Belkin F1DN102KVM-UN-4, F1DN102KVM-UN4Z, F1DN102KVM-UN4C, F1DN102KVM-UN4W, F1DN202KVM-UN-4, F1DN202KVM-UN4Z, F1DN202KVM-UN4C, F1DN202KVM-UN4W, F1DN104KVM-UN-4, F1DN104KVM-UN4Z, F1DN104KVM-UN4C, F1DN104KVM-UN4W, F1DN204KVM-UN-4, F1DN204KVM-UN4Z, F1DN204KVM-UN4C, F1DN204KVM-UN4W, F1DN204KVM-UN4M, F1DN108KVM-UN-4, F1DN108KVM-UN4Z, F1DN108KVM-UN4W, F1DN208KVM-UN-4, F1DN208KVM-UN4Z, F1DN208KVM-UN4W, F1DN116KVM-UN-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices

Security Target

Doc No: 2344-003-D102
Version: 2.0
14 October 2026

Belkin International, Inc.
12045 E. Waterfront Drive
Playa Vista, CA 90094 USA

Prepared by:

Saffire Systems and
Carmel, IN
46032

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

CONTENTS

1 SECURITY TARGET INTRODUCTION 1
1.1 DOCUMENT ORGANIZATION 1
1.2 SECURITY TARGET REFERENCE 2
1.3 TOE REFERENCE 2
1.4 TOE OVERVIEW 2
1.4.1 Security Features 3
1.4.2 TOE Environment 5
1.5 TOE DESCRIPTION 6
1.5.1 Evaluated Configurations 6
1.5.2 Physical Scope 6
1.5.3 Logical Scope 9
2 CONFORMANCE CLAIMS 10
2.1 COMMON CRITERIA CONFORMANCE CLAIM 10
2.2 PP-CONFIGURATION CONFORMANCE CLAIM 10
2.3 TECHNICAL DECISIONS 10
2.4 PACKAGE CLAIM 12
2.5 CONFORMANCE RATIONALE 12
3 SECURITY PROBLEM DEFINITION 13
3.1 THREATS 13
3.2 ORGANIZATIONAL SECURITY POLICIES 14
3.3 ASSUMPTIONS 14
4 SECURITY OBJECTIVES 16
4.1 SECURITY OBJECTIVES FOR THE TOE 16
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 23
4.3 SECURITY OBJECTIVES RATIONALE 23
5 EXTENDED COMPONENTS DEFINITION 30
6 SECURITY FUNCTIONAL REQUIREMENTS 32
6.1 CONVENTIONS 32
6.2 SECURITY FUNCTIONAL REQUIREMENTS 32
6.2.1 Security Audit (FAU) 37
6.2.2 User Data Protection (FDP) 37

6.2.3 Identification and Authentication 45
6.2.4 Security Management (FMT) 45
6.2.5 Protection of the TSF (FPT) 46
6.2.6 TOE Access (FTA) 47

7 SECURITY ASSURANCE REQUIREMENTS 48

8 SECURITY REQUIREMENTS RATIONALE 49

8.1 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE 49
8.2 DEPENDENCY RATIONALE 49
8.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE 51

9 TOE SUMMARY SPECIFICATION 52

9.1 SECURITY AUDIT 52
9.2 USER DATA PROTECTION 53
9.2.1 System Controller 53
9.2.2 Keyboard and Mouse Functionality 54
9.2.3 Video Switching Functionality 57
9.2.4 Video Compatible Device Types 61
9.2.5 User Authentication Device Switching Functionality 61
9.2.6 Audio Switching Functionality 63
9.3 IDENTIFICATION AND AUTHENTICATION AND SECURITY MANAGEMENT 64
9.4 PROTECTION OF THE TSF 65
9.4.1 No Access to TOE 65
9.4.2 Anti-tampering Functionality 65
9.4.3 Reliable Timestamps 66
9.4.4 TSF Testing 66
9.5 TOE ACCESS 66

10 TERMINOLOGY AND ACRONYMS 69

10.1 TERMINOLOGY 69
10.2 ACRONYMS 69

11 REFERENCES 72

ANNEX A – LETTER OF VOLATILITY 73

LIST OF TABLES

Table 1 – Non-TOE Hardware and Software 5
Table 2 – TOE Peripheral Sharing Devices 7
Table 3 – TOE Remote Control Devices 8
Table 4 – Logical Scope of the TOE 9
Table 5 – Applicable Technical Decisions 12
Table 6 – Threats 14
Table 7 – Assumptions 15
Table 8 – Security Objectives for the TOE 22
Table 9 – Security Objectives for the Operational Environment 23
Table 10 – Security Objectives Rationale 29
Table 11 – Functional Families of Extended Components 31
Table 12 – Summary of Security Functional Requirements 37
Table 13 – Audio Filtration Specifications 38
Table 14 – Security Assurance Requirements 48
Table 15 – Functional Requirement Dependencies 51
Table 16 – Terminology 69
Table 17 – Acronyms 71
Table 18 – References 72

LIST OF FIGURES

Figure 1 – KVM Switch Evaluated Configuration 6
Figure 2 – SC Switching Diagram 56
Figure 3 – Display EDID Read Function 58
Figure 4 – Display EDID Write Function 59
Figure 5 – Display Normal Mode 60
Figure 6 – Remote Control Channel Selection 67
Figure 7 – Switch Channel Selection 68

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 F1DN102KVM-UN-4, F1DN102KVM-UN4Z, F1DN102KVM-UN4C, F1DN102KVM-UN4W, F1DN202KVM-UN-4, F1DN202KVM-UN4Z, F1DN202KVM-UN4C, F1DN202KVM-UN4W, F1DN104KVM-UN-4, F1DN104KVM-UN4Z, F1DN104KVM-UN4C, F1DN104KVM-UN4W, F1DN204KVM-UN-4, F1DN204KVM-UN4Z, F1DN204KVM-UN4C, F1DN204KVM-UN4W, F1DN204KVM-UN4M, F1DN108KVM-UN-4, F1DN108KVM-UN4Z, F1DN108KVM-UN4W, F1DN208KVM-UN-4, F1DN208KVM-UN4Z, F1DN208KVM-UN4W, F1DN116KVM-UN-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices Security Target
ST Version:	2.0
ST Date:	14 October 2026

1.3 TOE REFERENCE

TOE Identification:	Belkin F1DN102KVM-UN-4, F1DN102KVM-UN4Z, F1DN102KVM-UN4C, F1DN102KVM-UN4W, F1DN202KVM-UN-4, F1DN202KVM-UN4Z, F1DN202KVM-UN4C, F1DN202KVM-UN4W, F1DN104KVM-UN-4, F1DN104KVM-UN4Z, F1DN104KVM-UN4C, F1DN104KVM-UN4W, F1DN204KVM-UN-4, F1DN204KVM-UN4Z, F1DN204KVM-UN4C, F1DN204KVM-UN4W, F1DN204KVM-UN4M, F1DN108KVM-UN-4, F1DN108KVM-UN4Z, F1DN108KVM-UN4W, F1DN208KVM-UN-4, F1DN208KVM-UN4Z, F1DN208KVM-UN4W, F1DN116KVM-UN-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices
TOE Developer:	Belkin International, Inc.
TOE Type:	Peripheral Sharing Device (Other Devices and Systems)

1.4 TOE OVERVIEW

The Belkin Secure Peripheral Sharing Devices (PSDs) are part of the El Capitan product line. The El Capitan products are KVM switches with active anti-tampering, user authentication and logging, analog audio support, user authentication device support, and DisplayPort and High-Definition Multimedia Interface (HDMI) video support. An

external remote control device can be used with these devices, except the F1DN116KVM-UN-4.

These switches allow users to share keyboard, video, mouse, audio, and USB peripherals between connected computers. These devices also allow for the sharing of audio and Universal Serial Bus (USB) authentication device peripherals. Security features ensure isolation between computers and peripherals to prevent data leakage between connected systems.

The switches allow users to view and control only one computer at a time while securely sharing keyboard, mouse, video, audio, and a user authentication device between a number of connected computers. The video input and video output is DisplayPort or HDMI and one or two displays are connected.

1.4.1 Security Features

The following security features are provided by the Peripheral Sharing 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.
  - Both DisplayPort and High-Definition Multimedia Interface (HDMI) video protocols are supported for both peripheral devices (video out) and video input.
  - Bi-directional interfaces of HDMI, for example, HEC, ARC, CEC and more are not connected.
- 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.
    - Devices may be whitelisted or blacklisted based on Vendor Identification/Product Identification (VID/PID) characteristics
    - Secure management functions allow configuration of allowed devices, and maintain a record of any changes to that configuration
- Audio Security
    - One-way computer to speaker sound flow is enforced through unidirectional optical data diodes
- 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.
- Logging
    - The TOE generates and stores audit records for security related events
- Security Management
    - The TOE provides the ability for administrative users to perform security management functions.
- User Authentication
    - The TOE requires users to be identified and authenticated prior to performing security management functions.

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 (e.g., display signaling, keyboard signaling, and power 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	1-16 General purpose computers
Keyboard	General purpose USB keyboard
Mouse	General purpose USB mouse
Audio output device	Analog audio output device (speakers or headphones) with a 3.5 mm Tip-Ring-Sleeve (TRS) connector
User authentication device	Standard USB smartcard reader/authentication device
User display	Standard computer display (DisplayPort 1.1, 1.2, or 1.3) Standard computer display (HDMI 2.0)
Cables	USB Type-A to USB Type-B (keyboard and mouse) Video cable (DisplayPort and HDMI) 3.5mm stereo TRS cable (Audio cable) USB Type-A to USB Type-B (authentication device)
Power Supply for the 2 port and 4 port devices (Note the 8 and 16 port devices have an internal power supply)	12 Volt Direct Current (VDC) power supply

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Evaluated Configurations

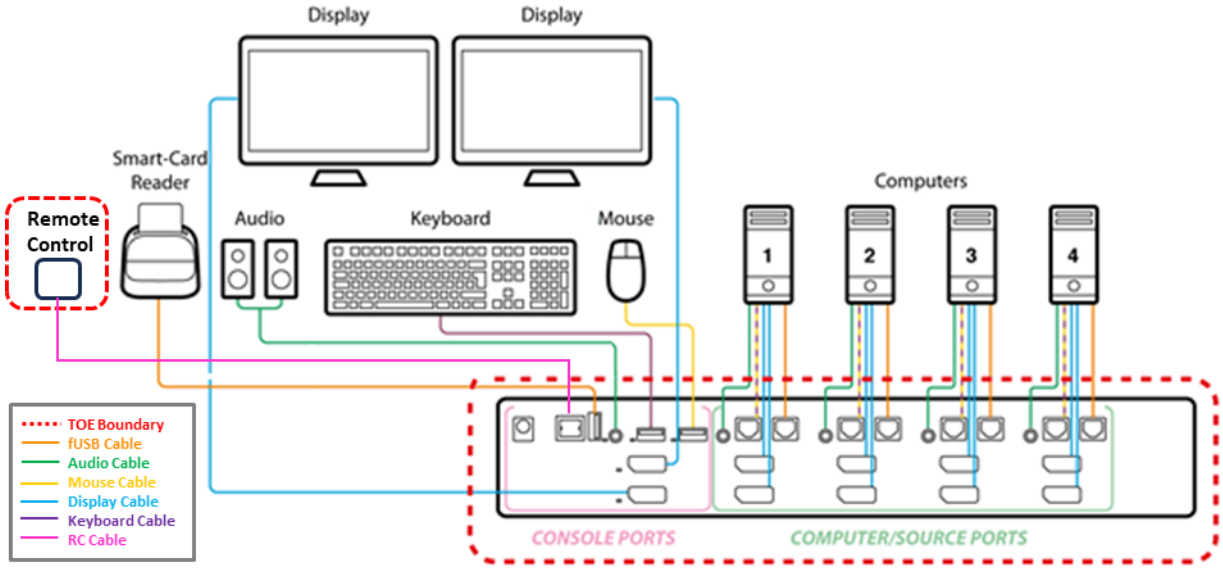


Figure 1 – KVM Switch Evaluated Configuration

Figure 1 shows a basic evaluated configuration. In the evaluated configuration, the TOE is connected to a keyboard, a mouse, an audio device (speakers or headphones), a user authentication device, and up to sixteen computers depending on the model. The video input is DisplayPort (DP) or HDMI, and one or two displays are connected. The peripheral sharing device is connected to speakers or headphones, and to a user authentication device.

Refer to Table 2 for a list of the number of computers supported, number of displays supported, and video protocols supported for each model. All of the switches except the F1DN116KVM-UN-4 can be used with a wired remote desktop control, also referred to as a remote control.

For this evaluation, the TOE was tested according to the PP requirements using devices supporting DP 1.1a, DP 1.2 (for some tests), HDMI 1.4, USB 2.0, and CCID Revision 1.1 (for UA). The TOE supports DP 1.3 and HDMI 2.0 subject to the limitations stated in the TSS. These limitations are due to the PP mandated blocking of specific parts of the protocols.

1.5.2 Physical Scope

The TOE consists of the KVM devices shown in Table 2, the Belkin Firmware Version 44444-E7E7, and the remote control devices shown in Table 3.

All of the switches include the following features:

- Active anti-tampering
- Tamper evident labels
- User authentication and audit logging

- Support for sharing keyboard, mouse, analog audio, user authentication device peripheral (DPP)
- Support for DP and HDMI video input and output

The remote controls include active anti-tampering and tamper evident labels.

Family	Switch Part Number	Switch Model	Number of hosts	Number of supported displays
El Capitan KVM Devices	CGA18316 CGA30753 CGA31539 CGA39560	F1DN102KVM-UN-4 F1DN102KVM-UN4Z F1DN102KVM-UN4C F1DN102KVM-UN4W	2	1
	CGA18326 CGA30754 CGA31537 CGA39561	F1DN202KVM-UN-4 F1DN202KVM-UN4Z F1DN202KVM-UN4C F1DN202KVM-UN4W	2	2
	CGA18322 CGA30755 CGA31540 CGA38804	F1DN104KVM-UN-4 F1DN104KVM-UN4Z F1DN104KVM-UN4C F1DN104KVM-UN4W	4	1
	CGA18329 CGA30756 CGA31538 CGA38805 CGA26469	F1DN204KVM-UN-4 F1DN204KVM-UN4Z F1DN204KVM-UN4C F1DN204KVM-UN4W F1DN204KVM-UN4M	4	2
	CGA18359 CGA30757 CGA38806	F1DN108KVM-UN-4 F1DN108KVM-UN4Z F1DN108KVM-UN4W	8	1
	CGA18360 CGA30758 CGA38807	F1DN208KVM-UN-4 F1DN208KVM-UN4Z F1DN208KVM-UN4W	8	2
	CGA18984	F1DN116KVM-UN-4	16	1

Table 2 – TOE Peripheral Sharing Devices

Note: The difference between the models grouped together in each of the rows in Table 2 is the front panel button color defaults. The rest of the product features are the same.

Remote Control Part Number	Remote Control Model	Number of ports / channels supported	Switch used with the Remote Control
CGA33637	F1DN-KVM-REM2	2	F1DN102KVM-UN-4 F1DN102KVM-UN4Z F1DN102KVM-UN4C F1DN102KVM-UN4W F1DN202KVM-UN-4 F1DN202KVM-UN4Z F1DN202KVM-UN4C F1DN202KVM-UN4W
CGA33638	F1DN-KVM-REM4	4	F1DN104KVM-UN-4 F1DN104KVM-UN4Z F1DN104KVM-UN4C F1DN104KVM-UN4W F1DN204KVM-UN-4 F1DN204KVM-UN4Z F1DN204KVM-UN4C F1DN204KVM-UN4W F1DN204KVM-UN4M
CGA33639	F1DN-KVM-REM8	8	F1DN108KVM-UN-4 F1DN108KVM-UN4Z F1DN108KVM-UN4W F1DN208KVM-UN-4 F1DN208KVM-UN4Z F1DN208KVM-UN4W

Table 3 – TOE Remote Control Devices

1.5.2.1 TOE Delivery

The TOE and its corresponding cables are 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:

- Quick Installation Guide 2/4/8 Port Secure Single/Dual-Head DP/HDMI-DP/HDMI KVM Switches, 8820-02951 Rev.A03
- Quick Installation Guide 8/16 Port Secure Single/Dual-Head DP/HDMI-DP/HDMI KVM Switches, 8820-02952 Rev. A02
- Belkin Administrator Guide, LNKPG-00666 Rev. C03
- Belkin Regulatory Information, 8820-02969 Rev. B00

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

The following guidance is available upon request by emailing KVM_Support@belkin.com:

- Belkin F1DN102KVM-UN-4, F1DN102KVM-UN4Z, F1DN102KVM-UN4C, F1DN102KVM-UN4W, F1DN202KVM-UN-4, F1DN202KVM-UN4Z, F1DN202KVM-UN4C, F1DN202KVM-UN4W, F1DN104KVM-UN-4, F1DN104KVM-UN4Z, F1DN104KVM-UN4C, F1DN104KVM-UN4W, F1DN204KVM-UN-4, F1DN204KVM-UN4Z, F1DN204KVM-UN4C, F1DN204KVM-UN4W, F1DN204KVM-UN4M, F1DN108KVM-UN-4, F1DN108KVM-UN4Z, F1DN108KVM-UN4W, F1DN208KVM-UN-4, F1DN208KVM-UN4Z, F1DN208KVM-UN4W, F1DN116KVM-UN-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices Common Criteria Guidance Supplement, Version 2.0

1.5.3 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 4 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events.
User Data Protection	The TOE provides secure switching and unidirectional data flow capabilities for keyboard, mouse, video, audio output, and authentication device peripherals. The TOE ensures that only authorized peripheral devices may be used. The TOE supports a factory reset capability.
Identification and Authentication	Administrators must be identified and authenticated prior to accessing administrative functions.
Security Management	The TOE provides management capabilities in support of Configurable Device Filtration. The Administrator role restricts this functionality to authorized administrators.
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. The TOE provides reliable timestamps in support of the audit function.
TOE Access	The TOE provides a continuous indication of which computer is currently selected.

Table 4 – 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, Analog Audio Output, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, 2019-07-19 [CFG_PSD-AO-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 Analog Audio Output Devices, Version 1.0 [MOD_AO_V1.0]
- 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 5 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]	Y
TD0539	Incorrect selection trigger in FTA_CIN_EXT.1 in MOD_VI_V1.0	[MOD_VI_V1.0]	Y
TD0557	Correction to Audio Filtration Specification table in FDP_AFL_EXT.1	[MOD_AO_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_V1.0]	Y
TD0585	Update to FDP_APC_EXT.1 Audio Output Tests	[MOD_AO_V1.0]	Y
TD0593	Equivalency Arguments for PSD	[MOD_AO_V1.0], [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
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
TD0842	Alternate Conversion Option for FDP_IPC_EXT.1	[MOD_VI_V1.0]	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.
TD0942	Updated EDID Read Requirements	[MOD_VI_V1.0]	Y

TD	Name	PP affected	Relevant Y/N
TD0959	Correction to Test 4 Step 3 of FDP_APC_EXT.1	[MOD_KM_V1.0]	Y

Table 5 – 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, Analog Audio Output Devices, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices [CFG_PSD-AO-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 6 lists the threats described in Section 3.1 of the [PP_PSD_V4.0] and [MOD_AO_V1.0]. 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

[1] Peripheral Sharing Device

Threat	Description
	alternate device that does not enforce the PSD security policies.
T.FAILED	Detectable failure of a PSD may cause an unauthorized information flow or weakening of PSD security functions.
T.MICROPHONE_USE	A malicious agent could use an unauthorized peripheral device such as a microphone, connected to the TOE audio out peripheral device interface to eavesdrop or transfer data across an air-gap through audio signaling.
T.AUDIO_REVERSED	A malicious agent could repurpose an authorized audio output peripheral device by converting it to a low-gain microphone to eavesdrop on the surrounding audio or transfer data across an air-gap through audio signaling.

Table 6 – 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 7. These assumptions are derived from Section 3.2 of [PP_PSD_V4.0], [MOD_AO_V1.0] 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.

Assumptions	Description
A.TRUSTED_ADMIN	PSD Administrators 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.
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.
A.NO_MICROPHONES	Users are trained not to connect a microphone to the TOE audio output interface.

Table 7 – 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>O.COMPUTER
_INTERFACE
_ISOLATION</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_AO</td><td>FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1</td></tr><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>

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td>O.COMPUTER
_INTERFACE
_ISOLATION
_TOE_UNPOWERED</td><td>The PSD shall not allow data to transit a PSD-Computer interface while the PSD is unpowered.
Addressed by:<table><tr><td>MOD_AO</td><td>FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1</td></tr><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>
<tr><td>O.USER_DATA
_ISOLATION</td><td>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:<table><tr><td>MOD_AO</td><td>FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1</td></tr><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>
<tr><td>O.NO_USER
_DATA_RETENTION</td><td>The PSD shall not retain user data in non-volatile memory after power up or, if supported, factory reset.
Addressed by:<table><tr><td>PP_PSD</td><td>FDP_RIP_EXT.1, FDP_RIP_EXT.2</td></tr><tr><td>MOD_KM</td><td>FDP_RIP.1/KM</td></tr></table></td></tr>
</table>

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td>O.NO_OTHER
_EXTERNAL
_INTERFACES</td><td>The PSD shall not have any external interfaces other than those implemented by the TSF.
Addressed by:<table><tr><td>PP_PSD</td><td>FDP_PDC_EXT.1</td></tr></table></td></tr>
<tr><td>O.LEAK
_PREVENTION
_SWITCHING</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>O.AUTHORIZED
_USAGE</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>FAU_GEN.1, FDP_SWI_EXT.1, FDP_SWI_EXT.2, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_SMF.1, FMT_SMR.1, FPT_STM.1, FTA_CIN_EXT.1</td></tr><tr><td>MOD_VI</td><td>FDP_CDS_EXT.1(1), FDP_CDS_EXT.1(2), 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>

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td>O.PERIPHERAL
_PORTS_ISOLATION</td><td>The PSD shall ensure that data does not flow between peripheral devices connected to different PSD interfaces.
Addressed by:<table>
<tr><td>MOD_AO</td><td>FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1</td></tr>
<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>
<tr><td>O.REJECT
_UNAUTHORIZED
_ENDPOINTS</td><td>The PSD shall reject unauthorized peripheral devices connected via a Universal Serial Bus (USB) hub.
Addressed by:<table>
<tr><td>PP_PSD</td><td>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>

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td>O.REJECT
_UNAUTHORIZED
_PERIPHERAL</td><td>The PSD shall reject unauthorized peripheral device types and protocols.
Addressed by:<table><tr><td>PP_PSD</td><td>FDP_PDC_EXT.1</td></tr><tr><td>MOD_AO</td><td>FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1</td></tr><tr><td>MOD_VI</td><td>FDP_PDC_EXT.2/VI, FDP_PDC_EXT.3/VI, FDP_IPC_EXT.1, FDP_SPR_EXT.1/DP, FDP_SPR_EXT.1/HDMI</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, FDP_PDC_EXT.2/KM, FDP_PDC_EXT.3/KM</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>
<tr><td>O.NO_TOE_ACCESS</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>O.TAMPER
_EVIDENT
_LABEL</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>
</table>

Security Objective	Description
O.ANTI_TAMPERING	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: PP_PSD: FPT_PHP.1, FPT_PHP.3
O.SELF_TEST	The PSD shall perform self-tests following power up or powered reset. Addressed by: PP_PSD: FPT_TST.1
O.SELF_TEST _FAIL_TOE _DISABLE	The PSD shall enter a secure state upon detection of a critical failure. Addressed by: PP_PSD: FPT_FLS_EXT.1, FPT_TST_EXT.1
O.SELF_TEST _FAIL_INDICATION	The PSD shall provide clear and visible user indications in the case of a self-test failure. Addressed by: PP_PSD: FPT_TST_EXT.1
O.EMULATED_INPUT	The TOE shall emulate the keyboard and/or mouse functions from the TOE to the connected computer. Addressed by: MOD_KM: FDP_PDC_EXT.2/KM, FDP_PDC_EXT.3/KM
O.UNIDIRECTIONAL _INPUT	The TOE shall enforce unidirectional keyboard and/or mouse device’s data flow from the peripheral device to only the selected computer. Addressed by: MOD_KM: FDP_UDF_EXT.1/KM

Security Objective	Description
O.USER_AUTHENTICATION_ISOLATION	The TOE shall isolate the user authentication function from all other TOE functions. Addressed by: MOD_UA: FDP_UAI_EXT.1
O.SESSION_TERMINATION	The TOE shall immediately terminate an open session with the selected computer upon disconnection of the authentication element. Addressed by: MOD_UA: FDP_TER_EXT.1, FDP_TER_EXT.2, FDP_TER_EXT.3
O.PROTECTED_EDID	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: MOD_VI: FDP_PDC_EXT.2/VI, FDP_SPR_EXT.1/DP, FDP_SPR_EXT.1/HDMI
O.UNIDIRECTIONAL_VIDEO	The TOE shall enforce unidirectional video data flow from the connected computer video interface to the display interface only. Addressed by: MOD_VI: FDP_UDF_EXT.1/VI
O.UNIDIRECTIONAL_AUDIO_OUT	The PSD shall enforce the unidirectional flow of audio data from the analog audio computer interface to the analog audio peripheral interface. Addressed by: MOD_AO: FDP_APC_EXT.1/AO, FDP_AFL_EXT.1, FDP_UDF_EXT.1/AO
O.COMPUTER_TO_AUDIO_ISOLATION	The PSD shall isolate the analog audio output function from all other TOE functions. Addressed by: MOD_AO: FDP_APC_EXT.1/AO, FDP_UDF_EXT.1/AO

Table 8 – 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.
OE.NO_MICROPHONES	The operational environment is expected to ensure that microphones are not plugged into the TOE audio output interfaces.

Table 9 – 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.

Threat or Assumption	Security Objective(s)	Rationale
	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.
	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.

Threat or Assumption	Security Objective(s)	Rationale
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.
	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.UNIDIRECTIONAL_AUDIO_OUT	O.UNIDIRECTIONAL_AUDIO_OUT mitigates this threat by preventing the exploitation of the analog audio output to receive signaled data from a connected computer. Analog audio output in standard computers may be exploited to become audio input in some audio codecs. Audio devices such as headphones may also be used as low-gain dynamic microphones. If the TOE design assures that analog audio reverse signal attenuation is below the noise floor level then the audio signal may not be recovered from the resultant audio stream. This prevents potential misuse of headphones connected to the TOE for audio eavesdropping.
	O.COMPUTER_TO_AUDIO_ISOLATION	O.COMPUTER_TO_AUDIO_ISOLATION mitigates this threat by ensuring that analog audio output converted to input by a malicious driver cannot pick up signals from other computer interfaces. A TOE design that ensures that audio signals are not leaked to any other TOE interface can effectively prevent a potential signaling leakage across the TOE through analog audio.
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.

Threat or Assumption	Security Objective(s)	Rationale
	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.
	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.

Threat or Assumption	Security Objective(s)	Rationale
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.
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.
T.MICROPHONE_USE	O.UNIDIRECTIONAL _AUDIO_OUT	O.UNIDIRECTIONAL_AUDIO_OUT mitigates this threat by attenuating the strength of any inbound transmission of audio data through the TOE from a connected peripheral. If the TOE design ensures that analog audio reverse signal attenuation is below the noise floor level then any audio signal should not have sufficient strength to be usable.
T.AUDIO_REVERSED	O.UNIDIRECTIONAL _AUDIO_OUT	O.UNIDIRECTIONAL_AUDIO_OUT mitigates this threat by ensuring that the TOE's audio peripheral interface(s) are exclusively used to output audio.

Threat or Assumption	Security Objective(s)	Rationale
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[2]	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.
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.
A.NO _MICROPHONES	OE.NO _MICROPHONES	The assumption is upheld by the objective since the users in the environment are trained not to connect a microphone to the TOE audio output interface,

Table 10 – Security Objectives Rationale

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

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 audio devices [MOD_AO_V1.0], 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_AFL_EXT Audio Filtration	[MOD_AO_V1.0]
	FDP_APC_EXT Active PSD Connections	[PP_PSD_V4.0] [MOD_AO_V1.0] [MOD_KM_V1.0] [MOD_UA_V1.0] [MOD_VI_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_AO_V1.0] [MOD_KM_V1.0] [MOD_UA_V1.0] [MOD_VI_V1.0]
	FDP_PUD_EXT Powering Unauthorized Devices	[MOD_AO_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]

Functional Class	Functional Families	Protection Profile Modules
	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_AO_V1.0] [MOD_KM_V1.0] [MOD_VI_V1.0]
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 11 – 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 defined 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
Security Audit (FAU)	FAU_GEN.1	Audit data generation	[PP_PSD_V4.0]	All
User Data Protection (FDP)	FDP_AFL_EXT.1	Audio Filtration	[MOD_AO_V1.0]	All
	FDP_APC_EXT.1/AO	Active PSD Connections	[MOD_AO_V1.0]	All
	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-UN-4 F1DN102KVM-UN4Z F1DN102KVM-UN4C F1DN102KVM-UN4W F1DN104KVM-UN-4 F1DN104KVM-UN4Z F1DN104KVM-UN4C F1DN104KVM-UN4W F1DN108KVM-UN-4 F1DN108KVM-UN4Z F1DN108KVM-UN4W F1DN116KVM-UN-4
	FDP_CDS_EXT.1(2)	Connected Displays Supported (2)	[MOD_VI_V1.0]	F1DN202KVM-UN-4 F1DN202KVM-UN4Z F1DN202KVM-UN4C F1DN202KVM-UN4W F1DN204KVM-UN-4 F1DN204KVM-UN4Z F1DN204KVM-UN4C F1DN204KVM-UN4W F1DN204KVM-UN4M F1DN208KVM-UN-4 F1DN208KVM-UN4Z F1DN208KVM-UN4W
	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

Class	Identifier	Name	Source	Applicable Devices
	FDP_PDC_EXT.1	Peripheral Device Connection	[PP_PSD_V4.0] [MOD_AO_V1.0][3] [MOD_VI_V1.0][4] [MOD_KM_V1.0][5] [MOD_UA_V1.0][6]	All
	FDP_PDC_EXT.2/AO	Peripheral Device Connection (Audio Output)	[MOD_AO_V1.0]	All
	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

[3] There is no modification to this SFR in the [MOD_AO_V1.0]. However, there are additions to the Peripheral Device Connections Policy associated with this SFR, and additional evaluation activities.

[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_PUD_EXT.1	Powering Unauthorized Devices	[MOD_AO_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
	FDP_RIP_EXT.2	Purge of Residual Information	[PP_PSD_V4.0]	All
	FDP_SPR_EXT.1/DP	Sub-Protocol Rules (DisplayPort Protocol)	[MOD_VI_V1.0]	All
	FDP_SPR_EXT.1/HDMI	Sub-Protocol Rules (HDMI 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

Class	Identifier	Name	Source	Applicable Devices
	FDP_UAI_EXT.1	User Authentication Isolation	[MOD_UA_V1.0]	All
	FDP_UDF_EXT.1/AO	Unidirectional Data Flow (Audio Output)	[MOD_AO_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
Identification and Authentication (FIA)	FIA_UAU.2	User Authentication Before Any Action	[PP_PSD_V4.0]	All
	FIA_UID.2	User Identification Before Any Action	[PP_PSD_V4.0]	All
Security Management (FMT)	FMT_MOF.1	Management of Security Functions Behavior	[PP_PSD_V4.0]	All
	FMT_SMF.1	Specification of Management Functions	[PP_PSD_V4.0]	All
	FMT_SMR.1	Security Roles	[PP_PSD_V4.0]	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
	FPT_PHP.3	Resistance to Physical Attack	[PP_PSD_V4.0]	All
	FPT_STM.1	Reliable Time Stamps	[PP_PSD_V4.0]	All

Class	Identifier	Name	Source	Applicable Devices
	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 12 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the audit functions;
b. All auditable events for the not specified level of audit; and
c. administrator login, administrator logout, self-test failures, peripheral device acceptance and rejections, **reset to factory default, create administrator account, change password, modify Configurable Device Filtration (CDF) list for authentication devices**.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, no other information.

6.2.2 User Data Protection (FDP)

6.2.2.1 FDP_AFL_EXT.1 Audio Filtration

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

Frequency (kHz)	Minimum Attenuation (dB)	Maximum Voltage After Attenuation
14	23.9	127.65 mV
15	26.4	95.73 mV
16	30.8	57.68 mV
17	35.0	35.57 mV
18	38.8	22.96 mV

Frequency (kHz)	Minimum Attenuation (dB)	Maximum Voltage After Attenuation
19	43.0	14.15 mV
20	46.0	10.02 mV
30	71.4	0.53 mV
40	71.4	0.53 mV
50	71.4	0.53 mV
60	71.4	0.53 mV

Table 13 – Audio Filtration Specifications

Application Note: TD0557 applies to this SFR definition.

6.2.2.2 FDP_APC_EXT.1/AO Active PSD Connections

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

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

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

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

6.2.2.3 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.

6.2.2.4 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.

6.2.2.5 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.

6.2.2.6 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-UN-4, F1DN102KVM-UN4Z, F1DN102KVM-UN4C, F1DN102KVM-UN4W,
F1DN104KVM-UN-4, F1DN104KVM-UN4Z, F1DN104KVM-UN4C, F1DN104KVM-UN4W,
F1DN108KVM-UN-4, F1DN108KVM-UN4Z, F1DN108KVM-UN4W, F1DN116KVM-UN-4.

6.2.2.7 FDP_CDS_EXT.1(2) Connected Displays Supported

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

Application Note: FDP_CDS_EXT.1(2) applies to the following models:
F1DN202KVM-UN-4, F1DN202KVM-UN4Z, F1DN202KVM-UN4C, F1DN202KVM-UN4W,
F1DN204KVM-UN-4, F1DN204KVM-UN4Z, F1DN204KVM-UN4C, F1DN204KVM-UN4W,
F1DN204KVM-UN4M, F1DN208KVM-UN-4, F1DN208KVM-UN4Z, F1DN208KVM-UN4W.

6.2.2.8 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.

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

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

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

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

6.2.2.10 FDP_IPC_EXT.1 Internal Protocol Conversion

FDP_IPC_EXT.1.1 The TSF shall convert the DisplayPort protocol at the *DisplayPort peripheral display interface(s), 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 *computer video interface, peripheral display interface(s)* as *DisplayPort protocol, HDMI protocol*.

Application Note: TD0842 applies to this SFR definition.

6.2.2.11 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.

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

FDP_PDC_EXT.2.1/AO The TSF shall allow connections with authorized devices as defined in Appendix E of [MOD_AO_V1.0] and

- *authorized devices as defined in the PP-Module for Keyboard/Mouse Devices,*
- *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/AO The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in Appendix E of [MOD_AO_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,*

- *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.

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

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

FDP_PDC_EXT.2.2/KM The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in Appendix E of [MOD_KM_V1.0] and

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

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

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

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

FDP_PDC_EXT.2.2/UA The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in Appendix E of [MOD_UA_V1.0] and

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

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

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

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

FDP_PDC_EXT.2.2/VI The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in Appendix E of [MOD_VI_V1.0] and

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

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

6.2.2.16 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.

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

FDP_PDC_EXT.3.1/VI The TSF shall have interfaces for the *HDMI, 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: TD0942 applies to this SFR definition.

6.2.2.18 FDP_PDC_EXT.4 Supported Authentication Devices

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

6.2.2.19 FDP_PUD_EXT.1 Powering Unauthorized Devices

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

6.2.2.20 FDP_PWR_EXT.1 Powered by Computer

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

6.2.2.21 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.

6.2.2.22 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.

6.2.2.23 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.

6.2.2.24 FDP_RIP_EXT.2 Purge of Residual Information

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

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

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.

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

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

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

6.2.2.27 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*.

6.2.2.28 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* *except for the F1DN116KVM-UN-4*.

6.2.2.29 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.

6.2.2.30 FDP_TER_EXT.1 Session Termination

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

6.2.2.31 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.

6.2.2.32 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.

6.2.2.33 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.

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

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

6.2.2.35 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.

6.2.2.36 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.

6.2.3 Identification and Authentication

6.2.3.1 FIA_UAU.2 User Authentication Before Any Action

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

6.2.3.2 FIA_UID.2 User Identification Before Any Action

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

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of the functions **Configurable Device Filtration behavior** to the authorized administrator.

6.2.4.2 FMT_SMF.1 Specification of Management Functions

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

- **Reset to factory default,**

- **Create administrator account,**
- **Change password,**
- **Modify Configurable Device Filtration (CDF) list for authentication devices**.

6.2.4.3 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles administrators.

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

6.2.5 Protection of the TSF (FPT)

6.2.5.1 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*.

6.2.5.2 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; the configuration data, settings, and logging data that may be accessible by authorized administrators*.

6.2.5.3 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.

6.2.5.4 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.

6.2.5.5 FPT_STM.1 Reliable Time Stamps

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

6.2.5.6 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*.

6.2.5.7 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, auditory* indication of failure and by shutdown of normal TSF functions.

6.2.6 TOE Access (FTA)

6.2.6.1 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 14.

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 14 – Security Assurance Requirements

8 SECURITY REQUIREMENTS RATIONALE

8.1 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

Table 8 provides a mapping between the SFRs and Security Objectives.

8.2 DEPENDENCY RATIONALE

Table 15 identifies the Security Functional Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependencies	Rationale Statement
FAU_GEN.1	FPT_STM.1	Included
FDP_AFL_EXT.1	FDP_PDC_EXT.1	Included
FDP_APC_EXT.1/AO	None	N/A
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)	None	N/A
FDP_CDS_EXT.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/AO	FDP_PDC_EXT.1	Included
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_PUD_EXT.1	FDP_PDC_EXT.1	Included

SFR	Dependencies	Rationale Statement
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_RIP_EXT.2	None	N/A
FDP_SPR_EXT.1/DP	FDP_PDC_EXT.3	Included
FDP_SPR_EXT.1/HDMI	FDP_PDC_EXT.3	Included
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	N/A
FDP_UDF_EXT.1/AO	FDP_APC_EXT.1	Included
FDP_UDF_EXT.1/KM	FDP_APC_EXT.1	Included
FDP_UDF_EXT.1/VI	FDP_APC_EXT.1	Included
FIA_UAU.2	FIA_UID.1	Included
FIA_UID.2	None	N/A
FMT_MOF.1	FMT SMF.1 FMT_SMR.1	Included Included
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	Included
FPT_FLS_EXT.1	FPT_TST.1 FPT_PHP.3	Included Included - failure of anti-tamper function 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

SFR	Dependencies	Rationale Statement
FPT_STM.1	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 15 – 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:

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

9.1 SECURITY AUDIT

The TOE is equipped with non-volatile memory for the storage of audit records. There are three separate event logs. The critical One Time Programming (OTP) log and the critical Random Access Memory (RAM) log store the same types of critical events. The difference between the critical OTP log and the critical RAM log is what happens when the log is full which is described below.

- Critical OTP Log and Critical RAM Log
    - Self-test failure – a record of the latest self-test failure is recorded with error code information
    - Peripheral device rejection
    - Tampering events – there are six possible event flags
    - Configuration changes to the Configurable Device Filtration (CDF) whitelist/blacklist made by the administrator
    - Reset to factory default event
    - Changes to the primary administrator password
- Non-critical RAM Log
    - Power up
    - Peripheral device acceptance
    - Non-security related configuration changes
    - Administrator login
    - Administrator logout
    - Creation and removal of administrator accounts
    - Administrator password changes (other than for the primary administrator)
    - Password lock events

All events include the date and time. Where applicable, the username of the administrator who initiated the action is also recorded.

The logs cannot be deleted by the administrator, not even during reset to factory default. The critical RAM log and OTP log hold up to 64 events each. The non-critical RAM log holds up to 128 events. In both RAM log files, the oldest events are overwritten when the storage space allocated to the logs becomes full. The critical OTP log and its event records can not be deleted by the administrator. When the allocated storage space for the critical OTP log becomes full, the event records are not overwritten, and the critical OTP log never changes after being full. New critical events are logged in the critical RAM log.

Audit records can only be read by authorized administrators through the TOE device's terminal mode. Instructions for logging into the device and entering terminal mode are detailed in the Administrator Guide [Admin].

TOE Security Functional Requirements addressed: FAU_GEN.1.

9.2 USER DATA PROTECTION

9.2.1 System Controller

Each device includes a System Controller which is responsible for device management, user interaction, system control security functions, and device monitoring. The device receives user input from the buttons on the front panel or from the remote control. (Note: The F1DN116KVM-UN-4 does not work with a remote control.) This user input 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 main video controller that controls the relevant multiplexer.

The user determines the host computer to be connected to the peripherals by pressing a button on the TOE front panel or by selecting the computer 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.

When a remote control device is used, the LED on the front panel button and remote control's channel indicator corresponding to the selected computer are illuminated to indicate the current selected channel. These are always consistent.

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

9.2.1.1 Active PSD Connections

The TOE ensures that data flows only between the peripherals and the connected computer selected by the user. 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/AO, FDP_APC_EXT.1/KM, FDP_APC_EXT.1/UA, FDP_APC_EXT.1/VI.

9.2.1.2 Connected Computer Interfaces

The connected computers are attached to the TOE as follows:

- 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 or HDMI.
- The TOE audio-in is connected to the computer audio-out using a 1/8” stereo plug cable.
- 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.

There are no wireless interfaces or additional external interfaces.

TOE Security Functional Requirements addressed: FDP_PDC_EXT.1.

9.2.1.3 Residual Information Protection

The Letter of Volatility is included as Annex A.

A Restore to Factory Default (RFD) action may be initiated by an authorized administrator through the administration console, or by selecting **Left Ctrl | Left Ctrl | f11 | r** from the keyboard of the connected computer.

When the RFD command is issued, it initiates the following actions:

- All peripheral devices are logically disconnected from the selected computer
- The front panel LEDs blink together
- The TOE resets, purging the appropriate data
- The TOE performs a normal power up and self-test sequence

When the device completes the reboot, the peripherals will be connected to channel #1 and all default settings will be restored. The data in the OTP and RAM logs, and the primary administrator username and password data are maintained in the OTP Memory of the System Controller.

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

9.2.2 Keyboard and Mouse Functionality

9.2.2.1 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 (same as the keyboard host emulator) 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.

9.2.2.2 Keyboard and Mouse Switching Functionality

Figure 2 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.

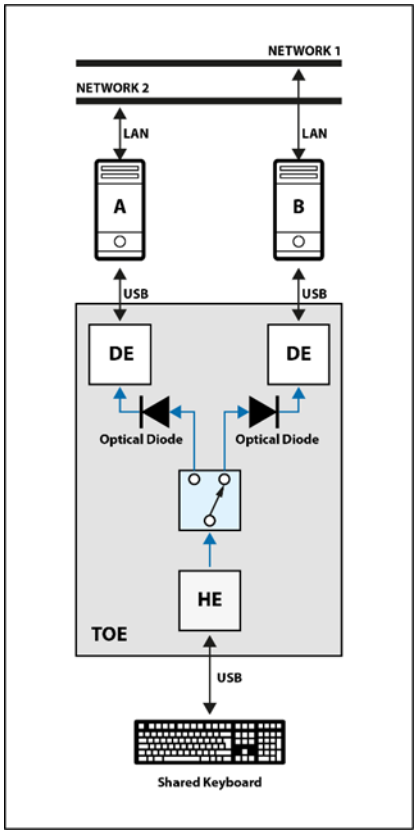


Figure 2 – SC Switching Diagram

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 and then to the port that is connected to the host computer. 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 (DEs) 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 TOE front panel, on the right hand side, as shown in Figure 7 in Section 9.5.

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

9.2.2.3 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 over Type A 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.

9.2.2.4 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. If the keyboard or mouse are not authorized, the lights will flicker or not illuminate.

TOE Security Functional Requirements addressed: FDP_RDR_EXT.1.

9.2.3 Video Switching Functionality

Video data flow is comprised of unidirectional Extended Display Identification Data (EDID) and video data flow paths. Figure 3 shows a data flow during the display EDID read function.

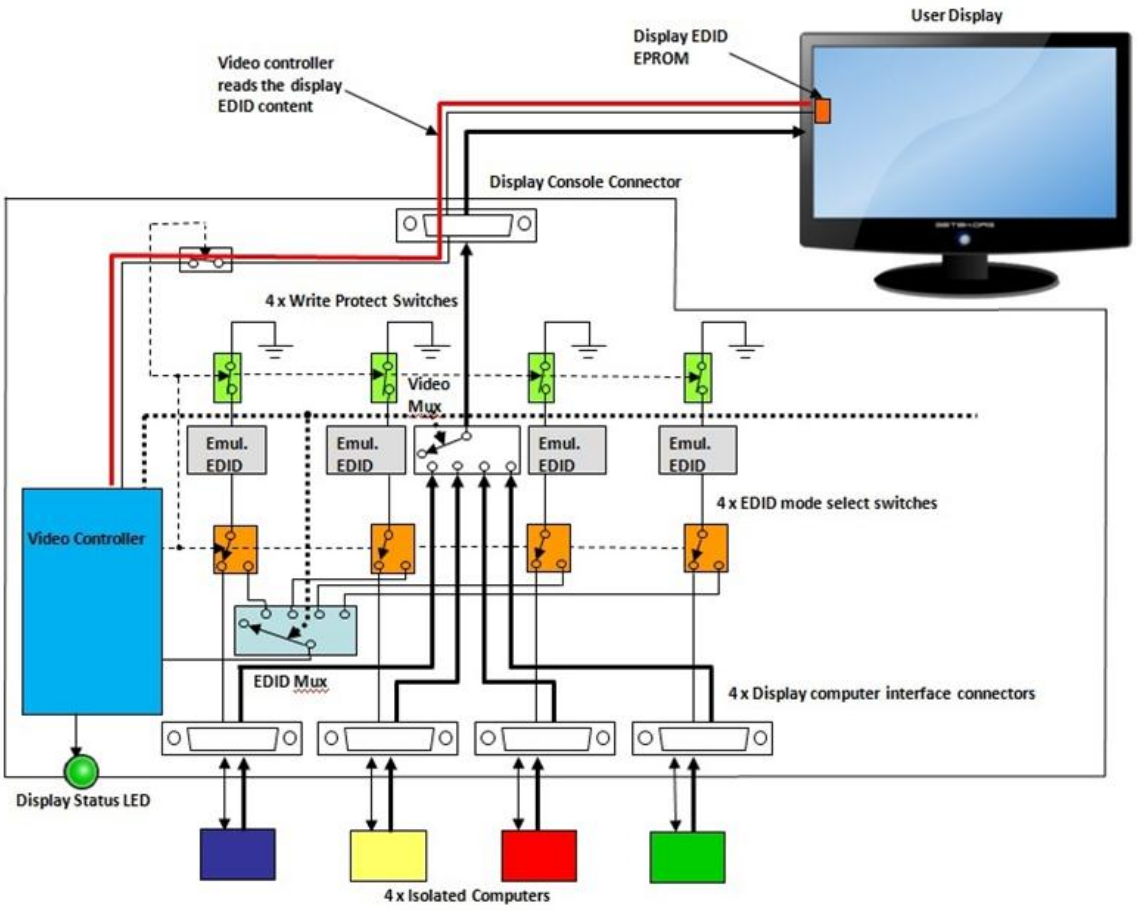


Figure 3 – Display EDID Read Function

For each display device, TOE reads the EDID only once as the TOE is powered up. The EDID content is read from the display device by the Main Video Controller to verify that it is valid and usable. If the EDID data is not valid, TOE operation will cease and wait for the display peripheral to be changed. To use the display port, a working display peripheral must be connected to the TOE and the TOE restarted.

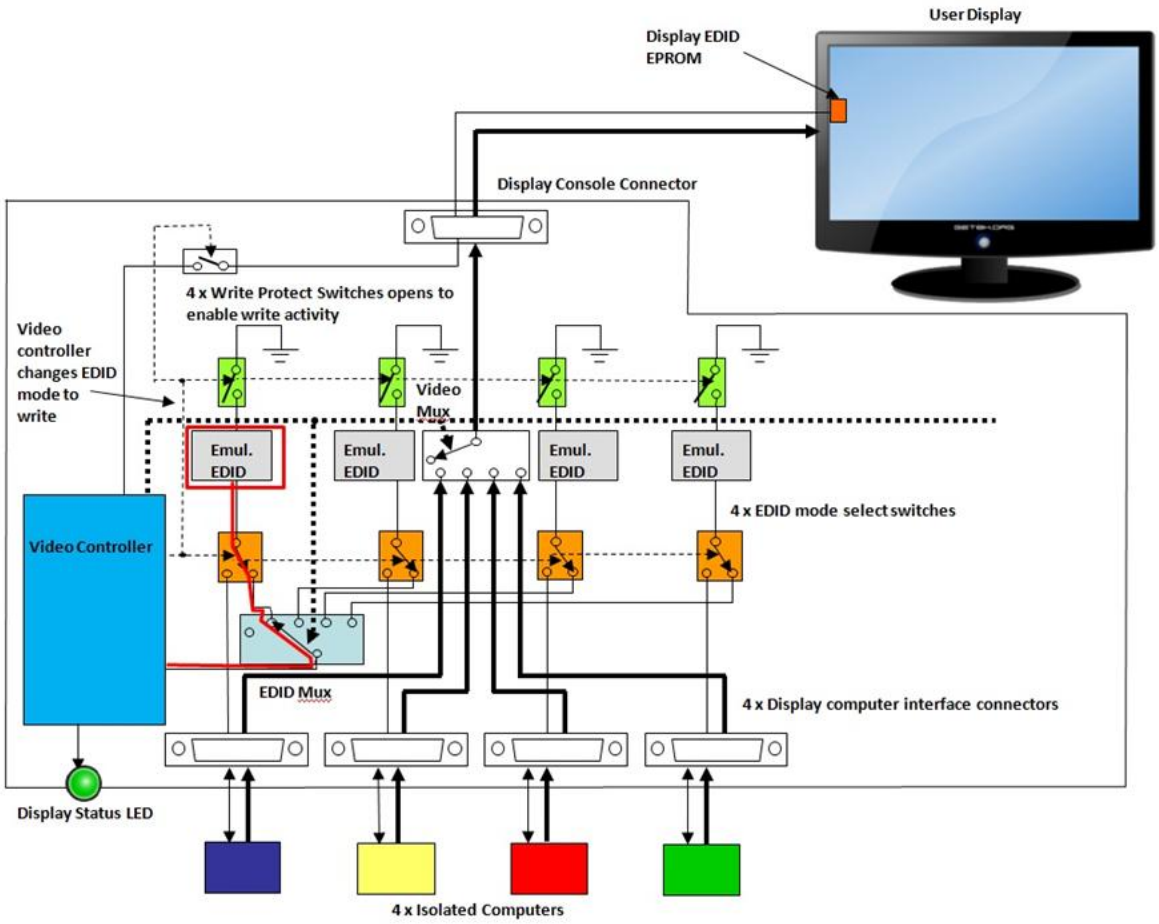


Figure 4 – Display EDID Write Function

Figure 4 illustrates the main video controller (shown in blue) as it writes the EDID content into the first channel emulated EDID Electrically Erasable Programmable Read-Only Memory (EEPROM) (shown in gray). Each emulated EDID EEPROM depicted in the figures is emulated by a separate, independent video channel controller. The thick lines in these figures 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 main video controller I2C lines to the first emulated EDID EEPROM (shown in gray). The write protect switch (shown in green) opens to enable writing. The main video controller uses the I2C lines to write to the first emulated EDID EEPROM. Once the write operation is complete and verified, the main video controller switches the EDID multiplexer to the next channel and the operation repeats until all video channel controllers are programmed. Once the write operation is complete, the main video controller switches to normal operating mode, as shown in Figure 5 below.

In EDID write mode, the Emulated EDID EEPROMs 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.

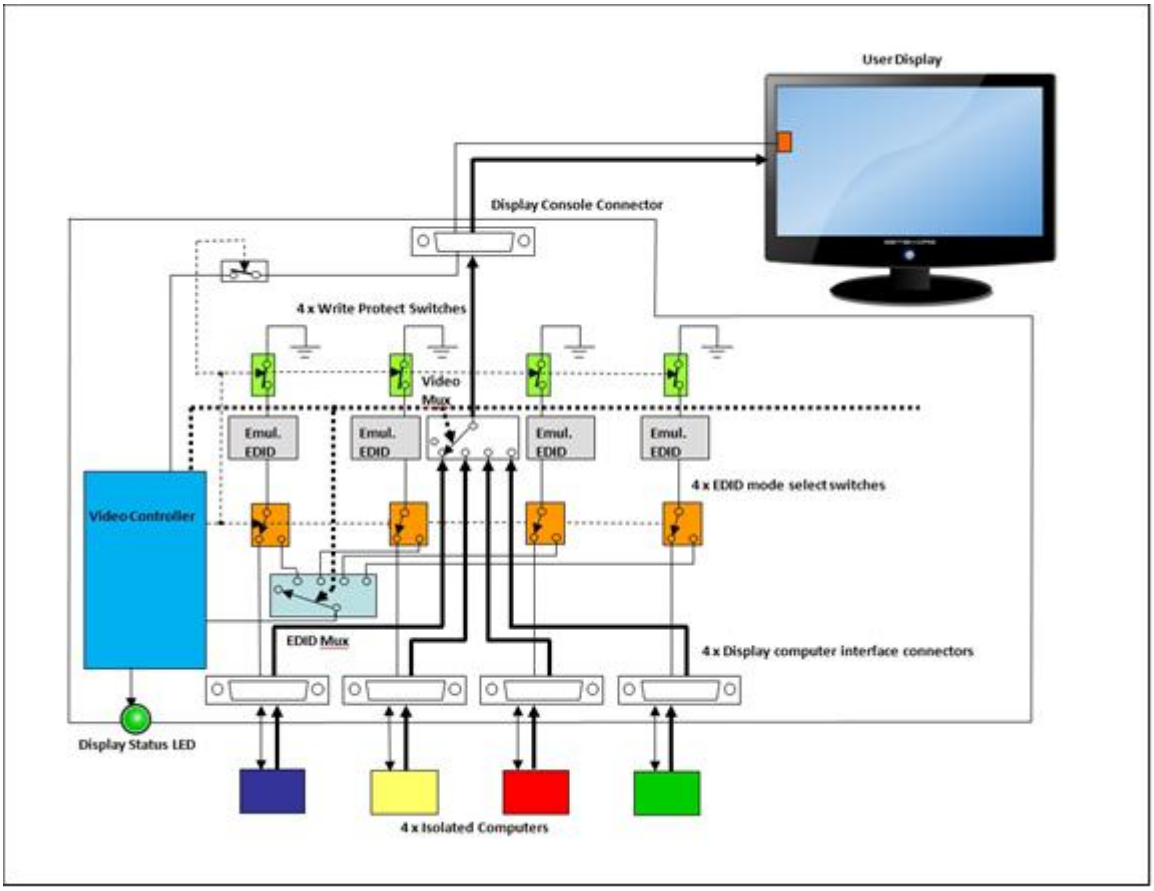


Figure 5 – Display Normal Mode

In normal mode, each computer interface operates independently. The power to each emulated EDID EEPROM (video channel controller) 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 by the main video controller.

During TOE normal operation (Figure 5), any attempt by a connected computer to affect the EDID channel is blocked by the architecture. Each computer is only able to reach 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 video channel controller (emulated EDID EEPROM) for each channel.

The EDID function is emulated by an independent video channel controller emulating an EDID EEPROM for each computer channel. Each emulated EDID EEPROM reads content obtained from the connected display once during first channel switch. 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, and HDMI 2. The TOE supports DisplayPort video input from the host. DisplayPort video input from the host is converted to HDMI, processed through the TOE as HDMI, and output as either DisplayPort (via an

HDMI to DP convertor) or HDMI video output. The TOE also supports HDMI video input from the host. HDMI video input is processed through the TOE and output as either DisplayPort (via an HDMI to DP convertor) or HDMI video 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.

For HDMI connections, EDID information is allowed to pass from the display to the computer, as described above. HPD information is also allowed to pass. Other protocols, including Audio Return Channel (ARC), EDID from the computer to the display, HDMI Ethernet and Audio Return Channel (HEAC), and HDMI Ethernet Channel (HEC) are blocked. 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. The video channel controllers emulating 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_SPR_EXT.1/HDMI, FDP_UDF_EXT.1/VI.

9.2.4 Video Compatible Device Types

The TOE accepts any DisplayPort or HDMI 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).

9.2.5 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.

An authorized administrator can configure the TOE to whitelist or blacklist particular device types for use on this port. The administrator must first log into the TOE administrative console. Using this interface, any USB 1.1, 2.0 or 3.0 compatible device can be whitelisted or blacklisted based on one or more of the following:

- USB Class
- USB Sub-class
- USB Protocol
- USB device ID
- USB Vendor ID
- USB Serial number

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 qualification microcontroller 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 qualification microcontroller 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 triggering of the anti-tampering function, 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.

9.2.5.1 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.

9.2.6 Audio Switching Functionality

The TOE audio data flow path is electrically isolated from all other functions and interfaces to prevent signaling data leakages to and from the audio paths.

Audio switching is controlled by the system controller function through dedicated unidirectional command lines. Audio signals cannot be digitized or otherwise sampled by any TOE circuitry. The TOE audio switching multiplexer uses a combination of mechanical relays and a solid-state multiplexer to ensure isolation. Unidirectional flow data diodes prevent audio data flow from an audio device to a selected computer. There is a separate audio interface for each computer. Each interface is electrically isolated from other interfaces, and from other TOE circuitry. These features ensure that the audio filtration specification requirements are met.

The TOE does not supply power to the analog audio output interface, and cannot be configured to do so. Therefore, it cannot be used to supply power to an unauthorized device on that interface.

When the TOE is powered off, an audio isolation relay is open, thereby isolating the audio input from the computer interfaces from all other circuitry and interfaces. Following triggering of the anti-tampering function, or following a failed self-test, the TOE will de-energize this audio isolation relay to isolate the audio inputs. The audio subsystem does not store, convert or delay audio data flows. Therefore, there is no risk of audio overflow when switching between channels.

The audio switching functionality features a separate channel selection control with an optional freeze function. This allows the audio port to stay connected to a specific computer while switching keyboard, video, mouse and authentication devices between other computers.

The use of analog microphone or line-in audio devices is strictly prohibited as indicated in the user guidance. The TOE will reject a microphone through the following two methods:

- There is an analog audio data diode that forces data to flow only from a computer to an audio peripheral device
- There is a microphone Direct Current (DC) bias barrier that blocks an electret microphone DC bias if the TOE is deliberately or inadvertently connected to the microphone input jack of a connected computer

TOE Security Functional Requirements addressed: FDP_AFL_EXT.1, FDP_PUD_EXT.1, FDP_UDF_EXT.1/AO.

9.2.6.1 Audio Compatible Device Types

The TOE accepts analog headphones or analog speakers connected via a 1/8” (3.5mm) audio jack at the audio peripheral port. The TOE does not support a wireless connection to an audio output device.

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

9.3 IDENTIFICATION AND AUTHENTICATION AND SECURITY MANAGEMENT

In order to access administrative functions, a user must be in possession of an administrator username and password. A single administrator role is supported by the TOE.

Administrators authenticate to the TOE by entering a username and password. The default administrator username is ‘admin1234’. The primary administrator account cannot be deleted. The password remains the same and does not revert to the default when an RFD is performed.

Up to nine additional administrator accounts may be created. These additional accounts and associated passwords are removed when an RFD is performed. For these accounts, usernames must be between 8 and 11 characters in length, and may be made up of uppercase and lowercase letters.

The default administrator password is ‘1234ABCDefg!@#’, and must be changed on the first login. Administrator passwords must be between 8 and 15 characters in length and may contain uppercase letters, lowercase letters, numbers or any of the following special characters: ‘!’, ‘@’, ‘#’, ‘$’, ‘%’, ‘^’, ‘&’, ‘*’, ‘(’, ‘)’, ‘-’, or ‘_’. The password must contain at least one uppercase letter, one lowercase letter, one number and one special character.

Passwords are stored in the non-volatile memory in a proprietary, obfuscated format.

Lost usernames or passwords cannot be recovered. The user is locked out after three (3) failed login attempts. The user may indefinitely cycle the device power and try again.

Once logged in, the administrator may use the functions described in the [Admin] to manage the TOE configuration. The administrator login and any configuration changes made are recorded in the audit logs along with the date and time of the event.

The administrator can use the administrator console function to perform the following tasks:

- Modify the CDF for authentication devices
- Manage administrator accounts (change password, create administrator account)
- Reset to factory defaults – note that this does not reset the username and password of the primary administrator, and does not reset the critical logs

TOE Security Functional Requirements addressed: FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_SMF.1, FMT_SMR.1.

9.4 PROTECTION OF THE TSF

9.4.1 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
- Authorized administrators use a connected computer to access configuration data and settings
- Authorized administrators use a connected computer to access TOE audit records

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.

9.4.2 Anti-tampering Functionality

The TOE provides passive physical tampering and active anti-tampering functionality.

9.4.2.1 Passive Detection of Physical Tampering

Passive anti-tampering is provided on the devices and on the remote control.

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 switch device 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. In addition, if a tamper evident label is removed, the word 'VOID' appears on both the label and the product surface.

TOE Security Functional Requirements addressed: FPT_PHP.1.

9.4.2.2 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. 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, this 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. If the remote control device is physically tampered with, it becomes permanently disabled. The TOE anti-tampering function is irreversible.

All anti-tampering events are recorded in TOE internal non-volatile memory with the time and date and may be read from the audit logs.

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

9.4.3 Reliable Timestamps

Each device includes a real-time clock powered by a battery. The time is set during production.

TOE Security Functional Requirements addressed: FPT_STM.1.

9.4.4 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 on all devices:

- 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 and the device makes a clicking sound to indicate the failure. The TOE disables the PSD switching functionality, and remains in a disabled state until the self-test is rerun and passes. All self-test failures are recorded in the log file, together with the date and time.

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

9.5 TOE ACCESS

The TOE user switches between computers by pressing the corresponding front panel button on the KVM device. The front panel button corresponding to the selected computer will illuminate; specifically, a lighted ring surrounding the button illuminates. There is also a light above the channel number to the left of each button that is the same color as the lighted ring around the button.

When a wired remote control is connected, the user can also switch between computers by selecting the corresponding device channel on the remote control for the desired KVM device. The user presses the up and down arrows at the right of the device to find the desired channel. When the desired channel has been identified, the user presses the select button (located between the up and down buttons).

When the user selects a channel using the remote control, the selected channel is highlighted on the screen, and a signal is sent from the wired remote control device to the KVM switch. The corresponding channel on the switch also illuminates and the TOE peripheral sharing device switches to the indicated channel.

Figure 6 shows the wired remote control device.



Figure 6 – Remote Control Channel Selection

On power up or power up following reset, all peripherals are connected to channel #1, the front panel push button LED for channel #1 will be illuminated, and channel #1 highlighted on the remote control screen.

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 corresponding to the selected computer will illuminate, and the selected channel on the remote control screen will be highlighted.

When switching between computers with authentication devices, the authentication device is switched accordingly. When switching to a computer that is not connected to an authentication device, the authentication device will remain mapped to the last channel that supported the connection. A user can select to 'Freeze USB' to a channel by performing a long press on the channel button to lock the authentication device to lock the authentication device to the currently connected computer. When the user switches the other peripherals to another channel, the authentication device will remain attached to the previously selected channel, and the 'Freeze USB' LED to the left of the channel selection button will be illuminated. The authentication device channel is indicated by an LED labeled DPP to the left of the channel. To release the freeze, the user performs a second long press on the channel button.

For devices that support audio output, there is a 'Freeze Audio' function. When the long press is performed, the audio remains connected to selected computer while the other peripherals are switched as indicated by the user. The audio channel is indicated by an audio LED to the left of the channel.

For devices that support both user authentication devices and audio output, these functions are put into 'Freeze USB' and 'Freeze Audio' mode together.

Figure 7 shows the selection buttons.



Figure 7 – Switch Channel Selection

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
AO	AO refers to the requirements for Analog Audio Devices.
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 16 – Terminology

10.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AC	Alternating Current
ARC	Audio Return Channel
CC	Common Criteria
CCID	Chip Card Interface Device
CDF	Configurable Device Filtration
CEC	Consumer Electronics Control
dB	decibel
DC	Direct Current
DE	Device Emulator
DP	DisplayPort
DPP	Dedicated Peripheral Port
EDID	Extended Display Identification Data
EEPROM	Electrically Erasable Programmable Read-Only Memory

Acronym	Definition
FET	Field-Effect Transistor
FPGA	Field Programmable Gate Array
fUSB	Freeze USB
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
HID	Human Interface Device
HPD	Hot-Plug Detection
I2C	Inter-Integrated Circuit
ID	Identification
IT	Information Technology
JTAG	Joint Test Action Group
kHZ	kilohertz
KVM	Keyboard, Video, Mouse
LED	Light Emitting Diode
MCCS	Monitor Control Command Set
mV	millivolt
NIAP	National Information Assurance Partnership
OTP	One Time Programming
PP	Protection Profile
PSD	Peripheral Sharing Device
RAM	Random Access Memory
RFD	Restore to Factory Default
ROM	Read Only Memory
SFR	Security Functional Requirement
SRAM	Static Random Access Memory

Acronym	Definition
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus
VID/PID	Vendor Identification/Product Identification

Table 17 – Acronyms

11 REFERENCES

Identifier	Title
[Admin]	Belkin SKVM/SKM Administration Guide, LNKPG-00666 Rev. A00
[Addenda]	CC and CEM addenda Exact Conformance, Selection-Based SFRs, Optional SFRs, 2021-Sep-30
[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
[CFG_PSD-AO-KM-UA-VI_V1.0]	PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, 19 July 2019
[MOD_AO_V1.0]	PP-Module for Analog Audio Output Devices, Version 1.0, 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
[PP_PSD_V4.0]	Protection Profile for Peripheral Sharing Device, Version: 4.0, 2019-07-19

Table 18 – References

ANNEX A – LETTER OF VOLATILITY

The table below provides volatility information and memory types for the Belkin PSD Switch with AO-KM-UA-VI and the remote control. User data is not retained in any TOE device when the power is turned off.

Product Models	Number in each product	Function, Manufacturer and Part Number	Storage Type	Size	Power Source (if not the TOE)	Volatility	Contains User Data	Effect of Restore Factory Default
All Models	1	System Controller, Host emulators: ST Microelectronics STM32F446ZCT6	Embedded SRAM[1]	128KB		Volatile	May contain user data	Data is purged
			Embedded Flash[2]	256KB		Non-Volatile	No user data Administrative passwords	Firmware and the primary administrator password are retained
			Backup SRAM[3]	4KB		Volatile	No user data	Data is purged
			OTP Memory	512bytes		Non-Volatile	Event logs are saved OR No user data	Data is not purged on RFD
	2P/4P/8P/16P/SH=1 2P/4P/8P/DH=2	Video Controller: Option #1 ST Microelectronics STM32F070RBT6	Embedded SRAM[1]	16KB		Volatile	May contain user data	Data is purged
			Embedded Flash[2]	128KB		Non-Volatile	No user data	Firmware is retained
		Video Controller: Option #2 ST Microelectronics STM32C071RBT6	Embedded SRAM[1]	24KB		Volatile	May contain user data	Data is purged
			Embedded Flash[2]	128KB		Non-Volatile	No user data	Firmware is retained

Product Models	Number in each product	Function, Manufacturer and Part Number	Storage Type	Size	Power Source (if not the TOE)	Volatility	Contains User Data	Effect of Restore Factory Default
	2P/SH=2 2P/DH=4 4P/SH=4 4P/DH=8 8P/SH=8 4P/DH=16 16P/SH=16	Video Channel Controller: Option#1 ST Microelectronics STM32F070CBT6	Embedded SRAM[1]	16KB		Volatile	May contain user data	Data is purged
			Embedded Flash[2]	128KB		Non-Volatile	No user data	Firmware is retained
		Video Channel Controller: Option#2 ST Microelectronics STM32C071CBT6	Embedded SRAM[1]	24KB		Volatile	May contain user data	Data is purged
			Embedded Flash[2]	128KB		Non-Volatile	No user data	Firmware is retained
		Device emulators: Option #1 ST Microelectronics STM32F070C6T6	Embedded SRAM[1]	6KB	Connected computer	Volatile	May contain user data	Data is purged
			Embedded Flash[2]	32KB		Non-Volatile	No user data	Firmware is retained
		Device emulators: Option #2 ST Microelectronics STM32C071C8T6	Embedded SRAM[1]	24KB	Connected computer	Volatile	May contain user data	Data is purged
			Embedded Flash[2]	64KB		Non-Volatile	No user data	Firmware is retained
Remote controls	1	System Controller, Host emulators: ST Microelectronics STM32F446ZCT6	Embedded SRAM[1]	128KB		Volatile	No user data	N/A
			Embedded Flash[2]	256KB		Non-Volatile	No user data	N/A
			Backup SRAM[3]	4KB		Volatile	No user data	N/A
			OTP Memory	512bytes		Non-Volatile	No user data	N/A

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.

[3] The Backup SRAM stores a key used in the implementation of the active anti-tamper mechanism. The Backup SRAM does not contain user data. The Backup SRAM is powered by a backup battery so it is functionally non-volatile because it retains memory when there is no main power, although the SRAM itself is volatile, requiring constant power.