Belkin Secure KVM F1DN102KVM-DC-4, F1DN202KVM-DC-4, F1DN104KVM-DC-4, F1DN204KVM-DC-4, F1DN108KVM-DC-4, F1DN208KVM-DC-4, F1DN104KVMDCU-4, F1DN204KVMDCU-4, F1DN104MKVMDC-4, F1DN108MKVMDC-4, F1DN104MVKVMDC4, F1DN108MVKVMDC4, Firmware Version 44444-D5D5

Security Target

Doc No: 2297-001-D102
Version: 1.2
2025 March 5

Belkin International, Inc.
555 S Aviation Blvd., Suite 180
El Segundo, CA 90245-4852 USA

Prepared by:

Saffire Systems
1061 W 136TH ST
Carmel, IN 46032

and

EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, Security Target Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria, Protection Profile (PP) and PP Modules.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Functional Requirements, specifies the security functional requirements that must be satisfied by the TOE and the IT environment.

Section 7, Security Assurance Requirements, specifies the security assurance requirements that must be satisfied by the TOE and the IT environment.

Section 8, Security Requirements Rationale, provides a rationale for the selection of functional and assurance requirements.

Section 9, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 10, Terminology and Acronyms, defines the acronyms and terminology used in this ST.

Section 11, References, provides a list of documents referenced in this ST.

Annex A – Letter of Volatility, provides volatility information and memory types for the devices.

1.2 SECURITY TARGET REFERENCE

ST Title:	Belkin Secure KVM F1DN102KVM-DC-4, F1DN202KVM-DC-4, F1DN104KVM-DC-4, F1DN204KVM-DC-4, F1DN108KVM-DC-4, F1DN208KVM-DC-4, F1DN104KVMDCU-4, F1DN204KVMDCU-4, F1DN104MKVMDC-4, F1DN108MKVMDC-4, F1DN104MVKVMDC4, F1DN108MVKVMDC4, Firmware Version 44444-D5D5 Security Target
ST Version:	1.2
ST Date:	2025 March 5

1.3 TOE REFERENCE

TOE Identification:	Belkin Firmware Version 44444-D5D5 running on the following hardware devices: F1DN102KVM-DC-4 F1DN202KVM-DC-4 F1DN104KVM-DC-4 F1DN204KVM-DC-4 F1DN108KVM-DC-4 F1DN208KVM-DC-4 F1DN104KVMDCU-4 F1DN204KVMDCU-4 F1DN104MVKVMDC4 F1DN108MVKVMDC4 F1DN104MKVMDC-4 F1DN108MKVMDC-4
TOE Developer:	Belkin International, Inc.
TOE Type:	Peripheral Sharing Device (Other Devices and Systems)

1.4 TOE OVERVIEW

These Belkin Secure KVM devices allow users to securely share keyboard, mouse video, and Universal Serial Bus (USB) authentication device peripherals between up to 8 connected computers. Security features ensure isolation between computers and peripherals to prevent data leakage between connected systems. These products are KVM switches with anti-tampering.

1.4.1 Security Features

The following security features are provided by the Belkin secure KVM Devices:

- Video Security
    - Computer video input interfaces are isolated through the use of separate electronic components, power and ground domains
    - The display is isolated by dedicated, read-only, Extended Display Identification Data (EDID) emulation for each computer
    - Access to the monitor's EDID is blocked
    - EDID file is transferred to connected hosts via a secure mechanism to assure uni-directional information flow.
    - Access to the Monitor Control Command Set (MCCS commands) is blocked
    - Only DisplayPort (DP) video peripherals are supported
- Keyboard and Mouse Security
    - Keyboard and mouse are isolated by dedicated, USB device emulation for each computer
    - One-way, peripheral-to-computer data flow is enforced through unidirectional optical data diodes
    - Communication from computer-to-keyboard/mouse is blocked
    - Non HID (Human Interface Device) data transactions are blocked
- Authentication Device
    - Unauthorized USB devices are blocked
    - USB authentication devices are authorized by default; all other devices are blocked
- Hardware Anti-Tampering
    - Any attempt to open the product enclosure will activate an anti-tampering system, making the product inoperable and indicating tampering via blinking Light Emitting Diodes (LEDs)
    - Special holographic tampering evident labels on the product's enclosure provide a clear visual indication if the product has been opened or compromised
- TOE Access
    - The TOE provides continuous indication of which computer is currently selected.

The secure peripheral sharing devices use multiple isolated microcontrollers (one microcontroller per connected computer) to emulate connected peripherals in order to prevent an unauthorized data flow through bit-by-bit signaling.

The TOE is a combined software and hardware TOE.

1.4.2 TOE Environment

The following components are required for operation of the TOE in the evaluated configuration.

Component	Description
Connected Computers	1-8 General purpose computers
Keyboard	General purpose USB keyboard
Mouse	General purpose USB mouse
User authentication device	Any standard USB smart card reader/authentication device (only USB Type A connections)
User display	Standard computer display (DisplayPort 1.1, 1.2, or 1.3)
KVM Peripheral Cables	USB Type-A to USB Type-B (keyboard and mouse) Video cable (DisplayPort) USB Type-C (Connecting a USB-C computer to F1DN104KVMDCU-4, F1DN204KVMDCU-4) RS-232 serial cable (for connecting to the wired remote control)
Power Supply	28 Volt Direct Current (VDC) Power Supply.

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Evaluated Configurations

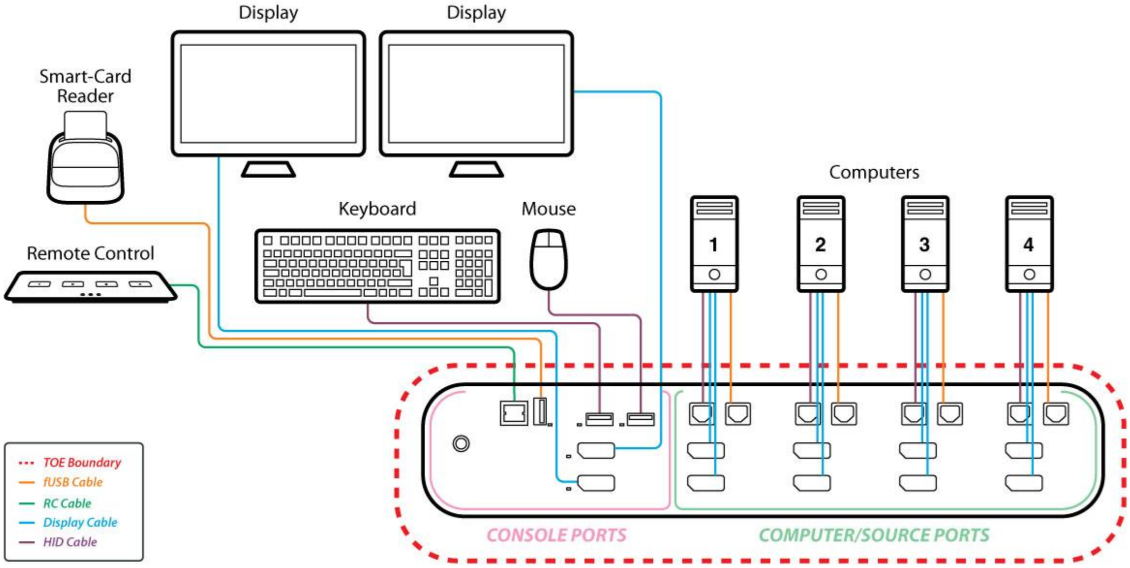

Figure 1 – KVM Evaluated Configuration

Figure 1 shows a basic evaluated configuration. In the evaluated configuration, the TOE is connected to a keyboard, a mouse, a user authentication device, and up to eight computers. The video input is DisplayPort and one or two displays are connected. The KVM can also be used with a wired remote control.

Figure 2 shows a KVM Device.

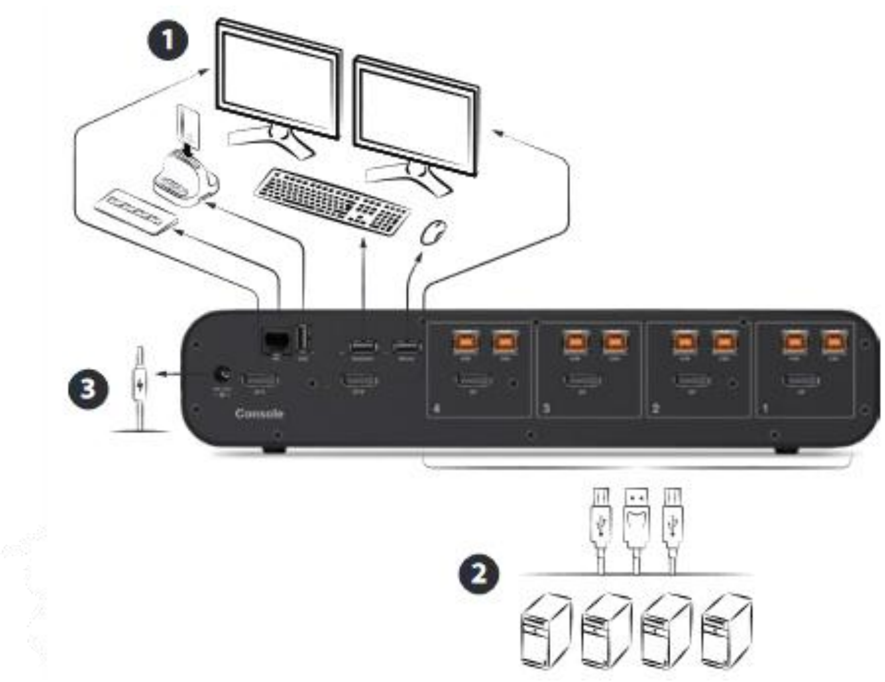

Figure 2 – KVM Devices

1.5.1.1 Switch Devices

The switch devices allow sharing of the keyboard, video, mouse, and USB peripherals between multiple computers. The video input is DisplayPort and one or two displays are connected. The F1DN104KVMDCU-4 and F1DN204KVMDCU-4 models accept USB-C connections between the computer and the KVM.

1.5.1.2 Matrix Devices

Matrix devices allow the video output from one connected computer to be shown on the primary display, and the video output from a second connected computer to be shown on the secondary display. The devices also allow sharing of the keyboard, mouse, and USB peripherals between multiple computers.

1.5.1.3 Multi-Viewer Devices

Multi-Viewer devices allow users to interact with multiple computers presented on the same displays at the same time using a single set of keyboard, mouse, and video peripherals. These devices simultaneously display output from multiple connected computers to one or more display devices. There are different layouts for displaying the video output from the connected computers. The monitor can display only the video output from only one of the connected computers, or it can display the video output from each of the connected computers. If two displays are connected, there are two possible modes:

- Duplicate Screen Mode – the secondary display duplicates the primary display.

- Extended Screen Mode – the video outputs can be arranged on either the primary or secondary display.

The devices also allow sharing of the keyboard, mouse, and USB peripherals between multiple computers.

1.5.1.4 Remote Control Devices

The user can use the wired remote control device to select the host computer to be connected to the peripherals by pressing a button on the wired remote control device. When the remote control is connected to the TOE, channel switching functionality is transferred from the front panel to the remote control. Remote control implementation eliminates the need for front panel operation. On the remote control, there is an LED indicator for each computer. When the remote control is connected to the TOE, the LED indicator of the selected computer is illuminated on the remote control.

1.5.2 Physical Scope

The TOE consists of the devices shown in Table 2 and the Belkin Firmware Version 44444-D5D5. All of the devices include tamper evident labels, active anti-tampering, and support a keyboard, mouse, user authentication device, DisplayPort video input and output. The only video interface supported by the TOE is DisplayPort. The KVM can also be used with a wired remote control.

Family	Part Number	Model	Number of hosts	Number of supported displays
Switches	CGA33595	F1DN102KVM-DC-4	2	1
	CGA33597	F1DN202KVM-DC-4	2	2
	CGA33596	F1DN104KVM-DC-4	4	1
	CGA33598	F1DN204KVM-DC-4	4	2
	CGA33599	F1DN108KVM-DC-4	8	1
	CGA33600	F1DN208KVM-DC-4	8	2
	CGA33607	F1DN104KVMDCU-4	3 regular + 1 USB-C	1
	CGA33608	F1DN204KVMDCU-4	3 regular + 1 USB-C	2
Matrix Devices	CGA33709	F1DN104MKVMDC-4	4	2
	CGA33710	F1DN108MKVMDC-4	8	2
Multi-Viewers	CGA33711	F1DN104MVKVMDC4	4	2
	CGA33712	F1DN108MVKVMDC4	8	2
	CGA33637	F1DN-KVM-REM2	2	N/A

Family	Part Number	Model	Number of hosts	Number of supported displays
Remote Control	CGA33638	F1DN-KVM-REM4	4	N/A
	CGA33639	F1DN-KVM-REM8	8	N/A

Table 2 – TOE Peripheral Sharing Devices and Features

1.5.2.1 TOE Delivery

The TOE is delivered to the customer via trusted carrier, such as Fed-Ex, that provide a tracking service for all shipments.

1.5.2.2 TOE Guidance

The TOE includes the following guidance documentation:

- Belkin Quick Installation Guide 4/8 Ports Secure DP-DP KVM Multi-Viewer, HLT34003 Rev.A01
- Belkin Quick Installation Guide 4/8 Ports Secure DP-DP KVM Matrix, HLT33816 Rev.A01
- Belkin Quick Installation Guide 2/4/8 Port Secure Single/Dual Head DP-DP KVM Switches, HLT33791 Rev.A01

Guidance may be downloaded from the Belkin website (www.belkin.com) in .pdf format.

The following guidance is available upon request by emailing:

- Belkin Secure KVM F1DN102KVM-DC-4, F1DN202KVM-DC-4, F1DN104KVM-DC-4, F1DN204KVM-DC-4, F1DN108KVM-DC-4, F1DN208KVM-DC-4, F1DN104KVMDCU-4, F1DN204KVMDCU-4, F1DN104MKVMDC-4, F1DN108MKVMDC-4, F1DN104MVKVMDC4, F1DN108MVKVMDC4, Firmware Version 44444-D5D5 Common Criteria Guidance Supplement, Version 1.0

1.5.3 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The TOE does not provide a management function to configure aspects of the TOE Security Functionality (TSF). The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 3 summarizes the logical scope of the TOE.

Functional Classes	Description
User Data Protection	The TOE provides secure switching and unidirectional data flow capabilities for keyboard, video, and mouse. The TOE ensures that only authorized peripheral devices may be used. The TOE does not support a factory reset capability.
Protection of the TSF	The TOE ensures a secure state in the case of failure, provides only restricted access, and performs self-testing. The TOE provides both passive detection of physical attack and active resistance to attack.
TOE Access	The TOE provides a continuous indication of which computer is currently selected.

Table 3 – Logical Scope of the TOE

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 and CC and CEM addenda Exact Conformance, Selection-Based SFRs, Optional SFRs, 2021-Sep-30 have been taken into account.

2.2 PP-CONFIGURATION CONFORMANCE CLAIM

This ST claims exact conformance with the National Information Assurance Partnership (NIAP) PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, 2019-07-19 [CFG_PSD-KM-UA-VI_V1.0].

This PP-Configuration includes the following components:

- Base-PP: Protection Profile for Peripheral Sharing Device, Version 4.0 [PP_PSD_V4.0]
- PP-Module: PP-Module for Keyboard/Mouse Devices, Version 1.0 [MOD_KM_V1.0]
- PP-Module: PP-Module for Video/Display Devices, Version 1.0 [MOD_VI_V1.0]
- PP-Module: PP-Module for User Authentication Devices, Version 1.0 [MOD_UA_V1.0]

2.3 TECHNICAL DECISIONS

The Technical Decisions in Table 4 apply to the PP and the modules and have been accounted for in the ST and in the evaluation.

TD	Name	PP affected	Relevant Y/N
TD0506	Missing Steps to disconnect and reconnect display	[MOD_VI_V1.0]	Y
TD0507	Clarification on USB plug type	[MOD_KM_V1.0]	Y
TD0514	Correction to MOD VI FDP_APC_EXT.1 Test 3 Step 6	[MOD_VI_V1.0]	Y
TD0518	Typographical errors in dependency Table	[PP_PSD_V4.0]	N FPT_STM.1 is not claimed in the ST
TD0539	Incorrect selection trigger in FTA_CIN_EXT.1 in MOD_VI_V1.0	[MOD_VI_V1.0]	Y
TD0583	FPT_PHP.3 modified for remote controllers	[PP_PSD_V4.0]	Y
TD0584	Update to FDP_APC_EXT.1 Video Tests	[MOD_VI_V.10]	Y
TD0586	DisplayPort and HDMI Interfaces in FDP_IPC_EXT.1	[MOD_VI_V.10]	Y
TD0593	Equivalency Arguments for PSD	[MOD_KM_V1.0], [MOD_UA_V1.0], [MOD_VI_V1.0]	Y
TD0619	Test EAs for internal UA devices	[MOD_UA_V1.0]	Y
TD0620	EDID Read Requirements	[MOD_VI_V1.0]	Y
TD0681	PSD purging of EDID data upon disconnect	[MOD_VI_V1.0]	Y
TD0686	DisplayPort CEC Testing	[MOD_VI_V1.0]	Y
TD0804	Clarification regarding Extenders in PSD Evaluations	[PP_PSD_V4.0]	Y
TD0844	Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim	[PP_PSD_V4.0]	N No ALC_FLR SARs are claimed in this ST.

Table 4 – Applicable Technical Decisions

2.4 PACKAGE CLAIM

This Security Target does not claim conformance with any Package.

2.5 CONFORMANCE RATIONALE

The TOE is inherently consistent with the Compliant Targets of Evaluation described in the [PP_PSD_V4.0] and in the PP modules listed in Section 2.2, and with the PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices [CFG_PSD-KM-UA-VI_V1.0].

The security problem definition, statement of security objectives and statement of security requirements in this ST conform exactly to the security problem definition, statement of security objectives and statement of security requirements contained in [PP_PSD_V4.0] and the modules listed in Section 2.2.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 5 lists the threats described in Section 3.1 of the [PP_PSD_V4.0]. Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.DATA_LEAK	A connection via the PSD[1] between one or more computers may allow unauthorized data flow through the PSD or its connected peripherals.
T.SIGNAL_LEAK	A connection via the PSD between one or more computers may allow unauthorized data flow through bit-by-bit signaling.
T.RESIDUAL_LEAK	A PSD may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer.
T.UNINTENDED_USE	A PSD may connect the user to a computer other than the one to which the user intended to connect.
T.UNAUTHORIZED_DEVICES	The use of an unauthorized peripheral device with a specific PSD peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSD or its connected computers.
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 PSD's volatile or non-volatile memory to allow unauthorized information flows.
T.PHYSICAL_TAMPER	A malicious user or human agent could physically modify the PSD to allow unauthorized information flows.
T.REPLACEMENT	A malicious human agent could replace the PSD during shipping, storage, or use with an alternate device that does not enforce the PSD security policies.

[1] Peripheral Sharing Device

Threat	Description
T.FAILED	Detectable failure of a PSD may cause an unauthorized information flow or weakening of PSD security functions.

Table 5 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

There are no Organizational Security Policies applicable to this TOE.

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 6. These assumptions are derived from Section 3.2 of [PP_PSD_V4.0] and [MOD_VI_V1.0].

Assumptions	Description
A.NO_TEMPEST	Computers and peripheral devices connected to the PSD are not TEMPEST approved. ST Note: The TSF may or may not isolate the ground of the keyboard and mouse computer interfaces (the USB ground). The Operational Environment is assumed not to support TEMPEST red-black ground isolation.
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	PSD Administrators[2] and users are trusted to follow and apply all guidance in a trusted manner.
A.TRUSTED_CONFIG	Personnel configuring the PSD and its operational environment follow the applicable security configuration guidance.
A.USER_ALLOWED_ACCESS	All PSD users are allowed to interact with all connected computers. It is not the role of the PSD 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.

[2] There are no administrative functions in the TOE. Therefore, there is no administrator so this assumption only refers to users.

Assumptions	Description
A.NO_SPECIAL_ANALOG_CAPABILITIES	The computers connected to the TOE are not equipped with special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, digital signal processing function, or analog video capture function.

Table 6 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE, and traces each Security Functional Requirement (SFR) back to a security objective of the TOE.

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td><b>O.COMPUTER _INTERFACE _ISOLATION</b></td><td>The PSD shall prevent unauthorized data flow to ensure that the PSD and its connected peripheral devices cannot be exploited in an attempt to leak data. The TOE-Computer interface shall be isolated from all other PSD-Computer interfaces while TOE is powered.
Addressed by:
<table>
<tr><td>MOD_VI</td><td>FDP_APC_EXT.1/VI, FDP_PDC_EXT.1</td></tr>
<tr><td>MOD_KM</td><td>FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1, FDP_SWI_EXT.3</td></tr>
<tr><td>MOD_UA</td><td>FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2</td></tr>
</table>
</td></tr>
</table>

Security Objective	Description		
O.COMPUTER _INTERFACE _ISOLATION _TOE_UNPOWERED	The PSD shall not allow data to transit a PSD-Computer interface while the PSD is unpowered. Addressed by:		
		MOD_VI	FDP_APC_EXT.1/VI, FDP_PDC_EXT.1
		MOD_KM	FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1, FDP_SWI_EXT.3
		MOD_UA	FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2
O.USER_DATA _ISOLATION	The PSD shall route user data, such as keyboard entries, only to the computer selected by the user. The PSD shall provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer. Addressed by:		
		MOD_VI	FDP_APC_EXT.1/VI, FDP_PDC_EXT.1
		MOD_KM	FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1, FDP_SWI_EXT.3
		MOD_UA	FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2
O.NO_USER _DATA_RETENTION	The PSD shall not retain user data in non-volatile memory after power up or, if supported, factory reset. Addressed by:		
		PP_PSD	FDP_RIP_EXT.1
		MOD_KM	FDP_RIP.1/KM
O.NO_OTHER _EXTERNAL _INTERFACES	The PSD shall not have any external interfaces other than those implemented by the TSF. Addressed by:		
		PP_PSD	FDP_PDC_EXT.1

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td><b>O.LEAK _PREVENTION _SWITCHING</b></td><td>The PSD shall ensure that there are no switching mechanisms that allow signal data leakage between connected computers.
Addressed by:<table><tr><td>PP_PSD</td><td>FDP_SWI_EXT.1, FDP_SWI_EXT.2</td></tr></table></td></tr>
<tr><td><b>O.AUTHORIZED _USAGE</b></td><td>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, console touch screen, wired remote control, and peripheral devices using a guard. Unauthorized switching mechanisms include keyboard shortcuts, also known as “hotkeys,” automatic port scanning, control through a connected computer, and control through keyboard shortcuts. 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.
A conformant TOE may also provide a management function to configure some aspects of the TSF. If the TOE provides this functionality, it shall ensure that whatever management functions it provides can only be performed by authorized administrators and that an audit trail of management activities is generated.
Addressed by:<table><tr><td>PP_PSD</td><td>FDP_SWI_EXT.1, FDP_SWI_EXT.2, FTA_CIN_EXT.1</td></tr><tr><td>MOD_VI</td><td>FDP_CDS_EXT.1, FTA_CIN_EXT.1</td></tr><tr><td>MOD_KM</td><td>FDP_FIL_EXT.1/KM</td></tr><tr><td>MOD_UA</td><td>FDP_FIL_EXT.1/UA</td></tr></table></td></tr>
</table>

Security Objective	Description		
O.PERIPHERAL _PORTS_ISOLATION	The PSD shall ensure that data does not flow between peripheral devices connected to different PSD interfaces. Addressed by:	MOD_VI	FDP_APC_EXT.1/VI, FDP_PDC_EXT.1
		MOD_KM	FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1, FDP_SWI_EXT.3
		MOD_UA	FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2
O.REJECT _UNAUTHORIZED _ENDPOINTS	The PSD shall reject unauthorized peripheral devices connected via a Universal Serial Bus (USB) hub. Addressed by:	PP_PSD	FDP_PDC_EXT.1
		MOD_KM	FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1, FDP_SWI_EXT.3
		MOD_UA	FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2
O.REJECT _UNAUTHORIZED _PERIPHERAL	The PSD shall reject unauthorized peripheral device types and protocols. Addressed by:	PP_PSD	FDP_PDC_EXT.1
		MOD_VI	FDP_PDC_EXT.2/VI, FDP_PDC_EXT.3/VI, FDP_IPC_EXT.1, FDP_SPR_EXT.1/DP
		MOD_KM	FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1, FDP_SWI_EXT.3, FDP_PDC_EXT.2/KM, FDP_PDC_EXT.3/KM
		MOD_UA	FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td><b>O.NO_TOE_ACCESS</b></td><td>The PSD firmware, software, and memory shall not be accessible via its external ports.
Addressed by:<table><tr><td>PP_PSD</td><td>FPT_NTA_EXT.1</td></tr></table></td></tr>
<tr><td><b>O.TAMPER _EVIDENT _LABEL</b></td><td>The PSD shall be identifiable as authentic by the user and the user must be made aware of any procedures or other such information to accomplish authentication. This feature must be available upon receipt of the PSD and continue to be available during the PSD deployment. The PSD shall be labeled with at least one visible unique identifying tamper-evident marking that can be used to authenticate the device. The PSD manufacturer must maintain a complete list of manufactured PSD articles and their respective identification markings' unique identifiers.
Addressed by:<table><tr><td>PP_PSD</td><td>FPT_PHP.1</td></tr></table></td></tr>
<tr><td><b>O.ANTI_TAMPERING</b></td><td>The PSD shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the PSD would be evident, and optionally thwarted through disablement of the TOE. Note: This applies to a wired remote control as well as the main chassis of the PSD.
Addressed by:<table><tr><td>PP_PSD</td><td>FPT_PHP.1, FPT_PHP.3</td></tr></table></td></tr>
<tr><td><b>O.SELF_TEST</b></td><td>The PSD shall perform self-tests following power up or powered reset.
Addressed by:<table><tr><td>PP_PSD</td><td>FPT_TST.1</td></tr></table></td></tr>
</table>

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td><b>O.SELF_TEST _FAIL_TOE _DISABLE</b></td><td>The PSD shall enter a secure state upon detection of a critical failure.
Addressed by:<table><tr><td>PP_PSD</td><td>FPT_FLS_EXT.1, FPT_TST_EXT.1</td></tr></table></td></tr>
<tr><td><b>O.SELF_TEST _FAIL_INDICATION</b></td><td>The PSD shall provide clear and visible user indications in the case of a self-test failure.
Addressed by:<table><tr><td>PP_PSD</td><td>FPT_TST_EXT.1</td></tr></table></td></tr>
<tr><td><b>O.EMULATED_INPUT</b></td><td>The TOE shall emulate the keyboard and/or mouse functions from the TOE to the connected computer.
Addressed by:<table><tr><td>MOD_KM</td><td>FDP_PDC_EXT.2/KM, FDP_PDC_EXT.3/KM</td></tr></table></td></tr>
<tr><td><b>O.UNIDIRECTIONAL _INPUT</b></td><td>The TOE shall enforce unidirectional keyboard and/or mouse device's data flow from the peripheral device to only the selected computer.
Addressed by:<table><tr><td>MOD_KM</td><td>FDP_UDF_EXT.1/KM</td></tr></table></td></tr>
<tr><td><b>O.USER _AUTHENTICATION _ISOLATION</b></td><td>The TOE shall isolate the user authentication function from all other TOE functions.
Addressed by:<table><tr><td>MOD_UA</td><td>FDP_UAI_EXT.1</td></tr></table></td></tr>
<tr><td><b>O.SESSION _TERMINATION</b></td><td>The TOE shall immediately terminate an open session with the selected computer upon disconnection of the authentication element.
Addressed by:<table><tr><td>MOD_UA</td><td>FDP_TER_EXT.1, FDP_TER_EXT.2, FDP_TER_EXT.3</td></tr></table></td></tr>
</table>

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td><b>O.PROTECTED_EDID</b></td><td>The TOE shall read the connected display Extended Display Identification Data (EDID) once during the TOE power up or reboot sequence and prevent any EDID channel write transactions that connected computers initiate.
Addressed by:<table><tr><td>MOD_VI</td><td>FDP_PDC_EXT.2/VI, FDP_SPR_EXT.1/DP</td></tr></table></td></tr>
<tr><td><b>O.UNIDIRECTIONAL_VIDEO</b></td><td>The TOE shall enforce unidirectional video data flow from the connected computer video interface to the display interface only.
Addressed by:<table><tr><td>MOD_VI</td><td>FDP_UDF_EXT.1/VI</td></tr></table></td></tr>
</table>

Table 7 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	Description
OE.NO_TEMPEST	The operational environment will not use TEMPEST approved equipment.
OE.PHYSICAL	The operational environment will provide physical security, commensurate with the value of the PSD and the data that transits it.
OE.NO_WIRELESS_DEVICES	The operational environment will not include wireless keyboards, mice, audio, user authentication, or video devices.
OE.TRUSTED_ADMIN	The operational environment will ensure that trusted PSD Administrators and users are appropriately trained.
OE.TRUSTED_CONFIG	The operational environment will ensure that administrators configuring the PSD and its operational environment follow the applicable security configuration guidance.
OE.NO_SPECIAL_ANALOG_CAPABILITIES	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.

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The security objectives rationale describes how the assumptions and threats map to the security objectives.

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.
	O.NO_OTHER _EXTERNAL _INTERFACES	The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked.
	O.PERIPHERAL_PORTS _ISOLATION	Isolation of peripheral ports prevents data from leaking between them without authorization.
	O.UNIDIRECTIONAL _INPUT	The TOE's enforcement of unidirectional input for keyboard/mouse data prevents leakage of computer data through a connected peripheral interface.
	O.USER _AUTHENTICATION _ISOLATION	The TOE's user authentication function mitigates this threat by ensuring that the bidirectional channel between the device and the connected computer through the user authentication function is isolated from all other TOE functions.
	O.SESSION _TERMINATION	The TOE mitigates the threat by ensuring that open sessions are terminated and no traffic flows upon disconnection of the authentication element.

Threat or Assumption	Security Objective(s)	Rationale
	O.PROTECTED_EDID	The TOE's protection of the EDID interface prevents its use as a vector for unauthorized data leakage via this channel.
	O.UNIDIRECTIONAL _VIDEO	The TOE's enforcement of unidirectional output for video data protects against data leakage via connected computers by ensuring that no video data can be input to a connected computer through this interface.
T.SIGNAL_LEAK	O.COMPUTER _INTERFACE _ISOLATION	Isolation of computer interfaces prevents data leakage through bit-wise signaling because there is no mechanism by which the signal data can be communicated.
	O.NO_OTHER _EXTERNAL _INTERFACES	The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked through bitwise signaling.
	O.LEAK_PREVENTION _SWITCHING	The TOE's use of switching methods that are not susceptible to signal leakage helps mitigate the signal leak threat.
	O.UNIDIRECTIONAL _INPUT	The TOE's enforcement of unidirectional input for keyboard/mouse data prevents leakage of computer data through bit-by-bit signaling to a connected peripheral interface.
	O.PROTECTED_EDID	The TOE's protection of the EDID interface prevents its use as a vector for bit-by-bit signal leakage via this channel.
	O.UNIDIRECTIONAL _VIDEO	The TOE's enforcement of unidirectional output for video data protects against signaling leakage via connected computers by ensuring that no video data can be input to a connected computer through this interface.

Threat or Assumption	Security Objective(s)	Rationale
	O.USER _AUTHENTICATION _ISOLATION	The TOE's user authentication function mitigates this threat by ensuring that the bidirectional channel between the device and the connected computer through the user authentication function is isolated from all other TOE functions.
	O.SESSION _TERMINATION	The TOE mitigates the threat by ensuring that open sessions are terminated and no traffic flows upon disconnection of the authentication element.
T.RESIDUAL _LEAK	O.NO_USER_DATA _RETENTION	The TOE's lack of data retention ensures that a residual data leak is not possible.
	O.PROTECTED_EDID	The TOE's protection of the EDID interface prevents the leakage of residual data by ensuring that no such data can be written to EDID memory.
	O.USER _AUTHENTICATION _ISOLATION	The TOE's user authentication function mitigates this threat by ensuring that the bidirectional channel between the device and the connected computer through the user authentication function is isolated from all other TOE functions.
	O.SESSION _TERMINATION	The TOE mitigates the threat by ensuring that open sessions are terminated and no traffic flows upon disconnection of the authentication element.
T.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.
T.UNAUTHORIZED _DEVICES	O.REJECT _UNAUTHORIZED _ENDPOINTS	The TOE's ability to reject unauthorized endpoints mitigates the threat of unauthorized devices being used to communicate with connected computers.

Threat or Assumption	Security Objective(s)	Rationale
	O.REJECT _UNAUTHORIZED _PERIPHERAL	The TOE's ability to reject unauthorized peripherals mitigates the threat of unauthorized devices being used to communicate with connected computers.
	O.EMULATED_INPUT	The TOE's emulation of keyboard/mouse data input ensures that a connected computer will only receive this specific type of data through a connected peripheral.
	O.UNIDIRECTIONAL _VIDEO	The TOE's limitation of supported video protocol interfaces prevents the connection of unauthorized devices.
	O.SESSION _TERMINATION	The TOE mitigates the threat by ensuring that open sessions are terminated and no traffic flows upon disconnection of the authentication element.
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.
	O.EMULATED_INPUT	The TOE's emulation of keyboard/mouse data input prevents logical tampering of the TSF ensuring that only known inputs to it are supported.
T.PHYSICAL _TAMPER	O.ANTI_TAMPERING	The TOE mitigates the threat of physical tampering through use of an enclosure that provides tamper detection functionality.
	O.TAMPER_EVIDENT _LABEL	The TOE mitigates the threat of physical tampering through use of tamper evident labels that reveal physical tampering attempts.
T.REPLACEMENT	O.TAMPER_EVIDENT _LABEL	The TOE's use of a tamper evident label that provides authenticity of the device mitigates the threat that it is substituted for a replacement device during the acquisition process.

Threat or Assumption	Security Objective(s)	Rationale
T.FAILED	O.SELF_TEST	The TOE mitigates the threat of failures leading to compromise of security functions through self-tests of its own functionality.
	O.SELF_TEST_FAIL _TOE_DISABLE	The TOE mitigates the threat of failures leading to compromise of security functions by disabling all data flows in the event a failure is detected.
	O.SELF_TEST_FAIL _INDICATION	The TOE mitigates the threat of failures leading to compromise of security functions by providing users with a clear indication when it is in a failure state and should not be trusted.
A.NO_TEMPEST	OE.NO_TEMPEST	If the TOE's operational environment does not include TEMPEST approved equipment, then the assumption is satisfied.
A.NO_PHYSICAL[3]	OE.PHYSICAL	If the TOE's operational environment provides physical security, then the assumption is satisfied.
A.NO_WIRELESS _DEVICES	OE.NO_WIRELESS _DEVICES	If the TOE's operational environment does not include wireless peripherals, then the assumption is satisfied.
A.TRUSTED_ADMIN	OE.TRUSTED _ADMIN	If the TOE's operational environment ensures that only trusted administrators will manage the TSF, then the assumption is satisfied.
A.TRUSTED _CONFIG	OE.TRUSTED _CONFIG	If TOE administrators follow the provided security configuration guidance, then the assumption is satisfied.
A.USER_ALLOWED _ACCESS	OE.PHYSICAL	If the TOE's operational environment provides physical access to connected computers, then the assumption is satisfied.

[3] Note: A.NO_PHYSICAL in this table is referring A.PHYSICAL in Section 3.3.

Threat or Assumption	Security Objective(s)	Rationale
A.NO_SPECIAL _ANALOG _CAPABILITIES	OE.NO_SPECIAL _ANALOG _CAPABILITIES	If administrators in the TOE's operational environment take care to ensure that computers with special analog data collection interfaces are not connected to the TOE, then the assumption that such components are not present is satisfied.

Table 9 – Security Objectives Rationale

5 EXTENDED COMPONENTS DEFINITION

The extended components definition is presented in Appendix C of the Protection Profile for Peripheral Sharing Device [PP_PSD_V4.0] and in the modules for keyboard/mouse devices [MOD_KM_V1.0], user authentication devices [MOD_UA_V1.0], and display devices [MOD_VI_1.0].

The families to which these components belong are identified in the following table:

Functional Class	Functional Families	Protection Profile Modules
User Data Protection (FDP)	FDP_APC_EXT Active PSD Connections	[PP_PSD_V4.0] [MOD_KM_V1.0] [MOD_VI_V1.0] [MOD_UA_V1.0]
	FDP_CDS_EXT Connected Displays Supported	[MOD_VI_V1.0]
	FDP_FIL_EXT Device Filtering	[MOD_KM_V1.0] [MOD_UA_V1.0]
	FDP_IPC_EXT Internal Protocol Conversion	[MOD_VI_V1.0]
	FDP_PDC_EXT Peripheral Device Connection	[PP_PSD_V4.0] [MOD_VI_V1.0] [MOD_KM_V1.0] [MOD_UA_V1.0]
	FDP_PWR_EXT Powered By Computer	[MOD_UA_V1.0]
	FDP_RDR_EXT Re-Enumeration Device Rejection	[MOD_KM_V1.0]
	FDP_RIP_EXT Residual Information Protection	[PP_PSD_V4.0]
	FDP_SPR_EXT Sub-Protocol Rules	[MOD_VI_V1.0]
	FDP_SWI_EXT PSD Switching	[PP_PSD_V4.0] [MOD_KM_V1.0] [MOD_UA_V1.0]
	FDP_TER_EXT Session Termination	[MOD_UA_V1.0]
	FDP_UAI_EXT User Authentication Isolation	[MOD_UA_V1.0]
	FDP_UDF_EXT Unidirectional Data Flow	[MOD_VI_V1.0] [MOD_KM_V1.0]

Functional Class	Functional Families	Protection Profile Modules
Protection of the TSF (FPT)	FPT_FLS_EXT Failure with Preservation of Secure State	[PP_PSD_V4.0]
	FPT_NTA_EXT No Access to TOE	[PP_PSD_V4.0]
	FPT_TST_EXT TSF Testing	[PP_PSD_V4.0]
TOE Access (FTA)	FTA_CIN_EXT Continuous Indications	[PP_PSD_V4.0] [MOD_VI_V1.0]

Table 10 **– Functional Families of Extended Components**

6 SECURITY FUNCTIONAL REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations are denoted as follows:

- Assignment: Indicated by bold text, e.g., **assigned item**.
- Selection: Indicated by text in italics, e.g., *selected item*.
- Refinement: Refined components are identified by using underlined text for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Iteration operations for iterations within the Protection Profile and associated modules are identified with a slash ('/') and an identifier (e.g. "/KM"). Where multiple iterations of the SFR are required within the ST, a number is appended to the SFR identifier (e.g. "FDP_CDS_EXT.1(1)").

Extended SFRs are identified by the inclusion of "_EXT" in the SFR name.

The CC operations that have already been performed in the PP and PP modules are reproduced in plain text and not denoted in this ST. The requirements have been copied from the PP and PP modules and any remaining operations have been completed herein. Refer to the PP and PP modules to identify those operations.

6.2 SECURITY FUNCTIONAL REQUIREMENTS

Section 6.2 details the security functional requirements.

Class	Identifier	Name	Source	Applicable Devices
User Data Protection (FDP)	FDP_APC_EXT.1/KM	Active PSD Connections	[MOD_KM_V1.0]	All
	FDP_APC_EXT.1/UA	Active PSD Connections	[MOD_UA_V1.0]	All
	FDP_APC_EXT.1/VI	Active PSD Connections	[MOD_VI_V1.0]	All

Class	Identifier	Name	Source	Applicable Devices
	FDP_CDS_EXT.1(1)	Connected Displays Supported (1)	[MOD_VI_V1.0]	F1DN102KVM-DC-4 F1DN104KVM-DC-4 F1DN108KVM-DC-4 F1DN104KVMDCU-4
	FDP_CDS_EXT.1(2)	Connected Displays Supported (2)	[MOD_VI_V1.0]	F1DN202KVM-DC-4 F1DN204KVM-DC-4 F1DN208KVM-DC-4 F1DN204KVMDCU-4 F1DN104MVKVMDC4 F1DN108MVKVMDC4 F1DN104MKVMDC-4 F1DN108MKVMDC-4
	FDP_FIL_EXT.1/KM	Device Filtering (Keyboard/ Mouse)	[MOD_KM_V1.0]	All
	FDP_FIL_EXT.1/UA	Device Filtering (User Authentication Devices)	[MOD_UA_V1.0]	All
	FDP_IPC_EXT.1	Internal Protocol Conversion	[MOD_VI_V1.0]	All
	FDP_PDC_EXT.1	Peripheral Device Connection	[PP_PSD_V4.0] [MOD_VI_V1.0][4] [MOD_KM_V1.0][5] [MOD_UA_V1.0][6]	All

[4] There is no modification to this SFR in the [MOD_VI_V1.0]. However, there are additions to the Peripheral Device Connections Policy associated with this SFR, and additional evaluation activities.

[5] There is no modification to this SFR in the [MOD_KM_V1.0]. However, there are additions to the Peripheral Device Connections associated with this SFR, modifications of the application note, and additional evaluation activities.

[6] There is no modification to this SFR in the [MOD_UA_V1.0]. However, because of additions to the Peripheral Device Connections Policy, there is an additional application note and additional evaluation activities for this SFR.

Class	Identifier	Name	Source	Applicable Devices
	FDP_PDC_EXT.2/KM	Authorized Devices (Keyboard/ Mouse)	[MOD_KM_V1.0]	All
	FDP_PDC_EXT.2/UA	Authorized Devices (User Authentication Devices)	[MOD_UA_V1.0]	All
	FDP_PDC_EXT.2/VI	Authorized Devices (Video Output)	[MOD_VI_V1.0]	All
	FDP_PDC_EXT.3/KM	Authorized Connection Protocols (Keyboard/Mouse)	[MOD_KM_V1.0]	All
	FDP_PDC_EXT.3/VI	Authorized Connection Protocols (Video Output)	[MOD_VI_V1.0]	All
	FDP_PDC_EXT.4	Supported Authentication Device	[MOD_UA_V1.0]	All
	FDP_PWR_EXT.1	Powered By Computer	[MOD_UA_V1.0]	All
	FDP_RDR_EXT.1	Re-Enumeration Device Rejection	[MOD_KM_V1.0]	All
	FDP_RIP.1/KM	Residual Information Protection (Keyboard Data)	[MOD_KM_V1.0]	All
	FDP_RIP_EXT.1	Residual Information Protection	[PP_PSD_V4.0]	All

Class	Identifier	Name	Source	Applicable Devices
	FDP_SPR_EXT.1/DP	Sub-Protocol Rules (DisplayPort Protocol)	[MOD_VI_V1.0]	All
	FDP_SWI_EXT.1	PSD Switching	[PP_PSD_V4.0]	All
	FDP_SWI_EXT.2	PSD Switching Methods	[PP_PSD_V4.0] [MOD_UA_V1.0]	All
	FDP_SWI_EXT.3	Tied Switching	[MOD_KM_V1.0]	All
	FDP_TER_EXT.1	Session Termination	[MOD_UA_V1.0]	All
	FDP_TER_EXT.2	Session Termination of Removed Devices	[MOD_UA_V1.0]	All
	FDP_TER_EXT.3	Session Termination upon Switching	[MOD_UA_V1.0]	All
	FDP_UAI_EXT.1	User Authentication Isolation	[MOD_UA_V1.0]	All
	FDP_UDF_EXT.1/KM	Unidirectional Data Flow (Keyboard/Mouse)	[MOD_KM_V1.0]	All
	FDP_UDF_EXT.1/VI	Unidirectional Data Flow (Video Output)	[MOD_VI_V1.0]	All
Protection of the TSF (FPT)	FPT_FLS_EXT.1	Failure with Preservation of Secure State	[PP_PSD_V4.0]	All
	FPT_NTA_EXT.1	No Access to TOE	[PP_PSD_V4.0]	All
	FPT_PHP.1	Passive Detection of Physical Attack	[PP_PSD_V4.0]	All

Class	Identifier	Name	Source	Applicable Devices
	FPT_PHP.3	Resistance to Physical Attack	[PP_PSD_V4.0]	All
	FPT_TST.1	TSF testing	[PP_PSD_V4.0]	All
	FPT_TST_EXT.1	TSF Testing	[PP_PSD_V4.0]	All
TOE Access (FTA)	FTA_CIN_EXT.1	Continuous Indications	[PP_PSD_V4.0] [MOD_VI_V1.0]	All

Table 11 – Summary of Security Functional Requirements

6.2.1 User Data Protection (FDP)

6.2.1.1 FDP_APC_EXT.1/KM Active PSD Connections

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.

6.2.1.2 FDP_APC_EXT.1/UA Active PSD Connections

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.

6.2.1.3 FDP_APC_EXT.1/VI Active PSD Connections

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.

6.2.1.4 FDP_CDS_EXT.1(1) Connected Displays Supported

FDP_CDS_EXT.1.1(1) The TSF shall support *one connected display* at a time.

Application Note: FDP_CDS_EXT.1(1) applies to the following models: F1DN102KVM-DC-4, F1DN104KVM-DC-4, F1DN108KVM-DC-4, F1DN104KVMDCU-4.

6.2.1.5 FDP_CDS_EXT.1(2) Connected Displays Supported

FDP_CDS_EXT.1.1(2) The TSF shall support *two* ~~*multiple*~~ *connected displays* at a time.

Application Note: FDP_CDS_EXT.1(2) applies to the following models: F1DN202KVM-DC-4, F1DN204KVM-DC-4, F1DN208KVM-DC-4, F1DN204KVMDCU-4, F1DN104MVKVMDC4, F1DN108MVKVMDC4, F1DN104MKVMDC-4, F1DN108MKVMDC-4.

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

FDP_FIL_EXT.1.1/KM The TSF shall have *fixed* 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.

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

FDP_FIL_EXT.1.1/UA The TSF shall have *fixed* 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.

6.2.1.8 FDP_IPC_EXT.1 Internal Protocol Conversion

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*.

Application Note: TD0586 applies to this SFR definition.

6.2.1.9 FDP_PDC_EXT.1 Peripheral Device Connection

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.

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

FDP_PDC_EXT.2.1/KM The TSF shall allow connections with authorized devices and functions as defined in Appendix E of [MOD_KM_V1.0] and

- *authorized devices and functions 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 [MOD_KM_V1.0] and

- *authorized devices and functions 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.

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

FDP_PDC_EXT.2.1/UA The TSF shall allow connections with authorized devices as defined in Appendix E of [MOD_UA_V1.0] and

- *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 [MOD_UA_V1.0] 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 Video/Display Devices*

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

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

FDP_PDC_EXT.2.1/VI The TSF shall allow connections with authorized devices as defined in Appendix E of [MOD_VI_V1.0] 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,*

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 [MOD_VI_V1.0] 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*

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

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

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.

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

FDP_PDC_EXT.3.1/VI The TSF shall have interfaces for the *DisplayPort* 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*.

Application Note: TD0620 applies to this SFR definition.

6.2.1.15 FDP_PDC_EXT.4 Supported Authentication Devices

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

6.2.1.16 FDP_PWR_EXT.1 Powered by Computer

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

6.2.1.17 FDP_RDR_EXT.1 Re-Enumeration Device Rejection

FDP_RDR_EXT.1.1 The TSF shall reject any device that attempts to enumerate again as a different unauthorized device.

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

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

6.2.1.19 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.

6.2.1.20 FDP_SPR_EXT.1/DP Sub-Protocol Rules

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.

6.2.1.21 FDP_SWI_EXT.1 PSD Switching

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

6.2.1.22 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 *console buttons, wired remote control, peripheral devices using a guard for the multi-viewer devices*.

6.2.1.23 FDP_SWI_EXT.3 Tied Switching

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.

6.2.1.24 FDP_TER_EXT.1 Session Termination

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

6.2.1.25 FDP_TER_EXT.2 Session Termination of Removed Devices

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

6.2.1.26 FDP_TER_EXT.3 Session Termination upon Switching

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.

6.2.1.27 FDP_UAI_EXT.1 User Authentication Isolation

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

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

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.

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

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.

6.2.2 Protection of the TSF (FPT)

6.2.2.1 FPT_FLS_EXT.1 Failure with Preservation of Secure State

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*.

6.2.2.2 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: *the Extended Display Identification Data (EDID) memory of Video TOEs may be accessible from connected computers*.

6.2.2.3 FPT_PHP.1 Passive Detection of Physical Attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

6.2.2.1 FPT_PHP.3 Resistance to Physical Attack

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.

Application Note: TD0583 applies to this SFR definition.

6.2.2.2 FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self-tests during initial start-up and at the conditions *no other conditions* 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*.

6.2.2.3 FPT_TST_EXT.1 TSF Testing

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.

6.2.3 TOE Access (FTA)

6.2.3.1 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: easily visible graphical and/or textual markings of each source video on the display, ***illuminated buttons***.

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*.

7 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 12.

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

Table 12 – Security Assurance Requirements

8 SECURITY REQUIREMENTS RATIONALE

8.1 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

Table 7 provides a mapping between the SFRs and Security Objectives.

8.2 DEPENDENCY RATIONALE

Table 13 identifies the Security Functional Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependencies	Rationale Statement
FDP_APC_EXT.1/KM	None	N/A
FDP_APC_EXT.1/UA	None	N/A
FDP_APC_EXT.1/VI	None	N/A
FDP_CDS_EXT.1(1), (2)	None	N/A
FDP_FIL_EXT.1/KM	FDP_PDC_EXT.1	Included
FDP_FIL_EXT.1/UA	FDP_PDC_EXT.1	Included
FDP_IPC_EXT.1	FDP_PDC_EXT.2	Included
FDP_PDC_EXT.1	None	N/A
FDP_PDC_EXT.2/KM	FDP_PDC_EXT.1	Included
FDP_PDC_EXT.2/UA	FDP_PDC_EXT.1	Included
FDP_PDC_EXT.2/VI	FDP_PDC_EXT.1	Included
FDP_PDC_EXT.3/KM	FDP_PDC_EXT.1	Included
FDP_PDC_EXT.3/VI	FDP_PDC_EXT.1	Included
FDP_PDC_EXT.4	FDP_PDC_EXT.1 FDP_PDC_EXT.2	Included Included
FDP_PWR_EXT.1	None	N/A
FDP_RDR_EXT.1	FDP_PDC_EXT.1	Included
FDP_RIP.1/KM	None	N/A
FDP_RIP_EXT.1	None	N/A
FDP_SPR_EXT.1/DP	FDP_PDC_EXT.3	Included

SFR	Dependencies	Rationale Statement
FDP_SWI_EXT.1	None	N/A
FDP_SWI_EXT.2	FDP_SWI_EXT.1	Included
FDP_SWI_EXT.3	FDP_SWI_EXT.1	Included
FDP_TER_EXT.1	None	N/A
FDP_TER_EXT.2	FDP_PDC_EXT.2	Included
FDP_TER_EXT.3	FDP_SWI_EXT.1	Included
FDP_UAI_EXT.1	None	Included
FDP_UDF_EXT.1/KM	FDP_APC_EXT.1	Included
FDP_UDF_EXT.1/VI	FDP_APC_EXT.1	Included
FPT_FLS_EXT.1	FPT_TST.1 FPT_PHP.3	Included Included -- anti-tamper is selected in FPT_FLS_EXT.1.1
FPT_NTA_EXT.1	None	N/A
FPT_PHP.1	None	N/A
FPT_PHP.3	None	N/A
FPT_TST.1	None	N/A
FPT_TST_EXT.1	FPT_TST.1	Included
FTA_CIN_EXT.1	FDP_APC_EXT.1	Included

Table 13 – Functional Requirement Dependencies

8.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE

The TOE assurance requirements for this ST consist of the requirements indicated in the [PP_PSD_V4.0] and in the PP modules listed in Section 2.2.

9 TOE SUMMARY SPECIFICATION

This section provides a description of the following TOE security functions that meet the TOE security requirements claimed in Section 6:

- User Data Protection
- Protection of the TSF
- TOE Access

Note: The TOE does not provide a management function to configure aspects of the TSF.

9.1 USER DATA PROTECTION

9.1.1 System Controller

Each device includes a System Controller which is responsible for device management, user interaction, system control security functions, and device monitoring. It receives user input from the switches on the front panel or the remote control and drives the TOE channel select lines that control switching circuits within the TOE.

The System Controller includes a microcontroller with internal non-volatile, Read Only Memory (ROM). The controller function manages the TOE functionality through a pre-programmed state machine loaded on the ROM as read-only firmware during product manufacturing.

Following boot up of the TOE, the channel select lines are set to Channel 1 by default. The channel select lines are also used to link the System Controller channel select commands to the Field Programmable Gate Array (FPGA) that supports video processing.

The user determines the host computer to be connected to the peripherals by pressing a button on the TOE front panel or on the wired remote control device. The front panel button of the selected computer is illuminated. Upon connection of the remote control connection, channel switching functionality is transferred from the front panel to the remote control. Remote control implementation eliminates the need for front panel operation. On the remote control, there is an LED indicator for each computer. When the remote control is connected to the TOE, the LED indicator of the selected computer is illuminated on the remote control. Switching can only be initiated through express user action and not through automated port scanning, connected computer control, or keyboard shortcuts.

The Multi-Viewer models (F1DN104MVKVMDC4 and F1DN108MVKVMDC4) may also be switched with peripheral devices using a guard[7]. This is performed using cursor navigation switching which requires the user to drag the mouse while pressing and holding the left CTRL key. The front panel button of the selected

[7] See Section 10.1 or [PP_PSD_V4.0] for the definition of a guard.

computer or the remote control indicator of the selected computer is illuminated when the guard is used to switch.

TOE Security Functional Requirements addressed: FDP_SWI_EXT.1, FDP_SWI_EXT.2.

9.1.1.1 Active PSD Connections

The TOE ensures that data flows only between the peripherals and the connected computer selected by the user. The TOE routes keyboard/mouse data only to the connected computer selected by the user. The TOE routes user authentication (smart card) data only to or from the connected computer selected by the user. The TOE routes video data only from the connected computer selected by the user.

No data or electrical signals flow between connected computers at any time. No data or electrical signal transits the TOE when the TOE is powered off, or when the TOE is in a failure state. A failure state occurs when the TOE fails a self-test when powering on, or when the anti-tampering function has been triggered.

TOE Security Functional Requirements addressed: FDP_APC_EXT.1/KM, FDP_APC_EXT.1/UA, FDP_APC_EXT.1/VI.

9.1.1.2 Connected Computer Interfaces

The connected computers are attached to the TOE as follows:

- The TOE connects to the computer USB peripheral port using a USB A to USB B cable. The USB A end attaches to the computer, and the USB B end attaches to the TOE.
- The TOE connects to the keyboard and mouse port using a USB A to USB B cable. The USB A end attaches to the computer, and the USB B end attaches to the TOE.
- The TOE is connected to the computer video port using a video cable supporting DisplayPort interface.
- The TOE connects to a computer on the F1DN104KVMDCU-4, F1DN204KVMDCU-4 modules using a USB-C cable from the computer USB-C port to the switch USB-C port.
- The TOE connects to the user authentication port using a USB A to USB B cable. The USB A end attaches to the computer, and the USB B end attaches to the TOE. Note: This connection to the computer requires a separate USB cable connection and allows the user to specify whether there is a connected device required for that computer or not. This allows the user authentication port to be connected and controlled separately to the keyboard, mouse and video.

There are no wireless interfaces or additional external interfaces.

TOE Security Functional Requirements addressed: FDP_PDC_EXT.1.

9.1.1.3 Residual Information Protection

The TOE does not support a factory reset capability. The Letter of Volatility is included as Annex A.

TOE Security Functional Requirements addressed: FDP_RIP_EXT.1.

9.1.2 Keyboard and Mouse Functionality

9.1.2.1 Keyboard and Mouse Enumeration

The TOE determines whether or not a peripheral device that has been plugged into the keyboard and mouse peripheral ports is allowed to operate with the TOE. The TOE uses optical data diodes to enforce a unidirectional data flow from the user peripherals to the coupled hosts, and uses isolated device emulators to prevent data leakage through the peripheral switching circuitry.

The Static Random Access Memory (SRAM) in the host and device emulator circuitry stores USB Host stack parameters and up to the last 4 key codes. User data may be briefly retained; however, there are no data buffers. Data is erased during power off of the KVM, and when the user switches channels. When the TOE switches from one computer to another, the system controller ensures that the keyboard and mouse stacks are deleted, and that any data received from the keyboard in the first 100 milliseconds following switching is deleted. This is done to ensure that any data buffered in the keyboard microcontroller is not passed to the newly selected computer.

The TOE supports USB Type A HIDs on keyboard and mouse ports. The USB bidirectional communication protocol is converted into a unidirectional proprietary protocol, and is then converted back into the USB bidirectional protocol to communicate with the coupled computer host(s).

A USB keyboard is connected to the TOE keyboard host emulator through the console keyboard port. The keyboard host emulator is a microcontroller which enumerates the connected keyboard and verifies that it is a permitted device type. Once the keyboard has been verified, the USB keyboard sends scan codes, which are generated when the user types. These scan codes are converted by the keyboard host emulator into a proprietary protocol data stream that is combined with the data stream from the mouse host emulator.

Similarly, the USB mouse is connected to the TOE mouse host emulator through the USB mouse port. The mouse host emulator is a microcontroller which enumerates the connected mouse and verifies that it is a permitted device type. Once the mouse device has been verified, it sends serial data generated by mouse movement and button use. The mouse serial data is converted by the mouse host emulator into a proprietary protocol data stream that is combined with the data stream from the keyboard host emulator.

TOE Security Functional Requirements addressed: FDP_PDC_EXT.3/KM, FDP_UDF_EXT.1/KM, FDP_RIP.1/KM.

9.1.2.2 Keyboard and Mouse Switching Functionality

Figure 3 is a simplified block diagram showing the TOE keyboard and mouse data path for two ports. A Host Emulator (HE) communicates with the user keyboard via the USB protocol. The Host Emulator converts user key strokes into unidirectional serial data.

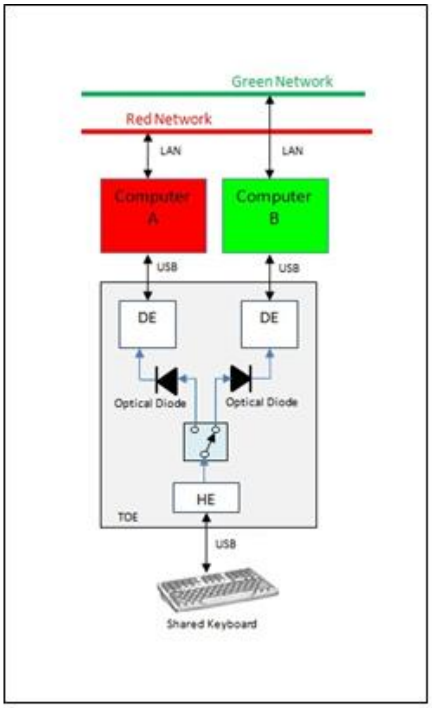

Figure 3 – Simplified Switching Diagram

The combined data stream is passed through the channel select lines to the selected host channel. The channel select lines are driven by the System Controller Module, and the selection is based on user input through use of the mouse or keyboard. Once a channel is selected, the combined mouse and keyboard data stream is passed through an optical data diode and routed to the specific host channel device emulator. The optical data diode is an opto-coupler designed to physically prevent reverse data flow. The keyboard and mouse can only be switched together.

Device emulators are USB enabled microcontrollers that are programmed to emulate a standard USB keyboard and mouse composite device. The combined data stream is converted back to bidirectional data before reaching the selected host computer.

Since the keyboard and mouse function are emulated by the TOE, the connected computer is not able to send data to the keyboard that would allow it to indicate that Caps Lock, Num Lock or Scroll Lock are set. These are indicated on the right-hand side of the TOE front panel.

TOE Security Functional Requirements addressed: FDP_APC_EXT.1/KM, FDP_UDF_EXT.1/KM, FDP_SWI_EXT.3.

9.1.2.3 Keyboard and Mouse Compatible Device Types

The TOE employs fixed device filtering and accepts only USB HID devices at the keyboard and mouse peripheral ports. Only USB Type A connections are permitted. The TOE does not support a wireless connection to a mouse, keyboard or USB hub and there are no additional external interfaces.

TOE Security Functional Requirements addressed: FDP_PDC_EXT.1, FDP_PDC_EXT.2/KM, FDP_FIL_EXT.1/KM.

9.1.2.4 Re-Enumeration Device Rejection

If a connected device attempts to re-enumerate as a different USB device type, it will be rejected by the TOE. The TOE will reject devices which are not allowed at any time during operation and start-up. This is indicated by an LED on the TOE next to the Keyboard and mouse ports. This LED shows a solid green light for an accepted device, flickering green light during enumeration, and no light for a rejected device.

TOE Security Functional Requirements addressed: FDP_RDR_EXT.1.

9.1.3 Video Switching Functionality

Video data flow is comprised of unidirectional Extended Display Identification Data (EDID) and video data flow paths. Figure 4 shows a data flow during the display EDID read function.

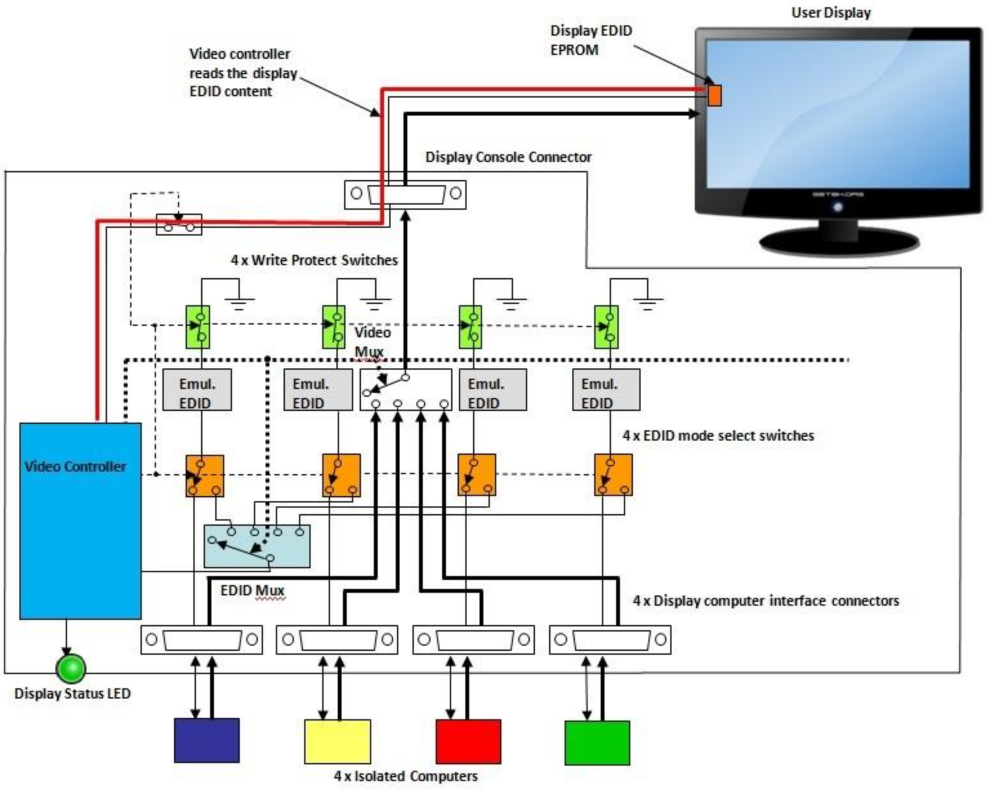
User Display
Display EDID EPROM
Video controller reads the display EDID content
Display Console Connector
4 x Write Protect Switches
Video Mux
Emul. EDID
Emul. EDID
Emul. EDID
Emul. EDID
4 x EDID mode select switches
Video Controller
EDID Mux
4 x Display computer interface connectors
Display Status LED
4 x Isolated Computers

Figure 4 – Display EDID Read Function

For each display device, an EDID read event only occurs as the TOE is being powered up. The video controller reads the EDID content from the display device to verify that it is valid and usable. If the EDID data is not valid, the TOE will not send data to the display peripheral. To use the display port, a working display peripheral must be connected to the TOE and the TOE restarted.

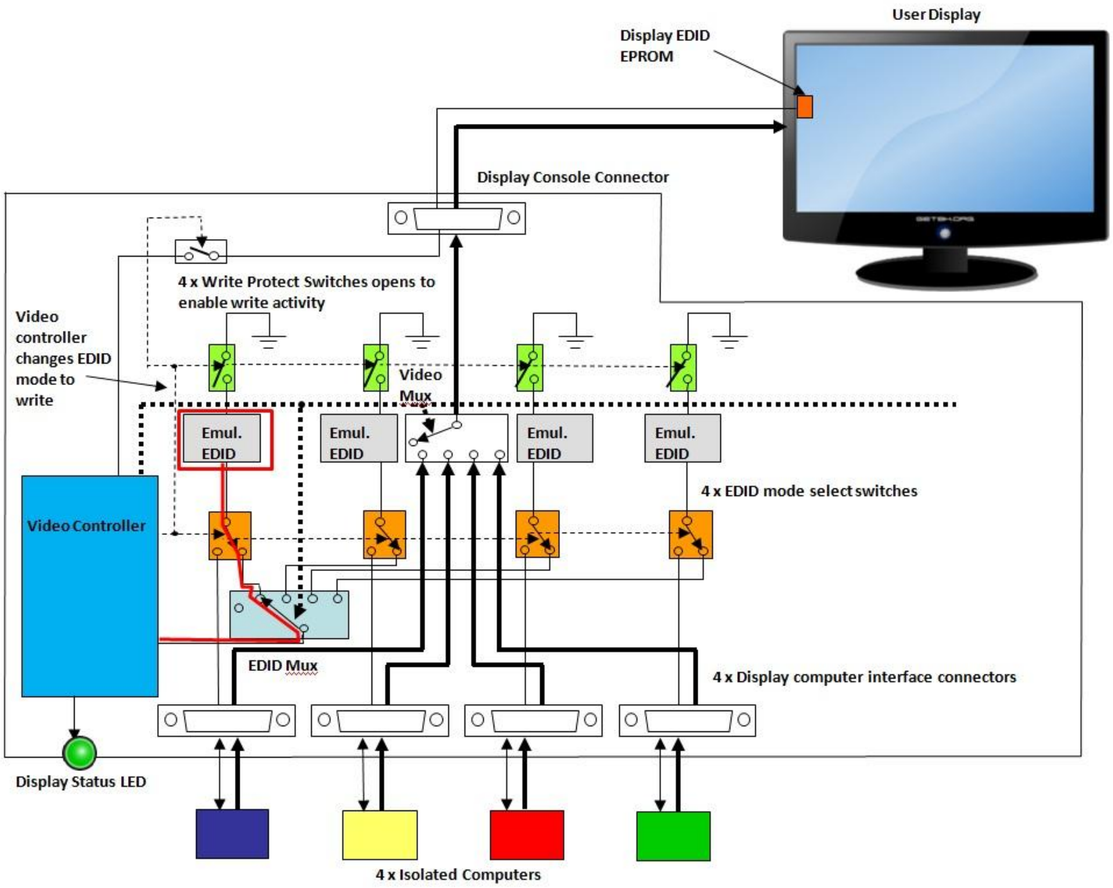
User Display
Display EDID EPROM
Display Console Connector
4 x Write Protect Switches opens to enable write activity
Video controller changes EDID mode to write
Video Mux
Emul. EDID
Emul. EDID
Emul. EDID
Emul. EDID
4 x EDID mode select switches
Video Controller
EDID Mux
4 x Display computer interface connectors
Display Status LED
4 x Isolated Computers

Figure 5 – Display EDID Write Function

Figure 5 illustrates the video controller (shown in blue) as it writes the EDID content into the first channel emulated EDID Electrically Erasable Programmable Read-Only Memory (EEPROM) chip (shown in gray). The thick lines in this figure indicate native video lines, and the thin lines indicate Inter-Integrated Circuit (I2C) lines. The EDID multiplexer couples the I2C lines to the first EDID mode switch (shown in orange). The first EDID mode switch switches the video controller I2C lines to the first emulated EDID EEPROM chip (shown in gray). The chip write protect switch opens to enable writing. The video controller uses the I2C lines to write to the first emulated EDID EEPROM chip. Once the write operation is complete and verified, the video controller switches the EDID multiplexer to the next channel and the operation repeats until all chips are programmed. Once the write operation is complete, the video controller switches to normal operating mode, as shown in Figure 6 below.

In EDID write mode, the Emulated EDID EEPROM chips are switched to their respective computers to enable reading of the EDID information. The write protect switches are switched back to protected mode to prevent any attempt to write to the EEPROM or to transmit MCCS commands.

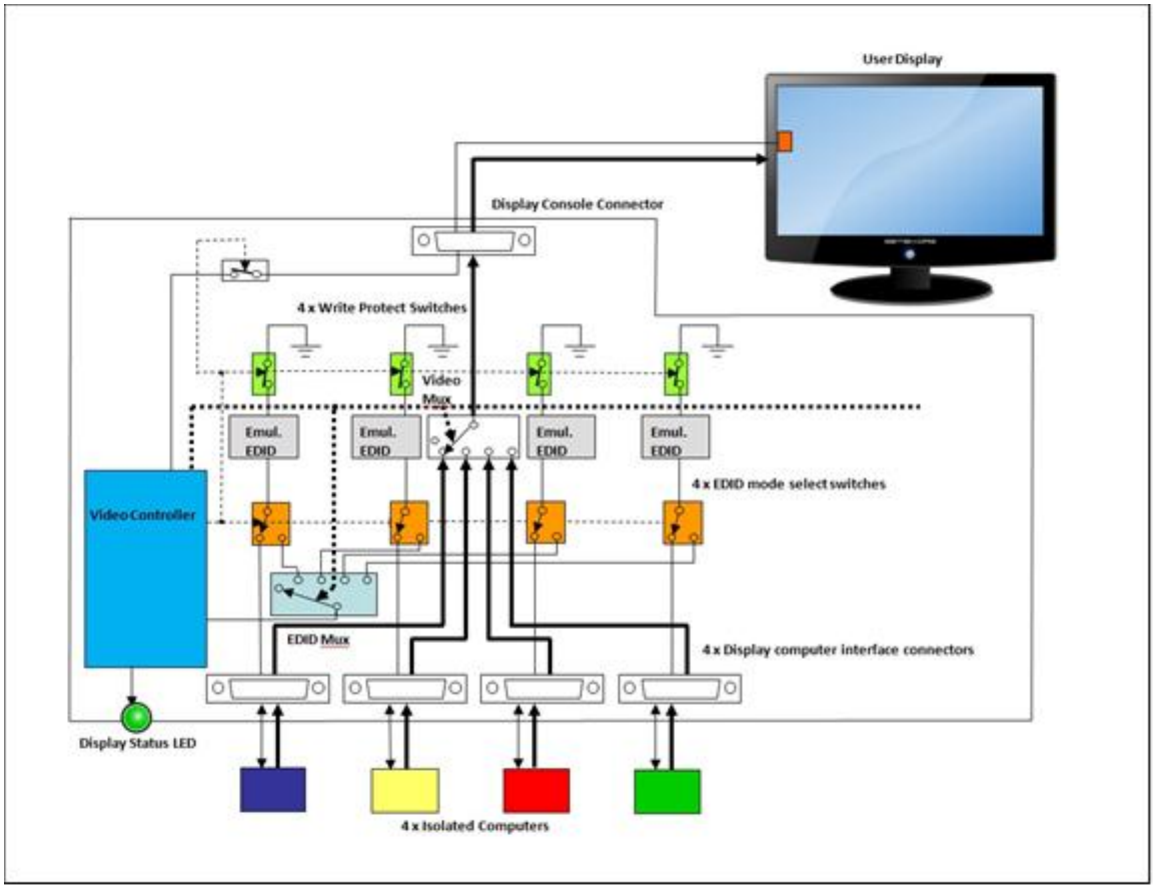

Figure 6 – Display Normal Mode

In normal mode, each computer interface operates independently. The power to each emulated EDID EEPROM is received from its respective computer through the video cable. The main video multiplexer is switched to the user selected computer to enable the proper video display.

During TOE normal operation (Figure 6), any attempt by a connected computer to affect the EDID channel is blocked by the architecture. Each computer is only able to affect its own emulated EDID EEPROM.

Video input interfaces are isolated from one another. Isolation is achieved through the use of separate power and ground planes, separate electronic components and a separate emulated EDID chip for each channel.

The EDID function is emulated by an independent emulation EEPROM chip for each computer channel. These chips read content from the connected display once during TOE power up. Any subsequent change to the display peripheral will be ignored.

The TOE will reject any display device that does not present valid EDID content. An LED on the rear panel of the TOE will indicate a rejected display device.

The TOE supports DisplayPort versions 1.1, 1.2 and 1.3 (video input/output). For DisplayPort connections, the TOE video function filters the AUX channel by converting it to I2C EDID only. DisplayPort video is converted into an HDMI video stream, and the I2C EDID lines connected to the emulated EDID EEPROM functions as shown in the figures above. This allows EDID to be passed from the display to the computer (as described above) and allows Hot-Plug Detection (HPD) and Link Training information to pass through the TOE. AUX channel threats are mitigated through the conversion from DisplayPort to HDMI protocols. Traffic types including USB, Ethernet, MCCS, and EDID write from the computer to the display are blocked by the TOE. High-bandwidth Digital Content Protection (HDCP) and Consumer Electronics Control (CEC) functions are not connected.

The TOE video function blocks MCCS write transactions through the emulated EDID EEPROMs. The emulated EEPROMs support only EDID read transactions, and are isolated by the write protect switch.

Following triggering of the anti-tampering function, following a failed self-test, or when the TOE is powered off, all video input signals are isolated from other video inputs and from the video output interfaces by the active video re-drivers. Emulated EDID EEPROMs may still operate since they are powered by their respective computers; however, the video function remains isolated.

TOE Security Functional Requirements addressed: FDP_IPC_EXT.1, FDP_SPR_EXT.1/DP, FDP_UDF_EXT.1/VI.

9.1.4 Video Compatible Device Types

The TOE accepts any DisplayPort display device at the video peripheral ports. The TOE does not support a wireless connection to a video display.

The number of video displays supported by each device model is indicated in Table 2.

TOE Security Functional Requirements addressed: FDP_PDC_EXT.1, FDP_PDC_EXT.2/VI, FDP_PDC_EXT.3/VI, FDP_CDS_EXT.1(1), FDP_CDS_EXT.1(2).

9.1.5 User Authentication Device Switching Functionality

The TOE supports the use of an external user authentication device with a feature called Freeze USB (fUSB). The TOE does not support internal user authentication devices.

By default, only standard USB smart-card readers or biometric authentication devices with USB smart-card class interfaces that comply with the USB Organization standard Chip Card Interface Device (CCID) Revision 1.1 or CCID Revision 1.0 will be accepted by the TOE on the fUSB port. This function is separate and physically isolated from the USB connections for keyboard and mouse. The user authentication device must be able to receive power from the

TOE. An external power source, such as power from the connected computer, is prohibited for this interface. The TOE does not receive power from the computer user authentication device interface. This restriction is indicated in the applicable user guidance.

Computer interfaces are isolated. Each fUSB computer interface uses independent circuitry and power planes. There is no shared circuitry, and no shared logical functions.

The System Controller drives the mode select switch that initially routes the device USB to the microcontroller. The qualification microcontroller uses the predefined USB qualification parameters and compares them with the discovered USB device parameters. If the parameters match, the device is accepted. The System Controller then switches the mode switch to the USB multiplexer. The USB multiplexer receives channel selected commands from the system controller function to allow the connection to the computer selected by the user. The data path used by the user authentication device is fully isolated from all other user data paths and functions.

When a user switches from one connected computer to another, the TOE resets the user authentication device through power supply switching, i.e. a temporary power dip. This is performed by High-side Power switches on the System Controller board that switch 5V power to the fUSB device jack. A load field-effect transistor (FET) shorts the supply voltage to the ground to quickly discharge any capacitance in the TOE or in the connected device to a level below 0.5V.

The TOE does not emulate or process user authentication device data. Therefore, no data retention is possible.

Following a failed self-test, or when the TOE is powered off, all user authentication device data paths are isolated through the peripheral multiplexer. These events effectively disconnect any open authentication session. Removal of the authentication device or removal of the authentication element (e.g., smart card) will also close the authentication session.

TOE Security Functional Requirements addressed: FDP_FIL_EXT.1/UA, FDP_PWR_EXT.1, FDP_TER_EXT.1, FDP_TER_EXT.2, FDP_TER_EXT.3, FDP_UAI_EXT.1.

9.1.5.1 User Authentication Compatible Device Types

The TOE does not include an authentication device, but accepts any USB Smart Card device at the fUSB peripheral port. Only USB Type A connections are permitted. The TOE does not support a wireless connection to an authentication device.

TOE Security Functional Requirements addressed: FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4.

9.2 PROTECTION OF THE TSF

9.2.1 No Access to TOE

Connected computers and peripherals do not have access to TOE firmware or memory, with the following exceptions:

- EDID data is accessible to connected computers from the TOE

All of the TOE microcontrollers run from internal protected flash memory. Firmware cannot be updated from an external source. Firmware cannot be read or rewritten through the use of Joint Test Action Group (JTAG) tools. Firmware is executed on Static Random Access Memory (SRAM) with the appropriate protections to prevent external access and tampering of code or stacks.

TOE Security Functional Requirements addressed: FPT_NTA_EXT.1.

9.2.2 Anti-tampering Functionality

The TOE provides both passive physical tampering detection and active resistance to physical tampering (anti-tampering) functionality. Active and passive anti-tampering is provided on the devices and on the remote control.

9.2.2.1 Passive Detection of Physical Tampering

The TOE enclosure was designed specifically to prevent physical tampering. It features a stainless-steel welded chassis and panels that prevent external access through bending or brute force.

Additionally, each device is fitted with one or more holographic Tampering Evident Labels placed at critical locations on the TOE enclosure. The remote control also has a Tampering Evident Label placed at a critical location. Any attempt to open the enclosure or remove a Tampering Evident Label results in the label being damaged so that the user can detect that the attempt to physically tamper with it occurred.

TOE Security Functional Requirements addressed: FPT_PHP.1.

9.2.2.2 Resistance to Physical Attack

The anti-tampering system is mechanically coupled to the TOE enclosure to detect any attempt to access the TOE internal circuitry. The active anti-tampering mechanism described in this section applies to both the KVM switch and the remote control.

Any attempt to separate the pieces of the enclosure to access the internal circuitry will trigger the anti-tampering function. Power is provided to the circuitry by the TOE power supply and by a backup battery. If the self-test detects that the battery is depleted or failing, the anti-tampering function will be triggered.

When the anti-tampering function is triggered, it causes an internal microscopic fuse on the System Controller (on-die) to melt. This permanently disables all interfaces and user functions of the device, and causes the front panel LEDs to blink sequentially and continuously. The TOE anti-tampering function is irreversible.

TOE Security Functional Requirements addressed: FPT_FLS_EXT.1, FPT_PHP.3.

9.2.3 TSF Testing

The TOE performs a self-test at initial start-up. The self-test runs independently at each microcontroller and performs the following checks:

- Verification of the front panel push-buttons
- Verification of the active anti-tampering functionality, including the continued functionality of the backup battery
- Verification of the integrity of the microcontroller firmware
- Verification of computer port isolation. This is tested by sending test packets to various interfaces and attempting to detect this traffic at all other interfaces

If the self-test fails, the LEDs on the front panel blink. The TOE disables the PSD switching functionality, and remains in a disabled state until the self-test is rerun and passes.

TOE Security Functional Requirements addressed: FPT_FLS_EXT.1, FPT_TST.1, FPT_TST_EXT.1.

9.3 TOE ACCESS

The TOE user switches between computers by pressing the corresponding front panel button on the device or on the remote control. The Multi-Viewer models (F1DN104MVKVMDC4 and F1DN108MVKVMDC4) may also be switched with peripheral devices using a guard. When the switching mechanism is initiated, a signal is sent and the TOE peripheral sharing device switches to the indicated channel. The front panel button of the KVM or the remote control button corresponding to the selected computer will illuminate.

On power up or power up following reset, all peripherals are connected to channel #1, and the corresponding push button LED will be illuminated.

TOE Security Functional Requirements addressed: FTA_CIN_EXT.1.

10TERMINOLOGY AND ACRONYMS

10.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
AUX	AUX refers to the auxiliary channel, particularly as it applies to the DisplayPort protocol.
Guard	'Guard' refers to a peripheral sharing device function that requires multiple express user actions in order to switch between connected computers using connected peripherals.
KM	KM refers to the requirements for Keyboard/Mouse Devices.
UA	UA refers to the requirements for User Authentication Devices
VI	VI refers to the requirements for Video Display Devices.

Table 14 – Terminology

10.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
ARC	Audio Return Channel
CC	Common Criteria
CEC	Consumer Electronics Control
DP	DisplayPort
EDID	Extended Display Identification Data
EEPROM	Electrically Erasable Programmable Read-Only Memory
FPGA	Field Programmable Gate Array
HDCP	High-bandwidth Digital Content Protection
HDMI	High-Definition Multimedia Interface
HE	Host Emulator
HEAC	HDMI Ethernet and Audio Return Channel
HEC	HDMI Ethernet Channel

Acronym	Definition
HID	Human Interface Device
HPD	Hot-Plug Detection
I2C	Inter-Integrated Circuit
IT	Information Technology
JTAG	Joint Test Action Group
KVM	Keyboard, Video, Mouse
LED	Light Emitting Diode
MCCS	Monitor Control Command Set
NIAP	National Information Assurance Partnership
OTP	One Time Programming
PP	Protection Profile
PSD	Peripheral Sharing Device
ROM	Read Only Memory
SFR	Security Functional Requirement
SRAM	Static Random Access Memory
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus

Table 15 – Acronyms

11 REFERENCES

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017
[Addenda]	CC and CEM addenda Exact Conformance, Selection-Based SFRs, Optional SFRs, 2021-Sep-30
[PKG_FLR_V1.0]	Assurance Package for Flaw Remediation Version 1.0, 2024-06-28
[PP_PSD_V4.0]	Protection Profile for Peripheral Sharing Device, Version: 4.0, 2019-07-19
[MOD_KM_V1.0]	PP-Module for Keyboard/Mouse Devices, Version 1.0, 2019-07-19
[MOD_UA_V1.0]	PP-Module for User Authentication Devices, Version 1.0, 2019-07-19
[MOD_VI_V1.0]	PP-Module for Video/Display Devices, Version 1.0, 2019-07-19
[CFG_PSD-KM-UA-VI_V1.0]	PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, 19 July 2019

Table 16 – References

ANNEX A – LETTER OF VOLATILITY

The table below provides volatility information and memory types for the Belkin Secure KVM DC-4 devices. User data is not retained in any TOE device when the power is turned off.

Product Model	No. in each product	Function, Manufacturer and Part Number	Storage Type	Size	Power Source (if not the TOE)	Volatility	Contains User Data
F1DN102KVM-DC-4 F1DN202KVM-DC-4 F1DN104KVM-DC-4 F1DN204KVM-DC-4 F1DN108KVM-DC-4 F1DN208KVM-DC-4 F1DN104KVMDCU-4 F1DN204KVMDCU-4 F1DN104MVKVM DC4	1	System Controller, Host emulators: ST Microelectronics STM32F446ZCT	Embedded SRAM[1]	128KB		Volatile	May contain user data
			Embedded Flash[2]	256KB		Non-Volatile	No user data
			Embedded EEPROM[3]	4KB		Non-Volatile	No user data
			OTP Memory	512bytes		Non-Volatile	Event logs are saved OR No user data
	1 in Single head or 2 in Dual head models	Video Controller: ST Microelectronics STM32F070RBT6	Embedded SRAM[1]	16KB		Volatile	May contain user data
			Embedded Flash[2]	128KB		Non-Volatile	No user data
	2 in 2 port	Device emulators:	Embedded SRAM[1]	6KB	Connected computer	Volatile	May contain user data

Product Model	No. in each product	Function, Manufacturer and Part Number	Storage Type	Size	Power Source (if not the TOE)	Volatility	Contains User Data
F1DN108MVKVMDC4 F1DN104MKVMDC-4 F1DN108MKVMDC-4	devices, 4 in 4 port devices, 8 in 8 port	ST Microelectronics STM32F070C6T6	Embedded Flash[2]	32KB		Non-Volatile	No user data
	4 in Single head or 8 in Dual head models	Video Channel Controller: STM32LF070CBT6	Embedded SRAM[1]	16KB		Volatile	May contain user data
			Embedded Flash[2]	128KB		Non-Volatile	No user data
F1DN104MVKVMDC4 F1DN108MVKVMDC4	1 in 4 port devices, 2 in 8 port devices	FPGA: Xilinx-AMD XC7K160T-1FFG676C	Embedded SRAM[1]	11,700Kb		Volatile	May contain user data
	1 in 4 port devices, 2 in 8 port devices	Serial Flash Memory: Spansion S25FL512SAGMFI011	Embedded Flash[2]	512Mb		Non-Volatile	No user data

Product Model	No. in each product	Function, Manufacturer and Part Number	Storage Type	Size	Power Source (if not the TOE)	Volatility	Contains User Data
	4 in 4 port devices, 8 in 8 port devices	DDR3 DRAM: Micron MT41K64M16TW-107:J	Embedded SRAM[1]	1Gb		Volatile	May contain user data
	1	System Controller, Host emulators: ST Microelectronics STM32F446ZCT	Embedded SRAM[1]	128KB		Volatile	May contain user data
			Embedded Flash[2]	256KB		Non-Volatile	No user data
			Embedded EEPROM[3]	4KB		Non-Volatile	No user data
			OTP Memory	512bytes		Non-Volatile	No user data
	4 in 4 port devices, 8 in 8 port	Device emulators: ST Microelectronics STM32F070C6T6	Embedded SRAM[1]	6KB	Connected computer	Volatile	May contain user data
			Embedded Flash[2]	32KB		Non-Volatile	No user data
	1	Video EDID Controller: STM32LF070CBT6	Embedded SRAM[1]	16KB		Volatile	No user data
			Embedded Flash[2]	128KB		Non-Volatile	No user data

Notes:

[1] SRAM stores USB Host stack parameters and up to the last 4 key-codes. Data is erased during power off of the KVM, and when the user switches channels. Device emulators receive power from the individual connected computers and therefore devices are powered on as long as the associated computer is powered on and connected.

[2] Flash storage is used to store firmware code. It contains no user data. Flash storage is permanently locked by fuses after initial programming to prevent rewriting. It is an integral part of the ST Microcontroller together with SRAM and EEPROM.

[3] EEPROM is used to store operational parameters, such as display Plug & Play. They contain no user data. These devices receive power from the individual computers connected to the TOE, and therefore are powered on as long as the associated computer is powered on and connected.

[4] EEPROM is used to store operational parameters, such as display Plug & Play, and contains no user data.