# Belkin F1DN102MOD-BA-4, F1DN202MOD-BA-4, F1DN104MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4, F1DN102MOD-HH-4, F1DN102MOD-PP-4, F1DN202MOD-HH-4, F1DN202MOD-PP-4, F1DN104MOD-HH-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN204MOD-HH-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4, F1DN104MOD-XX-4, F1DN204MOD-XX-4 Firmware Version 44404-E7E7 Peripheral Sharing Devices

## Security Target

*Doc No: 2346-001-D102*
*Version: 1.2*
*17 July 2026*

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

**Prepared by:**

*Saffire Systems*
*Carmel, IN  46032*

*and*

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

# CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

# 1 SECURITY TARGET INTRODUCTION

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

## 1.1 DOCUMENT ORGANIZATION

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

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

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

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

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

**Section 6, Security Requirements**, specifies the security functional requirements and the security assurance requirements that must be satisfied by the TOE and the IT environment. It also provides a rationale for the selection of security functional and assurance requirements.

**Section 7, TOE Summary Specification**, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

**Section 8, Terminology and Acronyms**, defines the acronyms and terminology used in this ST.

**Section 9, References**, provides a list of documents referenced in this ST.

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

## 1.2 SECURITY TARGET REFERENCE

| | |
|---|---|
| **ST Title:** | Belkin F1DN102MOD-BA-4, F1DN202MOD-BA-4, F1DN104MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4, F1DN102MOD-HH-4, F1DN102MOD-PP-4, F1DN202MOD-HH-4, F1DN202MOD-PP-4, F1DN104MOD-HH-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN204MOD-HH-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4, F1DN104MOD-XX-4, F1DN204MOD-XX-4 Firmware Version 44404-E7E7 Peripheral Sharing Devices Security Target |
| **ST Version:** | 1.2 |
| **ST Date:** | 17 July 2026 |

## 1.3 TOE REFERENCE

| | |
|---|---|
| **TOE Identification:** | Belkin F1DN102MOD-BA-4, F1DN202MOD-BA-4, F1DN104MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4, F1DN102MOD-HH-4, F1DN102MOD-PP-4, F1DN202MOD-HH-4, F1DN202MOD-PP-4, F1DN104MOD-HH-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN204MOD-HH-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4, F1DN104MOD-XX-4, F1DN204MOD-XX-4 Firmware Version 44404-E7E7 Peripheral Sharing Devices |
| **TOE Developer:** | Belkin International, Inc. |
| **TOE Type:** | Peripheral Sharing Device (Other Devices and Systems) |

## 1.4 TOE OVERVIEW

The Belkin Secure Peripheral Sharing Devices are part of the Modular Secure KVM Series product line. These KVMs are modular KVM switches that support keyboard, mouse and video switching only. The units natively support High-Definition Multimedia Interface (HDMI) for switching, but also support the DisplayPort video protocol through the use of proprietary cables. For devices that support DisplayPort, the cables convert the source protocol to HDMI. The cables are considered to be part of the TOE.

A breakdown of the models, base model and cables may be found in Section 1.5.2, below.

### 1.4.1 Security Features

The Belkin Secure Keyboard, Video, Mouse (KVM) Switches allow users to share keyboard, video, and mouse 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 Peripheral Sharing Devices (PSDs):

- 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
    - Various video input protocols are supported:
        - HDMI is supported on the F1DN102MOD-BA-4, F1DN104MOD-BA-4, F1DN202MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4, F1DN102MOD-HH-4, F1DN202MOD-HH-4, F1DN104MOD-HH-4, F1DN204MOD-HH-4, F1DN104MOD-XX-4 and F1DN204MOD-XX-4 models
        - DisplayPort is supported on the F1DN102MOD-BA-4, F1DN104MOD-BA-4, F1DN202MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4, F1DN102MOD-PP-4, F1DN202MOD-PP-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4, F1DN104MOD-XX-4 and F1DN204MOD-XX-4 models
    - Various video peripheral types are supported:
        - DisplayPort peripherals are supported on the F1DN102MOD-BA-4, F1DN104MOD-BA-4, F1DN202MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4, F1DN102MOD-PP-4, F1DN202MOD-PP-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4 models
        - HDMI peripherals are supported on the F1DN102MOD-BA-4, F1DN202MOD-BA-4, F1DN104MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4, F1DN102MOD-HH-4, F1DN202MOD-HH-4, F1DN104MOD-HH-4, F1DN204MOD-HH-4, F1DN104MOD-XX-4 and F1DN204MOD-XX-4 models
- 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

- Hardware Anti-Tampering
  - Special holographic tampering evident labels or fitted moldings are utilized to provide a clear visual indication if the TOE components have 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 an unauthorized data flow through bit-by-bit signaling.

The Host Emulator (HE) module communicates with the user keyboard via the USB protocol and converts user keystrokes 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 keystroke is converted by the selected DE into a bi-directional stream to communicate with the computer.

The TOE is a combined software and hardware TOE. A mapping showing the applicable Security Functional Requirements (SFRs) for each device is included in Table 14.

### 1.4.2 TOE Environment

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

| Component | Description |
|---|---|
| Connected Computers | 2-8 General purpose computers |
| Keyboard | General purpose USB keyboard |
| Mouse | General purpose USB mouse |
| User display | Standard computer display (HDMI 2.0, DisplayPort 1.1, 1.2 or 1.3) |
| Power Supply | 12 Volt Direct Current (VDC) power supply |

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

# 1.5 TOE DESCRIPTION

## 1.5.1 Evaluated Configurations

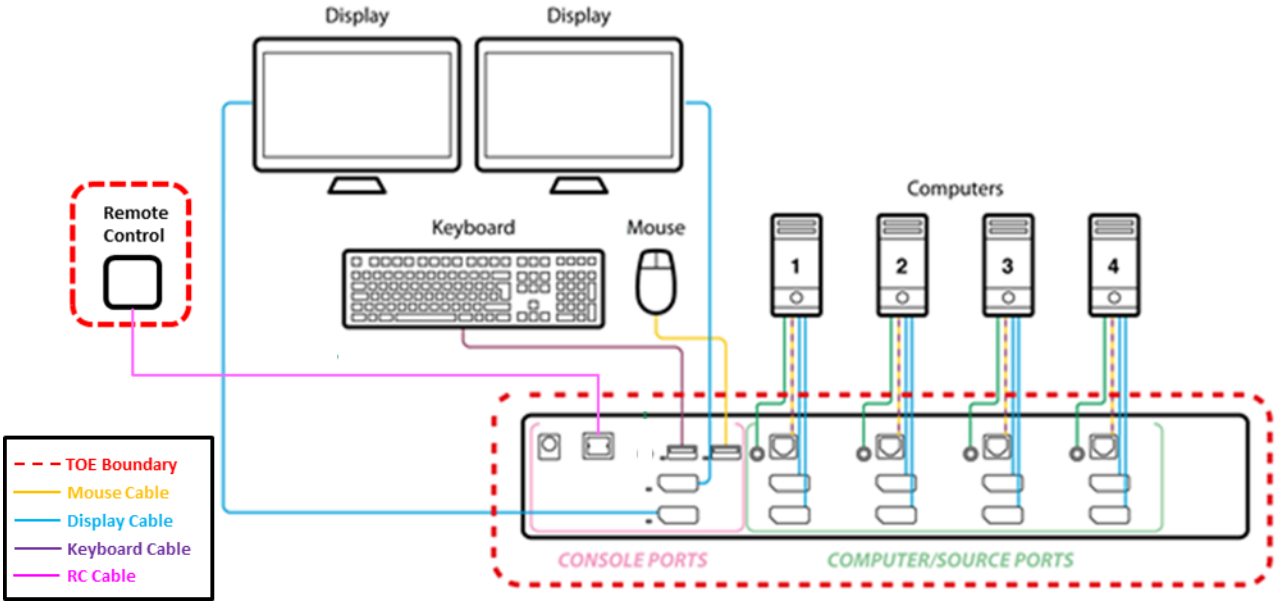


**Figure 1 – KVM Switch Sample Evaluated Configuration**

Figure 1 shows a basic evaluated configuration. The evaluated configuration includes the switch device and the remote control. The switch devices are connected to a keyboard, mouse and up to eight computers. (Note: In the sample evaluated configuration shown above, the TOE can be connected to up to four computers.) The base units support HDMI switching. The devices support HDMI or DisplayPort video input. The video format is converted using proprietary cables purchased with the base unit. One or two displays are supported, and may be DisplayPort or HDMI video output.

The TOE also includes the Console cable (which connects peripherals to the switch) and the Host cables (which connect the computer to the switch). The cables are either provided with the device or are available separately. The HDMI protocol is processed throughout the KVM switches.

## 1.5.2 Physical Scope

The TOE consists of the Belkin Firmware Version 44404-E7E7, one of the remote control devices listed in Table 2, and one of the following hardware options:

- Base model listed in Table 3 with the associated cables listed in Table 4. The base models are compatible with any of the cables listed in Table 4. In this option, the base models and cables are purchased separately. A separate cable is needed for each host. Except for the F1DN104MOD-XX-4 and F1DN204MOD-XX-4 series sets, the video input and video output protocols are the same in the evaluated configuration.
- Modular Secure KVM Series sets (combination of a base model with cables) listed in Table 5.
  Note: The Modular Secure KVM Series Part Number and Modular Secure KVM

Series Set Model are used for purchasing and packaging of the devices. The part number and model number on the devices are the numbers of the base models listed in Table 3 with the associated cables listed in Table 4, not the numbers listed in Table 5.

All of the devices include tamper evident labels and support a keyboard, mouse, video input and video output.

| Description | Part Number | Model |
|---|---|---|
| Belkin Universal 2nd Gen and Modular SKVM/SKM Remote Control 2-Port | CMA19091 | F1DN-MOD-REM2 |
| Belkin Universal 2nd Gen and Modular SKVM/SKM Remote Control 4-Port | CMA19085 | F1DN-MOD-REM4 |
| Belkin Universal 2nd Gen and Modular SKVM/SKM Remote Control 8-Port | CMA28707 | F1DN-MOD-REM8 |

**Table 2 –Remote Control Devices**

| Model Family | Base Model Part Number | Base Model | Video in | Video out | Number of hosts | Number of supported displays |
|---|---|---|---|---|---|---|
| Modular Secure KVM Series KVMs | CGA18717 | F1DN102MOD-BA-4 | Note 1 | Note 1 | 2 | 1 |
| | CGA18715 | F1DN104MOD-BA-4 | Note 1 | Note 1 | 4 | 1 |
| | CGA18718 | F1DN202MOD-BA-4 | Note 1 | Note 1 | 2 | 2 |
| | CGA18247 | F1DN204MOD-BA-4 | Note 1 | Note 1 | 4 | 2 |
| | CGA22661 | F1DN108MOD-BA-4 | Note 1 | Note 1 | 8 | 1 |
| | CGA22662 | F1DN208MOD-BA-4 | Note 1 | Note 1 | 8 | 2 |

**Table 3 – TOE Peripheral Sharing Devices and Features**

Note 1: Video in and video out support depends upon the cables selected for use with the Modular Secure KVM Series base model. Internal switching is performed using HDMI.

The TOE cables connect to the switch using a proprietary connector. Though the KVM has proprietary connectors on the console and peripheral ports, the connections at each port are only for the specific computer or peripheral devices. In other words, there is a separate connector for each computer and a separate connector on the peripheral side. The use of proprietary connectors does not allow unauthorized flows to occur between the connected computers or peripherals. The Console cables have standard video connector(s). The Host cables have standard video connector(s) and a USB connector for the HID.

| Cable Part Number | Cable Model | Description |
|---|---|---|
| CGA22622 | F1DN1MOD-HC-H06 | Modular HDMI Single-Head Host Cable |
| CGA22624 | F1DN1MOD-HC-P06 | Modular DP Single-Head Host Cable |
| CGA22626 | F1DN2MOD-HC-H06 | Modular HDMI Dual-Head Host Cable |
| CGA22628 | F1DN2MOD-HC-P06 | Modular DP Dual-Head Host Cable |
| CGA22623 | F1DN1MOD-CC-H06 | Modular HDMI Single-Head Console Cable |
| CGA22266 | F1DN1MOD-CC-P06 | Modular DP Single-Head Console Cable |
| CGA22627 | F1DN2MOD-CC-H06 | Modular HDMI Dual-Head Console Cable |
| CGA20164 | F1DN2MOD-CC-P06 | Modular DP Dual -Head Console Cable |

**Table 4 – TOE Cables and Features**

Table 5 shows the Modular Secure KVM Series sets included in the evaluation. The HDMI (-HH) and DisplayPort (-PP) models are made up of the Base Unit (BA) and the cables required to support the video protocol. The video in and video out protocols are identified in the Modular Secure KVM Series Model name and Cable Model names. The cables supporting HDMI are denoted with "-H##"; those supporting DisplayPort are denoted with "-P##".

| Modular Secure KVM Series Part Number | Modular Secure KVM Series Set Model | Base Model | Host Cable Model (video in) | Console Cable Model (video out) |
|---|---|---|---|---|
| CGA19157 | F1DN102MOD-HH-4 | F1DN102MOD-BA-4 | F1DN1MOD-HC-H06 | F1DN1MOD-CC-H06 |
| CGA19159 | F1DN102MOD-PP-4 | F1DN102MOD-BA-4 | F1DN1MOD-HC-P06 | F1DN1MOD-CC-P06 |
| CGA19162 | F1DN202MOD-HH-4 | F1DN202MOD-BA-4 | F1DN2MOD-HC-H06 | F1DN2MOD-CC-H06 |
| CGA19164 | F1DN202MOD-PP-4 | F1DN202MOD-BA-4 | F1DN2MOD-HC-P06 | F1DN2MOD-CC-P06 |
| CGA19169 | F1DN104MOD-HH-4 | F1DN104MOD-BA-4 | F1DN1MOD-HC-H06 | F1DN1MOD-CC-H06 |
| CGA19170 | F1DN104MOD-PP-4 | F1DN104MOD-BA-4 | F1DN1MOD-HC-P06 | F1DN1MOD-CC-P06 |
| CGA22318 | F1DN108MOD-PP-4 | F1DN108MOD-BA-4 | F1DN1MOD-HC-P06 | F1DN1MOD-CC-P06 |
| CGA19174 | F1DN204MOD-HH-4 | F1DN204MOD-BA-4 | F1DN2MOD-HC-H06 | F1DN2MOD-CC-H06 |
| CGA19177 | F1DN204MOD-PP-4 | F1DN204MOD-BA-4 | F1DN2MOD-HC-P06 | F1DN2MOD-CC-P06 |
| CGA22319 | F1DN208MOD-PP-4 | F1DN208MOD-BA-4 | F1DN2MOD-HC-P06 | F1DN2MOD-CC-P06 |
| CGA19186 | F1DN104MOD-XX-4 | F1DN104MOD-BA-4 | F1DN1MOD-HC-H06<br>F1DN1MOD-HC-P06 | F1DN1MOD-CC-H06 |
| CGA19187 | F1DN204MOD-XX-4 | F1DN204MOD-BA-4 | F1DN2MOD-HC-H06<br>F1DN2MOD-HC-P06 | F1DN2MOD-CC-H06 |

**Table 5 – Modular Secure KVM Series Set Models and Cables**

#### 1.5.2.1 TOE Delivery

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

#### 1.5.2.2 TOE Guidance

The TOE includes the following guidance documentation:

- Quick Installation Guide 2/4/8 Port Single/Dual-Head Modular Secure KVM Switches, 8820-02949 Rev.J02, HLT28818

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

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

- Belkin F1DN102MOD-BA-4, F1DN202MOD-BA-4, F1DN104MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4, F1DN102MOD-HH-4, F1DN102MOD-PP-4, F1DN202MOD-HH-4, F1DN202MOD-PP-4, F1DN104MOD-HH-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN204MOD-HH-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4, F1DN104MOD-XX-4, F1DN204MOD-XX-4 Firmware Version 44404-E7E7 Peripheral Sharing Devices Common Criteria Guidance Supplement, Version 1.8

### 1.5.3 Logical Scope

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

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

**Table 6 – Logical Scope of the TOE**

# 2 CONFORMANCE CLAIMS

## 2.1 COMMON CRITERIA CONFORMANCE CLAIM

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

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

As follows:

- CC Part 2 extended
- CC Part 3 conformant

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

## 2.2 PP-CONFIGURATION CONFORMANCE CLAIM

This ST claims exact conformance with the National Information Assurance Partnership (NIAP) PP-Configuration for Peripheral Sharing Device Keyboard/Mouse Devices, and Video/Display Devices, Version 1.0, 2019-07-19 [CFG_PSD-KM-VI_V1.0].

This PP-Configuration includes the following components:

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

## 2.3 TECHNICAL DECISIONS

The Technical Decisions in Table 7 apply to the PP and the modules and have been accounted for in the ST and in the evaluation.

| TD | Name | PP affected | Relevant Y/N |
|---|---|---|---|
| TD0506 | Missing Steps to disconnect and reconnect display | [MOD_VI_V1.0] | Y |
| TD0507 | Clarification on USB plug type | [MOD_KM_V1.0] | Y |
| TD0514 | Correction to MOD VI FDP_APC_EXT.1 Test 3 Step 6 | [MOD_VI_V1.0] | Y |
| TD0518 | Typographical errors in dependency Table | [PP_PSD_V4.0] | N<br>FPT_STM.1 is not claimed in the ST |
| TD0539 | Incorrect selection trigger in FTA_CIN_EXT.1 in MOD_VI_V1.0 | [MOD_VI_V1.0] | Y |
| TD0583 | FPT_PHP.3 modified for remote controllers | [PP_PSD_V4.0] | N<br>FPT_PHP.3 is not claimed in the ST |
| TD0584 | Update to FDP_APC_EXT.1 Video Tests | [MOD_VI_V1.0] | Y |
| TD0593 | Equivalency Arguments for PSD | [MOD_KM_V1.0]<br>[MOD_VI_V1.0] | Y |
| TD0681 | PSD purging of EDID data upon disconnect | [MOD_VI_V1.0] | Y |
| TD0686 | DisplayPort CEC Testing | [MOD_VI_V1.0] | Y |
| TD0804 | Clarification regarding Extenders in PSD Evaluations | [PP_PSD_V4.0] | Y |
| TD0842 | Alternate Conversion Option for FDP_IPC_EXT.1 | [MOD_VI_V1.0] | Y |
| TD0844 | Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim | [PP_PSD_V4.0] | N<br>No ALC_FLR SARs are claimed in this ST. |
| TD0942 | Updated EDID Read Requirements | [MOD_VI_V1.0] | Y |
| TD0959 | Correction to Test 4 Step 3 of FDP_APC_EXT.1 | [MOD_KM_V1.0] | Y |

**Table 7 – Applicable Technical Decisions**

## 2.4 PACKAGE CLAIM

This Security Target does not claim conformance with any package.

## 2.5 CONFORMANCE RATIONALE

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

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

# 3 SECURITY PROBLEM DEFINITION

## 3.1 THREATS

Table 8 lists the threats described in Section 3.1 of the [PP_PSD_V4.0]. Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

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

[1] Peripheral Sharing Device

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

**Table 8 – Threats**

## 3.2 ORGANIZATIONAL SECURITY POLICIES

There are no Organizational Security Policies applicable to this TOE.

## 3.3 ASSUMPTIONS

Table 9 lists the assumptions described in Section 3.2 of the [PP_PSD_V4.0] and Section 3.2 of the [MOD_VI_V1.0]. The assumptions required to ensure the security of the TOE are listed in Table 9.

| Assumptions | Description |
|---|---|
| **A.NO_TEMPEST** | Computers and peripheral devices connected to the PSD are not TEMPEST approved.<br>ST Note: The TSF may or may not isolate the ground of the keyboard and mouse computer interfaces (the USB ground). The Operational Environment is assumed not to support TEMPEST red-black ground isolation. |
| **A.PHYSICAL** | The environment provides physical security commensurate with the value of the TOE and the data it processes and contains. |
| **A.NO_WIRELESS_DEVICES** | The environment includes no wireless peripheral devices. |
| **A.TRUSTED_ADMIN** | PSD Administrators and users are trusted to follow and apply all guidance in a trusted manner. |
| **A.TRUSTED_CONFIG** | Personnel configuring the PSD and its operational environment follow the applicable security configuration guidance. |
| **A.USER_ALLOWED_ACCESS** | All PSD users are allowed to interact with all connected computers. It is not the role of the PSD to prevent or otherwise control user access to connected computers. Computers or their connected network shall have the required means to authenticate the user and to control access to their various resources. |

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

**Table 9 – 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:<table><tr><td>MOD_VI</td><td>FDP_APC_EXT.1/VI, FDP_PDC_EXT.1</td></tr><tr><td>MOD_KM</td><td>FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1, FDP_SWI_EXT.3</td></tr></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:<table><tr><td>MOD_VI</td><td>FDP_APC_EXT.1/VI, FDP_PDC_EXT.1</td></tr><tr><td>MOD_KM</td><td>FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1, FDP_SWI_EXT.3</td></tr></table></td></tr>
<tr><td>O.USER_DATA<br>_ISOLATION</td><td>The PSD shall route user data, such as keyboard entries, only to the computer selected by the user. The PSD shall provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.<br>Addressed by:<table><tr><td>MOD_VI</td><td>FDP_APC_EXT.1/VI, FDP_PDC_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_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.NO_USER _DATA_RETENTION</td><td>The PSD shall not retain user data in non-volatile memory after power up or, if supported, factory reset.<br>Addressed by:<table><tr><td>PP_PSD</td><td>FDP_RIP_EXT.1</td></tr><tr><td>MOD_KM</td><td>FDP_RIP.1/KM</td></tr></table></td></tr>
<tr><td>O.NO_OTHER _EXTERNAL _INTERFACES</td><td>The PSD shall not have any external interfaces other than those implemented by the TSF.<br>Addressed by:<table><tr><td>PP_PSD</td><td>FDP_PDC_EXT.1</td></tr></table></td></tr>
<tr><td>O.LEAK _PREVENTION _SWITCHING</td><td>The PSD shall ensure that there are no switching mechanisms that allow signal data leakage between connected computers.<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 _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>FDP_SWI_EXT.1, FDP_SWI_EXT.2, FTA_CIN_EXT.1</td></tr></table></td></tr>
</table>

| Security Objective | Description |
|---|---|
| | MOD_VI: FDP_CDS_EXT.1(1), FDP_CDS_EXT.1(2), FTA_CIN_EXT.1<br>MOD_KM: FDP_FIL_EXT.1/KM |
| **O.PERIPHERAL _PORTS_ISOLATION** | The PSD shall ensure that data does not flow between peripheral devices connected to different PSD interfaces.<br>Addressed by:<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.REJECT _UNAUTHORIZED _PERIPHERAL** | The PSD shall reject unauthorized peripheral device types and protocols.<br>Addressed by:<br>PP_PSD: FDP_PDC_EXT.1<br>MOD_VI: FDP_PDC_EXT.2/VI, FDP_PDC_EXT.3/VI(1-3), FDP_IPC_EXT.1(1-3), FDP_SPR_EXT.1/DP, FDP_SPR_EXT.1/HDMI<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, FDP_PDC_EXT.2/KM, FDP_PDC_EXT.3/KM |
| **O.REJECT _UNAUTHORIZED _ENDPOINTS** | The PSD shall reject unauthorized peripheral devices connected via a Universal Serial Bus (USB) hub.<br>Addressed by:<br>PP_PSD: 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_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 |

| Security Objective | Description |
|---|---|
| **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 |
| **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 |
| **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 |

| Security Objective | Description |
|---|---|
| **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.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 10 – 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. |

| Security Objective | Description |
|---|---|
| **OE.NO_WIRELESS_DEVICES** | The operational environment will not include wireless keyboards, mice, audio, user authentication, or video devices. |
| **OE.TRUSTED_ADMIN** | The operational environment will ensure that trusted PSD Administrators and users are appropriately trained. |
| **OE.TRUSTED_CONFIG** | The operational environment will ensure that administrators configuring the PSD and its operational environment follow the applicable security configuration guidance. |
| **OE.NO_SPECIAL_ANALOG _CAPABILITIES** | The operational environment will not have special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, or a component with digital signal processing or analog video capture functions. |

**Table 11 – Security Objectives for the Operational Environment**

## 4.3 SECURITY OBJECTIVES RATIONALE

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

| Threat or Assumption | Security Objective(s) | Rationale |
|---|---|---|
| T.DATA_LEAK | O.COMPUTER _INTERFACE _ISOLATION | Isolation of computer interfaces prevents data from leaking between them without authorization. |
| | O.COMPUTER _INTERFACE _ISOLATION _TOE_UNPOWERED | Maintaining interface isolation while the TOE is in an unpowered state ensures that data cannot leak between computer interfaces. |
| | O.USER_DATA _ISOLATION | The TOE's routing of data only to the selected computer ensures that it will not leak to any others. |
| | O.NO_OTHER _EXTERNAL _INTERFACES | The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked. |
| | O.PERIPHERAL_PORTS _ISOLATION | Isolation of peripheral ports prevents data from leaking between them without authorization. |
| | O.UNIDIRECTIONAL _INPUT | The TOE's enforcement of unidirectional input for |

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

| Threat or Assumption | Security Objective(s) | Rationale |
|---|---|---|
| | | connected computer through this interface. |
| 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. |
| T.UNINTENDED _USE | O.AUTHORIZED _USAGE | The TOE's support for only switching mechanisms that require explicit user action to engage ensures that a user has sufficient information to avoid interacting with an unintended computer. |
| T.UNAUTHORIZED _DEVICES | O.REJECT _UNAUTHORIZED _ENDPOINTS | The TOE's ability to reject unauthorized endpoints mitigates the threat of unauthorized devices being used to communicate with connected computers. |
| | O.REJECT _UNAUTHORIZED _PERIPHERAL | The TOE's ability to reject unauthorized peripherals mitigates the threat of unauthorized devices being used to communicate with connected computers. |
| | O.EMULATED_INPUT | The TOE's emulation of keyboard/mouse data input ensures that a connected computer will only receive this specific type of data through a connected peripheral. |
| | O.UNIDIRECTIONAL _VIDEO | The TOE's limitation of supported video protocol interfaces prevents the connection of unauthorized devices. |
| T.LOGICAL _TAMPER | O.NO_TOE_ACCESS | The TOE's prevention of logical access to its firmware, software, and memory mitigates the threat of logical tampering. |
| | O.EMULATED_INPUT | The TOE's emulation of keyboard/mouse data input prevents logical tampering of the TSF ensuring that only known inputs to it are supported. |

| Threat or Assumption | Security Objective(s) | Rationale |
|---|---|---|
| T.PHYSICAL _TAMPER | O.ANTI_TAMPERING | The TOE mitigates the threat of physical tampering through use of an enclosure that provides tamper detection functionality. |
| | O.TAMPER_EVIDENT _LABEL | The TOE mitigates the threat of physical tampering through use of tamper evident labels that reveal physical tampering attempts. |
| T.REPLACEMENT | O.TAMPER_EVIDENT _LABEL | The TOE's use of a tamper evident label that provides authenticity of the device mitigates the threat that it is substituted for a replacement device during the acquisition process. |
| T.FAILED | O.SELF_TEST | The TOE mitigates the threat of failures leading to compromise of security functions through self-tests of its own functionality. |
| | O.SELF_TEST_FAIL _TOE_DISABLE | The TOE mitigates the threat of failures leading to compromise of security functions by disabling all data flows in the event a failure is detected. |
| | O.SELF_TEST_FAIL _INDICATION | The TOE mitigates the threat of failures leading to compromise of security functions by providing users with a clear indication when it is in a failure state and should not be trusted. |
| 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. |
| 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. |

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

**Table 12 – Security Objectives Rationale**

# 5 EXTENDED COMPONENTS DEFINITION

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

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

| Functional Class | Functional Families | Protection Profile Modules |
|---|---|---|
| User Data Protection (FDP) | FDP_APC_EXT Active PSD Connections | [PP_PSD_V4.0] [MOD_KM_V1.0] [MOD_VI_V1.0] |
| | FDP_CDS_EXT Connected Displays Supported | [MOD_VI_V1.0] |
| | FDP_FIL_EXT Device Filtering | [MOD_KM_V1.0] |
| | FDP_IPC_EXT Internal Protocol Conversion | [MOD_VI_V1.0] |
| | FDP_PDC_EXT Peripheral Device Connection | [PP_PSD_V4.0] [MOD_VI_V1.0] [MOD_KM_V1.0] |
| | FDP_RDR_EXT Re-Enumeration Device Rejection | [MOD_KM_V1.0] |
| | FDP_RIP_EXT Residual Information Protection | [PP_PSD_V4.0] |
| | FDP_SPR_EXT Sub-Protocol Rules | [MOD_VI_V1.0] |
| | FDP_SWI_EXT PSD Switching | [PP_PSD_V4.0] [MOD_KM_V1.0] |
| | FDP_UDF_EXT Unidirectional Data Flow | [MOD_VI_V1.0] [MOD_KM_V1.0] |
| Protection of the TSF (FPT) | FPT_FLS_EXT Failure with Preservation of Secure State | [PP_PSD_V4.0] |
| | FPT_NTA_EXT No Access to TOE | [PP_PSD_V4.0] |
| | FPT_TST_EXT TSF Testing | [PP_PSD_V4.0] |
| TOE Access (FTA) | FTA_CIN_EXT Continuous Indications | [PP_PSD_V4.0] [MOD_VI_V1.0] |

**Table 13 – Functional Families of Extended Components**

# 6 SECURITY REQUIREMENTS

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

## 6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. This is defined as:

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

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

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

## 6.2 SECURITY FUNCTIONAL REQUIREMENTS

Section 6.2 details the security functional requirements.

| Class | Identifier | Name | Source | Applicable Devices |
|---|---|---|---|---|
| User Data Protection (FDP) | FDP_APC_EXT.1/KM | Active PSD Connections | [MOD_KM_V1.0] | All |
| | FDP_APC_EXT.1/VI | Active PSD Connections | [MOD_VI_V1.0] | All |
| | FDP_CDS_EXT.1(1) | Connected Displays Supported (1) | [MOD_VI_V1.0] | F1DN102MOD-BA-4, F1DN104MOD-BA-4, F1DN108MOD-BA-4, F1DN102MOD-HH-4, F1DN102MOD-PP-4, F1DN104MOD-HH-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN104MOD-XX-4 |

| Class | Identifier | Name | Source | Applicable Devices |
|---|---|---|---|---|
| | FDP_CDS_EXT.1(2) | Connected Displays Supported (2) | [MOD_VI_V1.0] | F1DN202MOD-BA-4, F1DN204MOD-BA-4, F1DN208MOD-BA-4, F1DN202MOD-HH-4, F1DN202MOD-PP-4, F1DN204MOD-HH-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4, F1DN204MOD-XX-4 |
| | FDP_FIL_EXT.1/KM | Device Filtering (Keyboard/ Mouse) | [MOD_KM_V1.0] | All |
| | FDP_IPC_EXT.1(1) | Internal Protocol Conversion (1) | [MOD_VI_V1.0] | F1DN102MOD-PP-4, F1DN202MOD-PP-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4 |
| | FDP_IPC_EXT.1(2) | Internal Protocol Conversion (2) | [MOD_VI_V1.0] | F1DN104MOD-XX-4, F1DN204MOD-XX-4 |
| | FDP_IPC_EXT.1(3) | Internal Protocol Conversion (3) | [MOD_VI_V1.0] | F1DN102MOD-BA-4, F1DN202MOD-BA-4, F1DN104MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4 |
| | FDP_PDC_EXT.1 | Peripheral Device Connection | [PP_PSD_V4.0] [MOD_VI_V1.0][2] [MOD_KM_V1.0][3] | All |
| | FDP_PDC_EXT.2/KM | Authorized Devices (Keyboard/ Mouse) | [MOD_KM_V1.0] | All |

[2] 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.

[3] 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.

| Class | Identifier | Name | Source | Applicable Devices |
|---|---|---|---|---|
| | FDP_PDC_EXT.2/VI | Authorized Devices (Video Output) | [MOD_VI_V1.0] | All |
| | FDP_PDC_EXT.3/KM | Authorized Connection Protocols (Keyboard/ Mouse) | [MOD_KM_V1.0] | All |
| | FDP_PDC_EXT.3/VI(1) | Authorized Connection Protocols (Video Output) (1) | [MOD_VI_V1.0] | F1DN102MOD-HH-4, F1DN202MOD-HH-4, F1DN104MOD-HH-4, F1DN204MOD-HH-4 |
| | FDP_PDC_EXT.3/VI(2) | Authorized Connection Protocols (Video Output)(2) | [MOD_VI_V1.0] | F1DN102MOD-PP-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN202MOD-PP-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4 |
| | FDP_PDC_EXT.3/VI(3) | Authorized Connection Protocols (Video Output) (3) | [MOD_VI_V1.0] | F1DN102MOD-BA-4, F1DN202MOD-BA-4, F1DN104MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4, F1DN104MOD-XX-4, F1DN204MOD-XX-4 |
| | FDP_RDR_EXT.1 | Re-Enumeration Device Rejection | [MOD_KM_V1.0] | All |
| | FDP_RIP.1/KM | Residual Information Protection (Keyboard Data) | [MOD_KM_V1.0] | All |
| | FDP_RIP_EXT.1 | Residual Information Protection | [PP_PSD_V4.0] | All |

| Class | Identifier | Name | Source | Applicable Devices |
|---|---|---|---|---|
| | FDP_SPR_EXT.1/DP | Sub-Protocol Rules (DisplayPort Protocol) | [MOD_VI_V1.0] | F1DN102MOD-BA-4, F1DN104MOD-BA-4, F1DN202MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4, F1DN102MOD-PP-4, F1DN202MOD-PP-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4, F1DN104MOD-XX-4, F1DN204MOD-XX-4 |
| | FDP_SPR_EXT.1/HDMI | Sub-Protocol Rules (HDMI Protocol) | [MOD_VI_V1.0] | F1DN102MOD-BA-4, F1DN104MOD-BA-4, F1DN202MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4, F1DN102MOD-HH-4, F1DN202MOD-HH-4, F1DN104MOD-HH-4, F1DN204MOD-HH-4, F1DN104MOD-XX-4, F1DN204MOD-XX-4 |
| | FDP_SWI_EXT.1 | PSD Switching | [PP_PSD_V4.0] | All |
| | FDP_SWI_EXT.2 | PSD Switching Methods | [PP_PSD_V4.0] [MOD_KM_V1.0][4] | All |
| | FDP_SWI_EXT.3 | Tied Switching | [MOD_KM_V1.0] | All |
| | FDP_UDF_EXT.1/KM | Unidirectional Data Flow (Keyboard/ Mouse) | [MOD_KM_V1.0] | All |
| | FDP_UDF_EXT.1/VI | Unidirectional Data Flow (Video Output) | [MOD_VI_V1.0] | All |

[4] There is no modification to this SFR in [MOD_KM_V1.0]; however, additional evaluation activities are triggered by the selections in FDP_SWI_EXT.2.2.

| Class | Identifier | Name | Source | Applicable Devices |
|---|---|---|---|---|
| Protection of the TSF (FPT) | FPT_FLS_EXT.1 | Failure with Preservation of Secure State | [PP_PSD_V4.0] | All |
| | FPT_NTA_EXT.1 | No Access to TOE | [PP_PSD_V4.0] | All |
| | FPT_PHP.1 | Passive Detection of Physical Attack | [PP_PSD_V4.0] | All |
| | FPT_TST.1 | TSF testing | [PP_PSD_V4.0] | All |
| | FPT_TST_EXT.1 | TSF Testing | [PP_PSD_V4.0] | All |
| TOE Access (FTA) | FTA_CIN_EXT.1 | Continuous Indications | [PP_PSD_V4.0] [MOD_VI_V1.0] | All |

**Table 14 – Summary of Security Functional Requirements**

## 6.2.1 User Data Protection (FDP)

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

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

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

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

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

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

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

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

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

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

#### 6.2.1.3 FDP_CDS_EXT.1(1) Connected Displays Supported (1)

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

Application Note: FDP_CDS_EXT.1(1) applies to the following model: F1DN102MOD-BA-4, F1DN104MOD-BA-4, F1DN108MOD-BA-4, F1DN102MOD-HH-4, F1DN102MOD-PP-4, F1DN104MOD-HH-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN104MOD-XX-4.

#### 6.2.1.4 FDP_CDS_EXT.1(2) Connected Displays Supported (2)

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

Application Note: FDP_CDS_EXT.1(2) applies to the following models: F1DN202MOD-BA-4, F1DN204MOD-BA-4, F1DN208MOD-BA-4, F1DN202MOD-HH-4, F1DN202MOD-PP-4, F1DN204MOD-HH-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4, F1DN204MOD-XX-4.

#### 6.2.1.5 FDP_FIL_EXT.1/KM Device Filtering (Keyboard/Mouse)

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

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

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

#### 6.2.1.6 FDP_IPC_EXT.1(1) Internal Protocol Conversion (1)

**FDP_IPC_EXT.1.1(1)** The TSF shall convert the DisplayPort protocol at the *DisplayPort peripheral display interface(s), DisplayPort computer video interface* into the *HDMI* protocol within the TOE.

**FDP_IPC_EXT.1.2(1)** The TSF shall output the *HDMI* protocol from inside the TOE to *computer video interface, peripheral display interface(s)* as *DisplayPort protocol*.

Application Note: FDP_IPC_EXT.1(1) applies to the following models: F1DN102MOD-PP-4, F1DN202MOD-PP-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4.

TD0842 applies to this SFR definition.

#### 6.2.1.7 FDP_IPC_EXT.1(2) Internal Protocol Conversion (2)

**FDP_IPC_EXT.1.1(2)** The TSF shall convert the DisplayPort protocol at the *DisplayPort computer video interface* into the *HDMI* protocol within the TOE.

**FDP_IPC_EXT.1.2(2)** The TSF shall output the *HDMI* protocol from inside the TOE to peripheral display interface(s) as *HDMI protocol*.

Application Note: FDP_IPC_EXT.1(2) applies to the following models: F1DN104MOD-XX-4, F1DN204MOD-XX-4.

TD0842 applies to this SFR definition.

### 6.2.1.8 FDP_IPC_EXT.1(3) Internal Protocol Conversion (3)

**FDP_IPC_EXT.1.1(3)** The TSF shall convert the DisplayPort protocol at the *DisplayPort peripheral display interface(s), DisplayPort computer video interface* into the *HDMI* protocol within the TOE.

**FDP_IPC_EXT.1.2(3)** The TSF shall output the *HDMI* protocol from inside the TOE to peripheral display interface(s) as *DisplayPort protocol, HDMI protocol*.

Application Note: FDP_IPC_EXT.1(3) applies to the following models: F1DN102MOD-BA-4, F1DN202MOD-BA-4, F1DN104MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4. For the base models, mixed cables can be used.
TD0842 applies to this SFR definition.

### 6.2.1.9 FDP_PDC_EXT.1 Peripheral Device Connection

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

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

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

**FDP_PDC_EXT.1.4** The TOE shall not have wireless interfaces.

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

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

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

- *authorized devices as defined in the PP-Module for Video/Display Devices*

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

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

- *authorized devices presenting authorized interface protocols as defined in the PP-Module for Video/Display Devices*

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

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

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

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

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

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

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

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

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

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

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

### 6.2.1.13 FDP_PDC_EXT.3/VI(1) Authorized Connection Protocols (Video Output) (1)

**FDP_PDC_EXT.3.1/VI(1)** The TSF shall have interfaces for the *HDMI* protocols.

**FDP_PDC_EXT.3.2/VI(1)** The TSF shall apply the following rules to the supported protocols: *the TSF shall read the connected display EDID information once during power-on or reboot automatically*.

Application Note: TD0942 applies to this SFR definition.

Application Note: FDP_PDC_EXT.3/VI(1) applies to the following models: F1DN102MOD-HH-4, F1DN202MOD-HH-4, F1DN104MOD-HH-4, F1DN204MOD-HH-4.

### 6.2.1.14 FDP_PDC_EXT.3/VI(2) Authorized Connection Protocols (Video Output) (2)

**FDP_PDC_EXT.3.1/VI(2)** The TSF shall have interfaces for the *DisplayPort* protocols.

**FDP_PDC_EXT.3.2/VI(2)** The TSF shall apply the following rules to the supported protocols: *the TSF shall read the connected display EDID information once during power-on or reboot automatically*.

Application Note: TD0942 applies to this SFR definition.

Application Note: FDP_PDC_EXT.3/VI(2) applies to the following models: F1DN102MOD-PP-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN202MOD-PP-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4.

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

**FDP_PDC_EXT.3.1/VI(3)** The TSF shall have interfaces for the *HDMI, DisplayPort* protocols.

**FDP_PDC_EXT.3.2/VI(3)** The TSF shall apply the following rules to the supported protocols: *the TSF shall read the connected display EDID information once during power-on or reboot automatically*.

Application Note: TD0942 applies to this SFR definition.

Application Note: FDP_PDC_EXT.3/VI(3) applies to the following models: F1DN102MOD-BA-4, F1DN202MOD-BA-4, F1DN104MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4, F1DN104MOD-XX-4, F1DN204MOD-XX-4.

#### 6.2.1.16 FDP_RDR_EXT.1 Re-Enumeration Device Rejection

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

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

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

#### 6.2.1.18 FDP_RIP_EXT.1 Residual Information Protection

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

#### 6.2.1.19 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,
  - Link Training.

Application Note: FDP_SPR_EXT.1/DP applies to the following models: F1DN102MOD-BA-4, F1DN104MOD-BA-4, F1DN202MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4, F1DN102MOD-PP-4,

F1DN202MOD-PP-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4, F1DN104MOD-XX-4, F1DN204MOD-XX-4.

### 6.2.1.20 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.

Application Note: FDP_SPR_EXT.1/HDMI applies to the following models: F1DN102MOD-BA-4, F1DN104MOD-BA-4, F1DN202MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4, F1DN102MOD-HH-4, F1DN202MOD-HH-4, F1DN104MOD-HH-4, F1DN204MOD-HH-4, F1DN104MOD-XX-4, F1DN204MOD-XX-4.

### 6.2.1.21 FDP_SWI_EXT.1 PSD Switching

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

### 6.2.1.22 FDP_SWI_EXT.2 PSD Switching Methods

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

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

### 6.2.1.23 FDP_SWI_EXT.3 Tied Switching

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

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

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

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

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

### 6.2.2 Protection of the TSF (FPT)

#### 6.2.2.1 FPT_FLS_EXT.1 Failure with Preservation of Secure State

**FPT_FLS_EXT.1.1** The TSF shall preserve a secure state when the following types of failures occur: failure of the power-on self-test and *no other failures*.

#### 6.2.2.2 FPT_NTA_EXT.1 No Access to TOE

**FPT_NTA_EXT.1.1** TOE firmware, software, and memory shall not be accessible via the TOE's external ports, with the following exceptions: *the Extended Display Identification Data (EDID) memory of Video TOEs may be accessible from connected computers*.

#### 6.2.2.3 FPT_PHP.1 Passive Detection of Physical Attack

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

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

#### 6.2.2.4 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 *no other functions*.

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

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

#### 6.2.2.5 FPT_TST_EXT.1 TSF Testing

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

### 6.2.3 TOE Access (FTA)

#### 6.2.3.1 FTA_CIN_EXT.1 Continuous Indications

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

**FTA_CIN_EXT.1.2** The TSF shall implement the visible indication using the following mechanism: easily visible graphical and/or textual markings of each source video on the display, ***illuminated buttons***.

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

## 6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 15.

| 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 |

| Assurance Class | Assurance Components | |
|---|---|---|
| | **Identifier** | **Name** |
| Vulnerability Assessment (AVA) | AVA_VAN.1 | Vulnerability Survey |

**Table 15 – Security Assurance Requirements**

# 6.4 SECURITY REQUIREMENTS RATIONALE

## 6.4.1 Security Functional Requirements Rationale

Table 10 provides a mapping between the SFRs and Security Objectives.

## 6.4.2 Dependency Rationale

Table 16 identifies the Security Functional Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

| SFR | Dependencies | Rationale Statement |
|---|---|---|
| FDP_APC_EXT.1/KM | None | N/A |
| FDP_APC_EXT.1/VI | None | N/A |
| FDP_CDS_EXT.1(1), (2) | None | N/A |
| FDP_FIL_EXT.1/KM | FDP_PDC_EXT.1 | Included |
| FDP_IPC_EXT.1(1), (2), (3) | FDP_PDC_EXT.2 | Included |
| FDP_PDC_EXT.1 | None | N/A |
| FDP_PDC_EXT.2/KM | FDP_PDC_EXT.1 | Included |
| FDP_PDC_EXT.2/VI | FDP_PDC_EXT.1 | Included |
| FDP_PDC_EXT.3/KM | FDP_PDC_EXT.1 | Included |
| FDP_PDC_EXT.3/VI(1), (2), (3) | FDP_PDC_EXT.1 | Included |
| FDP_RDR_EXT.1 | FDP_PDC_EXT.1 | Included |
| FDP_RIP_EXT.1 | None | N/A |
| FDP_RIP.1/KM | 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 |

| SFR | Dependencies | Rationale Statement |
|---|---|---|
| FDP_SWI_EXT.2 | FDP_SWI_EXT.1 | Included |
| FDP_SWI_EXT.3 | FDP_SWI_EXT.1 | Included |
| FDP_UDF_EXT.1/KM | FDP_APC_EXT.1 | Included |
| FDP_UDF_EXT.1/VI | FDP_APC_EXT.1 | Included |
| FPT_FLS_EXT.1 | FPT_TST.1<br>FPT_PHP.3 | Included<br>Included only if anti-tamper is selected in FPT_FLS_EXT.1.1 |
| FPT_NTA_EXT.1 | None | N/A |
| FPT_PHP.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 16 – Functional Requirement Dependencies**

### 6.4.3 Security Assurance Requirements Rationale

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

# 7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions of the TOE that meet the TOE security requirements claimed in Section 6.2.

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

Unless otherwise stated, the description applies to all devices.

## 7.1 USER DATA PROTECTION

### 7.1.1 System Controller

Each device includes a System Controller which is responsible for device management, user interaction, system control security functions, and device monitoring. It receives user input from the switches on the top panel or remote control and drives the TOE channel select lines that control switching circuits within the TOE. Both the Host Emulator and the Video Controller are independent modules that are included in the System Controller.

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 video controller module that controls the relevant multiplexer.

The user determines the host computer to be connected to the peripherals by pressing a button on the switch top panel or by selecting a channel on the remote control. Switching can only be initiated through express user action and not through automated port scanning, connected computer control, or keyboard shortcuts.

When the remote control device is used, both the switch top panel button and the remote's channel indicator for the selected computer is illuminated. These are always consistent.

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

#### 7.1.1.1 Active PSD Connections

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

The TOE ensures that no electrical signal flows between the connected computers. No data or electrical signal transits the TOE when the TOE is powered off or when the TOE is in a failure state. A failure state occurs when the TOE fails a self-test when powering on.

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

#### 7.1.1.2 Connected Computer Interfaces

The connected computers are attached to the TOE (peripheral sharing switch and video cable(s)) as follows:

- The switch connects to the keyboard and mouse port using a USB A cable.
- The switch is connected to the computer video port using a video cable supporting DisplayPort or HDMI.

There are no wireless interfaces or additional external interfaces.

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

#### 7.1.1.3 Residual Information Protection

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

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

### 7.1.2 Keyboard and Mouse Functionality

#### 7.1.2.1 Keyboard and Mouse Enumeration

The TOE determines whether a peripheral device that has been plugged into the keyboard and mouse peripheral USB ports is allowed to operate with the TOE.

The TOE uses optical data diodes to enforce a unidirectional data flow from the user peripherals to the coupled hosts and uses isolated device emulators to prevent data leakage through the peripheral switching circuitry.

The Static Random Access Memory (SRAM) in the host and device emulator circuitry stores USB Host stack parameters and up to the last 4 key codes. User data may be briefly retained; however, there are no data buffers. Data is erased during power off of the peripheral sharing device, and when the user switches channels. When the TOE switches from one computer to another, the system controller (SC) 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 (KBD) microcontroller (mCU) is not passed to the newly selected computer.

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

A USB keyboard is connected to the TOE keyboard host emulator module through the console keyboard port. The keyboard host emulator module is an independent module in the System Controller 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 module into a proprietary

protocol data stream that is combined with the data stream from the mouse host emulator module.

Similarly, the USB mouse is connected to the TOE mouse host emulator module through the console USB mouse port. The mouse host emulator module is an independent module in the System Controller 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 module into a proprietary protocol data stream that is combined with the data stream from the keyboard host emulator module.

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

#### 7.1.2.2 Keyboard and Mouse Switching Functionality

A Host Emulator (HE) module communicates with the user keyboard via the USB protocol. The HE module converts user keystrokes into unidirectional serial data.

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, routed to the specific host channel device emulator, and then to the port that is connected to the host computer. The optical data diode is an opto-coupler designed to physically prevent reverse data flow. The keyboard and mouse can only be switched together.

Device emulators 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 top panel.

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

#### 7.1.2.3 Keyboard and Mouse Compatible Device Types

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

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

#### 7.1.2.4 Re-Enumeration Device Rejection

If a connected device attempts to re-enumerate as a different USB device type, it will be rejected by the TOE. The TOE will reject devices which are not allowed at any time during operation and start-up. This is indicated by a Light Emitting Diode (LED) on the TOE next to the Keyboard and mouse ports. This LED shows a solid green light for an accepted device, flickering green during enumeration, and a solid red light for a rejected device

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

### 7.1.3 Video Switching Functionality

Video data flow is comprised of unidirectional Extended Display Identification Data (EDID) and video data flow paths. Figure 2 shows a data flow during the display EDID read function.

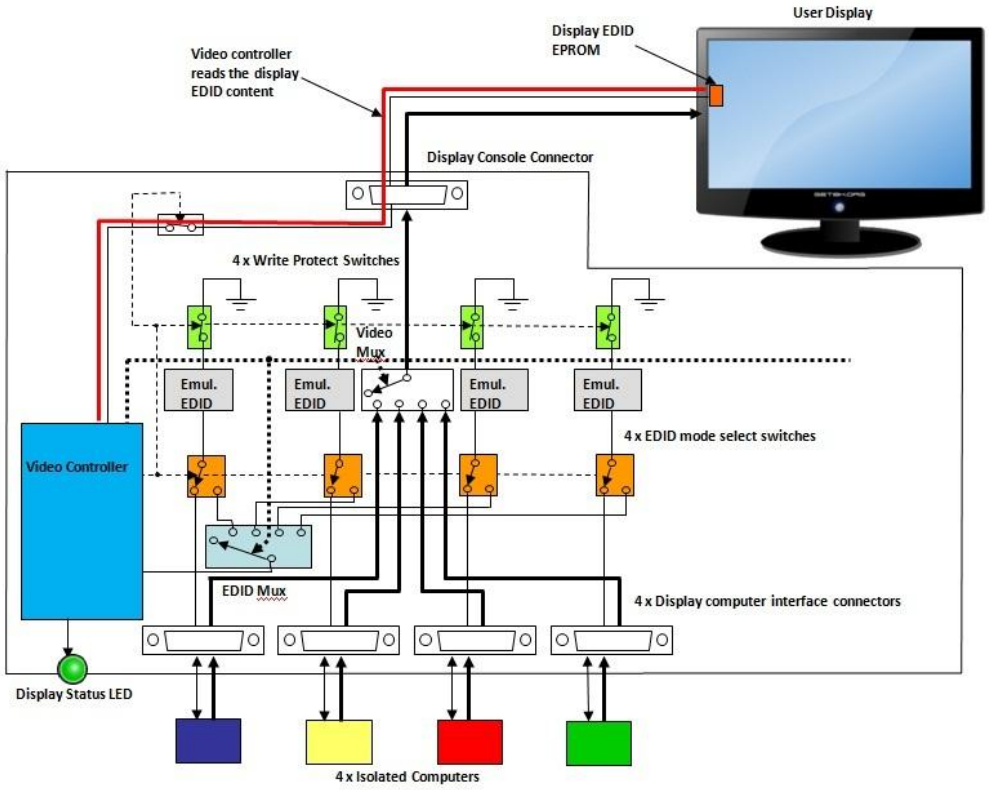


**Figure 2 – Display EDID Read Function**

For each connected display, an EDID read event only occurs as the TOE is being powered up. The video controller module 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.

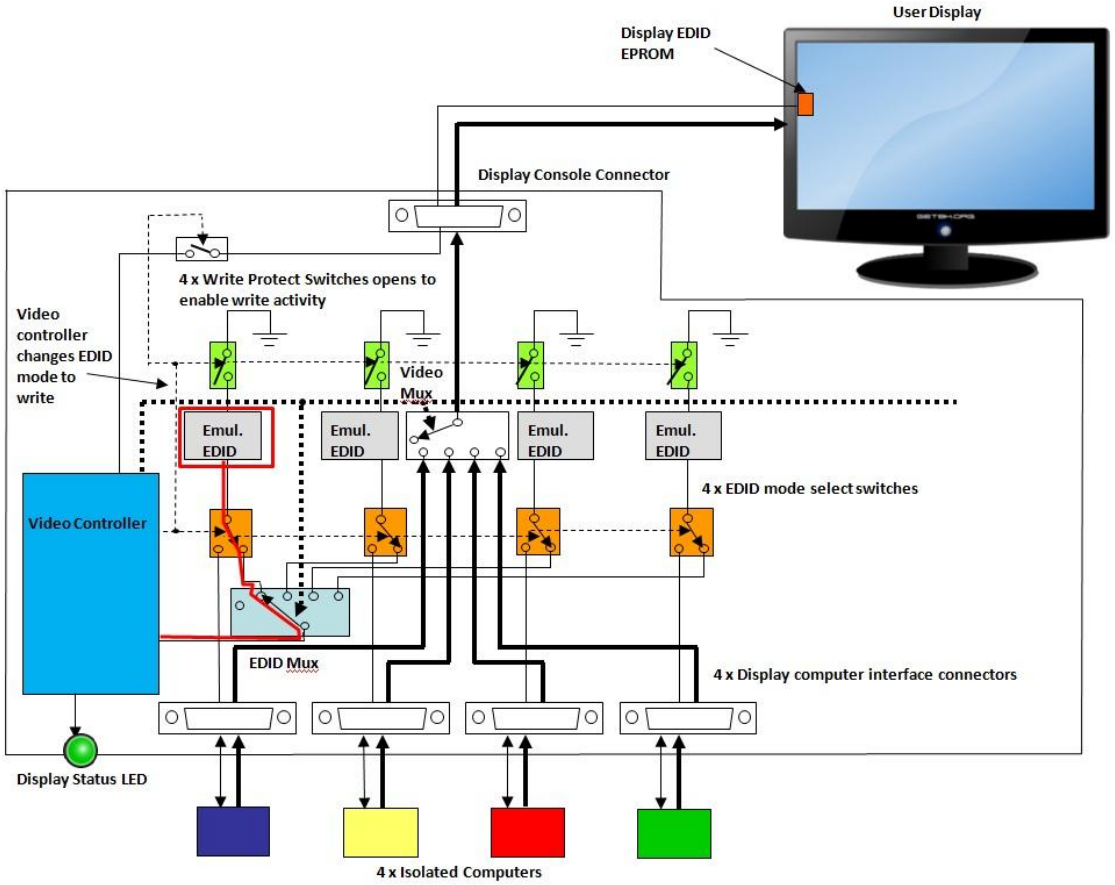


**Figure 3 – Display EDID Write Function**

Figure 3 illustrates the video controller module (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 I2C lines to the first emulated EDID EEPROM chip (shown in gray). The write protect switch (shown in green) opens to enable writing. The video controller module uses the I2C lines to write to the first emulated EDID EEPROM chip. Once the write operation is complete and verified, the video controller module switches the EDID multiplexer to the next channel and the operation repeats until all EDID EEPROM chips are programmed. Once the write operation is complete, the video controller module switches to normal operating mode, as shown in Figure 4 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.

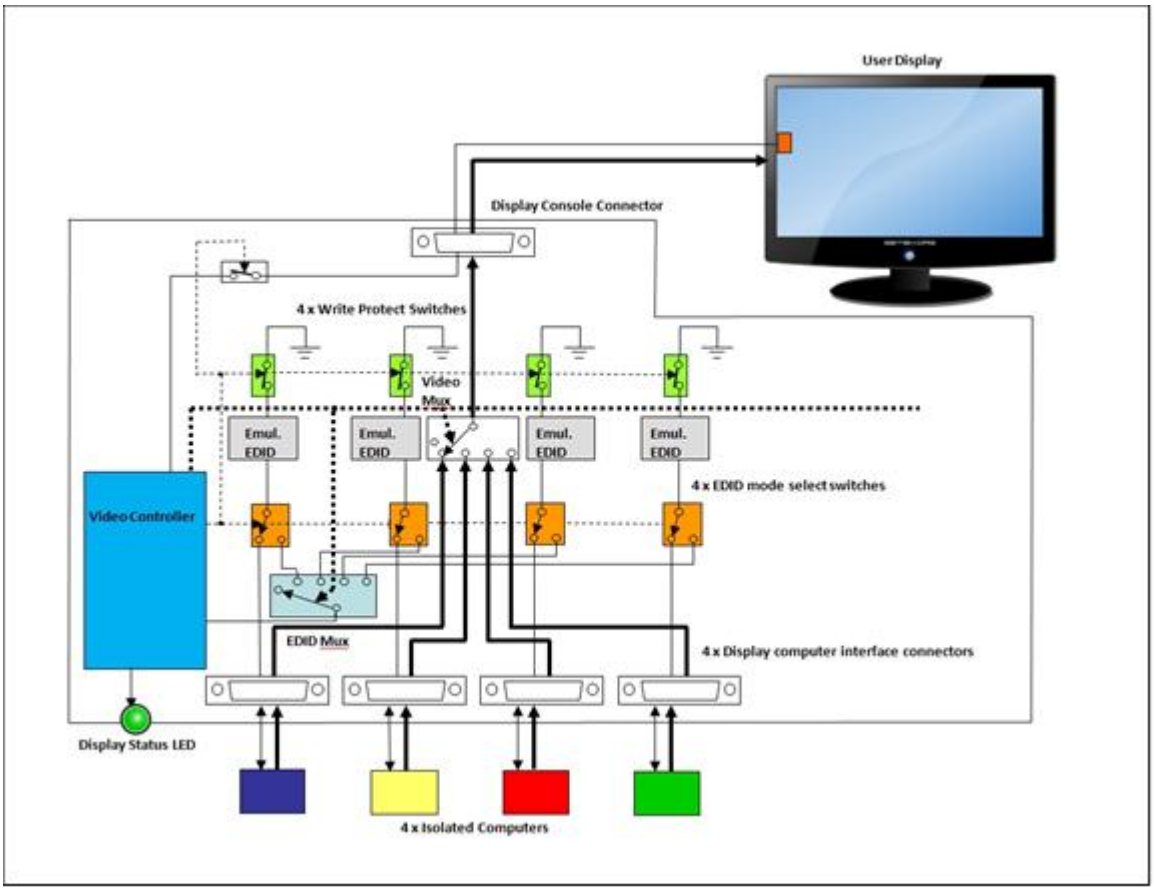


**Figure 4 – Display Normal Mode**

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 4), any attempt by a connected computer to affect the EDID channel is blocked by the architecture. Each computer is only able to reach its own emulated EDID EEPROM when the TOE is powered on.

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 EEPROM chip for each channel.

The EDID function is emulated by an independent emulation EEPROM chip for each computer channel. Each chip reads content from the connected display once during TOE power up. Any subsequent change to the display peripheral will be ignored. The only data stored in the emulated EDID EEPROM chips is the EDID data obtained from the connected monitor(s) at power up.

The TOE will reject any display device that does not present valid EDID content. An LED on the top 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 connections. The base models (F1DN102MOD-BA-4, F1DN104MOD-BA-4, F1DN202MOD-BA-4, F1DN204MOD-BA-4, F1DN108MOD-BA-4, F1DN208MOD-BA-4) can support any

combination of video connections because the video in and video out support is dependent upon the cables selected for use with the base models. However, in the evaluated configuration, except for the F1DN104MOD-XX-4 and F1DN204MOD-XX-4 series sets, the video input and video output are the same in the evaluated configuration. The secure switch does not support Hot-Plug Detection (HPD).

- 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 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.
    - DisplayPort input is supported on the F1DN102MOD-PP-4, F1DN202MOD-PP-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4, F1DN104MOD-XX-4 and F1DN204MOD-XX-4 devices.
    - DisplayPort peripherals are supported by the F1DN102MOD-PP-4, F1DN202MOD-PP-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4, F1DN204MOD-PP-4 and F1DN208MOD-PP-4 devices.
- For HDMI connections, EDID information is allowed to pass from the display to the computer, as described above. 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 HDMI protocol is supported on the F1DN102MOD-HH-4, F1DN202MOD-HH-4, F1DN104MOD-HH-4, F1DN204MOD-HH-4, F1DN104MOD-XX-4 and F1DN204MOD-XX-4 devices for both input and peripheral devices.

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

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. When the TOE is powered off or in a failure state, no data transits from the peripherals to the connected computers, from the connected computers to the peripherals or between the connected computers.

**TOE Security Functional Requirements addressed**: FDP_IPC_EXT.1(1), FDP_IPC_EXT.1(2), FDP_IPC_EXT.1(3), FDP_SPR_EXT.1/DP, FDP_SPR_EXT.1/HDMI.

### 7.1.4 Video Compatible Device Types

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

The F1DN102MOD-BA-4, F1DN104MOD-BA-4, F1DN108MOD-BA-4, F1DN102MOD-HH-4, F1DN102MOD-PP-4, F1DN104MOD-HH-4, F1DN104MOD-PP-4, F1DN108MOD-PP-4 and F1DN104MOD-XX-4 devices support a single display.

The F1DN202MOD-BA-4, F1DN204MOD-BA-4, F1DN208MOD-BA-4, F1DN202MOD-HH-4, F1DN202MOD-PP-4, F1DN204MOD-HH-4, F1DN204MOD-PP-4, F1DN208MOD-PP-4 and F1DN204MOD-XX-4 devices support two displays.

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

## 7.2 PROTECTION OF THE TSF

### 7.2.1 No Access to TOE

Connected computers and peripherals do not have access to TOE firmware or memory, with the following exception of EDID data, which is accessible to connected computers from the TOE

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

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

### 7.2.2 Anti-tampering Functionality

The TOE provides passive physical tampering detection on the devices, cables, and remote controls. The TOE enclosure was designed specifically to prevent physical tampering. It features a chassis and panels that prevent external access through bending or brute force.

Each device is fitted with one or more holographic Tampering Evident Labels placed at critical locations on the enclosure.  Any attempt to open the enclosure or remove a Tampering Evident Label results in the label being damaged so that the user can detect that the attempt to physically tamper with it occurred. In addition, if a tamper evident label is removed, the word ‘VOID’ appears on both the label and the product surface.

The cables and separate remote controls are constructed with fitted molding (no screws) so tampering with the cables and separate remote controls will be evident on visual inspection.

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

### 7.2.3 TSF Testing

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

- Verification of the top panel push buttons
- 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 top 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.

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

## 7.3 TOE ACCESS

### 7.3.1 Continuous Indications

The TOE user switches between computers by pressing the corresponding top panel button on the device or on the remote control. When the button to switch computers is pressed, a signal is sent and the TOE peripheral sharing device switches to the indicated channel. The top panel button and the remote control button corresponding to the selected computer will illuminate.

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

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

### 7.3.2 Remote Control

When a remote control is connected, the user switches between computers by selecting the corresponding device channel button on the remote control for the desired KVM device.

When the user selects a channel using the either remote control, the selected channel indicator of the remote control illuminates, and a signal is sent from the 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.

When the switching mechanism is initiated, a signal is sent and the TOE peripheral sharing device switches to the indicated channel. The front panel button corresponding to the selected computer will illuminate, and the selected channel on the remote control screen will be highlighted.

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

# 8 TERMINOLOGY AND ACRONYMS

## 8.1 TERMINOLOGY

The following terminology is used in this ST:

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

**Table 17 – Terminology**

## 8.2 ACRONYMS

The following acronyms are used in this ST:

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

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

**Table 18 – Acronyms**

# 9 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 |
| **[Addenda]** | CC and CEM addenda Exact Conformance, Selection-Based SFRs, Optional SFRs, 2021-Sep-30 |
| **[PKG_FLR_V1.0]** | Assurance Package for Flaw Remediation Version 1.0, 2024-06-28 |
| **[PP_PSD_V4.0]** | Protection Profile for Peripheral Sharing Device, Version: 4.0, 2019-07-19 |
| **[MOD_KM_V1.0]** | PP-Module for Keyboard/Mouse Devices, Version 1.0, 2019-07-19 |
| **[MOD_VI_V1.0]** | PP-Module for Video/Display Devices, Version 1.0, 2019-07-19 |
| **[CFG_PSD-KM-VI_V1.0]** | PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and Video/Display Devices, Version 1.0, 2019-07-19 |

**Table 19 – References**

# ANNEX A – LETTER OF VOLATILITY

The table below provides volatility information and memory types for the Belkin Peripheral Sharing Devices and the remote control. User data is not retained in any TOE device when the power is turned off.

The proprietary Host cables and Console cables have no programmable components and no data storage. The cables only perform format conversion to HDMI (Host cable) or from HDMI (Console cables).

| Product Models | Number in each product | Function, Manufacturer and Part Number | Storage Type | Size | Power Source (if not the TOE) | Volatility | Contains User Data |
|---|---|---|---|---|---|---|---|
| F1DN102MOD-BA-4<br>F1DN104MOD-BA-4<br>F1DN108MOD-BA-4<br>F1DN202MOD-BA-4<br>F1DN204MOD-BA-4<br>F1DN208MOD-BA-4<br>F1DN102MOD-HH-4<br>F1DN102MOD-PP-4<br>F1DN202MOD-HH-4<br>F1DN202MOD-PP-4<br>F1DN104MOD-HH-4<br>F1DN104MOD-PP-4<br>F1DN108MOD-PP-4<br>F1DN204MOD-HH-4<br>F1DN204MOD-PP-4<br>F1DN208MOD-PP-4<br>F1DN104MOD-XX-4<br>F1DN204MOD-XX-4 | 1 | System Controller, Host emulators:<br>ST Microelectronics STM32F446ZCT6 | Embedded SRAM[1] | 128KB | | Volatile | May contain user data |
| | | | Embedded Flash[2] | 256KB | | Non-Volatile | No user data |
| | | | Backup SRAM [3] | 4KB | | Volatile | No user data |
| | | | OTP Memory | 512bytes | | Non-Volatile | No user data |
| | 2 in 2 port,<br>4 in 4 port or<br>8 in 8 port models | Device emulators:<br>ST Microelectronics STM32F070C6T6 | Embedded SRAM[1] | 6KB | Connected computer | Volatile | May contain user data |
| | | | Embedded Flash[2] | 32KB | | Non-Volatile | No user data |
| | 2 in 2 port Single head,<br>4 in 4 port Single head and 2 port Dual head,<br>8 in 8 port Single head and 4 port Dual head and 16 in 8 port Dual head | EDID Emulator:<br>ST Microelectronics M24C02-WMN6TP | EEPROM[4] | 2 K bit | | Non-Volatile | No user data |

| Product Models | Number in each product | Function, Manufacturer and Part Number | Storage Type | Size | Power Source (if not the TOE) | Volatility | Contains User Data |
|---|---|---|---|---|---|---|---|
| F1DN-MOD-REM2<br>F1DN-MOD-REM4<br>F1DN-MOD-REM8 | 1 | System Controller, Host emulators:<br>ST Microelectronics STM32F446ZCT6 | Embedded SRAM[1] | 128KB | | Volatile | No user data |
| | | | Embedded Flash[2] | 256KB | | Non-Volatile | No user data |
| | | | Backup SRAM[3] | 4KB | | Volatile | No user data |
| | | | OTP Memory | 512bytes | | Non-Volatile | No user data |

***Notes:***

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

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

[3] The Backup SRAM does not contain user data. The Backup SRAM is powered by a backup battery so it is functionally non-volatile because it retains memory when there is no main power, although the SRAM itself is volatile, requiring constant power.