ATEN Universal Secure KVM Switch Series (CAC Models)

Security Target

Version 1.2

2025-05-02

Prepared for:

ATEN
3F, No. 125, Section 2, Datung Road, Sijhih District,
New Taipei City, 221
Taiwan

Prepared by:

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

Revision History		
Version	**Author**	**Modifications**
1.0	Leidos	Initial Version
1.1	Leidos	Updated Version
1.2	Leidos	Updated Version

Table of Contents

List of Figures and 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 ATEN Secure KVM Switch Series (CAC Models) provided by ATEN.

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, Target of Evaluation, and Common Criteria Identification

ST Title: ATEN Secure KVM Switch Series (CAC Models) Security Target

ST Version: Version 1.22

ST Date: 2025-05-0202

Target of Evaluation (TOE) Identification: ATEN Secure KVM Switch Series (CAC Models)

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

Table 1: ATEN Secure KVM Switch TOE Models

Configuration (with CAC function)		2-Port	4-Port
DisplayPort/ HDMI	Single Head	CS1182DPH4C	CS1184DPH4C
	Dual Head	CS1142DPH4C	CS1144DPH4C

The TOE includes a wired remote controller: Remote Port Selector (RPS) that is available to customers as an additional purchase. This device has the same firmware version as the models above.

TOE Developer: ATEN

Evaluation Sponsor: ATEN

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

1.2 Conformance Claims

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

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1 Revision 5, April 2017
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1 Revision 5, April 2017
    - Part 3 Conformant

This ST and the TOE it describes claim exact conformance to the following PP-Configuration: PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, 19 July 2019 (CFG_PSD-AO-KM-UA-VI_V1.0) This PP-Configuration includes the following components:

- *Protection Profile for Peripheral Sharing Device*, Version 4.0, 19 July 2019 (PP_PSD_V4.0) or [PSD]
    - including the following optional and selection-based SFRs: FAU_GEN.1, FDP_RIP_EXT.2, FDP_SWI_EXT.2, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_SMF.1, FMT_SMR.1, FPT_PHP.3, FPT_STM.1, and FTA_CIN_EXT.1.
- *PP-Module for Analog Audio Output Devices*, Version 1.0, 19 July 2019 (MOD_AO_V1.0).
- *PP-Module for Keyboard/Mouse Devices*, Version 1.0, 19 July 2019 (MOD_KM_V1.0)
    - including the following optional and selection-based SFRs: FDP_FIL_EXT.1/KM, FDP_RIP.1/KM, and FDP_SWI_EXT.3.
- *PP-Module for User Authentication Devices*, Version 1.0, 19 July 2019 (MOD_UA_V1.0)
    - including the following selection-based SFRs: FDP_TER_EXT.2 and FDP_TER_EXT.3.
- *PP-Module for Video/Display Devices*, Version 1.0, 19 July 2019 (MOD_VI_V1.0)
    - *including the following selection-based SFRs: FDP_CDS_EXT.1, FDP_IPC_EXT.1, FDP_SPR_EXT.1/DP, and FDP_SPR_EXT.1/HDMI.*

The following NIAP Technical Decisions are applicable to the claimed Protection Profile and Modules:

- TD0506 – Missing Steps to Disconnect and Reconnect Display
- TD0507 – Clarification on USB Plug Type
- TD0514 – Correction to MOD_VI FDP_APC_EXT.1 Test 3 Step 6
- TD0518 – Typographical Error in Dependency Table
- TD0539 – Incorrect Selection Trigger in FTA_CIN_EXT.1 in MOD_VI_V1.0
- TD0557 – Correction to Audio Filtration Specification Table in FDP_AFL_EXT.1
- TD0583 – FPT_PHP.3 modified for PSD remote controllers
- TD0584 – Update to FDP APC_EXT.1 Video Tests
- TD0585 – Update to FDP_APC_EXT.1 Audio Output Tests
- TD0593 – Equivalency Arguments for PSD
- TD0619 – Update to MOD_UA FDP_FIL_EXT.1 Test 3
- TD0620 – EDID Read Requirements
- TD0681 – PSD purging of EDID data upon disconnect
- TD0686 – DisplayPort CEC Testing
- TD0804 – Clarification regarding Extenders in PSD Evaluations

- TD0842 – Alternate Conversion Option for FDP_IPC_EXT.1
- TD0844 – Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim

1.3 Conventions

The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, with additional extended functional components.

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections, iterations, and refinements. This document retains all operations completed by the PP author (i.e. selections/assignments they already filled out). These are formatted as italicized text.

This document uses the following font conventions to identify iterations, extended SFRs and operations performed by the ST author:

- **Refinement** operation (denoted by **bold text** and underline) is used to add details to a requirement, and thus further restricts a requirement.
- **Selection** operation (denoted by italicized ***bold*** text): is used to select one or more options provided by the [CC] in stating a requirement. Selection operations completed in the PP are shown in brackets.
- **Assignment** operation (denoted by **bold** text) is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment. Assignments within Selections are denoted by italicized ***bold*** text).
- **Iteration** operation is identified with a slash ('/') and an identifier (e.g. "/KM"). Additional iterations made by the ST author are defined with a reference in parentheses to the specific TOE models they apply to, e.g. "(DP)" indicates the SFR only applies to DisplayPort models. Though technically not an iteration FDP_IPC_EXT.1, also uses this convention to clarify that this requirement only applies to certain models.
- **Extended** SFRs are identified by having a label "EXT" after the SFR name.

1.3.1 Terminology

Table 2: Terms and Definitions

Term	Definition
Aligned	Detected and accepted the connection by the KVM.
Assurance	Grounds for confidence that a TOE meets the SFRs.
Authorized Peripheral	A Peripheral Device that is both technically supported and administratively permitted to have an active interface with the PSD.
Combiner (multi-viewer)	A PSD with video integration functionality that is used to simultaneously display output from multiple personal computers (PCs).
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Computer Interface	The PSD's physical receptacle or port for connecting to a computer.

Term	Definition
Configurable Device Filtration (CDF)	A PSD function that filters traffic based on properties of a connected peripheral device and criteria that are configurable by an Administrator.
Connected Computer	A computing device connected to a PSD. May be a personal computer, server, tablet, or any other computing device.
Connected Peripheral	A Peripheral that is connected to a PSD.
Connection	A physical or logical conduit that enables Devices to interact through respective interfaces. May consist of one or more physical (e.g., a cable) or logical (e.g., a protocol) components.
Connector	The plug on a Connection that attaches to a Computer or Peripheral Interface.
Device	An information technology product. In the context of this PP, a Device is a PSD, a Connected Computer, or a Connected Peripheral.
Display	A device that visually outputs user data, such as a monitor.
Interface	A shared boundary across which two or more Devices exchange information through a Connection.
KM	A type of PSD that shares a keyboard and pointing device between Connected Computers. A KM may optionally include an analog audio device.
KVM	A type of PSD that shares a keyboard, video, and pointing device between Connected Computers. A KVM may optionally include an analog audio device and user authentication device.
Letter of Volatility	A letter issued by the manufacturer outlining whether onboard memory can store data when the device is powered off (non-volatile) or not (volatile).
Monitoring	The ability of a User to receive an indicator of the current Active Interface.
Non-Selected Computer	A Connected Computer that has no Active Interfaces with the PSD.
Peripheral Interface	The PSD's physical receptacle or port for connecting to a Peripheral Device.
Peripheral/Peripheral Device	A Device with access that can be Shared or Filtered by a PSD.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Remote Controller	Remote component of the PSD that extends the controls and indications through a cable.
Secure State	An operating condition in which the PSD disables all connected peripheral and connected computer interfaces when the correctness of its functions cannot be ensured.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	Implementation-independent documentation that describes a TOE, its Operational Environment, and its claimed security functionality.
Selected Computer	A Connected Computer that has Active Interfaces with the PSD.
Supported Peripheral	A Peripheral Device that is technically supported by the PSD.

Term	Definition
Target of Evaluation (TOE)	A product or component, consisting of hardware, software, and/or firmware, that claims to implement certain security functionality in a specific and well-defined manner.
TOE Security Functionality (TSF)	The combined hardware, software, and firmware capabilities of a TOE that are responsible for implementation of its claimed SFRs.
TOE Security Functionality Interface (TSFI)	Any external interface between the TOE and its Operational Environment that has a security-relevant purpose or is used to transmit security-relevant data.
TOE Summary Specification (TSS)	Documentation contained within the Security Target that provides the reader with a description of how the TOE implements the claimed SFRs.
User	A person that interacts with a PSD (or a process or mechanism acting on behalf of a person).
User Authentication Device	A Peripheral Device that is used to affirm the identity of a User attempting to authenticate to a computer (e.g., smart card reader, biometric authentication device, proximity card reader).
User Data	Information that the User inputs to the Connected Computer or is output to the User from the Connected Computer (and including user authentication and credential information)

1.3.2 Acronyms

Table 3: Acronyms

Acronym	Definition
ARC	Audio Return Channel
AUX	Display Port Auxiliary Channel
CAC	Common Access Card
CDF	Configurable Device Filtering
CEC	Consumer Electronics Control
EDID	Extended Display Identification Data
EEPROM	Electrically Erasable Programmable Read-Only Memory
FIPS	Federal Information Processing Standards
HD	High Definition
HDCP	High-bandwidth Digital Content Protection
HDMI	High Definition Multimedia Interface
HEAC	HDMI Ethernet Audio Control
HEC	HDMI Ethernet Channel
HID	Human Interface Device
HPD	Hot Plug Detect
IT	Information Technology
KVM	Keyboard, Video, and Mouse

Acronym	Definition
LED	Light-Emitting Diode
MCCS	Hot Plug Detect
PC	Personal Computer
PSD	Peripheral Sharing Device
RPS	Remote Port Selector
SFP	Security Function Policy
USB	Universal Serial Bus

2 TOE Description

2.1 Product Overview

The TOE is the ATEN Secure KVM Switch Series (CAC Models). Each of the 4 models identified in Section 1.1 is a Peripheral Sharing Device that include console ports and computer ports. The console ports are used to connect a single set of peripherals, including a mouse, keyboard, user authentication device such as smart card or CAC reader, speaker, and one or two video displays (depending on specific device type) to the TOE. The TOE's computer ports are connected to up to 2 or 4 separate computers (again depending on specific device type). The user can then securely switch the connected console peripherals between any of the connected computers while preventing unauthorized data flows or leakage between computers. The TOE supports manual port switching using a press and release a port selection push button (on the switch, or on the Remote Port Selector (RPS) if connected and aligned) to bring the KVM focus to the computer attached to its corresponding port.

2.2 TOE Overview

The TOE is the ATEN Secure Switch series of products with CAC. The TOE allows users to connect a single set of peripherals to its console ports to interact with multiple computers that are connected to it via its computer ports. Controls on the TOE chassis or on the RPS allow the user to select which of the connected computers is 'active' such that the peripherals connected to the console can be used to interact with the selected computer.

The TOE's console ports support USB keyboard and mouse, analog audio out (speakers), a USB smart card/CAC port, and DisplayPort/HDMI display interface.

The TOE's computer ports also support the same interfaces as above.

The TOE includes multiple models, all with the same basic functionality. The differences between models are:

- The number of sets of computer ports, which determines how many computers can be connected to the TOE at one time (up to 2 or 4).
- The number of heads for the display interface, which determines whether single or dual monitors are supported.

2.3 TOE Architecture

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

- 2/4 port USB DP/HDMI single and dual display for DP/HDMI (4 devices)

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

To interface with connected computers, the Secure KVM Switch products support analog audio output and USB connections for the keyboard, mouse, and user authentication device. They support DisplayPort/HDMI for the computer video display interface. The switched peripherals on the console side are analog audio output, USB keyboard and mouse, USB user authentication device, and DisplayPort/HDMI video output.

Separate USB cables are used to connect the keyboard/mouse combination and the user authentication device to the connected computers. The video interface is a combined DP/HDMI port on a single bus where either connector can be used interchangeably. If a DisplayPort output is connected to the TOE, the TSF will convert the signal to HDMI. It will then output the signal as either HDMI or DisplayPort, depending on the physical ports used for the connected monitors. 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. The following tables show the supported interfaces on the console (Table 4) and computer (Table 5) interfaces. Note that all TOE models support the same interfaces; the differences between models are based entirely on the number of video interfaces (heads) and number of computer ports.

Table 4: ATEN Secure KVM Switch Console Interfaces and TOE Models

Model No.	Console Video Output Interface		Console Keyboard	Console Mouse	Console Audio output	Console CAC Reader
	DisplayPort	HDMI	USB 1.1/2.0	USB 1.1/2.0	3.5mm Analog Audio output (Speaker)	USB 1.1/2.0
CS1182DPH4C	·	·	·	·	·	·
CS1142DPH4C	·	·	·	·	·	·
CS1184DPH4C	·	·	·	·	·	·
CS1144DPH4C	·	·	·	·	·	·

Table 5: ATEN Secure KVM Switch Computer Interfaces and TOE Models

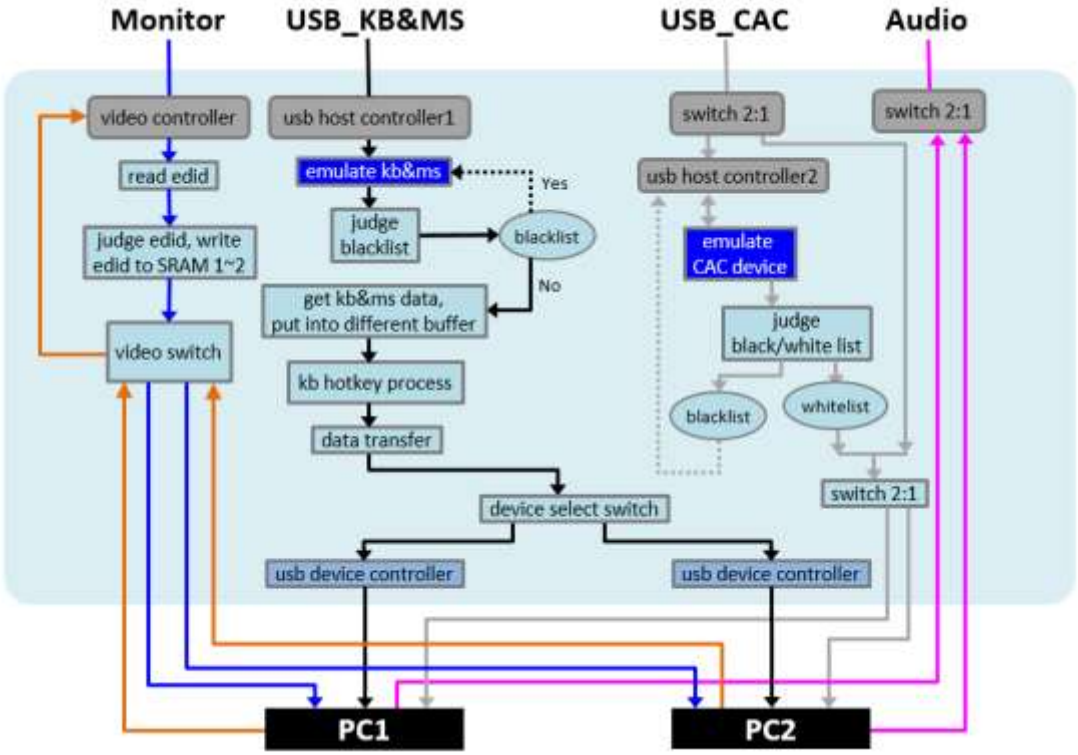
Model No.	Computer Video Input Interface		Computer Keyboard / Mouse	Computer Audio Input	Computer CAC Input
	DisplayPort	HDMI	USB 1.1/2.0	3.5mm Analog Audio Input (Speaker)	USB 1.1/2.0
CS1182DPH4C	·	·	·	·	·
CS1142DPH4C	·	·	·	·	·
CS1184DPH4C	·	·	·	·	·
CS1144DPH4C	·	·	·	·	·

The ATEN Secure KVM products implement a secure isolation design for all models to share a single set of peripheral components. 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 TOE has combined DP/HDMI video ports for both the computer and peripheral side so that both can be used interchangeably. When a computer is connected to a DisplayPort interface, video from the selected computer is converted internally to HDMI. It is then either output directly as HDMI or converted back to DisplayPort for communication with the connected video display, depending on which port is used.

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 [PSD]. Data leakage is prevented across the TOE to avoid compromise of the user's information. The Secure KVM Switch products automatically clear the internal TOE keyboard and mouse buffers.

Figure 1 shows the data path design using a 2-Port KVM as an example.

Figure 1: Simplified Block Diagram of a 2-Port KVM TOE



As shown in Figure 1 above, the internal components of the KVM consist of switches, emulators, USB host controllers, processors, and embedded with non-updateable firmware v1.1.101. The internal hardware components are identified in Appendix A and include the manufacturer and the part number. The data flow of USB keyboard/mouse is controlled by the host controller for console HID keyboard and pointing devices. 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 keyboard and mouse to USB data for computer sources.

The TOE's 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 a peripheral device connected to a console port 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 components including the RPS, 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 ATEN Port Authentication Utility must be installed on a separate secure source computer using an installation wizard. The Port Authentication Utility tool is used to define or modify a secondary whitelist and/or blacklist for the device. The utility supports Microsoft Windows 8 and higher. The Port Authentication Utility computer connects to the TOE via USB connection to Computer Port 1. 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).

2.3.1 Physical Boundary

The TOE includes the RPS and hardware models identified in Section 1.1 along with embedded firmware v1.1.101 and corresponding documentation identified in Section 2.5 below.

An optional KVM cable set (not supplied with the TOE) is available as a separate purchase. The KVM cable sets are built for the KVM connection to the PCs, providing better compatibility. Users can connect the KVM and PCs using their own cable sets as long as the protocols are compatible but the vendor KVM cable sets are recommended.

While the cable sets and adapters were supplied, they were not included in the evaluation because they are considered part of the operational environment, along with the switched PCs, peripheral devices, DisplayPort / HDMI monitors, USB keyboard, USB mouse, 3.5mm audio output (e.g. speakers), smart card/CAC reader, and the host computers.

The ATEN Port Authentication Utility requires a dedicated secure source computer with Microsoft Windows 8 or higher, along with its own monitor, keyboard, and mouse.

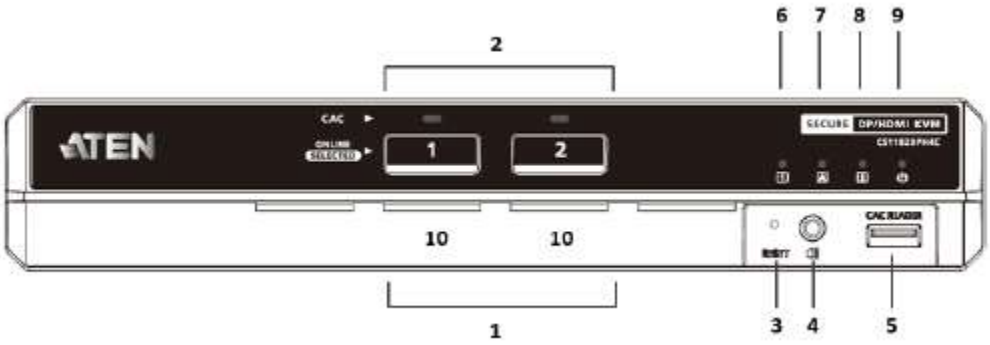
The following figure shows a representative TOE and its environment. In particular, it shows a two port, single-head KVM and its connections.

The dual-head device includes an additional layer of video ports, allowing multiple monitors per system, unlike the single-head device, which supports only one display.

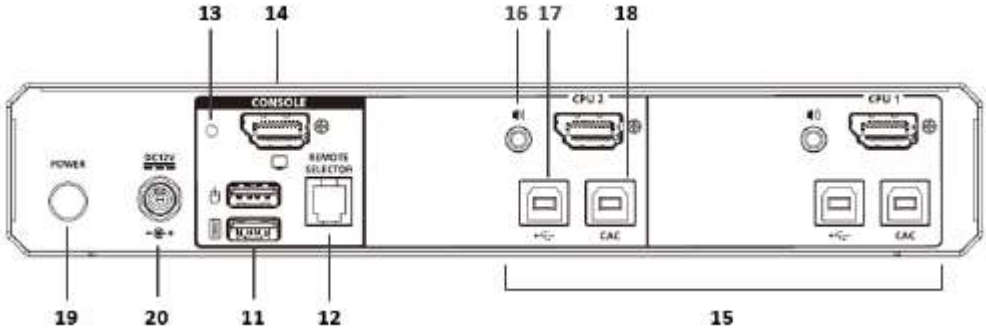
This enables extended display support for secure multi-monitor setups.

Figure 2: Representative ATEN Secure KVM Switch TOE Model in its environment

CS1182DPH4C (front)



CS1182DPH4C (rear)



The numbers on the diagram indicate the following:

- 1: Push buttons for port selection
- 2: Selected port and CAC enable/disable LEDs (port LEDs backlighting the push buttons, CAC LEDs above the push buttons)
- 3: Reset button
- 4: Audio port
- 5: CAC port
- 6: Num lock LED
- 7: Caps lock LED

- 8: Scroll lock LED
- 9: Power LED
- 10: Area for adding physical labels for port identification
- 11: USB console ports
- 12: RPS port

  RPS port is used to connect an external wired remote controller for switching between connected computers.

  RPS is a wired remote device that connects to the KVM switch via RPS port. It allows the user to remotely change the active input port on the KVM by pressing the selector button on the remote, without needing to physically interact with the KVM unit itself.
- 13: Video LED(s)
- 14: Console monitor port(s)
- 15: Computer port area
- 16: Computer audio port
- 17: Computer USB port
- 18: Computer CAC port
- 19: Power button
- 20: Power jack

The ATEN Secure KVM devices do not include any wireless interfaces. The ATEN Secure KVM devices have been tested and found to comply with the radio frequency emissions limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission rules. If not installed and used in accordance with the guidance instructions, the device may cause harmful interference to radio communications. This evaluation did not test for RFI leakage of information.

2.4 Logical Boundary

This section summarizes the security functions provided by the TOE:

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

2.4.1 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.

2.4.2 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; USB authentication device (CAC reader and smart card); audio output; and DisplayPort/HDMI video. When DisplayPort devices are connected, the TOE accepts DisplayPort signals at the computer interface and internally converts them to HDMI signals. HDMI signals are either converted back to DisplayPort or output as HDMI depending on the devices connected to the console interface. When HDMI devices are connected, the TOE accepts the HDMI signal without conversion.

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 switches to another selected computer and on start-up of the TOE.

The TOE provides a Reset to Factory Default function allowing authenticated authorized Administrators to remove all settings previously configured by the Administrator (such as USB device whitelist/blacklist). Once the Reset to Factory 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.

2.4.3 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 whitelist and blacklist. The authorized administrator must logon by providing a valid password.

2.4.4 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 configure the keyboard/mouse device filtration, Reset to Factory Default and to change the administrator password.

2.4.5 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 main TOE enclosure as well as the RPS 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.

2.4.6 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.

2.5 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:

- ATEN PSD PP v4.0 Secure KVM Switch Series 2/4-Port USB DP/HDMI Single/Dual Display Universal Secure KVM Switch User Manual, Version 1.3, 2025-06-26
- ATEN PSD PP v4.0 Secure KVM Switch Series 2/4-Port USB DP/HDMI Single/Dual Display Universal Secure KVM Switch Port Authentication Utility Guide, Version 1.1, 2024-09-06
- ATEN PSD PP v4.0 Secure KVM Switch Series 2/4-Port USB DP /HDMI/Single/Dual Display Universal Secure KVM Switch Administrator Guide, Version 1.1, 2024-09-06
- ATEN PSD PP v4.0 Secure KVM Switch Series 2/4-Port USB DP/HDMI Single/Dual Display Universal Secure KVM Switch Admin Log Audit Code, Version 1.0, 2024-07-11

TOE Documentation:

- ATEN PP4.0 DP/HDMI Universal Secure KVM Isolation Document, Version 1.1, 2025-03-11 (Proprietary)
    - **Note**: The PP4.0 Secure KVM Isolation Document is **proprietary** as permitted by PSD 4.0 Annex D.1 Isolation Document and Assessment.
    - The isolation document supplements the 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 PSD 4.0 Annex D and Evaluation Activities specified in the PP v4.0 and modules.

3 Security Problem Definition

This security target includes by reference the Security Problem Definition from the [PSD], [MOD_AO_V1.0], and [MOD_VI_V1.0]. 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 [PSD] has presented a Security Problem Definition appropriate for peripheral sharing devices. The ATEN Secure KVM Switch Series supports KVM (USB Keyboard/Mouse, analog audio (out), DisplayPort/HDMI video) peripheral switch functionality by combining a 2/4 port KVM switch, an audio output port, and a USB authentication device (CAC port and smart card). As such, the [PSD] 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 [PSD], [MOD_VI_V1.0], [MOD_AO_V1.0], [MOD_KM_V1.0], and [MOD_UA_V1.0].

The [PSD], [MOD_AO_V1.0], and [MOD_VI_V1.0] 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 [PSD] has presented a Security Objectives statement appropriate for peripheral sharing devices. Consequently, the [PSD] security objectives are suitable for the TOE.

4.1 Security Objectives for the Operational Environment

Table 6: Security Objectives for the Operational Environment

Objective	Description
OE.NO_MICROPHONES (from [MOD_AO_V1.0])	The operational environment is expected to ensure that microphones are not plugged into the TOE audio output interfaces.
OE.NO_SPECIAL_ANALOG_CAPABILITIES (from [MOD_VI_V1.0])	The operational environment will not have special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, or a component with digital signal processing or analog video capture functions.
OE. NO_TEMPEST (from [PSD])	The operational environment will not use TEMPEST approved equipment.
OE.NO_WIRELESS_DEVICES (from [PSD])	The operational environment will not include wireless keyboards, mice, audio, user authentication, or video devices.
OE.PHYSICAL (from [PSD])	The operational environment will provide physical security, commensurate with the value of the PSD and the data that transits it.
OE.TRUSTED_ADMIN (from [PSD])	The operational environment will ensure that trusted PSD Administrators and users are appropriately trained.
OE.TRUSTED_CONFIG (from [PSD])	The operational environment will ensure that administrators configuring the PSD and its operational environment follow the applicable security configuration guidance.

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: [PSD] and the modules: [MOD_AO_V1.0], [MOD_KM_V1.0], [MOD_UA_V1.0], and [MOD_VI_V1.0], and include some of the optional and selection-based SFRs. As a result, refinements and operations already performed in that PP and modules 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 [PSD] and modules 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.

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

5.1 Extended Requirements

All of the extended requirements in this ST have been drawn from the [PSD] and the modules: [MOD_AO_V1.0], [MOD_KM_V1.0], [MOD_UA_V1.0], and [MOD_VI_V1.0]. The [PSD] and modules define the following extended SFRs and since they are not redefined in this ST, the [PSD] and associated modules should be consulted for more information in regard to those CC extensions.

- FDP_AFL_EXT.1 – Audio Filtration
- FDP_APC_EXT.1 – Active PSD Connections
- FDP_CDS_EXT.1 – Connected Displays Supported
- FDP_FIL_EXT.1/KM – Device Filtering (Keyboard/Mouse)
- FDP_FIL_EXT.1/UA – Device Filtering (User Authentication Devices)
- FDP_IPC_EXT.1 – Internal Protocol Conversion
- FDP_PDC_EXT.1 – Peripheral Device Connection
- FDP_PDC_EXT.2/AO – Peripheral Device Connection (Audio Output)
- FDP_PDC_EXT.2/KM – Authorized Devices (Keyboard/Mouse)
- FDP_PDC_EXT.2/UA – Authorized Devices (User Authentication Devices)
- FDP_PDC_EXT.2/VI – Peripheral Device Connection (Video Output)
- FDP_PDC_EXT.3/KM – Authorized Connection Protocols (Keyboard/Mouse)
- FDP_PDC_EXT.3/VI – Authorized Connection Protocols (Video Output)
- FDP_PDC_EXT.4 – Supported Authentication Devices
- FDP_PUD_EXT.1 – Powering Unauthorized Devices
- FDP_PWR_EXT.1 – Powered by Computer
- FDP_RIP_EXT.1 – Residual Information Protection
- FDP_RIP_EXT.2 – Purge of Residual Information
- FDP_SPR_EXT.1/DP – Sub-Protocol Rules (DisplayPort Protocol)
- FDP_SPR_EXT.1/HDMI – Sub-Protocol Rules (HDMI Protocol)
- FDP_SWI_EXT.1 – PSD Switching
- FDP_SWI_EXT.2 – PSD Switching Methods
- FDP_SWI_EXT.3 – Tied Switching

- FDP_TER_EXT.1 – Session Termination
- FDP_TER_EXT.2 – Session Termination of Removed Devices
- FDP_TER_EXT.3 – Session Termination Upon Switching
- FDP_UAI_EXT.1 – User Authentication Isolation
- FDP_UDF_EXT.1/AO – Unidirectional Data Flow (Audio Output)
- FDP_UDF_EXT.1/KM – Unidirectional Data Flow (Keyboard/Mouse)
- FDP_UDF_EXT.1/VI – Unidirectional Data Flow (Video Output)
- FDP_IPC_EXT.1.1 – Internal Protocol Conversion
- FPT_FLS_EXT.1 – Failure with Preservation of Secure State
- FPT_NTA_EXT.1 – No Access to TOE
- FPT_TST_EXT.1 – TSF Testing
- FTA_CIN_EXT.1 – Continuous Indications

5.2 TOE Security Functional Requirements (PSD, MOD-AO, MOD-KM, MOD_UA_V1.0)

This section identifies the TOE Security Functional Requirements for the PSD 4.0, and modules [MOD_AO_V1.0], [MOD_KM_V1.0], [MOD_UA_V1.0] and [MOD_VI_V1.0].

Table 7 identifies the SFRs that are satisfied by the TOE.

Table 7: TOE Security Functional Components

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1 – Audit Data Generation
FDP: User Data Protection	FDP_AFL_EXT.1 – Audio Filtration
	FDP_APC_EXT.1/AO – Active PSD Connections (Audio Output)
	FDP_APC_EXT.1/KM – Active PSD Connections (Keyboard/Mouse)
	FDP_APC_EXT.1/UA – Active PSD Connections (User Authentication)
	FDP_APC_EXT.1/VI – Active PSD Connections (Video/Display)
	FDP_CDS_EXT.1 – Connected Displays Supported
	FDP_FIL_EXT.1/KM – Device Filtering (Keyboard/Mouse)
	FDP_FIL_EXT.1/UA – Device Filtering (User Authentication Devices)
	FDP_IPC_EXT.1 – Internal Protocol Conversion
	FDP_PDC_EXT.1 – Peripheral Device Connection
	FDP_PDC_EXT.2/AO – Peripheral Device Connection (Audio Output)
	FDP_PDC_EXT.2/KM – Authorized Devices (Keyboard/Mouse)
	FDP_PDC_EXT.2/VI – Peripheral Device Connection (Video Output)

Requirement Class	Requirement Component
	FDP_PDC_EXT.2/UA – Authorized Devices (User Authentication Devices)
	FDP_PDC_EXT.3/KM – Authorized Connection Protocols (Keyboard/Mouse)
	FDP_PDC_EXT.3/VI – Authorized Connection Protocols (Video Output)
	FDP_PDC_EXT.4 – Supported Authentication Device
	FDP_PUD_EXT.1 – Powering Unauthorized Devices
	FDP_PWR_EXT.1 Powered By Computer
	FDP_RIP.1/KM – Residual Information Protection (Keyboard Data)
	FDP_RIP_EXT.1 – Residual Information Protection
	FDP_RIP_EXT.2 – Purge of Residual Information
	FDP_SPR_EXT.1/DP – Sub-Protocol Rules (DisplayPort Protocol)
	FDP_SPR_EXT.1/HDMI – Sub-Protocol Rules (HDMI Protocol)
	FDP_SWI_EXT.1 – PSD Switching
	FDP_SWI_EXT.2 – PSD Switching Methods
	FDP_SWI_EXT.3 – Tied Switching
	FDP_TER_EXT.1 Session Termination
	FDP_TER_EXT.2 Session Termination or Removed Devices
	FDP_TER_EXT.3 Session Termination upon Switching
	FDP_UAI_EXT.1 User Authentication Isolation
	FDP_UDF_EXT.1/AO – Unidirectional Data Flow (Audio Output)
	FDP_UDF_EXT.1/KM – Unidirectional Data Flow (Keyboard/Mouse)
	FDP_UDF_EXT.1/VI – Unidirectional Data Flow (Video Output)
FIA: Identification and Authentication	FIA_UAU.2 – User Authentication 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

Requirement Class	Requirement Component
FPT: Protection of the TSF	FPT_FLS_EXT.1 – Failure with Preservation of Secure State
	FPT_NTA_EXT.1 – No Access to TOE
	FPT_PHP.1 – Passive Detection of Physical Attack
	FPT_PHP.3 – Resistance to Physical Attack
	FPT_STM.1 Reliable Time Stamps
	FPT_TST.1 – TSF Testing
	FPT_TST_EXT.1 – TSF Testing
FTA: TOE Access	FTA_CIN_EXT.1 – Continuous Indications

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, self-test failures, peripheral device acceptance and rejections, [**modification of the TOE user authentication device filtering whitelist and blacklist, modification of the TOE keyboard, mouse filtering blacklist, Reset to Factory Default, view audit logs, 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 Audio Filtration (FDP_AFL_EXT.1)

FDP_AFL_EXT.1.1 The TSF shall ensure outgoing audio signals are filtered as per [*Audio Filtration Specifications table*[1]].

[1] TD0557 modified the Maximum Voltage After Attenuation for 30-60 kHz to 0.53 mV in Table 8.

Table 8: Audio Filtration Specifications

Frequency (kHz)	Minimum Attenuation (dB)	Maximum Voltage After Attenuation
14	23.9	127.65 mV
15	26.4	95.73 mV
16	30.8	57.68 mV
17	35.0	35.57 mV
18	38.8	22.96 mV
19	43.0	14.15 mV
20	46.0	10.02 mV
30	71.4	0.53 mV
40	71.4	0.53 mV
50	71.4	0.53 mV
60	71.4	0.53 mV

5.2.2.2 Active PSD Connections (Audio Output) (FDP_APC_EXT.1/AO)

FDP_APC_EXT.1.1/AO The TSF shall route user data only from the interfaces selected by the user.

FDP_APC_EXT.1.2/AO The TSF shall ensure that no data or electrical signals flow between connected computers whether the TOE is powered on or powered off.

FDP_APC_EXT.1.3/AO The TSF shall ensure that no data transits the TOE when the TOE is powered off.

FDP_APC_EXT.1.4/AO The TSF shall ensure that no data transits the TOE when the TOE is in a failure state.

Application Note: *This SFR is originally defined in the Base-PP but is refined and iterated to apply to the audio output interface per section 5.1.2 of the Audio Output PP-Module.*

5.2.2.3 Active PSD Connections (Keyboard/Mouse) (FDP_APC_EXT.1/KM)

FDP_APC_EXT.1.1/KM The TSF shall route user data only to the interfaces selected by the user.

FDP_APC_EXT.1.2/KM The TSF shall ensure that no data or electrical signals flow between connected computers whether the TOE is powered on or powered off.

FDP_APC_EXT.1.3/KM The TSF shall ensure that no data transits the TOE when the TOE is powered off.

FDP_APC_EXT.1.4/KM The TSF shall ensure that no data transits the TOE when the TOE is in a failure state

Application Note: *This SFR is originally defined in the Base-PP but is refined and iterated to apply to the keyboard/mouse interface per section 5.1.2 of the Keyboard/Mouse PP-Module.*

5.2.2.4 Active PSD Connections (User Authentication) (FDP_APC_EXT.1/UA)

FDP_APC_EXT.1.1/UA The TSF shall route user data only to or from the interfaces selected by the user.

FDP_APC_EXT.1.2/UA The TSF shall ensure that no data or electrical signals flow between connected computers whether the TOE is powered on or powered off.

FDP_APC_EXT.1.3/UA The TSF shall ensure that no data transits the TOE when the TOE is powered off.

FDP_APC_EXT.1.4/UA The TSF shall ensure that no data transits the TOE when the TOE is in a failure state

Application Note: *This SFR is originally defined in the Base-PP but is refined and iterated to apply to the user authentication interface per section 5.1.2 of the User Authentication PP-Module.*

5.2.2.5 Active PSD Connections (Video/Display) (FDP_APC_EXT.1/VI)

FDP_APC_EXT.1.1/VI The TSF shall route user data only from the interfaces selected by the user.

FDP_APC_EXT.1.2/VI The TSF shall ensure that no data or electrical signals flow between connected computers whether the TOE is powered on or powered off.

FDP_APC_EXT.1.3/VI The TSF shall ensure that no data transits the TOE when the TOE is powered off.

FDP_APC_EXT.1.4/VI The TSF shall ensure that no data transits the TOE when the TOE is in a failure state.

Application Note: *This SFR is originally defined in the Base-PP but is refined and iterated to apply to the video interface per section 5.1.2 of the Video/Display PP-Module.*

5.2.2.6 Connected Displays Supported (FDP_CDS_EXT.1)

FDP_CDS_EXT.1.1 The TSF shall support [***one connected display for CS1182DPH4C, CS1184DPH4C, multiple connected displays for CS1142DPH4C, CS1144DPH4C***] at a time.

5.2.2.7 Device Filtering (Keyboard/Mouse) (FDP_FIL_EXT.1/KM)

FDP_FIL_EXT.1.1/KM The TSF shall have [***configurable***] device filtering for **[*keyboard, mouse*]** interfaces.

FDP_FIL_EXT.1.2/KM The TSF shall consider all [*PSD KM*] blacklisted devices as unauthorized devices for **[*keyboard, mouse*]** interfaces in peripheral device connections.

FDP_FIL_EXT.1.3/KM The TSF shall consider all [*PSD KM*] whitelisted devices as authorized devices for **[*keyboard, mouse*]** interfaces in peripheral device connections only if they are not on the [*PSD KM*] blacklist or otherwise unauthorized.

5.2.2.8 Device Filtering (User Authentication Devices) (FDP_FIL_EXT.1/UA)

FDP_FIL_EXT.1.1/UA The TSF shall have [***configurable***] device filtering for [user authentication device] interfaces.

FDP_FIL_EXT.1.2/UA The TSF shall consider all [*PSD UA*] blacklisted devices as unauthorized devices for [user authentication device] interfaces in peripheral device connections.

FDP_FIL_EXT.1.3/UA The TSF shall consider all [*PSD UA*] whitelisted devices as authorized devices for [user authentication device] interfaces in peripheral device connections only if they are not on the [*PSD UA*] blacklist or otherwise unauthorized.

5.2.2.9 Peripheral Device Connection (FDP_PDC_EXT.1)

FDP_PDC_EXT.1.1 The TSF shall reject connections with unauthorized devices upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.1.2 The TSF shall reject connections with devices presenting unauthorized interface protocols upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.1.3 The TOE shall have no external interfaces other than those claimed by the TSF.

FDP_PDC_EXT.1.4 The TOE shall not have wireless interfaces.

FDP_PDC_EXT.1.5 The TOE shall provide a visual or auditory indication to the User when a peripheral is rejected.

5.2.2.10 Peripheral Device Connection (Audio Output) (FDP_PDC_EXT.2/AO)

FDP_PDC_EXT.2.1/AO The TSF shall allow connections with authorized devices as defined in [*Appendix E* **of the AO Module**] and [

- ***authorized devices and functions as defined in the PP-Module for Keyboard/Mouse Devices,***
- ***authorized devices as defined in the PP-Module for User Authentication Devices,***
- ***authorized devices as defined in the PP-Module for Video/Display Devices,***

] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.2.2/AO The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*Appendix E* **of the AO Module**] and [

- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for Keyboard/Mouse Devices,***
- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for User Authentication Devices,***
- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for Video/Display Devices***,

] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

5.2.2.11 Authorized Devices (Keyboard/Mouse) (FDP_PDC_EXT.2/KM)

FDP_PDC_EXT.2.1/KM The TSF shall allow connections with authorized devices and functions as defined in [*Appendix E* **of the KM Module**] and [

- ***authorized devices as defined in the PP-Module for Audio Output Devices,***
- ***authorized devices as defined in the PP-Module for User Authentication Devices,***
- ***authorized devices as defined in the PP-Module for Video/Display Devices,***

] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.2.2/KM The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*Appendix E* **of the KM Module**] and [

- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for Audio Output Devices,***
- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for User Authentication Devices,***
- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for Video/Display Devices,***

] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

5.2.2.12 Authorized Devices (User Authentication Devices) (FDP_PDC_EXT.2/UA)

FDP_PDC_EXT.2.1/UA The TSF shall allow connections with authorized devices as defined in [*Appendix E* **of the UA Module**] and [

- ***authorized devices as defined in the PP-Module for Audio Output Devices,***
- ***authorized devices and functions as defined in the PP-Module for Keyboard/Mouse Devices,***
- ***authorized devices as defined in the PP-Module for Video/Display Devices,***

] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.2.2/UA The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*Appendix E* **of the UA Module**] and [

- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for Audio Output Devices,***
- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for Keyboard/Mouse Devices,***
- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for Video/Display Devices,***

] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

5.2.2.13 Peripheral Device Connection (Video Output) (FDP_PDC_EXT.2/VI)

FDP_PDC_EXT.2.1/VI The TSF shall allow connections with authorized devices as defined in [*Appendix E* **of the VI Module**] and [

- ***authorized devices as defined in the PP-Module for Audio Output Devices,***
- ***authorized devices and functions as defined in the PP-Module for Keyboard/Mouse Devices,***
- ***authorized devices as defined in the PP-Module for User Authentication Devices,***

] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.2.2/VI The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*Appendix* E **of the VI Module**] and [

- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for Audio Output Devices,***
- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for Keyboard/Mouse Devices,***
- ***authorized devices presenting authorized interface protocols as defined in the PP-Module for User Authentication Devices,***

] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

5.2.2.14 Authorized Connection Protocols (Keyboard/Mouse) (FDP_PDC_EXT.3/KM)

FDP_PDC_EXT.3.1/KM The TSF shall have interfaces for the [***USB (keyboard), USB (mouse)***] protocols.

FDP_PDC_EXT.3.2/KM The TSF shall apply the following rules to the supported protocols: [*the TSF shall emulate any keyboard or mouse device functions from the TOE to the connected computer*].

5.2.2.15 Authorized Connection Protocols (Video Output) (FDP_PDC_EXT.3/VI)

FDP_PDC_EXT.3.1/VI The TSF shall have interfaces for the [***DisplayPort, HDMI***] protocols.

FDP_PDC_EXT.3.2/VI The TSF shall apply the following rules to the supported protocols: [the TSF shall read the connected display EDID information once during power-on or reboot [***automatically***]].

Note: [ST] section 5.2.2.15, FDP_PDC_EXT.3.2/VI is Modified by **TD0620.**

5.2.2.16 Sub-Protocol Rules (DisplayPort Protocol) FDP_SPR_EXT.1/DP

FDP_SPR_EXT.1.1/DP The TSF shall apply the following rules for the [*DisplayPort*] protocol:

- block the following video/display sub-protocols:
  - [CEC,
  - EDID from computer to display,
  - HDCP,
  - MCCS]
- allow the following video/display sub-protocols:
  - [EDID from display to computer,
  - HPD from display to computer,
  - Link Training].

5.2.2.17 Sub-Protocol Rules (HDMI Protocol) (FDP_SPR_EXT.1/HDMI)

FDP_SPR_EXT.1.1/HDMI The TSF shall apply the following rules for the [HDMI] protocol:

- block the following video/display sub-protocols:
  - [ARC,
  - CEC,
  - EDID from computer to display,
  - HDCP,
  - HEAC,
  - HEC,
  - MCCS]
- allow the following video/display sub-protocols:
  - [EDID from display to computer,
  - HPD from display to computer].

5.2.2.18 Supported Authentication Device (FDP_PDC_EXT.4)

FDP_PDC_EXT.4.1 The TSF shall have an [***external***] user authentication device.

5.2.2.19 Powering Unauthorized Devices (FDP_PUD_EXT.1)

FDP_PUD_EXT.1.1 The TSF shall not provide power to any unauthorized device connected to the analog audio peripheral interface.

5.2.2.20 Powered By Computer (FDP_PWR_EXT.1)

FDP_PWR_EXT.1.1 The TSF shall not be powered by a connected computer.

5.2.2.21 Residual Information Protection (Keyboard Data) (FDP_RIP.1/KM)

FDP_RIP.1.1/KM The TSF shall ensure that any keyboard data in volatile memory is purged upon switching computers.

5.2.2.22 Residual Information Protection (FDP_RIP_EXT.1)

FDP_RIP_EXT.1.1 The TSF shall ensure that no user data is written to TOE non-volatile memory or storage.

5.2.2.23 Purge of Residual Information (FDP_RIP_EXT.2)

FDP_RIP_EXT.2.1 The TOE shall have a purge memory or restore factory defaults function accessible to the administrator to delete all TOE stored configuration and settings except for logging.

5.2.2.24 PSD Switching (FDP_SWI_EXT.1)

FDP_SWI_EXT.1.1 The TSF shall ensure that [***switching can be initiated only through express user action***].

5.2.2.25 PSD Switching Methods (FDP_SWI_EXT.2)

FDP_SWI_EXT.2.1 The TSF shall ensure that no switching can be initiated through automatic port scanning, control through a connected computer, or control through keyboard shortcuts.

FDP_SWI_EXT.2.2 The TSF shall ensure that switching can be initiated only through express user action using [***console buttons, wired remote control***].

5.2.2.26 Tied Switching (FDP_SWI_EXT.3)

FDP_SWI_EXT.3.1 The TSF shall ensure that [*connected keyboard and mouse peripheral devices*] are always switched together to the same connected computer.

5.2.2.27 Session Termination (FDP_TER_EXT.1)

FDP_TER_EXT.1.1 The TSF shall terminate an open session upon removal of the authentication element.

5.2.2.28 Session Termination of Removed Devices (FDP_TER_EXT.2)

FDP_TER_EXT.2.1 The TSF shall terminate an open session upon removal of the user authentication device.

5.2.2.29 Session Termination upon Switching (FDP_TER_EXT.3)

FDP_TER_EXT.3.1 The TSF shall terminate an open session upon switching to a different computer.

FDP_TER_EXT.3.2 The TSF shall reset the power to the user authentication device for at least one second upon switching to a different computer.

5.2.2.30 User Authentication Isolation (FDP_UAI_EXT.1)

FDP_UAI_EXT.1.1 The TSF shall isolate the user authentication function from all other TOE USB functions.

5.2.2.31 Unidirectional Data Flow (Audio Output) (FDP_UDF_EXT.1/AO)

FDP_UDF_EXT.1.1/AO The TSF shall ensure [*analog audio output data*] transits the TOE unidirectionally from [the TOE analog audio output computer] interface to [the TOE analog audio output peripheral] interface.

5.2.2.32 Unidirectional Data Flow (Keyboard/Mouse) (FDP_UDF_EXT.1/KM)

FDP_UDF_EXT.1.1/KM The TSF shall ensure [***keyboard, mouse***] data transits the TOE unidirectionally from the [TOE [***keyboard, mouse***]] peripheral interface(s) to the [TOE [***keyboard, mouse***]] interface.

5.2.2.33 Unidirectional Data Flow (Video Output) (FDP_UDF_EXT.1/VI)

FDP_UDF_EXT.1.1/VI The TSF shall ensure [*video*] data transits the TOE unidirectionally from the [*TOE computer video*] interface to the [*TOE peripheral device display*] interface.

5.2.2.34 Internal Protocol Conversion (FDP_IPC_EXT.1)[i]

FDP_IPC_EXT.1.1 The TSF shall convert the [*DisplayPort*] protocol at the [***DisplayPort computer video interface***] into the [***HDMI***] protocol within the TOE.

FDP_IPC_EXT.1.2 The TSF shall output the [***HDMI***] protocol from inside the TOE to [***peripheral display interface(s)***] as [***[DisplayPort] protocol, [HDMI] protocol***].

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 administrator.

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 administrator.

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 [*modify the behavior of*] the functions [**TOE user authentication device filtering whitelist and blacklist**, **TOE keyboard and mouse filtering blacklist**] to [*the authorized administrators*].

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: [**modify TOE user authentication device filtering whitelist and blacklist, modify TOE keyboard and mouse filtering blacklist, 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 [*administrators*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 Failure with Preservation of Secure State (FPT_FLS_EXT.1)

FPT_FLS_EXT.1.1 The TSF shall preserve a secure state when the following types of failures occur: failure of the power-on self-test and [***failure of the anti-tamper function***].

5.2.5.2 No Access to TOE (FPT_NTA_EXT.1)

FPT_NTA_EXT.1.1 TOE firmware, software, and memory shall not be accessible via the TOE's external ports, with the following exceptions: [***the Extended Display Identification Data (EDID) memory of Video TOEs may be accessible from connected computers; the configuration data, settings, and logging data that may be accessible by authorized administrators***].

5.2.5.3 Passive Detection of 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.

5.2.5.4 Resistance to Physical Attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist [*a physical attack for the purpose of gaining access to the internal components, to damage the anti-tamper battery, to drain or exhaust the anti-tamper battery*] to the [*TOE enclosure and any remote controllers*] by the attacked component becoming permanently disabled.

5.2.5.5 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.2.5.6TSF Testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self-tests [during initial start-up and at the conditions ***[upon reset button activation]***] to demonstrate the correct operation of [user control functions and ***[active anti-tamper functionality]***].

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

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

5.2.5.7 TSF Testing (FPT_TST_EXT.1)

FPT_TST_EXT.1.1 The TSF shall respond to a self-test failure by providing users with a [***visual***] indication of failure and by shutdown of normal TSF functions.

5.2.6 TOE Access (FTA)

5.2.6.1 Continuous Indications (FTA_CIN_EXT.1)

FTA_CIN_EXT.1.1 The TSF shall display a visible indication of the selected computers at all times when the TOE is powered.

FTA_CIN_EXT.1.2[2] The TSF shall implement the visible indication using the following mechanism: easily visible graphical and/or textual markings of each source video on the display, [***a button, a panel with lights***].

Application Note: *The refined text: "*easily visible graphical and/or textual markings of each source video on the display", *is added per the Video/Display Devices Module.*

Application Note: *The selected computer is indicated with a panel with lights that corresponds to the computer selection buttons. The CAC function of each port can be enabled or*

[2] TD0539 clarifies that the mandatory selection (refined by the VI-Module) applies if the TOE fits the Combiner Use Case selecting "multiple connected displays" in FDP_CDS_EXT.1.1. The TOE does not fit the Combiner User Case but rather selects "multiple connected displays" because some models support dual-displays from a single source video feed. Therefore, the selection does not apply.

disabled for a particular computer. The CAC LED lights bright green to indicate that the CAC function is enabled for that corresponding port. Each port has its own Port LED and CAC LED.

FTA_CIN_EXT.1.3 The TSF shall ensure that while the TOE is powered the current switching status is reflected by [***multiple indicators which never display conflicting information***].

Application Note: *As indicated in FTA_CIN_EXT.1.2, the TOE has a light panel that shows the selected computer and whether the CAC port for the computer is enabled. There is no situation in which the selected computer will be indicated with the light panel and a different computer will be indicated with the selection button.*

5.3 TOE Security Assurance Requirements

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

Table 9: Assurance Components

Requirement Class	Requirement Component
Security Target (ASE)	Conformance Claims (ASE_CCL.1)
	Extended Components Definition (ASE_ECD.1)
	ST Introduction (ASE_INT.1)
	Security Objectives (ASE_OBJ.2)
	Derived Security Requirements (ASE_REQ.2)
	Security Problem Definition (ASE_SPD.1)
	TOE Summary Specification (ASE_TSS.1)
Development (ADV)	Basic Functional Specification (ADV_FSP.1)
Guidance Documents (AGD)	Operational User Guidance (AGD_OPE.1)
	Preparative Procedures (AGD_PRE.1)
Life Cycle Support (ALC)	Labeling of the TOE (ALC_CMC.1)
	TOE CM Coverage (ALC_CMS.1)
Tests (ATE)	Independent Testing – Conformance (ATE_IND.1)
Vulnerability Assessment (AVA)	Vulnerability Survey (AVA_VAN.1)

6 TOE Summary Specification

This chapter describes the following security functions:

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

6.1 Security Audit (FAU_GEN.1)

The TOE logs security events such as start-up and shutdown of the audit functions; power cycle events, self-test failures; peripheral device acceptance and rejections; and 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 login, 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 and time (UTC), a code that indicates the type of event and the outcome (success or failure) of the event. The critical audit events recorded and identified in the code include:

- administrator logon events (login failed, last login ok),
- administrator actions (password changes, Reset to Factory Default),
- KVM locked due to Administrator's failed attempts to login,
- peripheral device rejections,
- all failed self-tests except button jam.

Non-critical audit events include:

- power-cycle events,
- administrator logon ok and logout,
- configuration of the whitelist/blacklist,
- peripheral device acceptance,
- button jam test failure, and
- all passing self-tests.

During normal operation, the TOE provides administrator access to all audit records. ATEN's assistance is required to read audit records from an inoperable switch (i.e., logs for self-test failures (except for button jam) and tamper detection that would cause the TOE to enter a failed state).

The logs are stored on EEPROM within 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 modify or delete any of the information stored on the TOE. The TOE stores the critical event logs only for the most recent occurrence of events. The TOE stores a maximum of thirty-two critical 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).

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, analog audio speakers, USB smart card / CAC readers and DisplayPort/HDMI display. All other devices are rejected. The TOE accepts either DisplayPort or HDMI signals at the computer interface. DisplayPort signals are internally converted to HDMI. These signals are then either converted back to DisplayPort or output as HDMI depending on the monitors connected to the TOE.

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 switches to another selected computer or when the TOE is powered down.

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

6.2.1 FDP_AFL_EXT.1 – Audio Filtration

The TOE's audio function implementation filters the audio passing through the TOE in accordance with Table 8: Audio Filtration Specifications above.

6.2.2 FDP_APC_EXT.1 (All Iterations); FDP_UDF_EXT.1/AO – Unidirectional Data Flow (Audio Output); FDP_UDF_EXT.1/KM – Unidirectional Data Flow (Keyboard/Mouse); FDP_UAI_EXT.1 User Authentication Isolation; FDP_UDF_EXT.1/VI – Unidirectional Data Flow (Video Output)

The TOE routes audio and video data only from the selected computer to the attached peripherals and routes the keyboard and mouse data only to the selected computer from the attached peripherals. User authentication data transits the TOE in both directions.

Each supported peripheral (i.e., audio signals, video signals, USB authentication device, and input data (i.e. HID data)) has its own dedicated data path implemented in circuitry. This ensures the data is isolated and only routed in the correct direction.

On device startup, once EDID data has been read into memory from any connected monitors, 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.

The USB authentication device connection is on a separate circuit isolated from all other TOE USB functions and, after filtering for qualification, has a direct connection path to the selected computer. The TOE does not emulate the user authentication device function.

All keyboard and mouse connections are filtered first to ensure that they are valid HID-class devices, and then only the authorized HID-class devices absent from the TOE's blacklist will be allowed. The data input by the authorized USB keyboard and mouse will be emulated by TOE as USB data for transmission to the selected computer.

No data or electrical signals flow between connected computers at any time. Each connected computer has its own independent device controller, power circuit, and EEPROM.

No data transits the TOE when the TOE is powered off or when the TOE is in a failure state.

6.2.3 FDP_CDS_EXT.1 – Connected Displays Supported

The TOE supports connected displays from a single selected computer's video feed (either single-head or multi-head). Because of this, the single selected source video feed is always the same channel and indication of the selected channel is through the channel selection LEDs on the TOE chassis.

The DisplayPort/HDMI models CS1182DPH4C and CS1184DPH4C each support one connected display. While CS1142DPH4C and CS1144DPH4C each support two connected displays at a time.

6.2.4 FDP_FIL_EXT.1/KM – Device Filtering (Keyboard/Mouse); FDP_PDC_EXT.3/KM – Authorized Connection Protocols (Keyboard/Mouse)

The TOE supports authorized USB keyboard and mouse peripherals as defined in **Table 10: Supported protocols by port** below. Keyboard/mouse peripherals are filtered and emulated. Device filtering for keyboard/mouse interfaces is configurable. Keyboard/mouse blacklisted devices are unauthorized devices. Whitelisted devices are authorized devices for the keyboard/mouse interfaces in peripheral device connections. The KVM includes a built in allowed list (whitelist) for the USB keyboard/mouse ports based on being valid HID-class devices. Individual HID-class devices can be blacklisted by the administrator for the USB keyboard/mouse ports, which then takes priority over the whitelist. The USB keyboard/mouse Ports do not support a "whitelist" function beyond ensuring that the USB device type is valid.

The configurable HID device function enables authorized administrators to assign a blacklist for HID devices. To blacklist a keyboard/mouse device, the admin connects the HID device that they want blacklisted directly to the Mouse Port (do not connect it to the KVM via a USB hub), and performs the configuration via administrator functions. After configuration, the blacklisted HID device will be rejected by both Keyboard/ Mouse Ports. The Reset KVM to Default function will clear the blacklist created by the Secure KVM administrator functions.

The TOE emulates data from authorized USB Keyboard and Mouse protocol interfaces to USB connected computers.

6.2.5 FDP_FIL_EXT.1/UA – Device Filtering (User Authentication Devices)

All TOE Secure KVM Switch models support configurable USB authentication device (CAC reader and smart card) peripheral devices.

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 (e.g. 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 on the TOE's administrative interface to configure CAC filters. Configuration options are limited to allowing or blocking the 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 secondary whitelist and/or blacklist for the TOE. As stated in Section 2.3, the Port Authentication Utility supports Microsoft Windows 8 and higher. The Port Authentication Utility computer connects to the TOE via USB connection to Computer Port 1. 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 blacklist and whitelist filtering lists created by the Port Authentication Utility. For example, if a device was by default blacklisted by the Port Authentication Utility, it will be allowed if it has been whitelisted by Administrator-defined list. If a device is blacklisted in Administrator-defined list, the device will be rejected even if was by default whitelisted in

Port Authentication Utility-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 and considered unauthorized. If there is no defined blacklist, the devices defined in the default built-in whitelist are allowed. If a device is not on any list, it is rejected.

6.2.6 FDP_PDC_EXT.1 – Peripheral Device Connection; FDP_PDC_EXT.2/AO – Peripheral Device Connection (Audio Output); FDP_PDC_EXT.2/KM – Authorized Devices (Keyboard/Mouse); FDP_PDC_EXT.2/UA – Authorized Devices (User Authentication Devices); FDP_PDC_EXT.2/VI – Peripheral Device Connection (Video Output); FDP_PDC_EXT.4 – Supported Authentication Device

The TOE allows the authorized devices and protocols for the PSD Console Ports as identified in the table below upon TOE power up and upon connection of a peripheral device to a powered-on TOE. The console USB keyboard and mouse ports are interchangeable, meaning you can connect a keyboard to the mouse port and vice versa. 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 TOE has both DisplayPort and HDMI interfaces on both the computer and peripheral ports. These are distinct physical connectors that interface with the same video board such that connections of either or both types can be used. If a computer is connected to the TOE via DisplayPort, the video signal is converted to HDMI. If a computer is connected to the TOE via HDMI, the video signal is already HDMI so no conversion is needed. Whether it is output as HDMI to any connected monitors or converted back to DisplayPort depends on which port(s) are used by the connected monitor(s).

The TOE supports external smartcard and CAC reader user authentication devices.

The TOE does not allow any other user data transmission to or from any other external entities including wireless devices. The TOE only recognizes those peripherals with an authorized interface type as described below and all other peripherals will be denied both upon TOE power up and upon connection of a peripheral device to a powered-on TOE. Peripheral LEDs (one per port) are located on the front (except video LEDs are located on the back) and provide a continuous visual indication of the status of the function associated with that port. The LED flashes when a connected peripheral is rejected.

Specifically the TOE supports the following peripherals on the console interfaces:

Table 10: Supported protocols by port

PSD Console Port	Authorized Devices	Authorized Protocol
Keyboard	Standard 108 key wired keyboard and keypad	USB 1.1/2.0
Display	Display, Video or KVM extender	DisplayPort/HDMI
Mouse/Point Device	Standard 2-button, 3-button, and 5-button wired mouse or trackball	USB 1.1/2.0

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

Additionally, the KVM has interfaces for DC power, reset (button), and LED indicators. The LEDs consist of Video, Num Lock, Caps Lock, Scroll Lock, power LEDs, Port LEDs, and CAC LEDs. For dual-display models there are two LEDs. Video LED(s) light green when the video connection(s) are up and running. The Video LEDs flash when a non-qualified monitor is connected. The Num Lock LED, Caps Lock LED, and Scroll Lock LED on the keyboard are disabled. The Port/CAC LEDs indicate Port/CAC reader selection/connection status. All LEDs are located on the RPS and on the front panel of the main KVM except the Video LED(s) that are located on the back panel. The TOE does not allow any other user data transmission to or from external entities.

Non-HID functions of a composite USB device; internal Hub; USB CAC Hub; docking protocols; and analog microphone or audio line inputs are not supported by the TOE. 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 ATEN Secure KVM Switch. If supported, only basic (HID) keyboard operations will function.

6.2.7 FDP_PUD_EXT.1 – Powering Unauthorized Devices

The TOE does not supply power to any device connected to the analog audio output interface.

6.2.8 FDP_PWR_EXT.1 Powered By Computer

The Secure KVM Switch provides power to connected user authentication devices via the USB protocol; is isolated from other circuitry; and cannot be powered by a user authentication device.

6.2.9 FDP_RIP.1/KM – Residual Information Protection (Keyboard Data), FDP_RIP_EXT.1 – Residual Information Protection and FDP_RIP_EXT.2 – Purge of Residual Information

No user data is written to TOE non-volatile memory or storage. User keyboard data is purged and not available to the next connected TOE computer interface when the TOE is switched to a different computer. The data input by the authorized keyboard/mouse will be kept in the console authorized keyboard/mouse buffer (in the microcontroller). Once the TOE is power cycled, reset, or port switching is detected, the data in the console authorized keyboard/mouse buffer will be deleted immediately, and not processed for emulation. Please refer to the Proprietary Isolation Document for more detail.

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 to Factory 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). Audit logs are retained and a log is generated for Reset to Factory Default.

The TOE also provides non-administrative users a front panel reset button. The reset function is performed by holding the Reset button for more than 5 seconds. This purges the Keyboard/Mouse buffer, resets the CAC enable/disable feature is restored to the default 'enabled' state, initiates a self-test, and switches the TOE to Port 1. CDF configured by Administrator, logs, Administrative tasks, or other secure functions are not affected by the front panel Reset function.

The Letter of Volatility provided in Appendix A identifies the TOE components that have non-volatile memory and provides details of the memory and its use.

6.2.10 FDP_SWI_EXT.1 – PSD Switching; FDP_SWI_EXT.2 – PSD Switching Methods; FDP_SWI_EXT.3 – Tied Switching

The keyboard, mouse, video, audio, and USB smart card CAC reader ports are always switched together to the same connected computer using a push button on the front of the device or the wired PSD remote control (i.e., the RPS). As such, the keyboard and mouse are always switched together and there are no options to switch peripherals independently from the keyboard and mouse. When the PSD is attached to a 2-Port Secure KVM Switch, only pushbuttons numbered 1 and 2 will be detected and functional. When the PSD is attached to a 4-Port Secure KVM Switch, only pushbuttons numbered 1, 2, 3, and 4 will be detected and functional. The TOE does not allow switching to be initiated through automatic port scanning, control through a connected computer, or control through keyboard shortcuts. Note that the CAC interface can be turned on/off independently of the other peripherals so when it is disabled, all peripherals except for the CAC will be switched to the same computer and the CAC will remain inactive.

6.2.11 FDP_TER_EXT.1 Session Termination; FDP_TER_EXT.2 Session Termination or Removed Devices; FDP_TER_EXT.3 Session Termination upon Switching

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 and not on a blacklist (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.

The Secure KVM Switch 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 0.2 sec, 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, terminating an open session. If an inserted 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 is no power to the switch, the CAC channel is like a broken path (open switch). This prevents active sessions from continuing.

6.2.12 TOE Video Security Function (FDP_IPC_EXT.1, FDP_PDC_EXT.3/VI, FDP_SPR_EXT.1/DP, FDP_SPR_EXT.1/HDMI)

In addition to the Base-PP SFRs and SFRs related to the video function described above, the TOE video input and output features in this section are also implemented in the TOE video subsystem.

The TOE video auxiliary channel (AUX) path blocks information flows other than the minimal set required to establish the DisplayPort 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 an HDMI video stream. The EDID of the connected monitor(s) is read once at startup and written to EEPROM associated with each computer port by an HDMI transceiver.

All AUX channel communications are filtered through the conversion from DisplayPort to HDMI protocols. This ensures that the only authorized sub-protocols for DisplayPort are EDID from display to computer, HPD from display to computer, and link training. All other types of traffic are filtered. All TOE models accept DisplayPort for the computer video display interface. The TOE will convert a DisplayPort signal to HDMI inside the TOE. It will then be either output as DisplayPort or as HDMI to the connected monitor(s), based on the connection used by the monitor(s). The TOE rejects communication of EDID information from computer to display, as well as CEC, HDCP, and MCCS communications. The TOE's video EDID read procedure is automatically activated once during power-on or reboot in order to read the connected display EDID information.

All TOE models accept HDMI for the computer video display interface. The HDMI signal will be output as DisplayPort or as HDMI to the connected monitor(s), based on the connection used by the monitor(s). The TOE blocks ARC, CEC, EDID from computer to display, HDCP, HEAC, HEC, and MCCS sub-protocols; only EDID from display to computer and HPD from display to computer are authorized.

6.3 Identification and Authentication (FIA_UAU.2/ FIA_UID.2)

Authentication is required to perform administrator functions such as configuring the user authentication device filtering (i.e. 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/keyboard/mouse filtering (i.e. 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 FMT_MOF.1 – Management of Security Functions Behavior

The TOE restricts the management functions such as the ability to modify the HID device filtering blacklist and user authentication device filtering (i.e. CDF) whitelist and blacklist to the authorized administrator.

The authorized administrator must successfully authenticate by providing a valid password. There is no login name parameter for the login function. Customers are provided with a default password. The administrator guide states that the administrator must change the password after the first successful logon. The password is case sensitive and new passwords must contain at least 1 lower case letter, at least 1 upper case letter, at least 1 numeric character, and at least 1 special character. The supported special characters are: !"#$%&' ()*+,-./ :;<=>? @ [\]^_ ` {|}~ (including "space"). Additionally, the password length must be at least 8 characters but no longer than 22 characters. With three failed attempts to log in, the administrator logon mode will be terminated and locked for 15 minutes. With nine failed login attempts, the Secure KVM Switch will become permanently inoperable. There is no mechanism to restore a lost/forgotten password.

6.4.2 FMT_SMF.1 – Specification of Management Functions

The TOE provides security management functions to configure the user authentication and keyboard/mouse device filtering (i.e. 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 and blacklist definitions for keyboard/ mouse devices. Once successfully authenticated, the Administrator can choose to add, edit, or remove a device to the user authentication device whitelist/blacklist or add a device to the keyboard/ mouse devices blacklist.

If a device is on the whitelist, the TOE considers the device as authorized. Otherwise, if the device is on the blacklist or is not on any list 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[3] (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 to Factory 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 Reset to Factory Default does not affect or erase Log data nor does it affect the previously changed Administrator password.

6.4.3 FMT_SMR.1 – Security Roles

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

[3] Vendor guidance documents also refer to this as 'Reset KVM to Default'.

password, and configure user authentication device/ keyboard/ mouse filtering (i.e. CDF). Users without an administrator role cannot use these functions and are not required to authenticate.

Since there are no usernames, any user who knows the password for the Port Authentication Utility or management console has administrator-level access. All other users are considered non-administrative users.

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's KVM has a tamper-evident label printed with the TOE's unique product serial number. The label is applied to the bottom of the chassis, over one of the screws used to secure the bottom of the enclosure. The label can be clearly seen when the device is turned over. The optional Remote Port Selector (RPS) includes its own tamper-evident tape to provide visual indications of intrusion to the RPS enclosure. Any attempt to open the KVM or RPS enclosures sufficient to gain access to internal components will change the labels to a tampered state. If the tamper-evident seal is missing or peeled, avoid using the product and contact the ATEN dealer.

6.5.1 FPT_FLS_EXT.1 – Failure with Preservation of Secure State

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 below 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.

6.5.2 FPT_NTA_EXT.1 – No Access to TOE

The TOE firmware, software, and memory is not accessible from the TOE's external ports, with the following exceptions:

- the Extended Display Identification Data (EDID) memory for Video is accessible from connected computers;
- the configuration data, settings, and logging data is accessible by authorized administrators.

6.5.3 FPT_PHP.1 – Passive Detection of Physical Attack and FPT_PHP.3 – Resistance to Physical Attack

The TOE becomes permanently inoperable and all front panel or RPS 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 ATEN.

The KVM and RPS contain internal batteries with a minimum lifetime of five years, are 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. See Section 6.5.5 for additional details. The admin guide instructs users to never attempt to replace the battery or open the switch or RPS enclosure.

If a mechanical intrusion is detected on the switch, the switch (without RPS connected) will be permanently disabled and all the front panel LEDs (except the Power LED) will flash continuously. A mechanical intrusion is detected by a pressure switch that trips when the enclosure is opened. If a mechanical intrusion is detected by the RPS (connected with the switch and aligned), this will permanently disable both the RPS itself and the switch, and all LEDs (on RPS) and the front panel LEDs except the Power LED (on switch) will flash continuously. When the RPS is tampered but unconnected to the KVM, the KVM will not accept the tampered RPS device but will be otherwise unaffected by the RPS's tamper. And if the RPS is connected to the KVM when the RPS is tampered, then both the KVM and the RPS device will be tampered. To disable the KVM in the event of an aligned RPS, the RPS will send a "tampering command" to the KVM.

6.5.4 FPT_STM.1 Reliable Time Stamps

The TOE includes its own time clock to provide reliable time stamps for its auditing functions and for measuring the lockout duration following three failed authentication attempts. The developer sets the time to UTC (Coordinated Universal Time) during manufacturing; the time zone is not configurable.

6.5.5 FPT_TST.1 – TSF Testing and FPT_TST_EXT.1 – TSF Testing

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 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.

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. Upon a failure, the TOE will be in a failure state (permanently inoperable).
- 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. Upon a failure, the TOE will be in a failure state (permanently inoperable).
- 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. Upon a failure, the TOE will be in a failure state (permanently inoperable).
- Key stuck test (KVM front panel Push button jam test): the TOE will check the status of all button values in the micro-controller to ensure the push buttons are operational. Upon a test failure, the TOE does not shut down, the front panel Port LED and CAC LED of that jammed button port will flash. The TOE will resume operation after the key stuck is fixed and power cycled.

- Anti-tampering mechanism test: the TOE will verify if the tamper detection switch is triggered (includes KVM and RPS battery is damaged or exhausted tests). Upon a test failure, the TOE will be in a failure state (permanently inoperable).
- RPS connection self-tests. Upon a test failure, the TOE does not shut down.

The anti-tampering self-tests include the correct operation and tampering of the internal KVM and RPS batteries.

- A KVM detecting tampering during normal operation will trigger the KVM inoperable.
- A connected and aligned RPS detecting tampering (including damaged or exhausted battery) during normal operation will trigger the RPS inoperable and also directly trigger the KVM inoperable in parallel.
- A damaged or exhausted KVM battery will be detected during self-test will trigger the KVM permanently inoperable.

RPS Connection test failure results from the following:

- Connecting a "tampered" RPS to KVM (before KVM power-up) → This RPS was already tampered before connecting to KVM, and therefore the RPS will not be detected and aligned with the KVM → The TOE does not shut down.
- Connecting a RPS with battery damaged or exhausted to KVM (before KVM power-up) → This RPS will not be detected and aligned with the KVM → The TOE does not shutdown.
- Connecting any other cable, RPS from other vendors, etc. → will not be detected by KVM → TOE does not shutdown.

Though the RPS Connection test failures do not result in a TOE shut down, this does not affect the TSF because the TOE can function normally without a remote control connected and the TSF does not interface with the remote control while it is in a failure state. This means that a compromised remote control cannot be used as a vector to operate the TOE maliciously.

Connecting a normal (non-tampered) and functional RPS, before KVM power-up, will be detected and aligned with KVM after KVM boots up and results in RPS connection self-test PASS. An RPS connected to the TOE while it is powered on will not be detected until the TOE is reset.

The status indicators on the KVM 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.

The RPS LEDs flash indicators operate as follows:

- Connecting a "tampered" RPS before KVM power-up → The KVM will detect that the RPS is tampered and reject the connection with RPS ⟶ The RPS LEDs flash.
- Connecting a RPS with battery damaged or exhausted to KVM before KVM power-up → The KVM will detect the RPS battery status and reject the connection with RPS ⟶ The RPS LEDs flash.

- A connected and aligned RPS will flash all LEDs when it is tampered during normal operation.

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, push buttons, 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 push button is broken and truly stuck), the KVM remains disabled since it fails the button jam self-test.

Users can verify the integrity of the TOE by triggering a self-test (e.g. by powering on or rebooting the TOE) and examining the front panel LEDs for self-test failures as identified above.

The TOE performs self-tests as described above to demonstrate the correct operation of active anti-tamper functionality (see also 6.5.3 FPT_PHP).

6.6 TOE Access

The TOE display a continuous visual indication of the computer to which the user is currently connected, and 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 FTA_CIN_EXT.1 – Continuous Indications

The TOE displays continuous visual indicators of the computer to which the user is currently connected at all times when the TOE is powered.

The Port LEDs on the Secure KVM Switch are located on the front panel (of the switch) and the upper-left side of each push button (of the RPS) provide a continuous visual indication of the selected Port and corresponding selected computer (green) and the connection status of all other connected computers (orange indicates the connected computer is running). If a RPS is detected and aligned with KVM, the status of KVM will reflect on both the KVM front panel LEDs and RPS front panel LEDs.

On power up and reset, Port 1 is selected by default.

The TOE supports connected displays from a single source video feed (either single-head or multi-head). Because of this, the single selected source video feed is always the same channel as all other peripherals, and indication of the selected channel is indicated through the channel selection LEDs on the TOE chassis.

CAC reader LEDs (one per Port) are also located on the front panel (of the switch) and the far right of the upper bar on the panel (of the RPS) 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 orange 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 Push button for more than 3 seconds (this is a toggle feature).

7 Protection Profile Claims

This ST is conformant to the Protection Profile [PSD], including the following optional and selection-based SFRs: FAU_GEN.1, FDP_RIP_EXT.2, FDP_SWI_EXT.2, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_SMF.1, FMT_SMR.1, FPT_PHP.3, FPT_STM.1, and FTA_CIN_EXT.1.

The ST is also conformant to the following PP-Modules

- PP-Module for Analog Audio Output Devices, Version 1.0, 19 July 2019 [MOD_AO_V1.0].
- *PP-Module for Keyboard/Mouse Devices*, Version 1.0, 19 July 2019 [MOD_KM_V1.0], including the following optional and selection-based SFRs: FDP_FIL_EXT.1/KM, FDP_RIP.1/KM, and FDP_SWI_EXT.3
- *PP-Module for User Authentication Devices*, Version 1.0, 19 July 2019 [MOD_UA_V1.0], including the following selection-based SFRs: FDP_TER_EXT.2 and FDP_TER_EXT.3
- *PP-Module for Video/Display Devices*, Version 1.0, 19 July 2019 [MOD_VI_V1.0], including the following selection-based SFRs: FDP_CDS_EXT.1, FDP_IPC_EXT.1, FDP_SPR_EXT.1/DP, and FDP_SPR_EXT.1/HDMI

As explained in Section 3, the Security Problem Definition of the [PSD] and modules have been included in this ST by reference.

As explained in Section 4, Security Objectives, the Security Objectives of the [PSD] and modules have been included by reference in this ST.

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

Table 11*1* identifies the SFRs that are satisfied by the TOE.

Table 11: SFR Protection Profile Sources

Requirement Class	Requirement Component	Source
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	[PSD]
FDP: User Data Protection	FDP_AFL_EXT.1 – Audio Filtration	[MOD_AO_V1.0]
	FDP_APC_EXT.1 – Active PSD Connections	[PSD]
	FDP_CDS_EXT.1 – Connected Displays Supported	[MOD_VI_V1.0]
	FDP_FIL_EXT.1/KM – Device Filtering (Keyboard/Mouse)	[MOD_KM_V1.0]
	FDP_FIL_EXT.1/UA – Device Filtering (User Authentication Devices)	[MOD_UA_V1.0]
	FDP_IPC_EXT.1 – Internal Protocol Conversion	[MOD_VI_V1.0]
	FDP_PDC_EXT.1 – Peripheral Device Connection	[PSD]
	FDP_PDC_EXT.2/AO – Peripheral Device Connection (Audio Output)	[MOD_AO_V1.0]
	FDP_PDC_EXT.2/KM – Authorized Devices (Keyboard/Mouse)	[MOD_KM_V1.0]

Requirement Class	Requirement Component	Source
	FDP_PDC_EXT.2/UA – Authorized Devices (User Authentication Devices)	[MOD_UA_V1.0]
	FDP_PDC_EXT.2/VI – Peripheral Device Connection (Video Output)	[MOD_VI_V1.0]
	FDP_PDC_EXT.3/KM – Authorized Connection Protocols (Keyboard/Mouse)	[MOD_KM_V1.0]
	FDP_PDC_EXT.3/VI – Authorized Connection Protocols (Video Output) (DP Models)	[MOD_VI_V1.0]
	FDP_PDC_EXT.4 – Supported Authentication Device	[MOD_UA_V1.0]
	FDP_PUD_EXT.1 – Powering Unauthorized Devices	[MOD_AO_V1.0]
	FDP_PWR_EXT.1 Powered By Computer	[MOD_UA_V1.0]
	FDP_RIP.1/KM – Residual Information Protection (Keyboard Data)	[MOD_KM_V1.0]
	FDP_RIP_EXT.1 – Residual Information Protection	[PSD]
	FDP_RIP_EXT.2 – Purge of Residual Information	[PSD]
	FDP_SPR_EXT.1/DP – Sub-Protocol Rules (DisplayPort Protocol)	[MOD_VI_V1.0]
	FDP_SPR_EXT.1/HDMI – Sub-Protocol Rules (HDMI Protocol)	[MOD_VI_V1.0]
	FDP_SWI_EXT.1 – PSD Switching	[PSD]
	FDP_SWI_EXT.2 – PSD Switching Methods	[PSD]
	FDP_SWI_EXT.3 – Tied Switching	[MOD_KM_V1.0]
	FDP_TER_EXT.1 Session Termination	[MOD_UA_V1.0]
	FDP_TER_EXT.2 Session Termination or Removed Devices	[MOD_UA_V1.0]
	FDP_TER_EXT.3 Session Termination upon Switching	[MOD_UA_V1.0]
	FDP_UAI_EXT.1 User Authentication Isolation	[MOD_UA_V1.0]
	FDP_UDF_EXT.1/AO – Unidirectional Data Flow (Audio Output)	[MOD_AO_V1.0]
	FDP_UDF_EXT.1/KM – Unidirectional Data Flow (Keyboard/Mouse)	[MOD_KM_V1.0]
	FDP_UDF_EXT.1/VI – Unidirectional Data Flow (Video Output)	[MOD_VI_V1.0]
FIA: Identification and Authentication	FIA_UAU.2 – User Authentication Before Any Action	[PSD]
	FIA_UID.2 – User Identification Before Any Action	[PSD]
FMT: Security Management	FMT_MOF.1 – Management of Security Functions Behavior	[PSD]
	FMT_SMF.1 – Specification of Management Functions	[PSD]
	FMT_SMR.1 – Security Roles	[PSD]
FPT: Protection of the TSF	FPT_FLS_EXT.1 – Failure with Preservation of Secure State	[PSD]
	FPT_NTA_EXT.1 – No Access to TOE	[PSD]
	FPT_PHP.1 – Passive Detection of Physical Attack	[PSD]
	FPT_PHP.3 – Resistance to Physical Attack	[PSD]
	FPT_STM.1 Reliable Time Stamps	[PSD]

Requirement Class	Requirement Component	Source
	FPT_TST.1 – TSF Testing	[PSD]
	FPT_TST_EXT.1 – TSF Testing	[PSD]
FTA: TOE Access	FTA_CIN_EXT.1 – Continuous Indications	[PSD]

8 Rationale

This security target includes by reference the [PSD], [MOD_AO_V1.0], [MOD_KM_V1.0], [MOD_UA_V1.0], and [MOD_VI_V1.0] Security Problem Definitions, Security Objectives, and Security Assurance Requirements. The security target makes no additions to the [PSD] or listed modules assumptions. The [PSD] and listed module's security functional requirements have been reproduced with the Protection Profile operations completed. Operations on the security requirements follow [PSD] and the module's application notes and assurance activities. Consequently, [PSD] and the module's 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. Table2 demonstrates the relationship between security requirements and security functions.

Table 12: Security Functions vs. Requirements Mapping

Specifications	Security Audit	User Data Protection	Identification and Authentication	Security Management	Protection of the TSF	TOE Access
FAU_GEN.1	X					
FDP_AFL_EXT.1		X				
FDP_APC_EXT.1		X				
FDP_CDS_EXT.1		X				
FDP_FIL_EXT.1/KM		X				
FDP_FIL_EXT.1/UA		X				
FDP_IPC_EXT.1		X				
FDP_PDC_EXT.1		X				
FDP_PDC_EXT.2/AO		X				
FDP_PDC_EXT.2/KM		X				

Specifications	Security Audit	User Data Protection	Identification and Authentication	Security Management	Protection of the TSF	TOE Access
FDP_PDC_EXT.2/UA		X				
FDP_PDC_EXT.2/VI		X				
FDP_PDC_EXT.3/KM		X				
FDP_PDC_EXT.3/VI		X				
FDP_PDC_EXT.4		X				
FDP_PUD_EXT.1		X				
FDP_PWR_EXT.1		X				
FDP_RIP.1/KM		X				
FDP_RIP_EXT.1		X				
FDP_RIP_EXT.2		X				
FDP_SPR_EXT.1/DP		X				
FDP_SPR_EXT.1/HDMI		X				
FDP_SWI_EXT.1		X				
FDP_SWI_EXT.2		X				
FDP_TER_EXT.1		X				
FDP_TER_EXT.2		X				
FDP_TER_EXT.3		X				
FDP_UAI_EXT.1		X				
FDP_UDF_EXT.1/AO		X				
FDP_UDF_EXT.1/KM		X				
FDP_UDF_EXT.1/VI		X				
FIA_UAU.2			X			
FIA_UID.2			X			
FMT_SMF.1				X		
FMT_SMR.1				X		
FPT_FLS_EXT.1					X	
FPT_NTA_EXT.1					X	
FPT_PHP.1					X	
FPT_PHP.3					X	
FPT_STM.1					X	

Specifications	Security Audit	User Data Protection	Identification and Authentication	Security Management	Protection of the TSF	TOE Access
FPT_TST.1					X	
FPT_TST_EXT.1					X	
FTA_CIN_EXT.1						X

Appendix A Letter of Volatility

Item No.	Component type, Manufacturer, and Part number	Memory Type	Memory Size	Memory Technology	User Data
1	System Controller Host Controller ATEN SICG8021A	Embedded RAM (1)	Undisclosed	Volatile	May contain user data
2	Host Controller Device Emulators ATEN SICG8022A	Embedded RAM (1)	Undisclosed	Volatile	May contain user data
3	System EEPROM ATMEL AT24C512	EEPROM (2)	512K bits	Non-volatile	No user data
4	System Flash EON EN29LV040A	Flash (3)	512K Bytes	Non-volatile	No user data
5	DP Video Controller Flash MXIC MX25L1606E	Flash (4)	16M bits	Non-volatile	No user data
6	HDMI2. 1 Transceiver ADI ADV7674	Embedded RAM (5)	512 Bytes	Volatile	No user data RAM: EDID DATA
7	HDMI2.1 Transceiver Flash MXIC MX25L4006E	Flash (6)	4M bits	Non-volatile	No user data

8	HDMI2.1 to DisplayPort1.4a Converter LT6711GXE	Embedded ROM (7)	64K Bytes	Non-volatile	No user data

Remarks

(1) The Embedded RAM may contain user data.
The Embedded RAM is cleared and user keyboard/mouse data is purged when the Secure KVM powers-off or power-cycles, after switching ports, after a KVM reset (reboot), or a trigger of the tamper-proof mechanism is detected.

(2) The EEPROM does not contain user data. User settings, Secure KVM configuration, and audit records are kept in EEPROM. The user settings and the Secure KVM configuration will be reset to KVM default settings after a Reset to Factory Default. but the audit records remain unchanged after a Reset to Factory Default, KVM reset (reboot), or power-cycle.

(3) The Flash does not contain user data. Firmware code is stored in the Flash and cannot be updated or rewritten. The firmware code remains unchanged after a Reset to Factory Default, KVM reset (reboot), or power-cycle.

(4) The Flash does not contain user data. The firmware code for the HDMI to DP Converter used is stored in the Flash, remaining unchanged after a Reset to Factory Default, KVM reset (reboot), or power-cycle.

(5) The switch's internal EDID RAM does not contain user data. It is for PC Read EDID. The EDID data will be cleared after a KVM reset (reboot) or power-cycle.

(6) The Flash does not contain user data. The firmware code for the HDMI2.1 Transceiver used is stored in the Flash, remaining unchanged after a Reset to Factory Default, KVM Reset (reboot), or power-cycle.

(7) The Flash does not contain user data. The firmware code for the HDMI2.1 to DP1.4a Converter used is stored in the Flash, remaining unchanged after a Reset to Factory Default, KVM Reset (reboot), or power-cycle.

All components are powered by the Secure KVM only.

[i] Modified by TD0842