PID values are required. A wildcard character asterisk "*" can be used in the PID field to represent one or more other characters. For example, the PID filtering rule (5***) would include all the devices whose PID starts with a 5.

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.

Whitelist/blacklist interaction and priority is as follows. The blacklist and whitelist defined by Administrator Functions (Configuration Menu) always supersedes the filtering list created by the Port Authentication Utility. If a device is blacklisted in Administrator-defined list, the device will be rejected even if it's also whitelisted in Port Authentication Utility-defined list. If a device is blacklisted by Port Authentication Utility, it will be allowed if it's also whitelisted by Administrator-defined list. If a device is assigned to both blacklist and whitelist (for example, by Administrator-defined black/whitelist), it will be defined as blacklisted. If there is no defined blacklist, the devices defined in the default built-in whitelist are allowed.

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

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 data held in any TOE component is 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 Port 1, 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. Performing the reset function by pressing the Reset button for more than 5 seconds, purges the Keyboard/Mouse buffer; 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 administrator 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.

6.4 Security management

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

6.4.1.1 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.

6.4.1.2 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, to view audit logs and to change the administrator password.

The TOE provides the authorized administrator with the ability 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 whitelist, the TOE considers the device as authorized. Otherwise, if the device is on the blacklist it is considered unauthorized. If a device has been added to both blacklist and whitelist, 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.

6.4.1.3 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 functions 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 printed with the TOEs unique product serial number and the vendor's specific design. One label is applied to the side of the device and the other to the bottom of the chassis, over the screw used to secure the front-top cover to the enclosure. Any attempt to open the enclosure sufficient to gain access to internal components will change the labels to a tampered state. The side-label is clearly visible to the user operating the TOE and the other label can be clearly seen when the device is turned over.

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

The TOE becomes permanently inoperable and all front panel LEDs (except for Power LED) flash constantly when a chassis intrusion, such as removal of the device cover is detected. These indications cannot be turned off by the TOE user and the guidance documentation instructs the user to stop using the TOE, remove it from service and contact IOGEAR. 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.

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

The TOE preserves a secure state by disabling the TOE when the following types of failures occur: failure of the power on self-test and failure of the anti-tampering function. The behavior as described above for FPT_PHP.1 and FPT_PHP.3 will occur if the Secure KVM Switch self-test fails or its security function detects a breach.

6.5.3 TSF testing (FPT_TST.1)

The Secure KVM Switch TOE self-tests include memory tests; firmware integrity tests; and tests of push-button functioning. The TOE executes self-tests during boot (after a power-on, Reset to Factory Default, or the reset button is pressed). The self-test function runs independently at each one of the TOE micro-controllers following power up.

The following details the particular self-tests:

- Firmware integrity: the TOE validates the integrity of firmware by calculating the checksum of the firmware binary file and comparing to a pre-calculated value that is stored in the TOE.
- Accessibility of internal memory of the micro-controller: the TOE writes a block of predefined data to SRAM and then reads the block out to compare if it is identical.
- Computer interfaces isolation functionality: the TOE validates correct functionality of isolation by generating data flow on one port and checking that it is not received on another port.
- Key stuck test (KVM front panel Push button jam test): the TOE will check that the status of all button values in the micro-controller to ensure the push-buttons are operational.
- Anti-tampering mechanism test: the TOE will verify if the tamper detection switch is triggered.

The KVM performs self-tests first before enabling the peripheral switching function. Before self-tests have completed successfully, the data paths between peripherals and connected computers are blocked and no data flow is allowed.

A Push 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 one of the self-tests fail, 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. The status indicators are as follows:

- For a Key stuck test failure, the front panel Port LED and CAC LED of that jammed button port will flash.
- For all other Self-test failures (Firmware integrity, Accessibility of internal memory of the micro-controller, Computer interfaces isolation functionality, Anti-tampering mechanism) all front panel LEDs (except for Power LED) flash.

6.6 TOE Access

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

The TOE resets the power supplied to the user authentication device for at least one second when the user switches the device from one computer to another.

6.6.1 User Authentication Device Reset (FTA_ATH_EXT.1)

The Secure KVM Switch provides power to connected user authentication devices via the USB protocol and does not require user authentication devices to be powered by an external power source. The TOE resets the power supplied to the user authentication device for at least one second when the user switches the device from one computer to another. The capacitance of the TOE is about 10μF. For a typical user authentication device power reset, voltage decreases from 5V to less than 2V in 0.2sec meeting the 2.0V in one second requirement. Capacitance is small enough to assure that low-power devices would reach less than 2.0 V during that one second power reset.

The micro-controller switches the CAC from computer channel back to micro-controller channel whenever the card reader is pulled out. If the CAC Reader is verified by the micro-controller to be on the whitelist, the CAC Reader data channel will be switched to the target connected computer. The Data Isolation document Section 2.3 provides more details (proprietary). The authentication procedure will start over again once a card reader insertion is detected

at the USB card reader port. When powering down, the TOE cuts the power to CAC switches. As there's no power to the switch, the CAC channel is like a broken path (open switch). This prevents active sessions from continuing.

6.6.2 Continuous Indications (FTA_CIN_EXT.1)

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

The Port LEDs on the Secure KVM Switch are located on the front panel and provide a continuous visual indication of the selected Port and corresponding selected computer (bright orange) and the connection status of all other connected computers (dim orange indicates the connected computer is running). On power up, Port 1 is selected by default.

CAC reader LEDs (one per Port) are also located on the front panel and provide a continuous visual indication of the status of the CAC function associated with that port. The CAC LED will light bright green to indicate that the CAC function is enabled and the computer attached to its corresponding port has the CAC focus (note that CAC switching is always synchronized with computer selection). The CAC LED lights dim green to indicate that the computer attached to its corresponding port has a USB CAC reader cable connected and CAC function is enabled (although the computer is not selected). If the CAC LED flashes when the corresponding Port is selected, this indicates a non-qualified USB smart card/CAC reader is connected.

The TOE has a reset button that resets the switch to the default settings when pressed. The switch is then powered up and behaves as described above.

The CAC reader function on each Port can be enabled or disabled by pressing the Port Selection Pushbutton for more than 3 seconds (this is a toggle feature).

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 including the following optional SFRs: FAU_GEN.1, 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	[PSS]

Requirement Class	Requirement Component	Source
	(Restore factory defaults)	
FIA: Identity and authentication	FIA_UAU.2: User identification before any action	[PSS]
	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 7 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 8** 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
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(1)		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 8 Security Functions vs. Requirements Mapping