Secure KVM Switches Family and Unidirectional HDMI Data Blockers Security Target

Version History

Version	Date	Description	Author
V0.1	13 October 2023	First draft	Fibernet
V0.2	14 December 2023	Second draft	Fibernet
V0.3	16 January 2024	Update due to discussion with SGS	Fibernet
V0.4	17 January 2024	Update according to developer comments	Fibernet
V0.5	8 March 2024	Update according to evaluation comments, updating TOE version	Fibernet
V0.6	18 June 2024	Update according to RR-EWP	Fibernet
V0.7	07 August 2024	Updating to address new changes	Fibernet
V0.8	19 August 2024	Update of Physical Scope	Fibernet
V0.9	02 October 2024	Update AGD version and AGD delivery method	Fibernet
V 0.10	30 July 2025	Update of TOE versions and HotKey functionality	Fibernet
V 0.11	5 October 2025	Updates and corrections	Fibernet
V 0.12	15 October 2025	Updates and corrections	Fibernet
V 0.13	16 October 2025	Updates and corrections	Fibernet
V 0.14	19 November 2025	Updates and corrections	Fibernet
V 0.15	1 December 2025	Updates and corrections	Fibernet
V 0.16	15 December 2025	Updates and corrections	Fibernet
V 0.17	19 December 2025	Updates and corrections	Fibernet

1 Introduction

1.1 ST Reference

Title: Fibernet Secure KVM Switches Family and Unidirectional HDMI Data Blockers Security Target
Version: v0.17
Date: 19 December 2025

1.2 TOE Reference

The TOE identifier: Fibernet Secure KVM Switches Family and Unidirectional HDMI Data Blockers
The TOE could be one of the following models listed in Table 1:

TOE model name	Description	TOE Version	PCB Version	Firmware versions
FIS-SKVM-11HDDP Rev-C	BLOCKER 1:1 Secure KVM HDMI or DisplayPort Input	REV C	PCBF0195 REV-C	SNK: SFW0195 v1.4.9 SRC: SOW0195 v1.3.10
FIS-SKVM-21HDDP Rev-C	BLOCKER 2:1 Secure KVM Switch HDMI Inputs or DisplayPort Input	REV C	PCBF0195 REV-C	SNK: SFW0195 v1.4.9 SRC: SOW0195 v1.3.10
FIS-SKVM-22HDDP Rev-C	BLOCKER 2:2 Secure KVM Switch HDMI Inputs or DisplayPort Input	REV C	PCBF0195 REV-C	SNK: SFW0195 v1.4.9 SRC: SOW0195 v1.3.10
FIS-SKVM-22HDDPD Rev-C	BLOCKER 2:2 Secure KVM Switch Dual Display HDMI Inputs or DisplayPort Input	REV C	PCBF0195 REV-C	SNK: SFW0195 v1.4.9 SRC: SOW0195 v1.3.10
FIS-SKVM-41HDDP Rev-C	BLOCKER 4:1 Secure KVM Switch HDMI Inputs or DisplayPort Input	REV C	PCBF0187 REV-C	SNK: SFW0187 v1.4.9 SRC: SOW0187 v1.3.10
FIS-SKVM-42HDDP Rev-C	BLOCKER 4:2 Secure KVM Switch HDMI Inputs or DisplayPort Input	REV C	PCBF0187 REV-C	SNK: SFW0187 v1.4.9 SRC: SOW0187 v1.3.10
FIS-SKVM-42HDDPD Rev-C	BLOCKER 4:2 Secure KVM Switch Dual Display HDMI Inputs or DisplayPort Input	REV C	PCBF0187 REV-C	SNK: SFW0187 v1.4.9 SRC: SOW0187 v1.3.10
FIS-SKVM-82HDDP Rev-C	BLOCKER 8:2 Secure KVM Switch HDMI Inputs or DisplayPort Input	REV C	PCBF0187 REV-C	SNK: SFW0187 v1.4.9 SRC: SOW0187 v1.3.10
FIS-SVID-11HD-4K/FHD Rev-B	myBLOCKER Audio/Video Blocker for HDMI Input	REV B	PCBF0193_REV_A	NA
FIS-SVID-11DP-4K/FHD Rev-B	myBLOCKER Audio/Video Blocker for DisplayPort Input	REV B	PCBF0183_REV_A	NA

Table 1 List of TOE models

TOE Developer: Fibernet

Note:

- The TOE labelled as FIS-SKVM-11HDDP Rev-C, FIS-SKVM-21HDDP Rev-C, FIS-KVM-22HDDP rev-C, and FIS-SKVM-22HDDDP Rev-C all share identical two input and two output secure KVM devices, but just labelled differently and delivered with different number of cables.
- The TOE labelled as FIS-41HDDP Rev-C, FIS-42HDDP Rev-C, and FIS-SKVM-42HDDPD Rev-C all share identical four input and two output secure KVM device, but just labelled differently and delivered with different number of cables.

1.3 TOE Overview

1.3.1 TOE Usage and Major Security Functions

The TOE, Fibernet BLOCKER Secure KVM switch family (hereafter called BLOCKER) and myBLOCKER unidirectional Audio/Video Data Blockers (hereafter called myBLOCKER), includes two possible types of devices:

- A peripheral switching device (PSD) (BLOCKER) which provides secure connection of a set of peripherals to one or more attached computers.
- A unidirectional Audio/Video blocker (myBLOCKER) which ensures one-way communication from the source computer to the display device.

The TOE provides safe and secure access to the local computers that connects to the TOE, and offers high quality, uncompressed and unidirectional HDMI (for both BLOCKER and myBLOCKER), USB and embedded audio transmission (for BLOCKER only).

The TOE has the following advantages:

- Enables Plug and Play functionality for easy setup and use.
- Does not require additional software for operation.
- Incorporates enhanced data protection.
- Offers simple control through front panel buttons for user convenience (for BLOCKER only).
- Enables multiple computers to be accessed using a single set of keyboard, mouse, and display monitors (for BLOCKER only).
- Isolates, filters and emulates communication.
- Enforces unidirectional signal flow.

The typical BLOCKER TOE applications include:

- Enables secure access to multiple PCs with varying security classifications.
- Provides Command and Control capabilities for enhanced system management.

Figure 1 shows the typical deployment scenario of the TOE (BLOCKER).

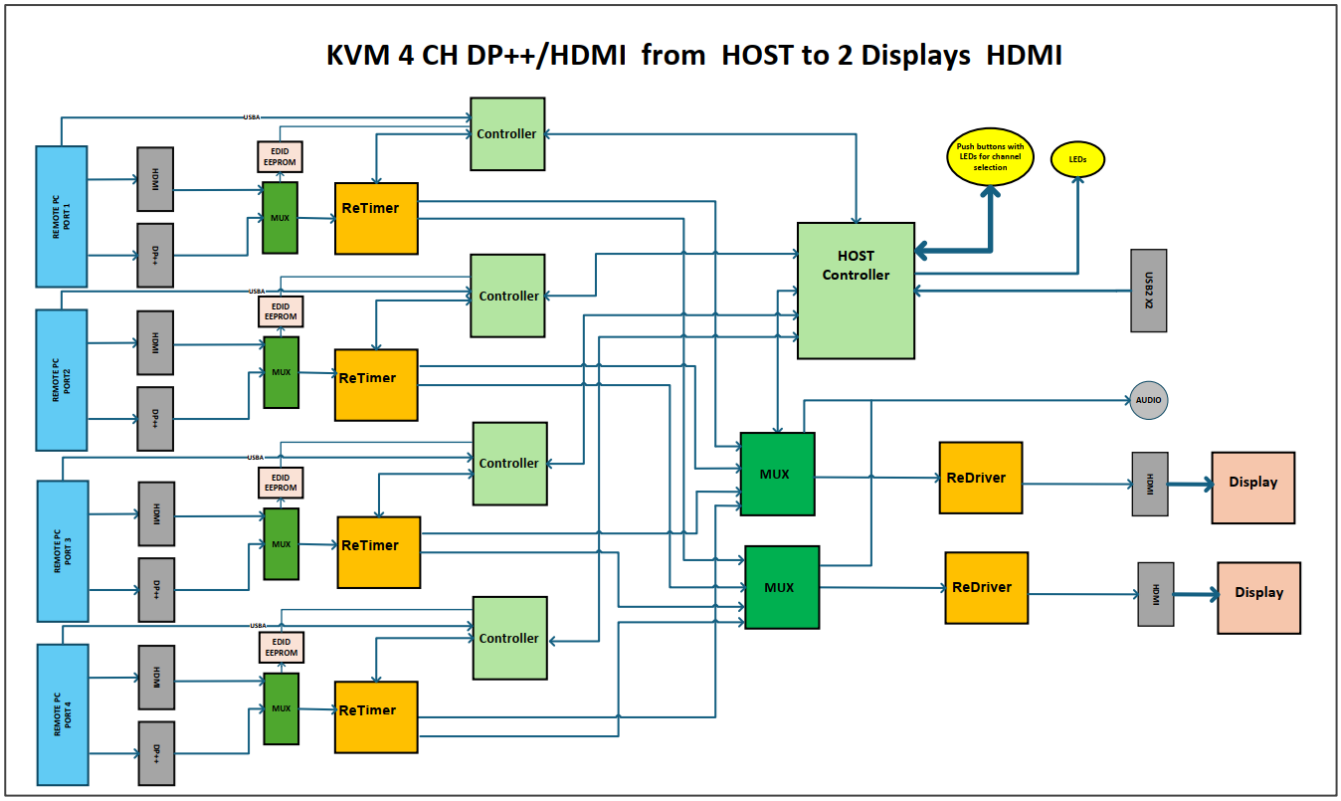
Figure 1 Typical deployment scenario of the TOE

1.3.2 Non-TOE Hardware, Software, and/or Firmware

The TOE does not need any other non-TOE hardware, Software, and/or Firmware to be operated securely[1].

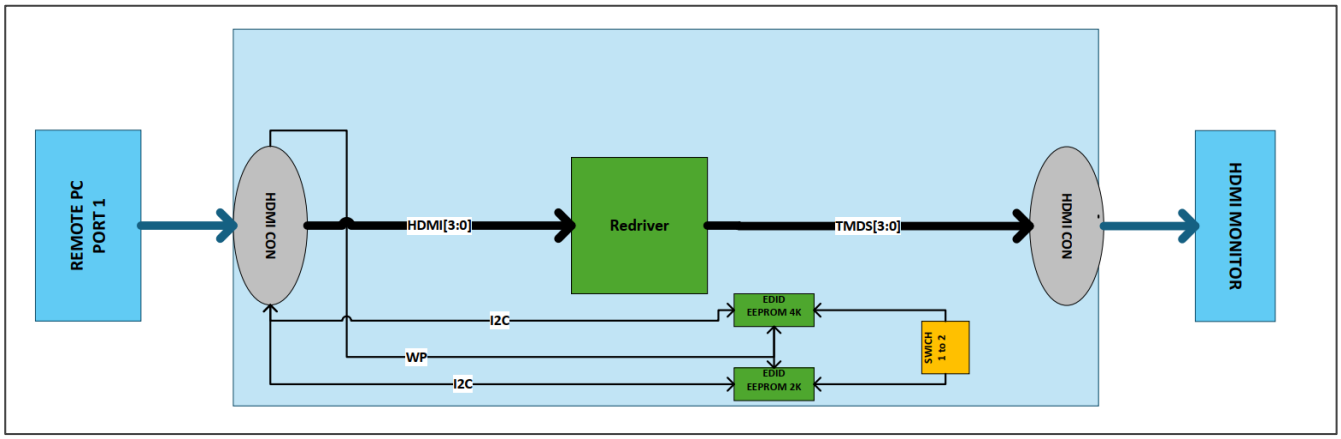
1.3.3 TOE Architecture

The following diagram shows the architecture of the Blocker devices. The different models all share the same architecture, the only difference is in the number of input ports per device (shown in blue in the diagram)

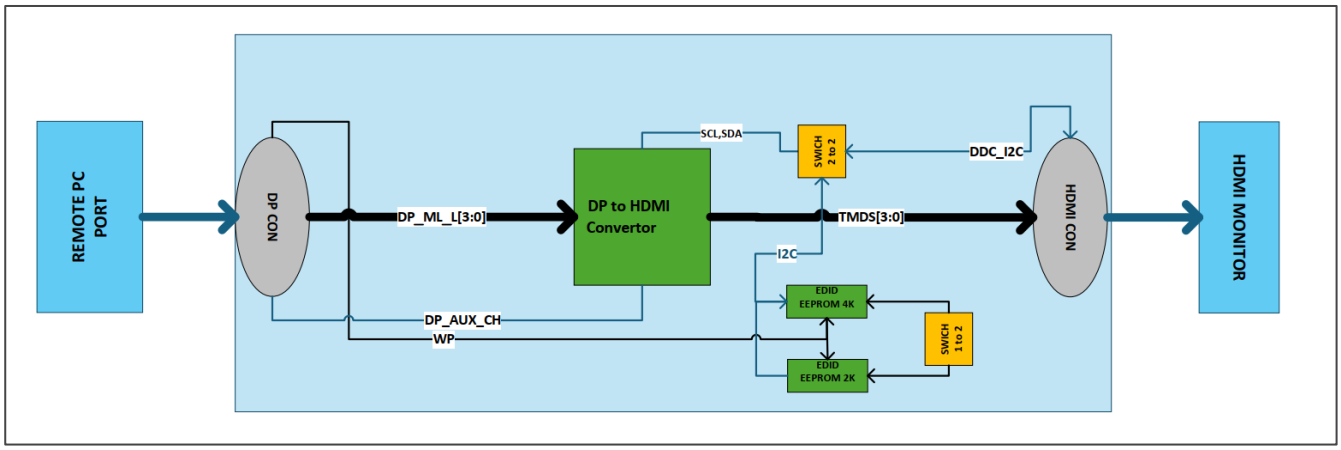


[1] However, for the TOE to be able to function, source computers and peripherals (keyboard, mouse, video, audio) are required.

The following diagrams show the architecture of the MyBlocker Devices:
For the FIS-SVID-11HD-4K/FHD Rev-B:



For the FIS-SVID-11DP-4K/FHD Rev-B:



1.4 TOE Description

1.4.1 Physical Scope

The TOE hardware models are described in Table 1. The TOE firmware is pre-installed in the TOE hardware and shipped together with the TOE hardware.
The following is the list of the TOE guidance:

Type	Name	Version	Format
Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration	Fibernet Secure KVM Switches Family and Unidirectional HDMI Data Blockers CC guidance	V0.7 15 December 2025	.pdf
MyBlocker Datasheet	Secure Video Blocker	Rev A, 20 August 2024	pdf

Table 2 List of TOE guidance

The TOE hardware is delivered by either by direct pick-up by the customer, sent by Fibernet employee, or by a trusted courier such as DHL or UPS.

The guidance documents can be downloaded by scanning the download link that comes with the TOE (for myBlocker series, it will be on the package. For Blocker series, it will be within the packaging box).
The link URL for the myBlocker datasheet is:

https://fibernet-tech.info/my-blocker-manual.pdf

The link URL for the guidance document is:

https://fibernet-tech.info/[AGD]%20Fibernet%20Secure%20KVM%20Switches%20Family%20and%20Unidirectional%20HDMI%20Data%20Blockers%20CC%20guidance%20v0.6.pdf

1.4.2 Logical Scope

The TOE provides user data protection security functionality. The TOE controls the information flow between the peripheral device interfaces and a computer interface. The peripheral devices supported (depending on the TOE type) include USB mouse, USB Keyboard, audio output, and DisplayPort or HDMI video. The security functions provided by the TOE are:

- The TOE ensures a one-way information flow from the computer interface to the display interface only (for both BLOCKER and myBLOCKER)
- The TOE ensures the isolation between the computers connected to the source ports (BLOCKER only).

2 Conformance Claims

2.1 CC Conformation Claim

The ST is CC Part 2 extended conformant [CC] and CC Part 3 conformant [CC]. The version of [CC] 3.1 Revision 5.
ST conforms to EAL4+ALC_FLR.2 as defined in [CC] part 3.
The methodology to be used for evaluation is [CEM] 3.1 Revision 5.

2.2 PP Conformance Claim

The ST does not claim any conformance to any protection profile.

3 Security Problem Definition

3.1 Threats

The threats for the TOE are listed in the sections below.

T.DATA_LEAK
An operator and/or attacker/viewer intentionally or unintentionally receives unauthorized data flow through a connection via the TOE between one or more computers or its connected peripherals. (Applies to Blocker and MyBlocker)

T.RESIDUAL_LEAK
An operator and/or attacker/viewer intentionally or unintentionally receives unauthorized user data between the intended connected computer and another unintended connected computer due to leakage of the TOE (partial, residual, or echo). (Applies to Blocker and MyBlocker)

T.LOGICAL_TAMPER
An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code or data stored in the TOE's volatile or non-volatile memory to allow unauthorized information flows. (Applies to Blocker)

3.2 Organizational security policies

The organizational security policies for the TOE are listed in the sections below.

OSP.UNINTENDED_USE

The TOE shall only be used by trained and approved operators and/or administrators.
The TOE must be installed in a secured environment . (Applies to Blocker)

3.3 Assumptions

This section describes the assumptions made in identification of the threats and security requirements for TOE. The TOE is not expected to provide assurance in any of these areas, and as a result, requirements are not included to mitigate the threats associated. This section applies to both Blocker and MyBlocker.

A.PHYSICAL
The environment provides physical security commensurate with the value of the TOE and the data it processes and contains.

A.NO_WIRELESS_DEVICES
The environment includes no wireless peripheral devices.

A.TRUSTED_ADMIN
TOE Administrators and users are trusted to follow and apply all guidance in a trusted manner.

A.TRUSTED_CONFIG
Personnel configuring the TOE and its operational environment follow the applicable security configuration guidance.

A.USER_ALLOWED_ACCESS

All TOE users are allowed to interact with all connected computers. It is not the role of the TOE to prevent or otherwise control user access to connected computers. Computers or their connected network shall have the required means to authenticate the user and to control access to their various resources.

4 Security Objectives

These security objectives describe how the threats described in the previous section will be addressed. It is divided into:

- The Security Objectives for the TOE, describing what the TOE will do to address the threats and the organizational security policies.
- The Security Objectives for the Operational Environment, describing what other entities must do to address the threats, organizational security policies, and/or assumptions.

A rationale that the combination of all these security objectives indeed addresses the threats may be found in section 6.3.1 of this Security Target.

4.1 Security Objectives for the TOE

The following subsections describe the security objectives for the TOE.

O.COMPUTER_INTERFACE_ISOLATION
The TOE shall prevent unauthorized data flow to ensure that the TOE and its connected peripheral devices cannot be exploited in an attempt to leak data. The TOE-Computer interface shall be isolated from all other TOE-Computer interfaces while TOE is powered. (Applies to Blocker and MyBlocker)

O.COMPUTER_INTERFACE_ISOLATION_ TOE_UNPOWERED
The TOE shall not allow data to transit a TOE-Computer interface while the TOE is unpowered. (Applies to Blocker and MyBlocker)

O.USER_DATA_ISOLATION
The TOE shall route user data, such as keyboard entries, only to the computer selected by the user. The TOE shall provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer. (Applies to Blocker)

O.NO_USER_DATA_RETENTION
The TOE shall not retain user data in non-volatile memory after power up. (Applies to Blocker)

O.AUTHORIZED_USAGE
The TOE shall explicitly prohibit or ignore unauthorized switching mechanisms, either because it supports only one connected computer or because it allows only authorized mechanisms to switch between connected computers. Authorized switching mechanisms shall require express user action restricted to console buttons, console switches, , or hotkeys as defined below. Unauthorized switching mechanisms include automatic port scanning or control through a connected computer.. Where applicable, the results of the switching activity shall be indicated by the TSF so that it is clear to the user that the switching mechanism was engaged as intended. (Applies to Blocker)

Hotkeys are defined as follows:

Shorcut	Action
LCTRL + LCTRL + [1-8]	Switch left channel/monitor 1 to source 1-8
RCTRL + RCTRL + [1-8]	Switch right channel/monitor 2 to source 1-8
LCTRL + LCTRL + F12	Print system info (short version)
RCTRL + RCTRL + F12	Print system info (full version)

CTRL + CTRL + 0 + SCROLLLOCK	Reset/reboot the system
CTRL + CTRL + 0 + R	Reset all configurations to default
CTRL + CTRL + 0 + A	Toggle audio channel locked/unlocked to current channel
CTRL + CTRL + 0 + U	Toggle USB audio interface enabled/disabled
LCTRL + LCTRL + 0 + M	Toggle mouse mode (relative ↔ absolute)
LCTRL + LCTRL + 0 + E	Set all channels to absolute mouse mode (bulk
RCTRL + RCTRL + 0 + E	Set all channels to relative mouse mode (bulk)
CTRL + CTRL + 0 + F	Toggle mouse roam enabled/disabled
CTRL + CTRL + 0 + L	Toggle KM channel locked/unlocked to current channel
CTRL + CTRL + 0 + B	Toggle USB locked/unlocked (blocks USB input to source)

O.NO_TOE_ACCESS
The TOE firmware and memory shall not be accessible via its external ports. (Applies to Blocker)

4.2 Security Objectives for the operational environment

The following subsections describe objectives for the Operational Environment. This applies to both Blocker and MyBlocker.

OE.PHYSICAL
The operational environment shall provide physical security, commensurate with the value of the TOE and the data that transits it.

OE.NO_WIRELESS_DEVICES
The operational environment shall not include wireless keyboards, mice, audio, user authentication, or video devices.

OE.TRUSTED_ADMIN
The operational environment shall ensure that trusted TOE Administrators and users are appropriately trained.

OE.TRUSTED_CONFIG
The operational environment shall ensure that administrators install and configuring the TOE and its operational environment follow the applicable security configuration guidance.

OE.USER_ALLOWED_ACCESS
The operational environment shall ensure connected computers or their connected network have the required means to authenticate the user and to control access to their various resources.

5 Extended components definition

This chapter provides a definition for all of the extended components introduced in this ST. The families to which these components belong are identified in the following table:

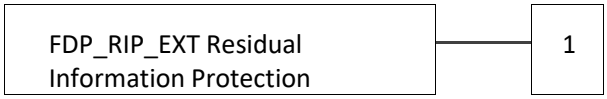
Functional Class	Functional Families
User Data Protection (FDP)	FDP_RIP_EXT Residual Information Protection
	FDP_SWI_EXT PSD Switching
Protection of the TSF (FPT)	FPT_NTA_EXT No Access to TOE
TOE Access (FTA)	FTA_CIN_EXT Continuous Indications

5.1 FDP_RIP_EXT Residual Information Protection

Family Behavior

Components in this family define the requirements for how the TSF prevents data disclosure from its memory.

Component Leveling



FDP_RIP_EXT.1 Residual Information Protection, requires the TSF to prevent the writing of user data to non-volatile memory.

Management: FDP_RIP_EXT.1

There are no management activities foreseen

Audit: FDP_RIP_EXT.1

No specific management functions are identified.

FDP_RIP_EXT.1 Residual Information Protection

Hierarchical to: No other components
Dependencies: No dependencies

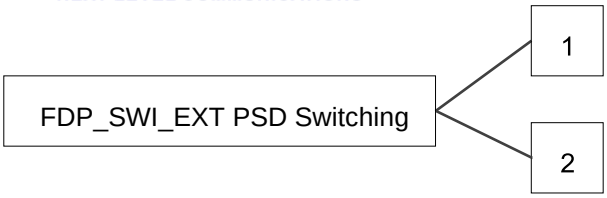
FDP_RIP_EXT.1.1 The TSF shall ensure that no user data is written to TOE non-volatile memory or storage.

5.2 FDP_SWI_EXT PSD Switching

Family Behavior

Components in this family define the requirements for how the TSF protects against inadvertent data switching.

Component Leveling



FDP_SWI_EXT.1 PSD Switching, requires action on the part of a user in order for the TSF's switching mechanisms to be activated.

FDP_SWI_EXT.2 PSD Switching Methods, places restrictions on how the TSF's switching mechanisms can be controlled.

Management: FDP_SWI_EXT.1, FDP_SWI_EXT.2

No specific management functions are identified.

Audit: FDP_SWI_EXT.1, FDP_SWI_EXT.2

There are no auditable events foreseen.

FDP_SWI_EXT.1 PSD Switching

Hierarchical to: No other components
Dependencies: No dependencies

FDP_SWI_EXT.1.1 The TSF shall ensure that [selection: the TOE supports only one connected computer, switching can be initiated only through express user action].

FDP_SWI_EXT.2 PSD Switching Methods

Hierarchical to: No other components
Dependencies: FDP_SWI_EXT.1 PSD Switching

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 [selection: console buttons, console switches, console touch screen, wired remote control, peripheral devices using a guard, hotkey selection]. Hotkeys for switching are used as follows:

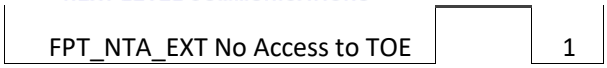
Shorcut	Action
LCTRL + LCTRL + [1-8]	Switch left channel/monitor 1 to source 1-8
RCTRL + RCTRL + [1-8]	Switch right channel/monitor 2 to source 1-8

5.3 FPT_NTA_EXT No Access to TOE

Family Behavior

Components in this family define what TSF information may be externally accessible.

Component Leveling



FPT_NTA_EXT.1 No Access to TOE, requires the TSF to block access to non-authorized TSF data via external ports.

Management: FPT_NTA_EXT.1

No specific management functions are identified.

Audit: FPT_NTA_EXT.1

There are no auditable events foreseen.

FPT_NTA_EXT.1 No Access to TOE

Hierarchical to: No other components
Dependencies: No dependencies

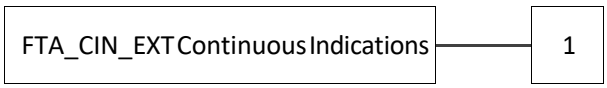
FPT_NTA_EXT.1.1 TOE firmware, software, and memory shall not be accessible via the TOE's external ports, with the following exceptions: [selection: the EDID memory of Video TOEs may be accessible from connected computers; the configuration data, settings, and logging data that may be accessible by authorized administrators; no other exceptions].

5.4 FTA_CIN_EXT Continuous Indications

Family Behavior

Components in this family define how the TSF displays its switching status.

Component Leveling



FTA_CIN_EXT.1 Continuous Indications, requires the TSF to display a visual indication of what computers are selected.

Management: FTA_CIN_EXT.1

No specific management functions are identified.

Audit: FTA_CIN_EXT.1

There are no auditable events foreseen.

FTA_CIN_EXT.1 Continuous Indications

Hierarchical to: No other components
Dependencies: FDP_IFC.1 Subset Information Flow Control

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 The TSF shall implement the visible indication using the following mechanism: [selection: a button, a panel with lights, a screen with dimming function, a screen with no dimming function, [assignment: description of visible indication]].
FTA_CIN_EXT.1.3 The TSF shall ensure that while the TOE is powered the current switching status is reflected by [selection: the indicator, multiple indicators which never display conflicting information].

6 Security Requirements

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 uses the following font conventions to identify the operations defined by the CC:

- Refinement operation (denoted by ***bold italic*** text) is used to add details to a requirement, and thus further restricts a requirement.
- Selection (denoted by **bold text and explicit spell-out "selection"**): is used to select one or more options provided by the [CC] in stating a requirement.
- Assignment operation (denoted by **bold text and explicit spell-out "assignment"**) 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.
- Iteration operation is identified with a slash ('/') and an identifier (e.g. "/KM").
- Extended SFRs are identified by having a label "EXT" after the SFR name.

6.1 Security Functional Requirements

6.1.1 User Data Protection (FDP)

6.1.1.1 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [**assignment: Data separation SFP**] on [**assignment:**

- **Subjects: Source ports, Peripheral ports**[2]
- **Information: User data, including:**
  - **Video data (and EDID**[3]**) flow between the source ports and the peripheral ports**
  - **Keyboard / mouse data flow between the source ports and the peripheral ports**
  - **Audio data flow between the source ports and the peripheral ports**
- **Operations:**
  - **Switching between source ports**
  - **Switching between peripheral ports**].

6.1.1.2 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [**assignment: Data separation SFP**] based on the following types of subject and information security attributes: [**assignment:**

- **Subjects: Source ports. Peripheral ports**
- **Information: User data**
- **Subject attribute: Source Port ID, Peripheral port ID**

].

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

Switching rule:

- **User data can flow between the source port and the peripheral port if the source port ID is selected by the user to be communicated with the peripheral port ID**].

FDP_IFF.1.3 The TSF shall enforce the [**assignment: none**].

---

[2] Source ports are the ports that connects to the source computers; peripheral ports are the ports that connect to the peripheral devices such as keyboard, mouse, video, and audio.

[3] Extended Display Identification Data

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**assignment: none**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**assignment:**

- **No information flow between source ports whether the TOE is powered on or off;**
- **No information flow between any ports when the TOE is powered off;**
- **No direct EDID information flow from the peripheral port to the source port**].

6.1.1.3 FDP_RIP_EXT.1 Residual Information Protection

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

6.1.1.4 FDP_SWI_EXT.1/DATA_BLOCKER PSD Switching

FDP_SWI_EXT.1.1 The TSF shall ensure that [**selection: the TOE supports only one connected computer**].

Application note: this SFR only applicable FIS-SVID-11HD-4K/FHD, and FIS-SVID-11DP-4K/FHD

6.1.1.5 FDP_SWI_EXT.1/SEC_SWITCH PSD Switching

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

Application note: this SFR is applicable to all TOEs except FIS-SVID-11HD-4K/FHD, and FIS-SVID-11DP-4K/FHD

6.1.1.6 FDP_SWI_EXT.2 PSD Switching Methods

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 [**selection: console buttons**].

Application note: this SFR applicable to all TOEs except FIS-SVID-11HD-4K/FHD, and FIS-SVID-11DP-4K/FHD

6.1.2 Protection of TSF (FPT)

6.1.2.1 FPT_NTA_EXT.1 No Access to TOE

FPT_NTA_EXT.1.1 TOE firmware, software, and memory shall not be accessible via the TOE's external ports, with the following exceptions: [**selection: the EDID memory of Video TOEs may be accessible *for read only* from connected computers**].

6.1.3 TOE Access (FTA)

6.1.3.1 FTA_CIN_EXT.1 Continuous Indications

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 The TSF shall implement the visible indication using the following mechanism: [**selection: [assignment: the LED indicator on the button]**].

FTA_CIN_EXT.1.3 The TSF shall ensure that while the TOE is powered the current switching status is reflected by [**selection: the indicator**].

Application note: this SFR applicable to all TOEs except FIS-SVID-11HD-4K/FHD, and FIS-SVID-11DP-4K/FHD

6.2 Security Assurance Requirements

The development and the evaluation of the TOE shall be done in accordance with the following security assurance requirements: EAL4 + ALC_FLR.2

The following table summarizes the EAL4 + ALC_FLR.2 assurance requirements:

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.2 Flaw reporting procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Table 3 Assurance Components

6.3 Security Requirements Rationale

6.3.1 Security Objective Rationale

This section describes how the assumptions and threats map to the security objectives. All mappings and rationale are included in the table below.

Threat or Assumption	Security Objective(s)	Rationale
T.DATA_LEAK	O.COMPUTER_INTERFACE_ISOLATION	Isolation of computer interfaces prevents data from leaking between them without authorization.
	O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED	Maintaining interface isolation while the TOE is in an unpowered state ensures that data cannot leak between computer interfaces.
	O.USER_DATA_ISOLATION	The TOE's routing of data only to the selected computer ensures that it will not leak to any others.
T.RESIDUAL_LEAK	O.NO_USER_DATA_RETENTION	The TOE's lack of data retention ensures that a residual data leak is not possible.
T.LOGICAL_TAMPER	O.NO_TOE_ACCESS	The TOE's prevention of logical access to its firmware, software, and memory mitigates the threat of logical tampering.
OSP.UNINTENDED_USE	O.AUTHORIZED_USAGE	The TOE's support for only switching mechanisms that require explicit user action to engage ensures that a user has sufficient information to avoid interacting with an unintended computer.
A.NO_PHYSICAL	OE.PHYSICAL	This assumption is upheld by the objective OE.PHYSICAL which restates the assumption
A.NO_WIRELESS_DEVICES	OE.NO_WIRELESS_DEVICES	This assumption is upheld by the objective OE.NO_WIRELESS_DEVICE which restates the assumption
A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN	This assumption is upheld by the objective OE.TRUSTED_ADMIN which restates the assumption
A.TRUSTED_CONFIG	OE.TRUSTED_CONFIG	This assumption is upheld by the objective OE.TRUSTED_CONFIG which restates the assumption
A.USER_ALLOWED_ACCESS	OE.PHYSICAL	This assumption is upheld by the objective OE.USER_ALLOWED_ACCESS which restates the assumption

6.3.2 Security Functional Requirements Rationale

Security Objective(s)	SFR addressing the security objectives
O.COMPUTER_INTERFACE_ISOLATION	This objective is met by: • FDP_IFC.1 and FDP_IFF.1 which defines a data flow policy that explicitly denies the information flow between source computers
O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED	This objective is met by: • FDP_IFC.1 and FDP_IFF.1 which defines a data flow policy that explicitly denies the information flow when the TOE is unpowered.
O.USER_DATA_ISOLATION	This objective is met by: • FDP_IFC.1 and FDP_IFF.1 which defines a data flow policy that states the user data will only transit the TOE to the computer that the user has explicitly selected it to go to, and provides isolation between the data directly flowing

	from the peripheral device to the selected computer and any non-selected computer.
O.NO_USER_DATA_RETENTION	This objective is met by: • FDP_RIP_EXT.1 which ensures no user data is retain in non-volatile memory when it is powered off.
O.AUTHORIZED_USAGE	This objective is met by: • FDP_SWI_EXT.1/DATA_BLOCKER and FDP_SWI_EXT.1/SEC_SWITCH which ensure when switching between different sources, it must be initiated through express user action • FDP_SWI_EXT.2 ensures the only express user action is by using the console buttons on the TOE • FTA_CIN_EXT.1 ensures the TOE will continuously indicate which source(s) is/are selected by using buttons equipped with LED lights
O.NO_TOE_ACCESS	This objective is met by: • FPT_NTA_EXT.1 which ensures the TOE firmware, software, and memory is not accessible via its external ports.

6.3.3 Security Assurance Requirements Rationale

The Security Assurance Requirements for this Security Target are EAL4+ALC_FLR.2. The reasons for this choice are that:

- EAL 4 permits a good balance between assurance and costs and is in line with Fibernet customer requirements.
- ALC_FLR.2 provides assurance that Fibernet has a clear and functioning process of accepting security flaws from users and updating the TOE when required. This is also in line with Fibernet customer requirements.

6.3.4 Dependencies

SFR	Dependencies
FDP_IFC.1	FDP_IFF.1: met
FDP_IFF.1	FDP_IFC.1: met FMT_MSA.3: not met as the TOE does not provide any management functionality, the dependency is unnecessary
FDP_RIP_EXT.1	-
FDP_SWI_EXT.1/DATA_BLOCKER	-
FDP_SWI_EXT.1/SEC_SWITCH	-
FDP_SWI_EXT.2	FDP_SWI_EXT.1: met by FDP_SWI_EXT.1/SEC_SWITCH
FPT_NTA_EXT.1	-
FTA_CIN_EXT.1	FDP_IFC.1: met
SAR	**Dependencies**
EAL4	All dependencies within EAL are satisfied
ALC_FLR.2	-

7 TOE Summary Specification

SFR	How SFR is met
FDP_IFC.1 FDP_IFF.1	The TOE routes video data and audio data only from the selected computer to the selected attached peripherals and routes the keyboard and mouse data only to the selected computer from the attached peripherals. The TOE blocks the EDID directly sent from the peripheral monitor to the source computers. The source computers only get EDID from the TOE (either generated by the TOE itself or learnt from the peripheral monitor). This ensures there will be no unauthorized video or video sub-protocol data flow from the monitor to a connected computer. In addition, the physical construction of the TOE prevents the information flow through the TOE: • When the TOE is powered off • No communication between the source ports
FDP_RIP_EXT.1	No user data is written to TOE non-volatile memory or storage.
FDP_SWI_EXT.1/DATA_BLOCKER	The myBLOCKERs (FIS-SVID-11HD-4K/FHD, FIS-VID-11DP-4K/FHD) only have one input and one output, and always connects to one computer and one display output.
FDP_SWI_EXT.1/SEC_SWITCH	All the TOE models other than the Data blockers must be switched using the button on the TOE to toggle the sources and the destinations.
FDP_SWI_EXT.2	When switching between the sources and the peripherals, it must be done via user manually press the buttons on the console. There is no automatic scanning possible.
FPT_NTA_EXT.1	The TOE firmware, software, and memory is not accessible from the TOE's external ports, with the following exception: • the Extended Display Identification Data (EDID) memory for Video is made available to the connected computers. However, the connected computers can only read the content of the EDID memory. They cannot change, affect, or add to the EDID data in the KVM.
FTA_CIN_EXT.1	The LEDs on the button indicates which source and which destination is selected. There is a visual notification signaling to the user which source and destinations are chosen. Changing source or destination can be made by physical access only (the user must press a physical button). Once a source or destination has changed, the LED light on the selected button will turn on/off and indicate the precise the selected destination or source.