# Belkin F1DN104KVM-UN-4, F1DN204KVM-UN-4, F1DN102KVM-UN-4, F1DN202KVM-UN-4, F1DN108KVM-UN-4, F1DN208KVM-UN-4, F1DN116KVM-UN-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices

## Security Target

*Doc No: 2149-001-D102B1*
*Version: 1.4B*
*19 February 2021*

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

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

# CONTENTS

# LIST OF TABLES



# LIST OF FIGURES

# 1 SECURITY TARGET INTRODUCTION

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

## 1.1 DOCUMENT ORGANIZATION

**Section 1, ST 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.

## 1.2 SECURITY TARGET REFERENCE

| | |
|---|---|
| **ST Title:** | Belkin F1DN104KVM-UN-4, F1DN204KVM-UN-4, F1DN102KVM-UN-4, F1DN202KVM-UN-4, F1DN108KVM-UN-4, F1DN208KVM-UN-4, F1DN116KVM-UN-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices Security Target |
| **ST Version:** | 1.4B |
| **ST Date:** | 19 February 2021 |

## 1.3 TOE REFERENCE

| | |
|---|---|
| **TOE Identification:** | Belkin F1DN104KVM-UN-4, F1DN204KVM-UN-4, F1DN102KVM-UN-4, F1DN202KVM-UN-4, F1DN108KVM-UN-4, F1DN208KVM-UN-4, 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

These 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 may be used with these devices.

### 1.4.1 Security Features

The Belkin Peripheral Sharing Devices allow users to share keyboard, video, mouse, audio and Universal Serial Bus (USB) authentication device peripherals between a number of connected computers. Security features ensure isolation between computers and peripherals to prevent data leakage between connected systems.

The following security features are provided by the Belkin Secure KVM Switches:

- 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

    - 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 and video input
- Keyboard and Mouse Security
    - The 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 by default
    - 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
- Hardware Anti-Tampering
    - Any attempt to open the product enclosure will activate an anti-tampering system, making the product inoperable and indicating tampering via blinking Light Emitting Diodes (LEDs)
    - Special holographic tampering evident labels on the product's enclosure provide a clear visual indication if the product has been opened or compromised

Belkin secure peripheral sharing devices use multiple isolated microcontrollers (one microcontroller per connected computer) to emulate connected peripherals in order to prevent display signaling, keyboard signaling, and power signaling attacks.

Figure 1 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. That unidirectional serial data is passed through the switch that is used to select between Computer A and Computer B. Isolated Device Emulators (DE) are connected to the data switch on one side and to the

respective computers on the other side. Each key stroke is converted by the selected DE into a bi-directional stream to communicate with the computer.

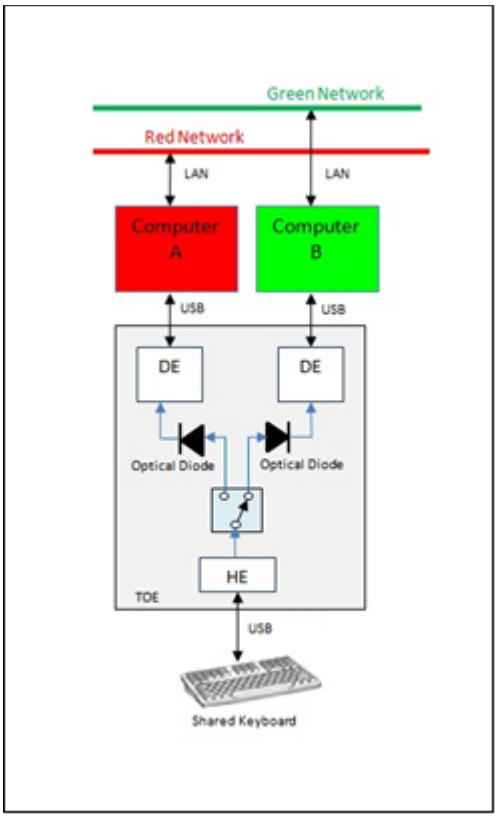



**Figure 1 – Simplified Switching Diagram**

The TOE is a combined software and hardware TOE. A mapping showing the applicable SFRs for each device is included in Annex B.

## 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[1] |
| Mouse | General purpose USB mouse |
| Audio output device | Analog audio output device (speakers or headphones) |

[1] A General purpose keyboard is used with the F1DN116KVM-UN-4 device only.

| Component | Description |
|---|---|
| User authentication device | Standard USB smartcard reader/authentication device |
| User display | Standard computer display (HDMI 2.0, or DisplayPort 1.1, 1.2 or 1.3) |
| Belkin KVM Cables | USB Type-A to USB Type-B (keyboard and mouse)<br>Video cable (DisplayPort and HDMI)<br>3.5mm stereo cable (Audio cable)<br>USB Type-A to USB Type-B (authentication device) |

**Table 1 – Non-TOE Hardware and Software**

# 1.5 TOE DESCRIPTION

## 1.5.1 Evaluated Configuration

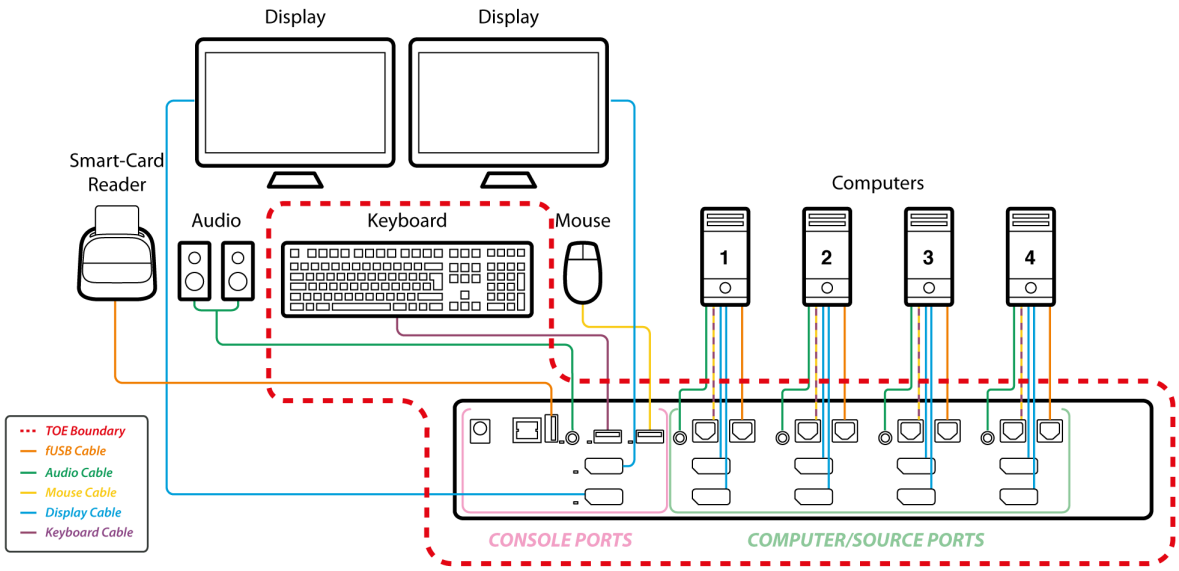



**Figure 2 – Primary KVM Switch Evaluated Configuration**

Figure 2 shows a basic evaluated configuration for the F1DN104KVM-UN-4, F1DN204KVM-UN-4, F1DN102KVM-UN-4, F1DN202KVM-UN-4, F1DN108KVM-UN-4, and F1DN208KVM-UN-4 models. In the evaluated configuration, the TOE is connected to two, four, or eight computers. The video input is DisplayPort 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. The Belkin Secure KVM USB Keyboard remote control is used with 2, 4 and 8 port devices in the evaluated configuration.

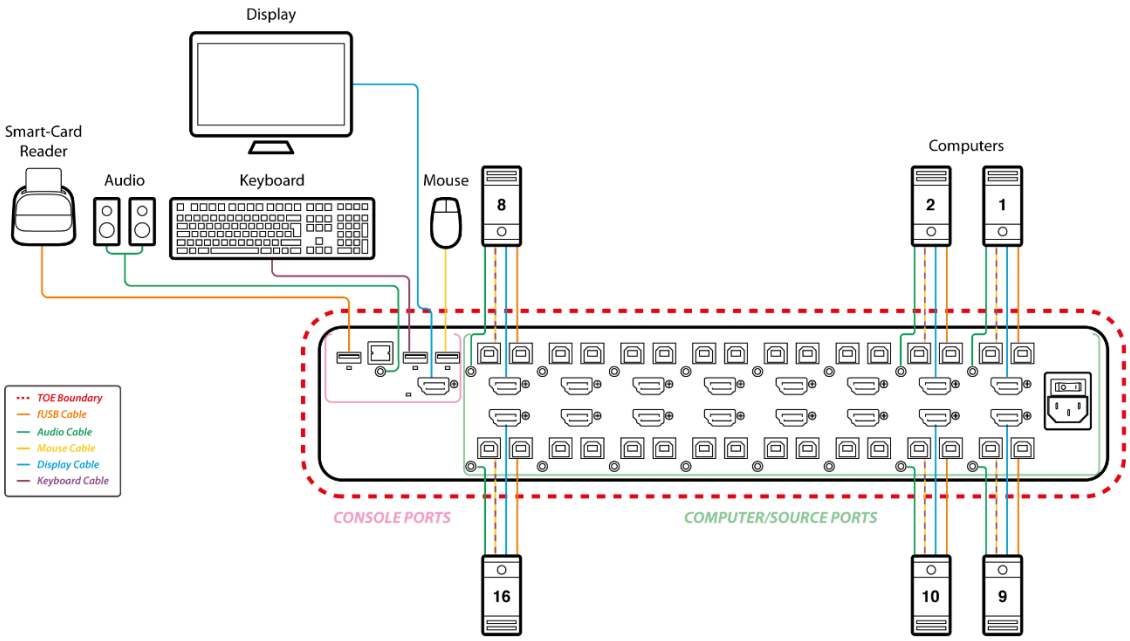



**Figure 3 – Secondary KVM Switch Evaluated Configuration**

Figure 3 shows the basic evaluated configuration for the F1DN116KVM-UN-4. A general purpose keyboard is used with the F1DN116KVM-UN-4 device. The video input is DisplayPort or HDMI, and one display is connected. The peripheral sharing device is connected to speakers or headphones, and to a user authentication device.

### 1.5.2 Physical Scope

The TOE consists of the devices shown in Table 2 and Table 3.

| Family | Family Description | Part Number | Model | Active Anti-tampering | Tamper Evident labels | User Authentication and audit logging | Analog Audio | Video in | Video out | Number of supported displays | KM | Authentication Device Peripheral (DPP) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| El Capitan KVM Devices | KVM devices with Active Anti-tampering, Analog Audio, user authentication devices (Dedicated Peripheral Port (DPP)), user authentication and audit logging, and support for remote control. | CGA18322 | F1DN104KVM-UN-4 | Yes | Yes | Yes | Yes | DP\HDMI | DP\HDMI | 1 | Yes | Yes |
| | | CGA18329 | F1DN204KVM-UN-4 | Yes | Yes | Yes | Yes | DP\HDMI | DP\HDMI | 2 | Yes | Yes |
| | | CGA18316 | F1DN102KVM-UN-4 | Yes | Yes | Yes | Yes | DP\HDMI | DP\HDMI | 1 | Yes | Yes |
| | | CGA18326 | F1DN202KVM-UN-4 | Yes | Yes | Yes | Yes | DP\HDMI | DP\HDMI | 2 | Yes | Yes |
| | | CGA18359 | F1DN108KVM-UN-4 | Yes | Yes | Yes | Yes | DP\HDMI | DP\HDMI | 1 | Yes | Yes |
| | | CGA18360 | F1DN208KVM-UN-4 | Yes | Yes | Yes | Yes | DP\HDMI | DP\HDMI | 2 | Yes | Yes |
| | | CGA18984 | F1DN116KVM-UN-4 | Yes | Yes | Yes | Yes | DP\HDMI | DP\HDMI | 1 | Yes | Yes |

**Table 2 – TOE Peripheral Sharing Devices and Features**

| Description | Part Number | Model |
|---|---|---|
| Belkin 2-4-8 Port Secure KVM USB Keyboard W/Lighting | CGA20166 | F1DN008KBD |

**Table 3 – Remote Control Device (Keyboard)**

#### 1.5.2.1 TOE Delivery

The TOE, together with its corresponding cables are delivered to the customer via a trusted carrier, such as Fed-Ex, that provides a tracking service for all shipments.

#### 1.5.2.2 TOE Guidance

The TOE includes the following guidance documentation:

- Quick Installation Guide 2/4 Port Secure Single/Dual-Head DP/HDMI-DP/HDMI KVM Switches, 8820-02951 Rev.A00
- Quick Installation Guide 8/16 Port Secure Single/Dual-Head DP/HDMI-DP/HDMI KVM Switches, 8820-02952 Rev. A00
- Belkin SKVM/SKM Administration Guide, LNKPG-00666 Rev. B00
- Belkin F1DN104KVM-UN-4, F1DN204KVM-UN-4, F1DN102KVM-UN-4, F1DN202KVM-UN-4, F1DN108KVM-UN-4, F1DN208KVM-UN-4, F1DN116KVM-UN-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices Common Criteria Guidance Supplement, Version 1.2
- Quick Installation Guide 2/4/8 Port SKVM USB Keyboard with Lighting, 8820-02953 Rev.B00
- Belkin Regulatory Information, 8820-02969 Rev. A00

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

### 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 capabilities for keyboard and mouse, display, authentication device, and audio output. The TOE ensures that only authorized peripheral devices may be used. |
| 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. |

| Functional Classes | Description |
|---|---|
| Protection of the TSF[2] | 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] TOE Security Functionality

# 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 has been taken into account.

## 2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST claims exact conformance to the National Information Assurance Partnership (NIAP) 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], which references the Protection Profile for Peripheral Sharing Device Version 4.0 [PP_PSD_V4.0], and the modules listed in Section 2.4. 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.

| Technical Decision | PP or Module |
|---|---|
| TD0506 | [MOD_VI_V1.0] |
| TD0507 | [MOD_KM_V1.0] |
| TD0514 | [MOD_VI_V1.0] |
| TD0518 | [PP_PSD_V4.0] |
| TD0539 | [MOD_VI_V1.0] |

| Technical Decision | PP or Module |
|---|---|
| TD0557 | [MOD_AO_V1.0] |

**Table 5 – Applicable Technical Decisions**

## 2.3 PACKAGE CLAIM

This Security Target does not claim conformance with any package.

## 2.4 MODULE CLAIM

The following PP-Modules are specified in a PP-Configuration with this PP:

- PP-Module for Analog Audio Output Devices, Version 1.0
- PP-Module for User Authentication Devices, Version 1.0
- PP-Module for Keyboard/Mouse Devices, Version 1.0
- PP-Module for Video/Display Devices, Version 1.0

## 2.5 CONFORMANCE RATIONALE

The TOE Keyboard, Video, Mouse (KVM) switches are inherently consistent with the Compliant Targets of Evaluation described in the [PP_PSD_V4.0] and in the PP modules listed in Section 2.4, 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 2.4.

# 3 SECURITY PROBLEM DEFINITION

## 3.1 THREATS

Table 6 lists the threats described in Section 3.1 of the [PP_PSD_V4.0] and in the modules listed in Section 2.4. 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 between one or more computers may allow unauthorized data flow through the PSD or its connected peripherals. |
| **T.SIGNAL_LEAK** | A connection via the PSD between one or more computers may allow unauthorized data flow through bit-by-bit signaling. |
| **T.RESIDUAL_LEAK** | A PSD may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer. |
| **T.UNINTENDED_USE** | A PSD may connect the user to a computer other than the one to which the user intended to connect. |
| **T.UNAUTHORIZED_DEVICES** | The use of an unauthorized peripheral device with a specific PSD peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSD or its connected computers. |
| **T.LOGICAL_TAMPER** | An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code or data stored in the PSD's volatile or non-volatile memory to allow unauthorized information flows. |
| **T.PHYSICAL_TAMPER** | A malicious user or human agent could physically modify the PSD to allow unauthorized information flows. |
| **T.REPLACEMENT** | A malicious human agent could replace the PSD during shipping, storage, or use with an alternate device that does not enforce the PSD security policies. |
| **T.FAILED** | Detectable failure of a PSD may cause an unauthorized information flow or weakening of PSD security functions. |

| Threat | Description |
|---|---|
| **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.

| Assumptions | Description |
|---|---|
| **A.NO_TEMPEST** | Computers and peripheral devices connected to the PSD are not TEMPEST approved.<br>The TSF may or may not isolate the ground of the keyboard and mouse computer interfaces (the USB ground). The Operational Environment is assumed not to support TEMPEST red-black ground isolation. |
| **A.PHYSICAL** | The environment provides physical security commensurate with the value of the TOE and the data it processes and contains. |
| **A.NO_WIRELESS_DEVICES** | The environment includes no wireless peripheral devices. |
| **A.TRUSTED_ADMIN** | PSD Administrators 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. |

| Assumptions | Description |
|---|---|
| **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<br>_INTERFACE<br>_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.<br>Addressed by:<br><table><tr><td>PP_PSD</td><td>FDP_APC_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_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><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></table></td></tr>
<tr><td>O.COMPUTER<br>_INTERFACE<br>_ISOLATION<br>_TOE_UNPOWERED</td><td>The PSD shall not allow data to transit a PSD-Computer interface while the PSD is unpowered.<br>Addressed by:<br><table><tr><td>PP_PSD</td><td>FDP_APC_EXT.1</td></tr></table></td></tr>
</table>

| Security Objective | Description |
|---|---|
| | MOD_AO: FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1<br>MOD_UA: FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2<br>MOD_VI: FDP_APC_EXT.1/VI, FDP_PDC_EXT.1<br>MOD_KM: FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1, FDP_SWI_EXT.3 |
| **O.USER_DATA_ISOLATION** | The PSD shall route user data, such as keyboard entries, only to the computer selected by the user. The PSD shall provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.<br>Addressed by:<br>PP_PSD: FDP_APC_EXT.1<br>MOD_AO: FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1<br>MOD_UA: FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2<br>MOD_VI: FDP_APC_EXT.1/VI, FDP_PDC_EXT.1<br>MOD_KM: FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1, FDP_SWI_EXT.3 |
| **O.NO_USER_DATA_RETENTION** | The PSD shall not retain user data in non-volatile memory after power up or, if supported, factory reset.<br>Addressed by:<br>PP_PSD: FDP_RIP_EXT.1, FDP_RIP_EXT.2<br>MOD_KM: FDP_RIP.1/KM |
| **O.NO_OTHER_EXTERNAL_INTERFACES** | The PSD shall not have any external interfaces other than those implemented by the TSF.<br>Addressed by: |

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td></td><td><table><tr><td>PP_PSD</td><td>FDP_PDC_EXT.1</td></tr></table></td></tr>
<tr><td>O.LEAK<br>_PREVENTION<br>_SWITCHING</td><td>The PSD shall ensure that there are no switching mechanisms that allow signal data leakage between connected computers.<br>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<br>_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.<br>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.<br>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_UA</td><td>FDP_FIL_EXT.1/UA</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></table></td></tr>
<tr><td>O.PERIPHERAL<br>_PORTS_ISOLATION</td><td>The PSD shall ensure that data does not flow between peripheral devices connected to different PSD interfaces.<br>Addressed by:<table><tr><td>PP_PSD</td><td>FDP_APC_EXT.1</td></tr></table></td></tr>
</table>

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td></td><td><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_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>
<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>
</table></td></tr>
<tr><td>O.REJECT _UNAUTHORIZED _PERIPHERAL</td><td>The PSD shall reject unauthorized peripheral device types and protocols.<br>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_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>
<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>
</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.<br>Addressed by:<table>
<tr><td>PP_PSD</td><td>FDP_PDC_EXT.1</td></tr>
<tr><td>MOD_UA</td><td>FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2</td></tr>
</table></td></tr>
</table>

| Security Objective | Description |
|---|---|
| | MOD_KM: FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1, FDP_SWI_EXT.3 |
| **O.NO_TOE_ACCESS** | The PSD firmware, software, and memory shall not be accessible via its external ports.<br>Addressed by:<br>PP_PSD: FPT_NTA_EXT.1 |
| **O.TAMPER_EVIDENT_LABEL** | 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.<br>Addressed by:<br>PP_PSD: FPT_PHP.1 |
| **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.<br>Addressed by:<br>PP_PSD: FPT_PHP.1, FPT_PHP.3 |
| **O.SELF_TEST** | The PSD shall perform self-tests following power up or powered reset.<br>Addressed by:<br>PP_PSD: FPT_TST.1 |
| **O.SELF_TEST_FAIL_TOE_DISABLE** | The PSD shall enter a secure state upon detection of a critical failure.<br>Addressed by:<br>PP_PSD: FPT_FLS_EXT.1, FPT_TST_EXT.1 |

| Security Objective | Description |
|---|---|
| **O.SELF_TEST _FAIL_INDICATION** | The PSD shall provide clear and visible user indications in the case of a self-test failure.<br>Addressed by:<br>PP_PSD: FPT_TST_EXT.1 |
| **O.USER _AUTHENTICATION _ISOLATION** | The TOE shall isolate the user authentication function from all other TOE functions.<br>Addressed by:<br>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.<br>Addressed by:<br>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.<br>Addressed by:<br>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.<br>Addressed by:<br>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.<br>Addressed by:<br>MOD_AO: FDP_APC_EXT.1, FDP_AFL_EXT.1, FDP_UDF_EXT.1/AO |

| Security Objective | Description |
|---|---|
| **O.COMPUTER_TO_AUDIO_ISOLATION** | The PSD shall isolate the analog audio output function from all other TOE functions.<br>Addressed by:<br>MOD_AO: FDP_APC_EXT.1, FDP_UDF_EXT.1/AO |
| **O.EMULATED_INPUT** | The TOE shall emulate the keyboard and/or mouse functions from the TOE to the connected computer.<br>Addressed by:<br>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.<br>Addressed by:<br>MOD_KM: FDP_UDF_EXT.1/KM |

**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. |

| Security Objective | Description |
|---|---|
| **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. |
| | 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.UNIDIRECTIONAL_INPUT | The TOE's enforcement of unidirectional input for keyboard/mouse data prevents leakage of computer data through a connected peripheral interface. |

| Threat or Assumption | Security Objective(s) | Rationale |
|---|---|---|
| | O.USER_AUTHENTICATION_ISOLATION | The TOE's user authentication function mitigates this threat by ensuring that the bidirectional channel between the device and the connected computer through the user authentication function is isolated from all other TOE functions. |
| | O.SESSION_TERMINATION | The TOE mitigates the threat by ensuring that open sessions are terminated and no traffic flows upon disconnection of the authentication element. |
| | O.PERIPHERAL_PORTS_ISOLATION | Isolation of peripheral ports prevents data from leaking between them without authorization. |
| | O.PROTECTED_EDID | The TOE's protection of the EDID interface prevents its use as a vector for unauthorized data leakage via this channel. |
| | O.UNIDIRECTIONAL_VIDEO | The TOE's enforcement of unidirectional output for video data protects against data leakage via connected computers by ensuring that no video data can be input to a connected computer through this interface. |
| T.SIGNAL_LEAK | O.COMPUTER_INTERFACE_ISOLATION | Isolation of computer interfaces prevents data leakage through bit-wise signaling because there is no mechanism by which the signal data can be communicated. |
| | O.NO_OTHER_EXTERNAL_INTERFACES | The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked through bitwise signaling. |
| | O.LEAK_PREVENTION_SWITCHING | The TOE's use of switching methods that are not susceptible to signal leakage helps mitigate the signal leak threat. |

| Threat or Assumption | Security Objective(s) | Rationale |
|---|---|---|
| | 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. |
| | 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 |

| Threat or Assumption | Security Objective(s) | Rationale |
|---|---|---|
| | | 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. |
| | 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. |

| Threat or Assumption | Security Objective(s) | Rationale |
|---|---|---|
| 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. |
| 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. |

| Threat or Assumption | Security Objective(s) | Rationale |
|---|---|---|
| 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. |
| 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 | OE.PHYSICAL | If the TOE's operational environment provides physical security, then the assumption is satisfied. |

| Threat or Assumption | Security Objective(s) | Rationale |
|---|---|---|
| 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**

# 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 analog audio output devices [MOD_AO_V1.0], user authentication devices [MOD_UA_V1.0], keyboard/mouse devices [MOD_KM_V1.0], and display devices [MOD_VI_1.0]. It is repeated here to ensure the completeness of this ST.

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

| Functional Class | Functional Families |
|---|---|
| User Data Protection (FDP) | FDP_AFL_EXT Audio Filtration |
| | FDP_APC_EXT Active PSD Connections |
| | FDP_CDS_EXT Connected Displays Supported |
| | FDP_FIL_EXT Device Filtering |
| | FDP_IPC_EXT Internal Protocol Conversion |
| | FDP_PDC_EXT Peripheral Device Connection |
| | FDP_PUD_EXT Powering Unauthorized Devices |
| | FDP_PWR_EXT Powered By Computer |
| | FDP_RDR_EXT Re-Enumeration Device Rejection |
| | FDP_RIP_EXT Residual Information Protection |
| | FDP_SPR_EXT Sub-Protocol Rules |
| | FDP_SWI_EXT PSD Switching |
| | FDP_TER_EXT Session Termination |
| | FDP_UAI_EXT User Authentication Isolation |
| | FDP_UDF_EXT Unidirectional Data Flow |
| Protection of the TSF (FPT) | FPT_FLS_EXT Failure with Preservation of Secure State |
| | FPT_NTA_EXT No Access to TOE |
| | FPT_TST_EXT TSF Testing |

| Functional Class | Functional Families |
|---|---|
| TOE Access (FTA) | FTA_CIN_EXT Continuous Indications |

**Table 11 – Functional Families of Extended Components**

# 5.1 CLASS FDP: USER DATA PROTECTION

## 5.1.1 FDP_AFL_EXT Audio Filtration

**Family Behavior**

Components in this family define the requirements for device filtering.

**Component Leveling**


FDP_AFL_EXT.1 Audio Filtration, requires the TSF to enforce outgoing audio filtration levels.

**Management: FDP_AFL_EXT.1**

No specific management functions are identified.

**Audit: FDP_AFL_EXT.1**

No specific audit functions are defined.

**FDP_AFL_EXT.1 Device Filtering**

Hierarchical to: No other components.

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

**FDP_AFL_EXT.1.1** The TSF shall ensure outgoing audio signals are filtered as per [*assignment: document reference to the table below*].

| 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 |

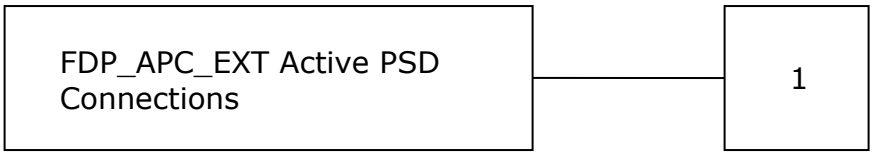
| Frequency (kHz) | Minimum Attenuation (dB) | Maximum Voltage After Attenuation |
|---|---|---|
| 19 | 43.0 | 14.15 mV |
| 20 | 46.0 | 10.02 mV |
| 30 | 71.4 | 0.53 mV |
| 40 | 71.4 | 0.53 mV |
| 50 | 71.4 | 0.53 mV |
| 60 | 71.4 | 0.53 mV |

### 5.1.2 FDP_APC_EXT Active PSD Connections

**Family Behavior**

Components in this family define the requirements for when an external interface to the TOE is authorized to transmit data related to peripheral sharing.

**Component Leveling**




FDP_APC_EXT.1 Active PSD Connections, restricts the flow of data through the TSF.

**Management: FDP_APC_EXT.1**

No specific management functions are identified.

**Audit: FDP_APC_EXT.1**

There are no auditable events foreseen.

**FDP_APC_EXT.1 Active PSD Connections**

Hierarchical to: No other components.

Dependencies: No dependencies

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

**FDP_APC_EXT.1.2** The TSF shall ensure that no data flows between connected computers whether the TOE is powered on or powered off.

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

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

## 5.1.3 FDP_CDS_EXT Connected Displays Supported

**Family Behavior**

Components in this family define requirements for the number of display interfaces contained within the TOE.

**Component Leveling**


FDP_CDS_EXT.1, Connected Displays Supported, requires the TSF to define whether it supports one connected display at a time or multiple connected displays simultaneously.

**Management: FDP_CDS_EXT.1**

There are no specific management functions identified.

**Audit: FDP_CDS_EXT.1**

There are no auditable events foreseen.

**FDP_CDS_EXT.1 Connected Displays Supported**

Hierarchical to: No other components

Dependencies: No other components

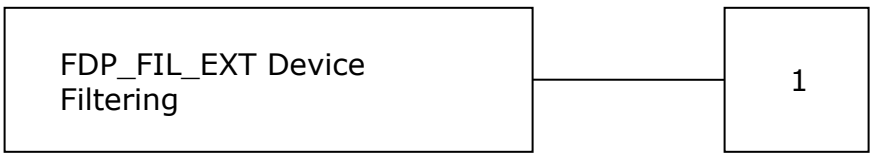
**FDP_CDS_EXT.1.1** The TSF shall support [*selection: one connected display, multiple connected displays*] at a time.

## 5.1.4 FDP_FIL_EXT Device Filtering

**Family Behavior**

Components in this family define the requirements for device filtering.

**Component Leveling**




FDP_FIL_EXT.1 Device Filtering, requires the TSF to specify the method of device filtering used for peripheral interfaces and defines requirements for handling whitelists and blacklists.

**Management: FDP_FIL_EXT.1**

The following actions could be considered for the management functions in FMT:

- Ability to configure whitelist/blacklist members

**Audit: FDP_FIL_EXT.1**

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Configuration of whitelist/blacklist members

**FDP_FIL_EXT.1 Device Filtering**

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | FDP_PDC_EXT.1 Peripheral Device Connection |
| **FDP_FIL_EXT.1.1** | The TSF shall have [*selection: configurable, fixed*] device filtering for [*assignment: list of supported peripheral interface types*] interfaces. |
| **FDP_FIL_EXT.1.2** | The TSF shall consider all [*assignment: blacklist name*] blacklisted devices as unauthorized devices for [*assignment: list of supported peripheral interface types*] interfaces in peripheral device connections. |
| **FDP_FIL_EXT.1.3** | The TSF shall consider all [*assignment: whitelist name*] whitelisted devices as authorized devices for peripheral device connections only if they are not on the [*assignment: blacklist name*] blacklist or otherwise unauthorized. |

### 5.1.5 FDP_IPC_EXT Internal Protocol Conversion

**Family Behavior**

Components in this family define requirements for the TOE's ability to convert one protocol into another for internal processing.

**Component Leveling**


FDP_IPC_EXT.1, Internal Protocol Conversion, requires the TSF to specify an input protocol that the TOE receives, the protocol that the TSF converts it to, and whether the data is output from the TOE as the original protocol or as the converted one.

**Management: FDP_IPC_EXT.1**

There are no specific management functions identified.

**Audit: FDP_IPC_EXT.1**

There are no auditable events foreseen.

**FDP_IPC_EXT.1 Internal Protocol Conversion**

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | FDP_PDC_EXT.2 Authorized Connection Protocols |
| **FDP_IPC_EXT.1.1** | The TSF shall convert the [*assignment: original protocol*] protocol at the [*assignment: TOE external interface(s)*] into the [*assignment: converted protocol*] protocol within the TOE. |
| **FDP_IPC_EXT.1.2** | The TSF shall output the [*assignment: converted protocol*] protocol from inside the TOE to [*assignment: TOE external interface(s)*] as [*selection: [assignment: original protocol] protocol], [assignment: converted protocol] protocol*]. |

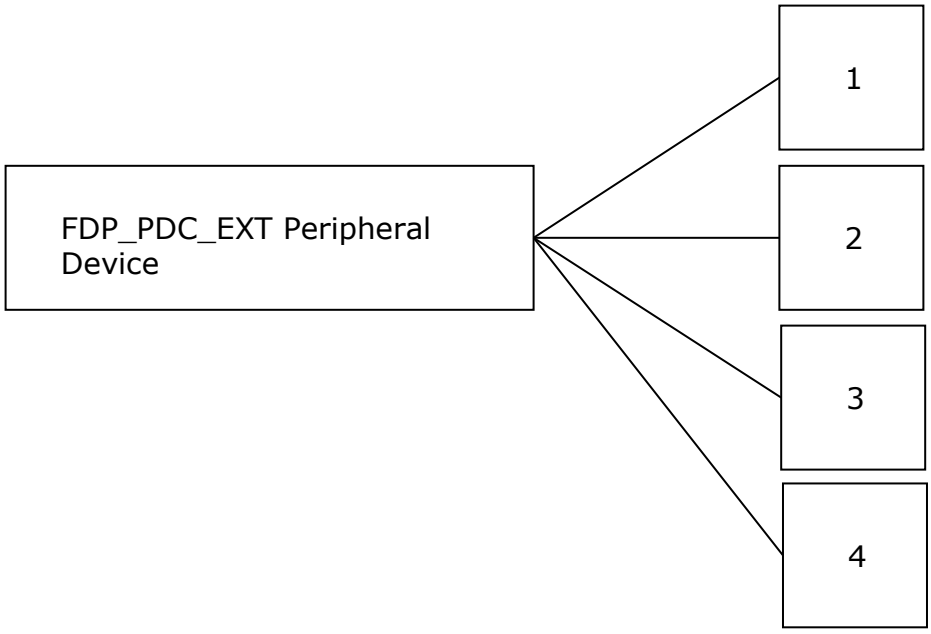
## 5.1.6 FDP_PDC_EXT Peripheral Device Connection

**Family Behavior**

Components in this family define the requirements for peripheral device connections.

This family is defined in the PSD PP. PP-Module [MOD_UA_V1.0] augments the extended family by adding two additional components, FDP_PDC_EXT.2 and FDP_PDC_EXT.4. PP-Modules [MOD_KM_V1.0] and [MOD_VI_V1.0] augment the extended family by adding two additional components, FDP_PDC_EXT.2 and FDP_PDC_EXT.3. The new components and their impact on the extended family's component leveling are shown below; reference the PSD PP for all other definitions for this family.

**Component Leveling**




FDP_PDC_EXT.1 Peripheral Device Connection, requires the TSF to limit external connections to only authorized devices.

FDP_PDC_EXT.2 Authorized Devices, defines the types of physical devices that the TSF will permit to connect to it.

FDP_PDC_EXT.3, Authorized Connection Protocols, defines the protocols that the TSF will authorize over its physical/logical interfaces, as well as any rules that are applicable to these interfaces.

FDP_PDC_EXT.4 Supported Authentication Devices, defines whether the TSF includes an internal or external authentication device.

**Management: FDP_PDC_EXT.1, FDP_PDC_EXT.2, FDP_PDC_EXT.3, FDP_PDC_EXT.4**

No specific management functions are identified.

**Audit: FDP_PDC_EXT.1**

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Acceptance or rejection of a peripheral

**Audit: FDP_PDC_EXT.2, FDP_PDC_EXT.3, FDP_PDC_EXT.4**

There are no specific auditable events foreseen.

### FDP_PDC_EXT.1 Peripheral Device Connection

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies |
| **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. |

### FDP_PDC_EXT.2 Authorized Devices

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FDP_PDC_EXT.1 Peripheral Device Connection |
| **FDP_PDC_EXT.2.1** | The TSF shall allow connections with authorized devices as defined in [*assignment: devices specified in the PP or PP-Module in which this SFR is defined*] and [*assignment: devices specified in another PP or PP-Module that shares a PP Configuration with the PP or PP-Module in which this SFR is defined*] upon TOE power up and upon connection of a peripheral device to a powered-on TOE. |
| **FDP_PDC_EXT.2.2** | The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*assignment: devices* |

*specified in the PP or PP Module in which this SFR is defined*] and [*assignment: devices specified in another PP or PP-Module that shares a PP-Configuration with the PP or PP-Module in which this SFR is defined*] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

**FDP_PDC_EXT.3 Authorized Connection Protocols**

Hierarchical to: No other components.

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

**FDP_PDC_EXT.3.1** The TSF shall have interfaces for the [*assignment: list of supported protocols associated with physical and/or logical TSF interfaces*] protocols.

**FDP_PDC_EXT.3.2** The TSF shall apply the following rules to the supported protocols: [*assignment: rules defining the handling for communications over this protocol (e.g. any processing that must be done by the TSF prior to transmitting it through the TOE, circumstances or frequency with which the protocol is invoked)*].

**FDP_PDC_EXT.4 Supported Authentication Devices**

Hierarchical to: No other components.

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection,
FDP_PDC_EXT.2 Authorized Devices

**FDP_PDC_EXT.4.1** The TSF shall have an [selection: internal, external] user authentication device.

## 5.1.7 FDP_PUD_EXT Powering Unauthorized Devices

**Family Behavior**

Components in this family define the requirements for unauthorized device powering.

**Component Leveling**


FDP_PUD_EXT.1 Powering Unauthorized Devices, requires the TSF to not power any unauthorized devices connected to the peripheral interface.

**Management: FDP_PUD_EXT.1**

No specific management functions are identified.

**Audit: FDP_PUD_EXT.1**

There are no specific auditable events foreseen.

**FDP_PUD_EXT.1 Powering Unauthorized Devices**

Hierarchical to: No other components.

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

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

## 5.1.8 FDP_PWR_EXT Powered By Computer

**Family Behavior**

Components in this family define the requirements for device powering.

**Component Leveling**


FDP_PWR_EXT.1 Powered by Computer, requires the TSF to not be powered by a connected computer.

**Management: FDP_PWR_EXT.1**

No specific management functions are identified.

**Audit: FDP_PWR_EXT.1**

There are no specific auditable events foreseen.

**FDP_PWR_EXT.1 Powered By Computer**

Hierarchical to: No other components.

Dependencies: No dependencies

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

## 5.1.9 FDP_RDR_EXT Re-Enumeration Device Rejection

**Family Behavior**

Components in this family define requirements to reject device spoofing attempts through reenumeration.

**Component Leveling**

FDP_RDR_EXT.1 Re-Enumeration Device Rejection, requires the TSF to reject re-enumeration as an unauthorized device.

**Management: FDP_RDR_EXT.1**

No specific management functions are identified.

**Audit: FDP_RDR_EXT.1**

There are no specific auditable events foreseen.

**FDP_RDR_EXT.1 Re-Enumeration Device Rejection**

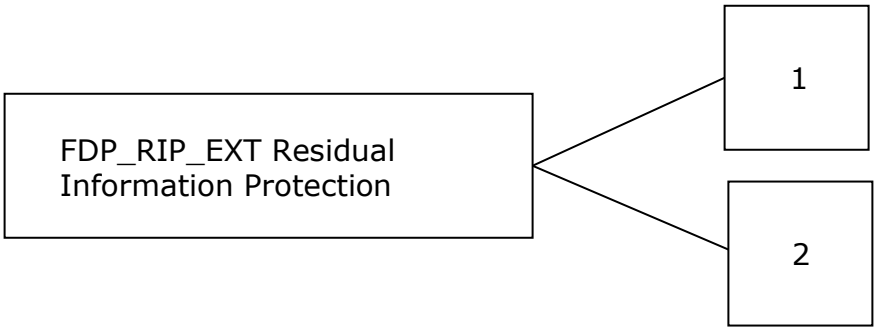
| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FDP_PDC_EXT.1 Peripheral Device Connection |
| **FDP_RDR_EXT.1.1** | The TSF shall reject any device that attempts to enumerate again as a different unauthorized device. |

## 5.1.10 FDP_RIP_EXT Residual Information Protection

**Family Behavior**

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

**Component Leveling**




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

FDP_RIP_EXT.2 Purge of Residual Information, requires the TSF to have a purge function to clear its memory of all stored non-audit data.

**Management: FDP_RIP_EXT.1, FDP_RIP_EXT.2**

The following actions could be considered for the management functions in FMT:

- Ability to trigger the TSF's purge function

**Audit: FDP_RIP_EXT.1**

There are no auditable events foreseen.

**Audit: FDP_RIP_EXT.2**

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Purging of the TSF's memory

**FDP_RIP_EXT.1 Residual Information Protection**

Hierarchical to: No other components.

Dependencies: No dependencies

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

**FDP_RIP_EXT.2 Purge of Residual Information**

Hierarchical to: No other components.

Dependencies: No dependencies

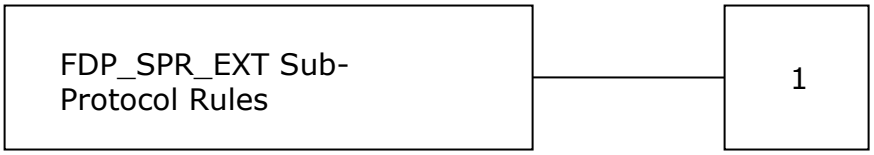
**FDP_RIP_EXT.2.1** The TOE shall have a purge memory or restore factory defaults function accessible to the administrator to delete all TOE stored configuration and settings except for logging.

## 5.1.11 FDP_SPR_EXT Sub-Protocol Rules

**Family Behavior**

Components in this family define the sub-protocols that the TSF allows or blocks depending on the protocols it supports.

**Component Leveling**




FDP_SPR_EXT.1 Sub-Protocol Rules, requires the TSF to specify the allowed and blocked sub-protocols based on the protocol it supports.

**Management: FDP_SPR_EXT.1**

No specific management functions are identified.

**Audit: FDP_SPR_EXT.1**

There are no auditable events foreseen.

**FDP_SPR_EXT.1 Sub-Protocol Rules**

Hierarchical to: No other components.

Dependencies: FDP_PDC_EXT.3 Authorized Connection Protocols

**FDP_SPR_EXT.1.1** The TSF shall apply the following rules for the [assignment: supported protocol] protocol:

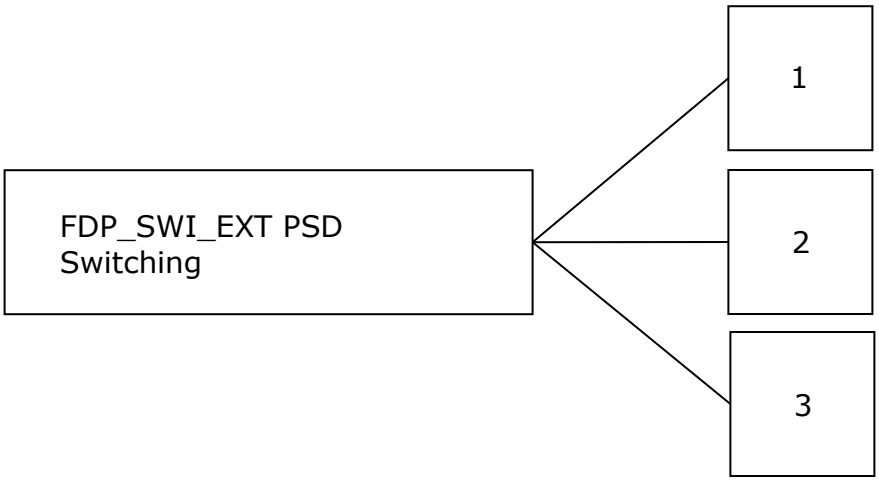
- block the following video/display sub-protocols:
  - [*assignment: list of blocked sub-protocols*]
- allow the following video/display sub-protocols:
  - [*assignment: list of allowed sub-protocols*].

## 5.1.12 FDP_SWI_EXT PSD Switching

**Family Behavior**

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

**Component Leveling**




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

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

FDP_SWI_EXT.3 Tied Switching, requires the TSF to ensure that multiple connected peripherals are always switched to the same connected computer.

**Management: FDP_SWI_EXT.1, FDP_SWI_EXT.2, FDP_SWI_EXT.3**

No specific management functions are identified.

**Audit: FDP_SWI_EXT.1, FDP_SWI_EXT.2, FDP_SWI_EXT.3**

There are no auditable events foreseen.

**FDP_SWI_EXT.1 PSD Switching**

Hierarchical to: No other components.

Dependencies: No dependencies

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

### FDP_SWI_EXT.2 PSD Switching Methods

Hierarchical to: No other components.

Dependencies: FDP_SWI_EXT.1 PSD Switching

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

**FDP_SWI_EXT.2.2** The TSF shall ensure that switching can be initiated only through express user action using [*selection: console buttons, console switches, console touch screen, wired remote control, peripheral devices using a guard*].

### FDP_SWI_EXT.3 Tied Switching

Hierarchical to: No other components.

Dependencies: FDP_SWI_EXT.1 PSD Switching

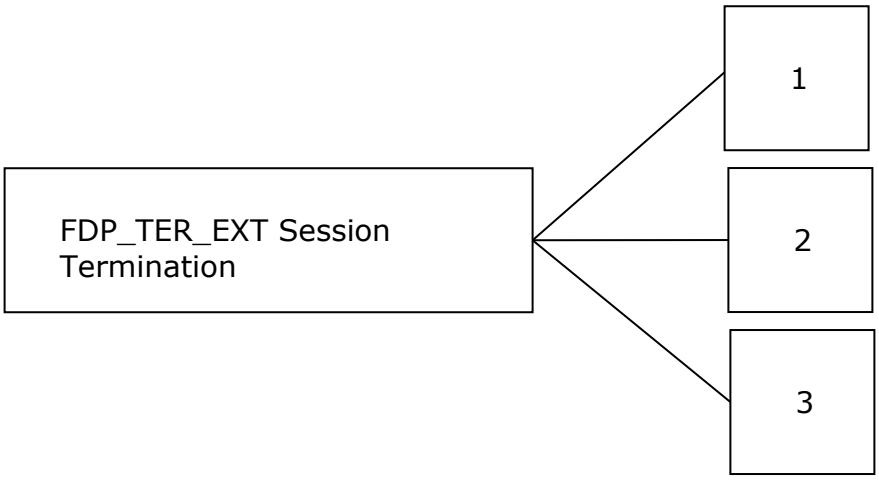
**FDP_SWI_EXT.3.1** The TSF shall ensure that [*assignment: two or more tied peripheral devices*] are always switched together to the same connected computer.

## 5.1.13 FDP_TER_EXT Session Termination

### Family Behavior

Components in this family define the requirements for termination of open sessions.

### Component Leveling




FDP_TER_EXT.1, Session Termination, requires the TSF to terminate an open session upon removal of the authentication element.

FDP_TER_EXT.2, Session Termination of Removed Devices, requires the TSF to terminate an open session upon removal of the user authentication device.

FDP_TER_EXT.3, Session Termination upon Switching, requires the TOE to terminate an open session upon switching to a different computer; and reset the

power to the user authentication device for at least one second upon switching to a different computer.

**Management: FDP_TER_EXT.1, FDP_TER_EXT.2, FDP_TER_EXT.3**

No specific management functions are identified.

**Audit: FDP_TER_EXT.1, FDP_TER_EXT.2, FDP_TER_EXT.3**

There are no specific auditable events foreseen.

**FDP_TER_EXT.1 Session Termination**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies |
| **FDP_TER_EXT.1.1** | The TSF shall terminate an open session upon removal of the authentication element. |

**FDP_TER_EXT.2 Session Termination of Removed Devices**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FDP_PDC_EXT.2 Authorized Devices |
| **FDP_TER_EXT.2.1** | The TSF shall terminate an open session upon removal of the user authentication device. |

**FDP_TER_EXT.3 Session Termination upon Switching**

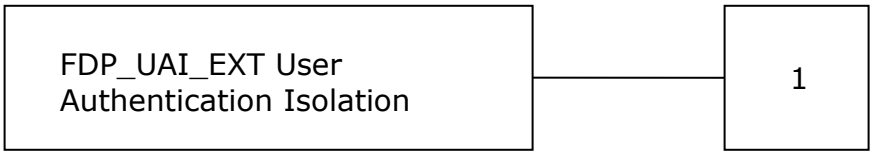
| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FDP_SWI_EXT.1 PSD Switching |
| **FDP_TER_EXT.3.1** | The TSF shall terminate an open session upon switching to a different computer. |
| **FDP_TER_EXT.3.2** | The TSF shall reset the power to the user authentication device for at least one second upon switching to a different computer. |

## 5.1.14 FDP_UAI_EXT User Authentication Isolation

**Family Behavior**

Components in this family define the requirements for user authentication isolation.

**Component Leveling**




FDP_UAI_EXT.1 User Authentication Isolation, requires the TSF to isolate the user authentication function from all other TOE USB functions.

**Management: FDP_UAI_EXT.1**

No specific management functions are identified.

**Audit: FDP_UAI_EXT.1**

There are no specific auditable events foreseen.

**FDP_UAI_EXT.1 User Authentication Isolation**

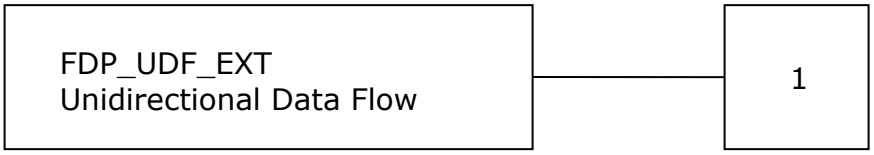
| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | None |
| **FDP_UAI_EXT.1.1** | The TSF shall isolate the user authentication function from all other TOE USB functions. |

### 5.1.15 FDP_UDF_EXT Unidirectional Data Flow

**Family Behavior**

Components in this family define unidirectional transmission of user data.

**Component Leveling**




FDP_UDF_EXT.1 Unidirectional Data Flow, requires the TSF to provide unidirectional (one-way) communications between a given pair of interface types.

**Management: FDP_UDF_EXT.1**

No specific management functions are identified.

**Audit: FDP_UDF_EXT.1**

There are no auditable events foreseen.

**FDP_UDF_EXT.1 Unidirectional Data Flow**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FDP_APC_EXT.1 Active PSD Connections |
| **FDP_UDF_EXT.1.1** | The TSF shall ensure [*assignment: type of data*] data transits the TOE unidirectionally from the [*assignment: origin point of data*] interface to the [*assignment: destination point of data*] interface. |

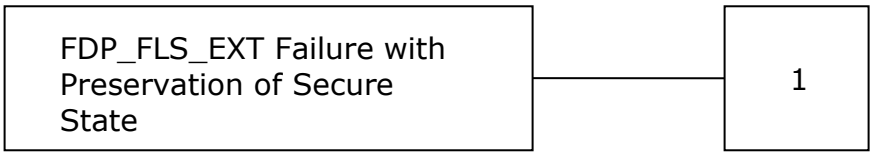
## 5.2 CLASS FPT: PROTECTION OF THE TSF

### 5.2.1 FPT_FLS_EXT Failure with Preservation of Secure State

**Family Behavior**

Components in this family define the secure failure requirements for the TSF.

**Component Leveling**




FPT_FLS_EXT.1 Failure with Preservation of Secure State, requires the TSF to go into a secure state upon the detection of selected failures.

**Management: FPT_FLS_EXT.1**

No specific management functions are identified.

**Audit: FPT_FLS_EXT.1**

There are no auditable events foreseen.

**FPT_FLS_EXT.1 Failure with Preservation of Secure State**

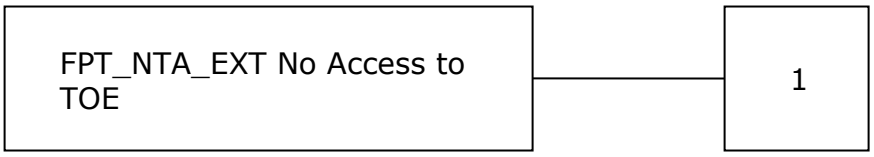
| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FPT_TST.1 TSF Testing<br>FPT_PHP.3 Resistance to Physical Attack |
| **FPT_FLS_EXT.1.1** | The TSF shall preserve a secure state when the following types of failures occur: failure of the power-on self-test and [*selection: failure of the anti-tamper function, no other failures*]. |

## 5.2.2 FPT_NTA_EXT No Access to TOE

**Family Behavior**

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

**Component Leveling**




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

**Management: FPT_NTA_EXT.1**

No specific management functions are identified.

**Audit: FPT_NTA_EXT.1**

There are no auditable events foreseen.

**FPT_NTA_EXT.1 No Access to TOE**

Hierarchical to: No other components.

Dependencies: No dependencies

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

### 5.2.3 FPT_TST_EXT TSF Testing

**Family Behavior**

Components in this family define how the TSF responds to a self-test failure.

**Component Leveling**


FPT_TST_EXT.1 TSF Testing, requires the TSF to shutdown normal functions and provide a visual or auditory indication that a self-test has failed.

**Management: FPT_TST_EXT.1**

No specific management functions are identified.

**Audit: FPT_TST_EXT.1**

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Indication that the TSF self-test was completed
- Failure of self-test

**FPT_TST_EXT.1 TSF Testing**

Hierarchical to: No other components.

Dependencies: FPT_TST.1 TSF Testing

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

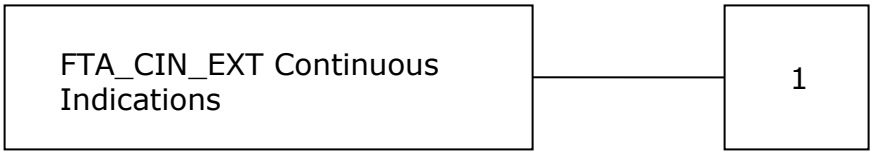
# 5.3 CLASS FTA: TOE ACCESS

## 5.3.1 FTA_CIN_EXT Continuous Indications

**Family Behavior**

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

**Component Leveling**




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

**Management: FTA_CIN_EXT.1**

No specific management functions are identified.

**Audit: FTA_CIN_EXT.1**

There are no auditable events foreseen.

**FTA_CIN_EXT.1 Continuous Indications**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FDP_APC_EXT.1 Active PSD Connections |
| **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,** [*selection: a button, a panel with lights, a screen with dimming function, a screen with no dimming function, [assignment: description of visible indication]*]. |
| **FTA_CIN_EXT.1.3** | The TSF shall ensure that while the TOE is powered the current switching status is reflected by [*selection: the indicator, multiple indicators which never display conflicting information*]. |

# 6 SECURITY FUNCTIONAL REQUIREMENTS

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

## 6.1 CONVENTIONS AND APPLICABILITY

### 6.1.1 Conventions

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations are shown using the same conventions as those in the PSD PP. This is defined in the PP as:

- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Selection: Indicated by surrounding brackets and italics, e.g., [*selected item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Iteration operations for iterations within the Protection Profile and associated modules are identified with a slash ('/') and an identifier (e.g. "/KM").
- Where an SFR does not apply equally to all devices, an additional tag has been added to indicate the products to which the SFR applies. This tag provides the applicable model names in brackets (e.g. FDP_CDS_EXT.1 (1) Connected Displays Supported (F1DN104KVM-UN-4, F1DN102KVM-UN-4, F1DN108KVM-UN-4, F1DN116KVM-UN-4)). Additionally, a number is appended to the SFR identifier where multiple iterations of the SFR are required.

Extended Security Functional Requirement (SFRs) are identified by the inclusion of "EXT" in the Security Functional Requirement SFR name.

### 6.1.2 Section Applicability

Table 12 shows the TOE models and the Section 6 Subsections that include the SFRs claimed for that device.

| TOE Model | Sections Describing Security Functionality |
|---|---|
| F1DN104KVM-UN-4 | Section 6.2 and Section 6.3 |
| F1DN204KVM-UN-4 | Section 6.2 and Section 6.4 |
| F1DN102KVM-UN-4 | Section 6.2 and Section 6.3 |

| TOE Model | Sections Describing Security Functionality |
|---|---|
| F1DN202KVM-UN-4 | Section 6.2 and Section 6.4 |
| F1DN108KVM-UN-4 | Section 6.2 and Section 6.3 |
| F1DN208KVM-UN-4 | Section 6.2 and Section 6.4 |
| F1DN116KVM-UN-4 | Section 6.2 and Section 6.3 |

**Table 12 – Devices and Applicable Sections**

## 6.2 SECURITY FUNCTIONAL REQUIREMENTS FOR ALL DEVICES

Section 6.2 details the security functional requirements that apply to all TOE devices.

| Class | Identifier | Name | Source |
|---|---|---|---|
| Security Audit (FAU) | FAU_GEN.1 | Audit data generation | [PP_PSD_V4.0] |
| User Data Protection (FDP) | FDP_AFL_EXT.1 | Audio Filtration | [MOD_AO_V1.0] |
| | FDP_APC_EXT.1 | Active PSD Connections | [PP_PSD_V4.0] |
| | FDP_APC_EXT.1/AO | Active PSD Connections | [MOD_AO_V1.0] |
| | FDP_APC_EXT.1/KM | Active PSD Connections | [MOD_KM_V1.0] |
| | FDP_APC_EXT.1/UA | Active PSD Connections | [MOD_UA_V1.0] |
| | FDP_APC_EXT.1/VI | Active PSD Connections | [MOD_VI_V1.0] |
| | FDP_FIL_EXT.1/KM | Device Filtering (Keyboard/Mouse) | [MOD_KM_V1.0] |
| | FDP_FIL_EXT.1/UA | Device Filtering (User Authentication Devices) | [MOD_UA_V1.0] |
| | FDP_IPC_EXT.1 | Internal Protocol Conversion | [MOD_VI_V1.0] |
| | FDP_PDC_EXT.1 | Peripheral Device | [PP_PSD_V4.0] [MOD_AO_V1.0][3] |

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

| Class | Identifier | Name | Source |
|---|---|---|---|
| | | Connection | [MOD_VI_V1.0][4] [MOD_KM_V1.0][5] [MOD_UA_V1.0][6] |
| | FDP_PDC_EXT.2/AO | Authorized Devices (Audio Output) | [MOD_AO_V1.0] |
| | FDP_PDC_EXT.2/KM | Authorized Devices (Keyboard/Mouse) | [MOD_KM_V1.0] |
| | FDP_PDC_EXT.2/UA | Authorized Devices (User Authentication Devices) | [MOD_UA_V1.0] |
| | FDP_PDC_EXT.2/VI | Authorized Devices (Video Output) | [MOD_VI_V1.0] |
| | FDP_PDC_EXT.3/KM | Authorized Connection Protocols (Keyboard/Mouse) | [MOD_KM_V1.0] |
| | FDP_PDC_EXT.3/VI | Authorized Connection Protocols (Video Output) | [MOD_VI_V1.0] |
| | FDP_PDC_EXT.4 | Supported Authentication Device | [MOD_UA_V1.0] |
| | FDP_PUD_EXT.1 | Powering Unauthorized Devices | [MOD_AO_V1.0] |
| | FDP_PWR_EXT.1 | Powered By Computer | [MOD_UA_V1.0] |
| | FDP_RDR_EXT.1 | Re-Enumeration Device Rejection | [MOD_KM_V1.0] |

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

[6] There is no modification to this SFR in the [MOD_UA_V1.0]. However, there are additions to the Peripheral Device Connections associated with this SFR, and additional application note and additional evaluation activities.

| Class | Identifier | Name | Source |
|---|---|---|---|
| | FDP_RIP_EXT.1 | Residual Information Protection | [PP_PSD_V4.0] |
| | FDP_RIP.1/KM | Residual Information Protection (Keyboard Data) | [MOD_KM_V1.0] |
| | FDP_RIP_EXT.2 | Purge of Residual Information | [PP_PSD_V4.0] |
| | FDP_SPR_EXT.1/DP | Sub-Protocol Rules (DisplayPort Protocol) | [MOD_VI_V1.0] |
| | FDP_SPR_EXT.1/HDMI | Sub-Protocol Rules (HDMI Protocol) | [MOD_VI_V1.0] |
| | FDP_SWI_EXT.1 | PSD Switching | [PP_PSD_V4.0] |
| | FDP_SWI_EXT.2 | PSD Switching Methods | [PP_PSD_V4.0] [MOD_KM_V1.0][7] |
| | FDP_SWI_EXT.3 | Tied Switching | [MOD_KM_V1.0] |
| | FDP_TER_EXT.1 | Session Termination | [MOD_UA_V1.0] |
| | FDP_TER_EXT.2 | Session Termination of Removed Devices | [MOD_UA_V1.0] |
| | FDP_TER_EXT.3 | Session Termination upon Switching | [MOD_UA_V1.0] |
| | FDP_UAI_EXT.1 | User Authentication Isolation | [MOD_UA_V1.0] |
| | FDP_UDF_EXT.1/AO | Unidirectional Data Flow (Audio Output) | [MOD_AO_V1.0] |
| | FDP_UDF_EXT.1/KM | Unidirectional Data Flow (Keyboard/Mouse) | [MOD_KM_V1.0] |
| | FDP_UDF_EXT.1/VI | Unidirectional Data Flow (Video Output) | [MOD_VI_V1.0] |

[7] There is no modification to this SFR in [MOD_KM_V1.0], and the additional evaluation activities are not triggered by the selections in FDP_SWI_EXT.2.2.

| Class | Identifier | Name | Source |
|---|---|---|---|
| Identification and Authentication (FIA) | FIA_UAU.2 | User Authentication Before Any Action | [PP_PSD_V4.0] |
| | FIA_UID.2 | User Identification Before Any Action | [PP_PSD_V4.0] |
| Security Management (FMT) | FMT_MOF.1 | Management of Security Functions Behavior | [PP_PSD_V4.0] |
| | FMT_SMF.1 | Specification of Management Functions | [PP_PSD_V4.0] |
| | FMT_SMR.1 | Security Roles | [PP_PSD_V4.0] |
| Protection of the TSF (FPT) | FPT_FLS_EXT.1 | Failure with Preservation of Secure State | [PP_PSD_V4.0] |
| | FPT_NTA_EXT.1 | No Access to TOE | [PP_PSD_V4.0] |
| | FPT_PHP.1 | Passive Detection of Physical Attack | [PP_PSD_V4.0] |
| | FPT_PHP.3 | Resistance to Physical Attack | [PP_PSD_V4.0] |
| | FPT_STM.1 | Reliable Time Stamps | [PP_PSD_V4.0] |
| | FPT_TST.1 | TSF testing | [PP_PSD_V4.0] |
| | FPT_TST_EXT.1 | TSF Testing | [PP_PSD_V4.0] |
| TOE Access (FTA) | FTA_CIN_EXT.1 | Continuous Indications | [PP_PSD_V4.0] [MOD_VI_V1.0][8] |

**Table 13 – 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

[8] The refinement from [MOD_VI_V1.0] has been included in FTA_CIN_EXT.1.2.

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 |
| 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 14 – Audio Filtration Specifications**

### 6.2.2.2 FDP_APC_EXT.1 Active PSD Connections

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

**FDP_APC_EXT.1.2** The TSF shall ensure that no data flows between connected computers whether the TOE is powered on or powered off.

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

**FDP_APC_EXT.1.4** 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/AO Active PSD Connections

**FDP_APC_EXT.1.1/AO** The TSF shall route user data only to ~~or 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.

#### 6.2.2.4 FDP_APC_EXT.1/KM Active PSD Connections

**FDP_APC_EXT.1.1/KM** The TSF shall route user data only to ~~or from~~ 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.

#### 6.2.2.5 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.

#### 6.2.2.6 FDP_APC_EXT.1/VI Active PSD Connections

**FDP_APC_EXT.1.1/VI** The TSF shall route user data only ~~to or~~ 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.

#### 6.2.2.7 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.

#### 6.2.2.8 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.

#### 6.2.2.9 FDP_IPC_EXT.1 Internal Protocol Conversion

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

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

### 6.2.2.10 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.

### 6.2.2.11 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*[9]] 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*] 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.

[9] This refers to Appendix E of [PP_PSD_V4.0].

### 6.2.2.12 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*] and [

- ***authorized devices as defined in the PP-Module for Audio Output 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/KM** The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*Appendix E*] 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.

### 6.2.2.13 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*] 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*] 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.

#### 6.2.2.14 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*] 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*] 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.

#### 6.2.2.15 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*].

#### 6.2.2.16 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*].

#### 6.2.2.17 FDP_PDC_EXT.4 Supported Authentication Device

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

#### 6.2.2.18 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.

#### 6.2.2.19 FDP_PWR_EXT.1 Powered By Computer

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

#### 6.2.2.20 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.

#### 6.2.2.21 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.

#### 6.2.2.22 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.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.

#### 6.2.2.24 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*].

#### 6.2.2.25 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*].

#### 6.2.2.26 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*].

#### 6.2.2.27 FDP_SWI_EXT.2 PSD Switching Methods

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

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

#### 6.2.2.28 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.

#### 6.2.2.29 FDP_TER_EXT.1 Session Termination

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

#### 6.2.2.30 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.

#### 6.2.2.31 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.

#### 6.2.2.32 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.

#### 6.2.2.33 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.

#### 6.2.2.34 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]*] interface(s) to the [*TOE [keyboard, mouse]*] interface.

#### 6.2.2.35 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 TOE 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 antitamper 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*] by **becoming permanently disabled**.

#### 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 authorised users with the capability to verify the integrity of [*TSF data*].

**FPT_TST.1.3** The TSF shall provide authorised 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*].

# 6.3 ADDITIONAL SECURITY REQUIREMENTS FOR F1DN104KVM-UN-4, F1DN102KVM-UN-4, F1DN108KVM-UN-4, AND F1DN116KVM-UN-4

Section 6.3 details the security functional requirements that are satisfied by the F1DN104KVM-UN-4, F1DN102KVM-UN-4, F1DN108KVM-UN-4, and F1DN116KVM-UN-4 devices.

| Class | Identifier | Name | Source |
|---|---|---|---|
| User Data Protection (FDP) | FDP_CDS_EXT.1(1) | Connected Displays Supported (F1DN104KVM-UN-4, F1DN102KVM-UN-4, F1DN108KVM-UN-4, F1DN116KVM-UN-4) | [MOD_VI_V1.0] |

**Table 15 – Summary of Additional Security Functional Requirements for the F1DN104KVM-UN-4, F1DN102KVM-UN-4, F1DN108KVM-UN-4, and F1DN116KVM-UN-4 Devices**

## 6.3.1 User Data Protection (FDP)

### 6.3.1.1 FDP_CDS_EXT.1(1) Connected Displays Supported (F1DN104KVM-UN-4, F1DN102KVM-UN-4, F1DN108KVM-UN-4, F1DN116KVM-UN-4)

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

# 6.4 ADDITIONAL SECURITY REQUIREMENTS FOR F1DN204KVM-UN-4, F1DN202KVM-UN-4, F1DN208KVM-UN-4

Section 0 details the security functional requirements that are satisfied by the F1DN204KVM-UN-4, F1DN202KVM-UN-4, and F1DN208KVM-UN-4 devices.

| Class | Identifier | Name | Source |
|---|---|---|---|
| User Data Protection (FDP) | FDP_CDS_EXT.1(2) | Connected Displays Supported (F1DN204KVM-UN-4, F1DN202KVM-UN-4, F1DN208KVM-UN-4) | [MOD_VI_V1.0] |

**Table 16 – Summary of Additional Security Functional Requirements for the F1DN204KVM-UN-4, F1DN202KVM-UN-4, and F1DN208KVM-UN-4 Devices**

## 6.4.1 User Data Protection (FDP)

### 6.4.1.1 FDP_CDS_EXT.1(2) Connected Displays Supported (F1DN204KVM-UN-4, F1DN202KVM-UN-4, F1DN208KVM-UN-4)

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

# 7 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 17.

| 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 17 – 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 18 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 | None | N/A |
| 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.2 | Included |
| FDP_PDC_EXT.3/KM | FDP_PDC_EXT.1 | Included |
| FDP_PDC_EXT.3/VI | FDP_PDC_EXT.2 | Included |

| SFR | Dependencies | Rationale Statement |
|---|---|---|
| FDP_PDC_EXT.4 | FDP_PDC_EXT.1<br>FDP_PDC_EXT.2 | Included |
| FDP_PUD_EXT.1 | FDP_PDC_EXT.1 | Included |
| FDP_PWR_EXT.1 | None | N/A |
| FDP_RDR_EXT.1 | FDP_PDC_EXT.1 | Included |
| FDP_RIP_EXT.1 | None | N/A |
| FDP_RIP.1/KM | 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<br>FMT_SMR.1 | Included<br>Included |
| FMT_SMF.1 | None | N/A |
| FMT_SMR.1 | FIA_UID.1 | Included |
| FPT_FLS_EXT.1 | FPT_TST.1<br>FPT_PHP.3 | Included<br>Included only if anti-tamper is selected in FPT_FLS_EXT.1.1 |

| SFR | Dependencies | Rationale Statement |
|---|---|---|
| FPT_NTA_EXT.1 | None | N/A |
| FPT_PHP.1 | None | N/A |
| FPT_PHP.3 | None | N/A |
| 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 18 – 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].

# 9 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

Unless otherwise stated, the description applies to all devices.

## 9.1 SECURITY AUDIT

The TOE is equipped with non-volatile memory for the storage of audit records. There are two separate storage areas:

- Critical One Time Programming (OTP) Logs
    - The critical log area stores the following information:
    - Tampering events – there are six possible event flags
    - Self-test failure – a record of the latest self-test failure is recorded with error code information
    - Peripheral device rejection
    - Configuration changes to the CDF whitelist/blacklist made by the administrator
    - Reset to factory default event
    - Changes to the primary administrator password
- Non-critical (Random Access Memory (RAM)) Logs
    - 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.

Logs cannot be deleted by the administrator. The critical logs hold up to 64 events. The non-critical logs hold up to 128 events. In both log files, the oldest logs are overwritten when the storage space allocated to the logs becomes full.

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 Belkin SKVM/SKM Administration Guide [Belkin 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. It receives user input from the switches on the front panel or from the wired remote control, and drives the TOE channel select lines that control switching circuits within the TOE.

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

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

The user determines which host computer is to be connected to the peripherals by pressing a button on the TOE front panel, or by using a remote control. The remote control for the units (see Table 3) also has push buttons. When a remote control device is used, both the front panel button and the remote's channel indicator for the selected computer are illuminated. These are always consistent. Switching can only be initiated through express user action.

KVM devices may be switched with peripheral devices using a guard[10]. This is done by moving the mouse to the edge of the screen while pressing the left CTRL key.

**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 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, 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:

[10] See Section 8.1 or [PP_PSD_V4.0] for the definition of a guard.

- 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 Display Port interface
- 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

**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 critical 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 Switching 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 Serial 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 hosts.

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

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

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

#### 9.2.2.2 Keyboard and Mouse Switching Functionality

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

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

Since the keyboard and mouse function are emulated by the TOE, the connected computer is not able to send data to the keyboard that would allow it to indicate that Caps Lock, Num Lock or Scroll Lock are set. These are indicated on the TOE front panel, on the right hand side, as shown in Figure 7 in Section 7.5.

**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 are permitted. The TOE does not support a wireless connection to a mouse, keyboard or USB hub.

**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.

**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 4 shows a data flow during the display EDID read function.

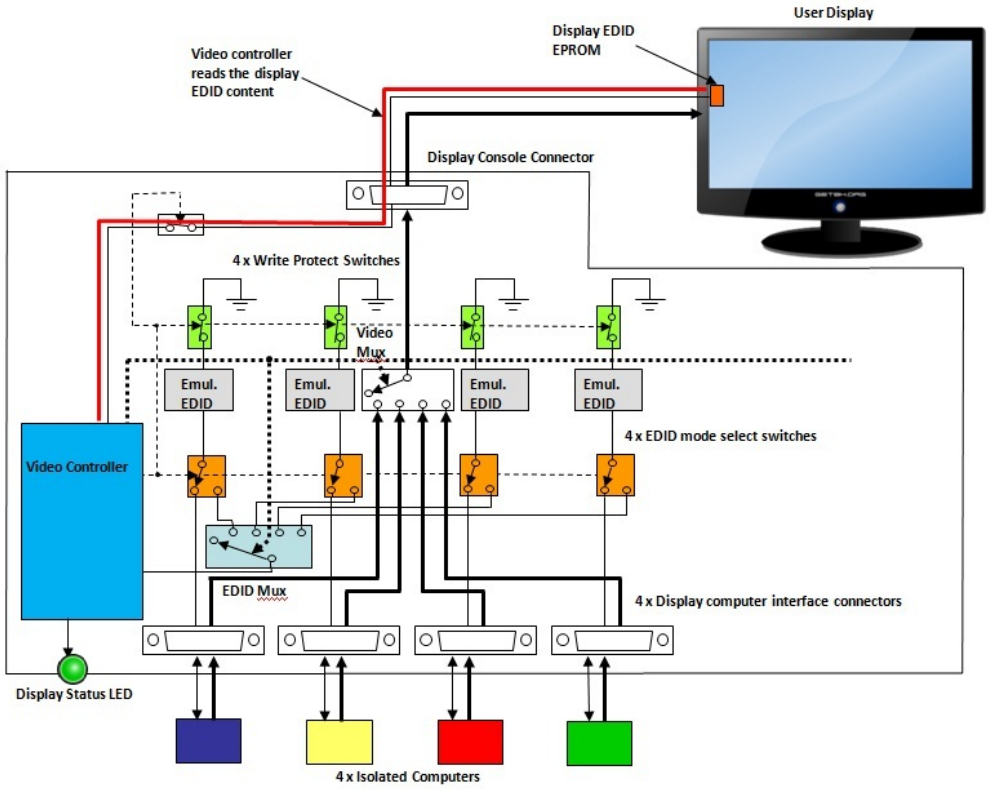



**Figure 4 – Display EDID Read Function**

An EDID read event only occurs as the TOE is being powered up. The video controller reads the EDID content from the display device to verify that it is valid

and usable. If data is not valid, TOE operation will cease and wait for the display peripheral to be changed.

Figure 4 shows a data flow during the display EDID read function.

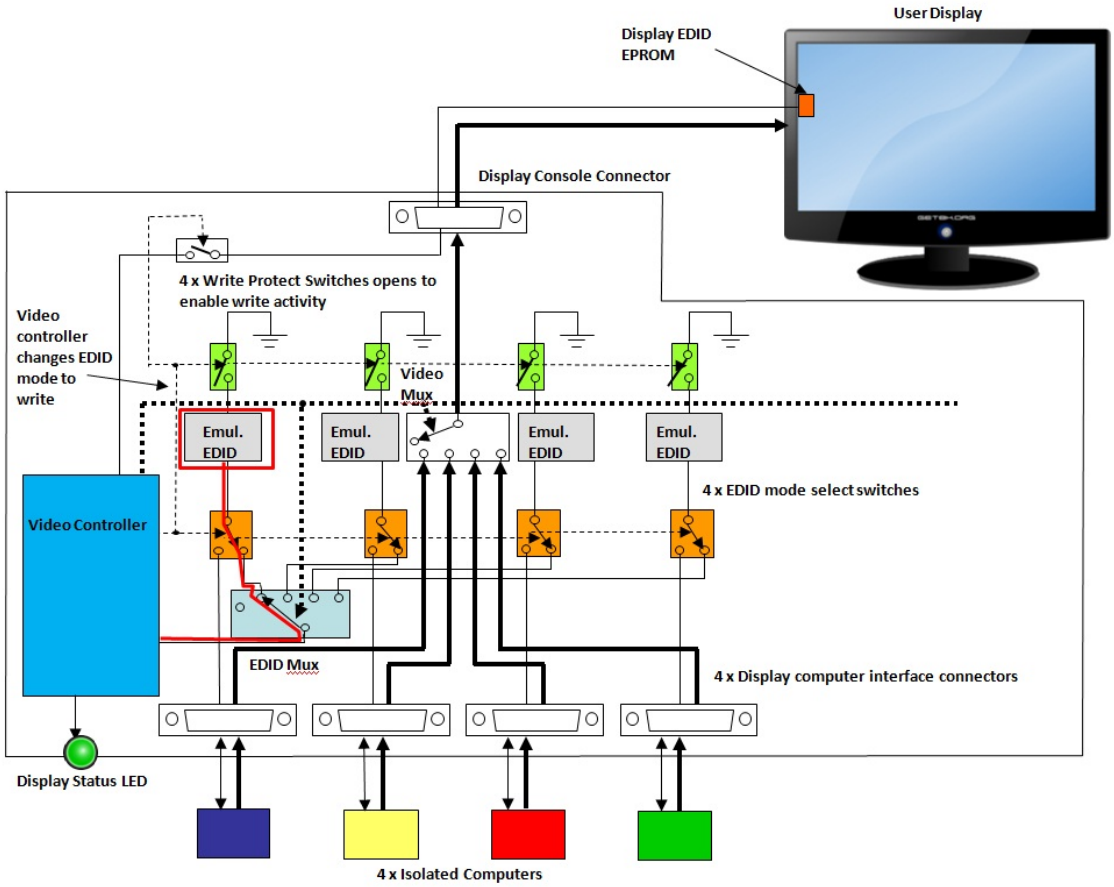



**Figure 5 – Display EDID Write Function**

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

In EDID write mode, the Emulated EDID EEPROM chips are switched to their respective computers to enable reading of the EDID information. The write

protect switches are switched back to protected mode to prevent any attempt to write to the EEPROM or to transmit MCCS commands.

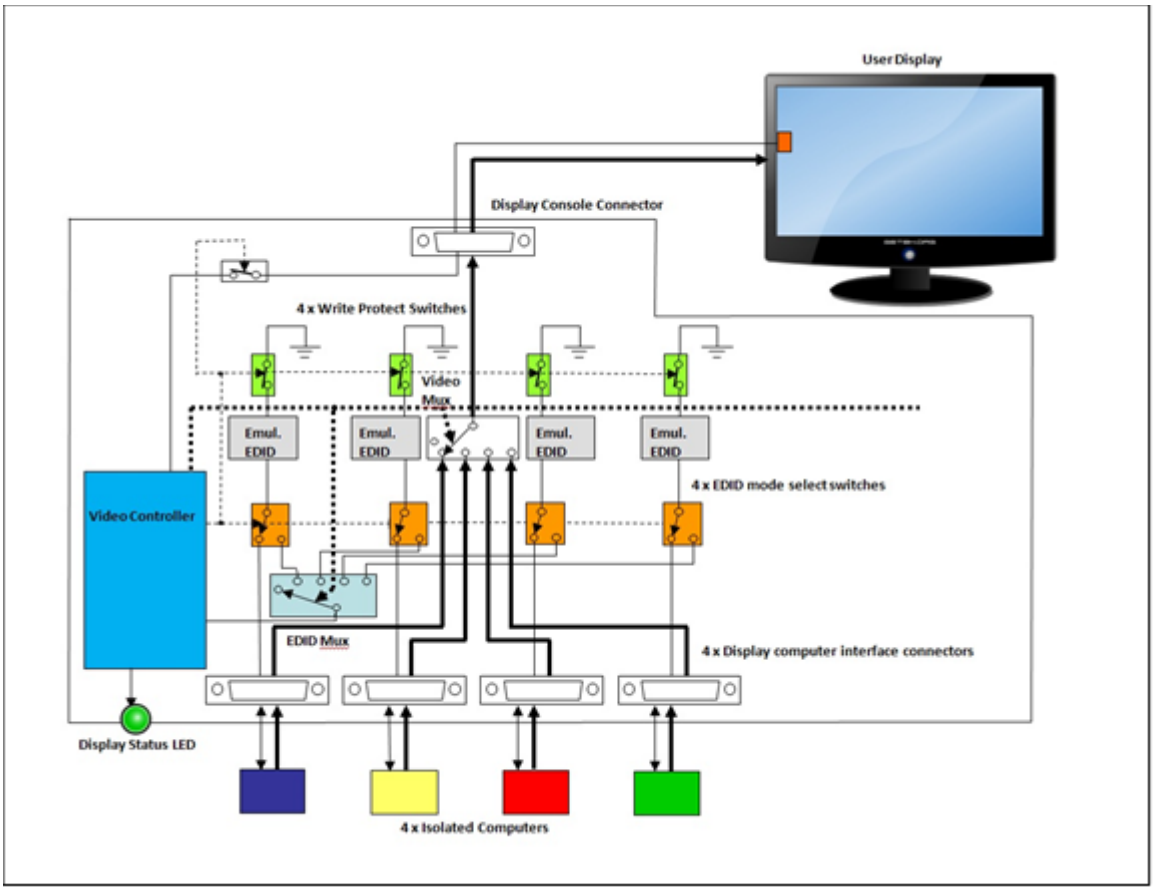



**Figure 6 – Display Normal Mode**

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

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

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

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

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

The TOE supports DisplayPort versions 1.1, 1.2 and 1.3, and HDMI 2.0:

- 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. Emulated EDID EEPROMs may still operate since they are powered by their respective computers; however, the video function remains isolated.

**TOE Security Functional Requirements addressed**: FDP_IPC_EXT.1, FDP_SPR_EXT.1/DP, FDP_SPR_EXT.1/HDMI.

#### 9.2.3.1 Video Compatible Device Types

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

The F1DN104KVM-UN-4, F1DN102KVM-UN-4, F1DN108KVM-UN-4 and F1DN116KVM-UN-4 models support a single display. Two displays are supported by the F1DN204KVM-UN-4, F1DN202KVM-UN-4 and F1DN208KVM-UN-4 models.

**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).

### 9.2.4 User Authentication Device Switching Functionality

The TOE supports the use of a user authentication device with a feature called Freeze USB (fUSB).

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.

A 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 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.

#### 9.2.4.1 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.

### 9.2.5 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.

#### 9.2.5.1 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 failed login attempts. The user may cycle the device power and try again.

Once logged in, the administrator may use the functions described in the [Belkin 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 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 both passive and active anti-tampering functionality.

### 9.4.2.1 Passive Detection of Physical Tampering

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

Additionally, each device is fitted with one or more holographic Tampering Evident Labels placed at critical locations on the TOE enclosure. If the 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, is causes an internal microscopic fuse on the System Controller (on-die) to melt. This permanently disables all interfaces and user functions of the device, and causes the front panel LEDs to blink sequentially and continuously. The TOE anti-tampering function is irreversible.

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:

- 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 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

## 9.5.1 Continuous Indications

The TOE user switches between computers by pressing the corresponding front panel button on the device. The front panel button corresponding to the selected computer will illuminate.

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 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. To release the freeze, the user performs a second long press on the channel button. This applies to all devices that support user authentication devices.

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

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

**TOE Security Functional Requirements addressed**: FTA_CIN_EXT.1.

## 9.5.2 Wired Remote Control

The remote control device for the El Capitan devices is built into a custom keyboard, and acts as a wired remote control as described in the [PP_PSD_V4.0].

When the user selects a channel using the remote control keyboard, the selected channel indicator on the left side of the remote control devices illuminates, 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.

Additionally, a holographic Tampering Evident Label is placed at a critical location on the remote control device. If the label is removed, the word 'VOID' appears on both the label and the product surface.

**TOE Security Functional Requirements addressed**: FTA_CIN_EXT.1, FPT_PHP.1.

# 10TERMINOLOGY AND ACRONYMS

## 10.1 TERMINOLOGY

The following terminology is used in this ST:

| Term | Description |
|---|---|
| AO | AO refers to the requirements for Audio Output Devices. |
| AUX | AUX refers to the auxiliary channel, particularly as it applies to the DisplayPort protocol. |
| 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 19 – Terminology**

## 10.2 ACRONYMS

The following acronyms are used in this ST:

| Acronym | Definition |
|---|---|
| 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 |
| DPP | Dedicated Peripheral Port |
| EDID | Extended Display Identification Data |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| FET | Field-Effect Transistor |
| FPGA | Field Programmable Gate Array |
| fUSB | Freeze USB |

| Acronym | Definition |
|---|---|
| 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 | Serial Random Access Memory |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |

| Acronym | Definition |
|---|---|
| USB | Universal Serial Bus |
| VID/PID | Vendor Identification/Product Identification |

**Table 20 – Acronyms**

# 11 REFERENCES

| Identifier | Title |
|---|---|
| **[CC]** | Common Criteria for Information Technology Security Evaluation –<br>• Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017<br>• Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017<br>• 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 |
| **[Belkin Admin]** | Belkin SKVM/SKM Administration Guide, LNKPG-00666 Rev. A00 |
| **[PP_PSD_V4.0]** | Protection Profile for Peripheral Sharing Device, Version: 4.0, 2019-07-19 |
| **[MOD_AO_V1.0]** | PP-Module for Analog Audio Output Devices, Version 1.0 |
| **[MOD_UA_V1.0]** | PP-Module for User Authentication Devices, Version 1.0 |
| **[MOD_KM_V1.0]** | PP-Module for Keyboard/Mouse Devices, Version 1.0 |
| **[MOD_VI_1.0]** | PP-Module for Video/Display Devices, Version 1.0 |
| **[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 |

**Table 21 – References**

# ANNEX A – LETTER OF VOLATILITY

The table below provides volatility information and memory types for the Belkin Peripheral Sharing Devices. 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 RFD |
|---|---|---|---|---|---|---|---|---|
| F1DN104KVM-UN-4<br>F1DN204KVM-UN-4 | 1 | System Controller, Host emulators:<br>ST Microelectronics STM32F446ZCT | Embedded SRAM[1] | 128KB | | Volatile | May contain user data | Data is purged |
| | | | Embedded Flash[2] | 256KB | | Non-Volatile | No user data | Firmware is retained |
| | | | Embedded EEPROM[3] | 4KB | | Non-Volatile | No user data | Log data is retained |
| | | | OTP Memory | 512bytes | | Non-Volatile | Event logs are saved | Data is not purged on RFD |
| | 5 in SH or 10 in DH models | Video Controller:<br>ST Microelectronics STM32F070C6T6 | Embedded SRAM[1] | 6KB | | Volatile | No user data | Data is purged |
| | | | Embedded Flash[2] | 32KB | | Non-Volatile | No user data | Firmware is retained |
| | | | Embedded EEPROM[3] | 4KB | | Non-Volatile | No user data | Data is purged on RFD |
| | 4 | Device emulators:<br>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 |
| | | | Embedded EEPROM[3] | 4KB | | Non-Volatile | No user data | Data is purged on RFD |
| F1DN102KVM-UN-4<br>F1DN202KVM-UN-4 | 1 | System Controller, Host emulators:<br>ST Microelectronics STM32F446ZCT | Embedded SRAM[1] | 128KB | | Volatile | May contain user data | Data is purged |
| | | | Embedded Flash[2] | 256KB | | 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 RFD |
|---|---|---|---|---|---|---|---|---|
| | | | Embedded EEPROM[3] | 4KB | | Non-Volatile | No user data | Log data is retained |
| | | | OTP Memory | 512bytes | | Non-Volatile | Event logs are saved | Data is not purged on RFD |
| | 3 in SH or 6 in DH models | Video Controller: ST Microelectronics STM32F070C6T6 | Embedded SRAM[1] | 16KB | | Volatile | No user data | Data is purged |
| | | | Embedded Flash[2] | 128KB | | Non-Volatile | No user data | Firmware is retained |
| | | | Embedded EEPROM[3] | 4KB | | Non-Volatile | No user data | Data is purged on RFD |
| | 2 | Device emulators: ST Microelectronics STM32F070C6T6 | Embedded SRAM[1] | 16KB | Connected computer | Volatile | May contain user data | Data is purged |
| | | | Embedded Flash[2] | 128KB | | Non-Volatile | No user data | Firmware is retained |
| | | | Embedded EEPROM[3] | 4KB | | Non-Volatile | No user data | Data is purged on RFD |
| F1DN108KVM-UN-4<br>F1DN208KVM-UN-4<br>F1DN116KVM-UN-4 | 1 | System Controller, Host emulators: ST Microelectronics STM32F446ZCT | Embedded SRAM[1] | 128KB | | Volatile | May contain user data | Data is purged |
| | | | Embedded Flash[2] | 256KB | | Non-Volatile | No user data | Firmware is retained |
| | | | Embedded EEPROM[3] | 4KB | | Non-Volatile | No user data | Log data is retained |
| | | | OTP Memory | 512bytes | | Non-Volatile | Event logs are saved | Data is not purged on RFD |
| | 9 in SH, 17 in 16P or 18 in DH models | Video Controller: ST Microelectronics STM32F070C6T6 | Embedded SRAM[1] | 6KB | | Volatile | No user data | Data is purged |
| | | | Embedded Flash[2] | 32KB | | Non-Volatile | No user data | Firmware is retained |
| | | | Embedded EEPROM[3] | 4KB | | Non-Volatile | No user data | Data is purged on RFD |

| 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 RFD |
|---|---|---|---|---|---|---|---|---|
| | 8 in 8P or 16 in 16P | Device emulators:<br>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 |
| | | | Embedded EEPROM[3] | 4KB | | Non-Volatile | No user data | Data is purged on RFD |

***Notes:***

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

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

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

# ANNEX B – SFR DEVICE MATRIX

Table 22 indicates the SFRs supported by each device.

| | FAU_GEN.1 | FDP_AFL_EXT.1 | FDP_APC_EXT.1 | FDP_APC_EXT.1/AO | FDP_APC_EXT.1/KM | FDP_APC_EXT.1/UA | FDP_APC_EXT.1/VI | FDP_CDS_EXT.1(1) | FDP_CDS_EXT.1(2) | FDP_FIL_EXT.1/KM | FDP_FIL_EXT.1/UA | FDP_IPC_EXT.1 | FDP_PDC_EXT.1 | FDP_PDC_EXT.2/AO | FDP_PDC_EXT.2/KM | FDP_PDC_EXT.2/UA | FDP_PDC_EXT.2/VI | FDP_PDC_EXT.3/KM | FDP_PDC_EXT.3/VI | FDP_PDC_EXT.4 | FDP_PUD_EXT.1 | FDP_PWR_EXT.1 | FDP_RDR_EXT.1 | FDP_RIP_EXT.1 | FDP_RIP.1/KM | FDP_RIP_EXT.2 | FDP_SPR_EXT.1/DP | FDP_SPR_EXT.1/HDMI | FDP_SWI_EXT.1 | FDP_SWI_EXT.2 | FDP_SWI_EXT.3 | FDP_TER_EXT.1 | FDP_TER_EXT.2 | FDP_TER_EXT.3 | FDP_UAI_EXT.1 | FDP_UDF_EXT.1/AO | FDP_UDF_EXT.1/KM | FDP_UDF_EXT.1/VI | FIA_UAU.2 | FIA_UID.2 | FMT_MOF.1 | FMT_SMF.1 | FMT_SMR.1 | FPT_FLS_EXT.1 | FPT_NTA_EXT.1 | FPT_PHP.1 | FPT_PHP.3 | FPT_STM.1 | FPT_TST.1 | FPT_TST_EXT.1 | FTA_CIN_EXT.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| F1DN104KVM-UN-4 | X | X | X | X | X | X | X | X | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| F1DN204KVM-UN-4 | X | X | X | X | X | X | X | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| F1DN102KVM-UN-4 | X | X | X | X | X | X | X | X | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| F1DN202KVM-UN-4 | X | X | X | X | X | X | X | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| F1DN108KVM-UN-4 | X | X | X | X | X | X | X | X | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| F1DN208KVM-UN-4 | X | X | X | X | X | X | X | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| F1DN116KVM-UN-4 | X | X | X | X | X | X | X | X | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| F1DN008KBD* | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | X |

**Table 22 – Security Functional Requirements and Devices**

*When used with another TOE device, the Belkin 2-4-8 Port Secure KVM USB Keyboard W/Lighting, F1DN008KBD contributes to the enforcement of the specified SFRs. This device is only used with another TOE device.