# High Sec Labs SK41D-4TR KVM Firmware Version 44404-E7E7 Security Target

Document Version: 1.3
Date: October 4, 2026

intertek acumen security

2400 Research Blvd
Suite 395
Rockville, MD 20850

**Revision History**

| Version | Date | Changes |
|---|---|---|
| Version 1.0 | 08-Jul-25 | Initial Release |
| Version 1.1 | 01-Aug-25 | Updated as per vendor inputs to review comments |
| Version 1.2 | 20-Aug-26 | Updated as per check-in ECR comments |
| Version 1.3 | 4-Oct-26 | Minor update to address checkout ECR comments |

# Contents

1. Introduction ..... 5
1.1 Security Target and TOE Reference ..... 5
1.2 TOE Overview ..... 5
1.3 TOE Description ..... 6
1.3.1 Evaluated Configuration ..... 6
1.3.2 Ports and Protocols ..... 7
1.3.3 Physical Boundaries ..... 10
1.3.4 Security Functions Provided by the TOE ..... 10
1.3.5 TOE Documentation ..... 11
1.4 TOE Environment ..... 11
2. Conformance Claims ..... 12
2.1 CC Conformance Claims ..... 12
2.2 Protection Profile Conformance ..... 12
2.3 Conformance Rationale ..... 12
2.3.1 Technical Decisions ..... 12
3. Security Problem Definition ..... 14
3.1 Threats ..... 14
3.2 Assumptions ..... 15
3.3 ORGANIZATIONAL SECURITY POLICIES ..... 15
4. Security Objectives ..... 15
4.1 Security Objectives for the TOE ..... 15
4.2 Security Objectives for the Operational Environment ..... 18
5. Security Requirements ..... 19
5.1 Conventions ..... 20
5.2 Security Functional Requirements ..... 20

5.2.1 Security Audit (FAU) ..... 20
5.2.2 User Data Protection (FDP) ..... 20
5.2.3 Identification and Authentication (FIA) ..... 25
5.2.4 Security Management (FMT) ..... 25
5.2.5 Protection of the TSF (FPT) ..... 26
5.2.6 TOE Access (FTA) ..... 27
5.3 TOE SFR Dependencies Rationale for SFRs ..... 27
5.4 Security Assurance Requirements ..... 28
5.5 Assurance Measures ..... 28
6. TOE Summary Specification ..... 30
6.1 TOE Summary Specification SFR Description ..... 30
6.1.1 Security Audit (FAU) ..... 30
6.1.2 User Data Protection (FDP) ..... 30
6.1.3 Identification and Authentication (FIA) and Security Management (FMT) ..... 39
6.1.4 Protection of the TSF (FPT) ..... 39
6.1.5 TOE Access (FTA) ..... 41
7. ANNEX A – LETTER OF VOLATILITY ..... 42
8. Acronym Table ..... 44

# 1. INTRODUCTION

The Security Target (ST) serves as the basis for the Common Criteria (CC) evaluation and identifies the Target of Evaluation (TOE), the scope of the evaluation, and the assumptions made throughout. This document will also describe the intended operational environment of the TOE, and the functional and assurance requirements that the TOE meets.

## 1.1 SECURITY TARGET AND TOE REFERENCE

This section provides the information needed to identify and control the TOE and the ST.

**Table 1 – TOE/ST Identification**

| Category | Identifier |
|---|---|
| ST Title | High Sec Labs SK41D-4TR KVM Firmware Version 44404-E7E7 Security Target |
| ST Version | 1.3 |
| ST Date | 4-Oct-26 |
| ST Author | Intertek Acumen Security |
| TOE Identifier | High Sec Labs SK41D-4TR KVM Firmware Version 44404-E7E7 |
| TOE Developer | High Sec Labs Ltd. |
| Key Words | KVM switch |

## 1.2 TOE OVERVIEW

The TOE is the High Sec Labs SK41D-4TR KVM Firmware Version 44404-E7E7 which is a Peripheral Sharing Device with video, keyboard and mouse functionality. The TOE is a combined software and hardware TOE. The High Sec Labs (HSL) SK41D-4TR Keyboard, Video, Mouse (KVM) switch allows 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 HSL Peripheral Sharing Devices:

- Security Audit
  - Audit entries are generated for security related events.
- User Data Protection
  - The TOE provides secure switching capabilities for keyboard, video and mouse. The TOE ensures that only authorized peripheral devices may be used.
- 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.
    - Digital Visual Interface (DVI)-D video is supported.
    - Keyboard and Mouse Security
    - The keyboard and mouse are isolated by dedicated, Universal Serial Bus (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.
- Identification and Authentication
    - Administrators must be identified and authenticated prior to accessing administrative functions.
- Security Management
    - The TOE provides management capabilities in support of the 'Restore to factory default' function. The Administrator role restricts this functionality to authorized administrators.
- Protection of the TSF
    - The TOE ensures a secure state in the case of failure, provides only restricted access, and performs self-testing.
    - The TOE provides both passive detection of physical attack and resistance to physical attack:
    - Any attempt to open the product enclosure will activate an anti-tampering system, making the product inoperable and indicating tampering via blinking Light Emitting Diodes (LEDs).
    - Special holographic tampering evident labels on the product's enclosure provide a clear visual indication if the product has been opened or compromised.
    - Reliable timestamps are provided for audit records.
- TOE Access
    - The TOE provides a continuous indication of which computer is currently selected.

The High Sec Labs SK41D-4TR KVM uses multiple isolated microcontrollers (one microcontroller per connected computer) to emulate connected peripherals in order to prevent an unauthorized data flow through bit-by-bit signaling.

The TOE is a combined software and hardware TOE.

## 1.3 TOE DESCRIPTION

This section provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references.

### 1.3.1 EVALUATED CONFIGURATION

Figure 1 below shows a basic evaluated configuration. The TOE is connected to four computers. The video input and output format is DVI-D, and a single display is connected to the KVM. The TOE uses ruggedized 32 pin connectors (MIL Spec MIL-DTL-38999) that support both DVI-D and USB 2.0 protocols. The evaluated configuration is specifically DVI-D and not the HDMI. Due to the secure keyboard/mouse emulation architecture of the TOE, the host computer does not communicate Caps Lock, Num Lock, or Scroll Lock status back to the shared physical keyboard. The KVM is used with a wired remote control.

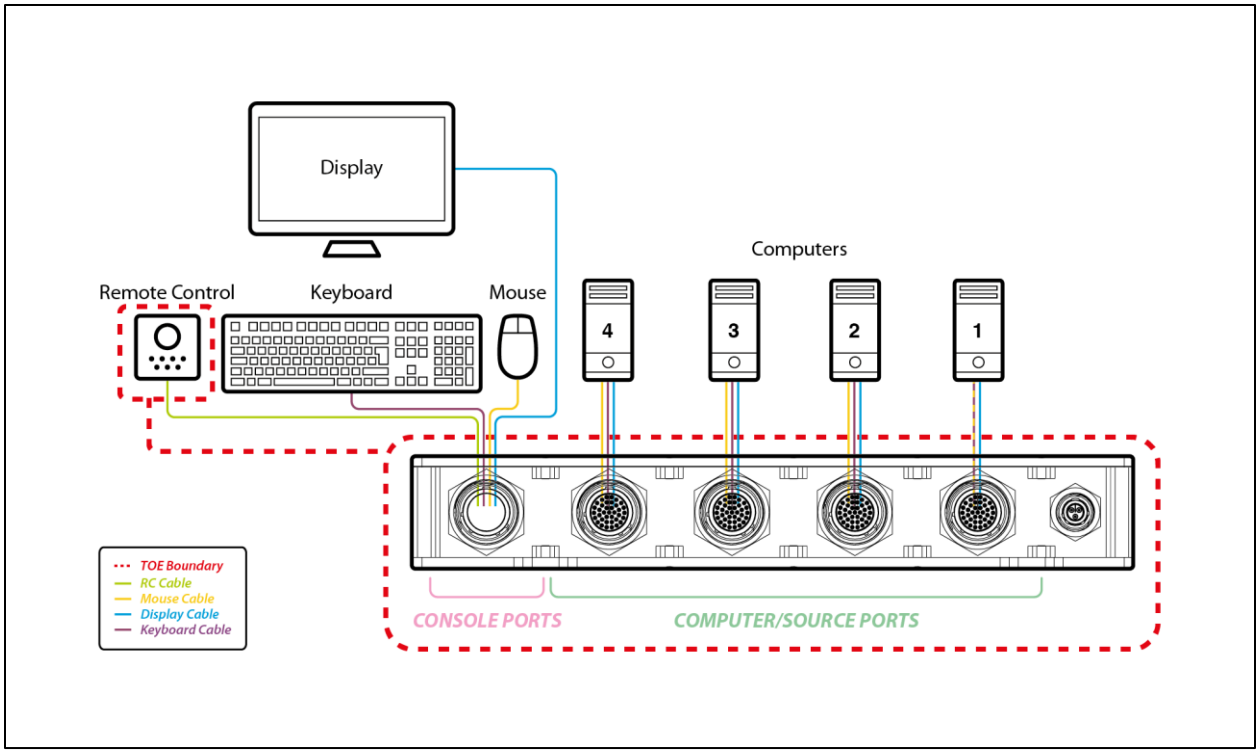



**Figure 1 – Representative TOE Deployment**

### 1.3.2 PORTS AND PROTOCOLS

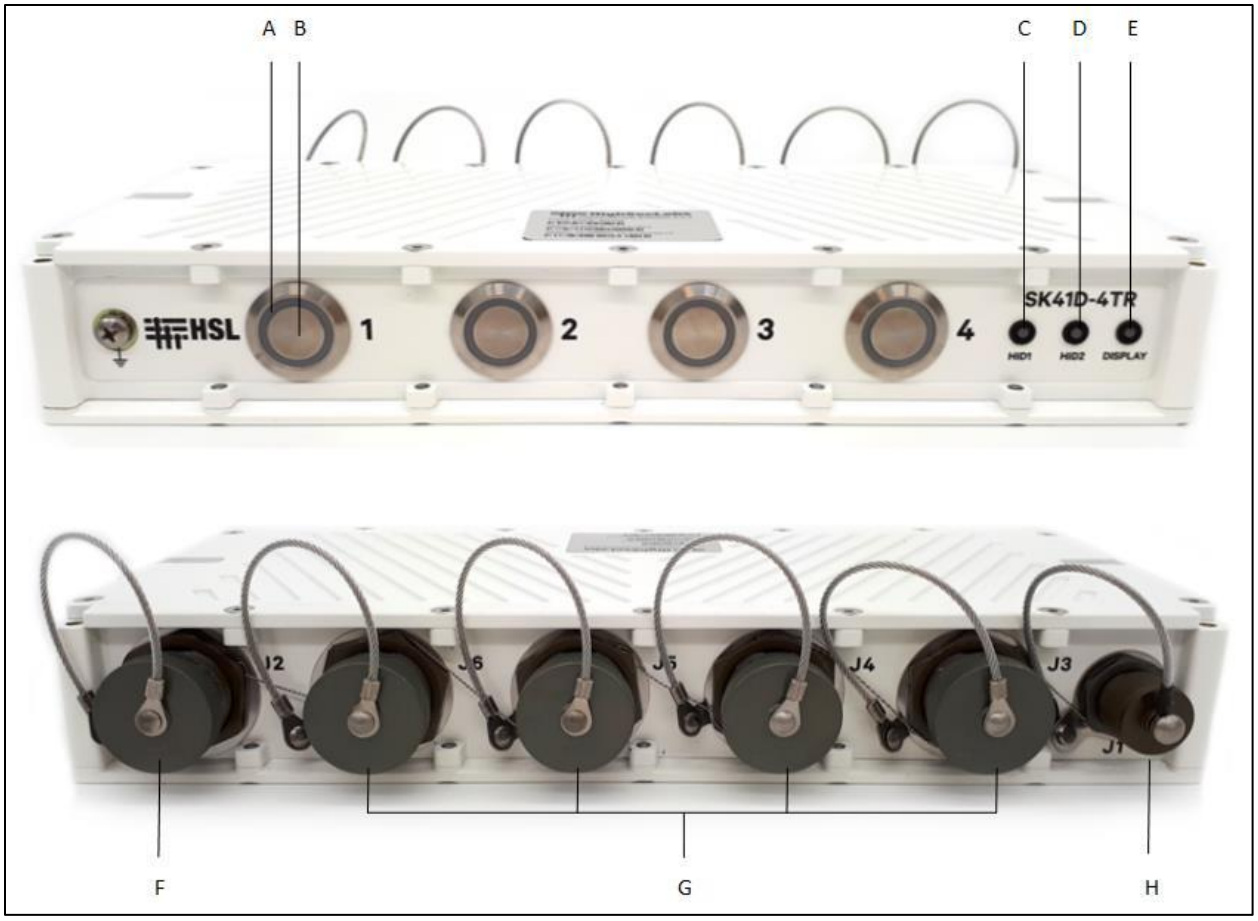



**Figure 2 – KVM Switch Front and Rear View**

Figure 2 shows the front and rear view of the KVM switch. The interfaces are described in Table 2.

**Table 2 – KVM Switch Interfaces and Protocols**

| | Interface | Protocol or Usage |
|---|---|---|
| A | Channel LED | Visual indication of the selected channel |
| B | Channel selection button | Manual pushbutton interface |
| C | USB (Keyboard or Mouse) LED | Visual indication of the HID status:<br>• Off indicates no device detected<br>• Red indicates device rejected<br>• Green indicates device approved |
| D | USB (Keyboard or Mouse) LED | Visual indication of the HID status:<br>• Off indicates no device detected<br>• Red indicates device rejected<br>• Green indicates device approved |
| E | EDID Capture LED | Visual indication of the EDID status:<br>• Off indicates no EDID<br>• Green flicker indicates EDID read in progress<br>• Green indicates EDID received |

| | Interface | Protocol or Usage |
|---|---|---|
| F | Console and RCU Cable Port | 32 pin connector supporting DVI-D, a serial connection (RS-232 protocol) and 2 USB 2.0 connections. This port is used with the provided cable. |
| G | PC Cable Ports | 32 pin connector supporting DVI-D and two USB 2.0 connections. These ports are used with the provided cables. |
| H | Power input | The input to the device is 28 VDC. |




**Figure 3 – Remote Control**

Figure 3 shows the TOE remote control. The interfaces are described in Table 3.

**Table 3 – Remote Control Interfaces and Protocols**

| | Interface | Protocol or Usage |
|---|---|---|
| I | Channel selection button | Manual pushbutton interface<br>Pressing the button causes the device to switch to the next sequential channel. The channel is set by pressing the remote control button until the desired channel is selected. |
| J | Channel LEDs | Visual indication of the selected channel<br>There are four LEDs in the first row. The LED is illuminated when the associated channel is selected. |
| K | USB (Keyboard or Mouse) LED | Visual indication of the HID status:<br>• Off indicates no device detected<br>• Flicker indicates device rejected<br>• On indicates device approved |

| | Interface | Protocol or Usage |
|---|---|---|
| L | USB (Keyboard or Mouse) LED | Visual indication of the HID status:<br>• Off indicates no device detected<br>• Flicker indicates device rejected<br>• On indicates device approved |
| M | EDID Capture LED | Visual indication of the EDID status:<br>• Off indicates no EDID<br>• Flicker indicates EDID read in progress<br>• On indicates EDID received |
| N | RCU Connector | This interface supports an RS-232 protocol serial connection. The interface is a round 32 pin ruggedized connector. |

### 1.3.3 PHYSICAL BOUNDARIES

Table 4 describes the TOE device.

**Table 4 – TOE Devices**

| Family Description | Part Number | Model |
|---|---|---|
| Ruggedized KVM Switch | CGA21853 | SK41D-4TR |
| Remote Control | CGA22528 | WR40-4R |

### 1.3.4 SECURITY FUNCTIONS PROVIDED BY THE TOE

The TOE provides the security functions required by the Protection Profile for Peripheral Sharing Device (PP_PSD_V4.0), (MOD_KM_V1.0) and (MOD_VI_V1.0).

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 5. This section summarizes the logical scope of the TOE.

#### 1.3.4.1 SECURITY AUDIT

Audit entries are generated for security related events.

#### 1.3.4.2 USER DATA PROTECTION

The TOE provides secure switching capabilities for keyboard, video and mouse. The TOE ensures that only authorized peripheral devices may be used.

#### 1.3.4.3 IDENTIFICATION AND AUTHENTICATION

Administrators must be identified and authenticated prior to accessing administrative functions.

#### 1.3.4.4 SECURITY MANAGEMENT

The TOE provides management capabilities in support of the 'Restore to factory default' function. The Administrator role restricts this functionality to authorized administrators.

#### 1.3.4.5 PROTECTION OF THE TSF

The TOE ensures a secure state in the case of failure, provides only restricted access, and performs self-testing. The TOE provides both passive detection of physical attack and resistance to physical attack. Reliable time stamps are provided for audit records.

#### 1.3.4.6 TOE ACCESS

The TOE provides a continuous indication of which computer is currently selected.

### 1.3.5 TOE DOCUMENTATION

The following documents are essential to understanding and controlling the TOE in the evaluated configuration, which may be downloaded from the High Sec Labs website (www.highseclabs.com) in .pdf format:

- HSL Quick Installation Guide 4 Ports Secure Ruggedized DVI-D KVM Switch, HDC23220 Rev 1.2
- HSL Administrator Guide, HDC19968, Rev. C

The following guidance is available upon request by emailing support@highseclabs.com as well as on NIAP portal:

- High Sec Labs SK41D-4TR KVM Firmware Version 44404-E7E7 Common Criteria Guidance Supplement, Version 0.6

## 1.4 TOE ENVIRONMENT

The following environmental components are required to operate the TOE in the evaluated configuration:

**Table 5 – Required Environmental Components**

| Components | Description |
|---|---|
| Connected Computers | 4 General purpose computers |
| Keyboard | General purpose USB keyboard |
| Mouse | General purpose USB mouse |
| User display | Standard DVI-D computer display |
| HSL KVM Cables | Ruggedized 32 pin console cable. The console cable has a round 32 pin connector on the KVM side. On the peripheral side, there is a DVI-D video connector, two USB 2.0 connectors for the keyboard and mouse and a port for connecting the WR40-4R remote control.<br>Ruggedized 32 pin PC cables. The PC cables have a single round 32 pin connector on the KVM side. On the PC side, there is a DVI-D video connector and two USB 2.0 connectors for the keyboard and mouse. |
| Power Supply | 28 Volt Direct Current (VDC) Power Supply. A Dr.Meter HY3005F-3 Programmable power supply is used in the evaluated configuration. |

# 2. CONFORMANCE CLAIMS

This section identifies the TOE conformance claims, conformance rationale, and relevant Technical Decisions (TDs).

## 2.1 CC CONFORMANCE CLAIMS

The TOE is conformant to the following:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017 (Extended)
- Common Criteria for Information Technology Security Evaluations Part 3, Version 3.1, Revision 5, April 2017 (Conformant)

## 2.2 PROTECTION PROFILE CONFORMANCE

This ST claims exact conformance to the following:

- PP - Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and Video/Display Devices, 19 July 2019
- As a shorthand reference, it can be identified as "CFG_PSD - KM - VI_V1.0"
    - 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 CONFORMANCE RATIONALE

This ST provides exact conformance to the items listed in the previous section. The security problem definition, security objectives, and security requirements in this ST are all taken from the Protection Profile (PP) and /Module/Package, performing only the operations defined there.

### 2.3.1 TECHNICAL DECISIONS

All NIAP TDs issued to date and applicable to PP_PSD_V4.0, MOD_KM_V1.0 and MOD_VI_V1.0 have been considered. Table 6, Table 7 and Table 8 identifies all applicable TDs.

**Table 6– Technical Decisions for PP_PSD_V4.0**

| Technical Decision | Applicable (Y/N) | Exclusion Rationale (if applicable) |
|---|---|---|
| TD0844: Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim | N | This TD addresses Flaw Remediation Conformance claim, and this TOE does not claim Flaw Remediation. |
| TD0804: Clarification regarding Extenders in PSD Evaluations | Y | |

| Technical Decision | Applicable (Y/N) | Exclusion Rationale (if applicable) |
|---|---|---|
| TD0583: FPT_PHP.3 modified for PSD remote controllers | Y | |
| TD0518: Typographical error in Dependency Table | Y | |

**Table 7– Technical Decisions for MOD_KM_V1.0**

| Technical Decision | Applicable (Y/N) | Exclusion Rationale (if applicable) |
|---|---|---|
| TD0959: Correction to Test 4 Step 3 of FDP_APC_EXT.1 | Y | |
| TD0593: Equivalency Arguments for PSD | Y | |
| TD0507: Clarification on USB plug type | Y | |

**Table 8– Technical Decisions for MOD_VI_V1.0**

| Technical Decision | Applicable (Y/N) | Exclusion Rationale (if applicable) |
|---|---|---|
| TD0942: Updated EDID Read Requirements | Y | |
| TD0842: Alternate Conversion Option for FDP_IPC_EXT.1 | N | This TD addresses FDP_IPC_EXT.1 SFR, and this TOE does not claim this SFR. |
| TD0686: DisplayPort CEC Testing | N | This TD addresses FDP_SPR_EXT.1/DP, and this TOE does not claim this SFR. |
| TD0681: PSD purging of EDID data upon disconnect | Y | |
| TD0593: Equivalency Arguments for PSD | Y | |
| TD0584: Update to FDP APC_EXT.1 Video Tests | Y | |
| TD0539: Incorrect selection trigger in FTA_CIN_EXT.1 in MOD_VI_V1.0 | Y | |
| TD0514: Correction to MOD_VI FDP_APC_EXT.1 Test 3 Step 6 | Y | |
| TD0506: Missing Steps to disconnect and reconnect display | Y | |

# 3. SECURITY PROBLEM DEFINITION

The security problem definition has been taken directly from the claimed PP and any relevant EPs/Modules/Packages specified in Section 2.2 and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any Organizational Security Policies (OSPs) that the TOE is expected to enforce.

## 3.1 THREATS

The threats included in Table 9 are drawn directly from the [PP_PSD_V4.0], [MOD_KM_V1.0] and [MOD_VI_V1.0] specified in Section 2.2.

**Table 9 – Threats**

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

## 3.2 ASSUMPTIONS

The assumptions included in Table 10 are drawn directly from [PP_PSD_V4.0], [MOD_KM_V1.0] and [MOD_VI_V1.0].

**Table 10 – Assumptions**

| ID | Assumption |
|---|---|
| A.NO_TEMPEST | Computers and peripheral devices connected to the PSD are not TEMPEST approved. |
| 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. |
| 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.<br>[MOD_VI_V1.0] |

## 3.3 ORGANIZATIONAL SECURITY POLICIES

There are no Organizational Security Policies applicable to this TOE.

# 4. SECURITY OBJECTIVES

The security objectives have been taken directly from the [PP_PSD_V4.0], [MOD_KM_V1.0] and [MOD_VI_V1.0] and are reproduced here for the convenience of the reader.

## 4.1 SECURITY OBJECTIVES FOR THE TOE

The security objectives in the following table apply to the TOE.

**Table 11 – Security Objectives**

| ID | Security Objectives |
|---|---|
| O.COMPUTER_INTERFACE_ISOLATION | 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. |
| O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED | The PSD shall not allow data to transit a PSD-Computer interface while the PSD is unpowered. |
| O.USER_DATA_ISOLATION | The PSD shall route user data, such as keyboard entries, only to the computer selected by the user. The PSD shall provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer. |
| O.NO_USER_DATA_RETENTION | The PSD shall not retain user data in non-volatile memory after power up or, if supported, factory reset. |
| O.NO_OTHER_EXTERNAL_INTERFACES | The PSD shall not have any external interfaces other than those implemented by the TSF. |
| O.LEAK_PREVENTION_SWITCHING | The PSD shall ensure that there are no switching mechanisms that allow signal data leakage between connected computers. |
| O.AUTHORIZED_USAGE | The TOE shall explicitly prohibit or ignore unauthorized switching mechanisms, either because it supports only one connected computer or because it allows only authorized mechanisms to switch between connected computers. Authorized switching mechanisms shall require express user action restricted to console buttons, console switches, 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><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 |

| ID | Security Objectives |
|---|---|
| | administrators and that an audit trail of management activities is generated. |
| O.PERIPHERAL_PORTS_ISOLATION | The PSD shall ensure that data does not flow between peripheral devices connected to different PSD interfaces. |
| O.REJECT_UNAUTHORIZED_PERIPHERAL | The PSD shall reject unauthorized peripheral device types and protocols. |
| O.REJECT_UNAUTHORIZED_ENDPOINTS | The PSD shall reject unauthorized peripheral devices connected via a Universal Serial Bus (USB) hub. |
| O.NO_TOE_ACCESS | The PSD firmware, software, and memory shall not be accessible via its external ports. |
| 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. |
| 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. |
| O.SELF_TEST | The PSD shall perform self-tests following power up or powered reset. |
| O.SELF_TEST_FAIL_TOE_DISABLE | The PSD shall enter a secure state upon detection of a critical failure. |
| O.SELF_TEST_FAIL_INDICATION | The PSD shall provide clear and visible user indications in the case of a self-test failure. |
| O.EMULATED_INPUT | The TOE shall emulate the keyboard and/or mouse functions from the TOE to the connected computer.<br>[MOD_KM_V1.0] |
| 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>[MOD_KM_V1.0] |

| ID | Security Objectives |
|---|---|
| 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>[MOD_VI_V1.0] |
| O.UNIDIRECTIONAL_VIDEO | The TOE shall enforce unidirectional video data flow from the connected computer video interface to the display interface only.<br>[MOD_VI_V1.0] |

## 4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

Security objectives for the operational environment assist the TOE in correctly providing its security functionality. These objectives, which are found in the table below, track with the assumptions about the TOE operational environment.

**Table 12 – Security Objectives for the Operational Environment**

| ID | Objectives for the Operational Environment |
|---|---|
| OE.NO_TEMPEST | The operational environment will not use TEMPEST approved equipment. |
| OE.PHYSICAL | The operational environment will provide physical security, commensurate with the value of the PSD and the data that transits it. |
| OE.NO_WIRELESS_DEVICES | The operational environment will not include wireless keyboards, mice, audio, user authentication, or video devices. |
| OE.TRUSTED_ADMIN | The operational environment will ensure that trusted PSD Administrators and users are appropriately trained. |
| OE.TRUSTED_CONFIG | The operational environment will ensure that administrators configuring the PSD and its operational environment follow the applicable security configuration guidance. |
| OE.NO_SPECIAL_ANALOG_CAPABILITIES | The operational environment will not have special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, or a component with digital signal processing or analog video capture functions.<br>[MOD_VI_V1.0] |

# 5. SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements (SFRs) for the TOE. The SFRs included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revisions 5, April 2017, and all international interpretations.

**Table 13 – SFRs**

| Requirement | Description |
|---|---|
| FAU_GEN.1 | Audit Data Generation |
| FDP_APC_EXT.1 | Active PSD Connections |
| FDP_APC_EXT.1/KM | Active PSD Connections |
| FDP_APC_EXT.1/VI | Active PSD Connections |
| FDP_CDS_EXT.1 | Connected Displays Supported |
| FDP_FIL_EXT.1/KM | Device Filtering (Keyboard/Mouse) |
| FDP_PDC_EXT.1 | Peripheral Device Connection |
| FDP_PDC_EXT.1/KM | Peripheral Device Connection |
| FDP_PDC_EXT.2/KM | Authorized Devices (Keyboard/Mouse) |
| FDP_PDC_EXT.2/VI | Peripheral Device Connection (Video Output) |
| FDP_PDC_EXT.3/KM | Authorized Connection Protocols (Keyboard/Mouse) |
| FDP_PDC_EXT.3/VI | Authorized Connection Protocols (Video Output) |
| FDP_RDR_EXT.1 | Re-enumeration Device Rejection |
| FDP_RIP_EXT.1 | Residual Information Protection |
| FDP_RIP.1/KM | Residual Information Protection |
| FDP_RIP_EXT.2 | Purge of Residual Information |
| FDP_SPR_EXT.1/DVI-D | Sub-Protocol Rules (DVI-D Protocol) |
| FDP_SWI_EXT.1 | PSD Switching |
| FDP_SWI_EXT.2 | PSD Switching Methods |
| FDP_SWI_EXT.3 | Tied Switching |
| FDP_UDF_EXT.1/KM | Unidirectional Data Flow (Keyboard/Mouse) |
| FDP_UDF_EXT.1/VI | Unidirectional Data Flow (Video Output) |
| FIA_UAU.2 | User Authentication Before Any Action |
| FIA_UID.2 | User Identification Before Any Action |
| FMT_MOF.1 | Management of Security Functions Behavior |
| FMT_SMF.1 | Specification of Management Functions |
| FMT_SMR.1 | Security Roles |
| FPT_FLS_EXT.1 | Failure with Preservation of Secure State |
| FPT_NTA_EXT.1 | No Access to TOE |
| FPT_PHP.1 | Passive Detection of Physical Attack |

| Requirement | Description |
|---|---|
| FPT_PHP.3 | Resistance to Physical Attack |
| FPT_STM.1 | Reliable Time Stamps |
| FPT_TST.1 | TSF Testing |
| FPT_TST_EXT.1 | TSF Testing |
| FTA_CIN_EXT.1 | Continuous Indications |

## 5.1 CONVENTIONS

The CC allows the following types of operations to be performed on the functional requirements: assignments, selections, refinements, and iterations. The following font conventions are used within this document to identify operations defined by CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration identifier after a slash, e.g., /SigGen.
- Where operations were completed in the PP and relevant EPs/Modules/Packages, the formatting used in the PP has been retained.
- Extended SFRs are identified by the addition of "EXT" after the requirement name.

## 5.2 SECURITY FUNCTIONAL REQUIREMENTS

This section includes the security functional requirements for this ST.

### 5.2.1 SECURITY AUDIT (FAU)

#### 5.2.1.1 FAU_GEN.1 AUDIT DATA GENERATION (PP_PSD_V4.0)

**FAU_GEN.1.1**

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

a. Start-up and shutdown of the audit functions;
b. All auditable events for the [not specified] level of audit; and
c. [*administrator login, administrator logout, self-test failures, peripheral device acceptance and rejections, [Restore to factory default, create administrator account, change password]*]

**FAU_GEN.1.2**

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

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

### 5.2.2 USER DATA PROTECTION (FDP)

#### 5.2.2.1 FDP_APC_EXT.1 ACTIVE PSD CONNECTIONS (PP_PSD_V4.0)

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

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

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

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

#### 5.2.2.2 FDP_APC_EXT.1/KM ACTIVE PSD CONNECTIONS (MOD_KM_V1.0)

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

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

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

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

#### 5.2.2.3 FDP_APC_EXT.1/VI ACTIVE PSD CONNECTIONS (MOD_VI_V1.0)

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

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

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

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

#### 5.2.2.4 FDP_CDS_EXT.1 CONNECTED DISPLAYS SUPPORTED (MOD_VI_V1.0)

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

#### 5.2.2.5 FDP_FIL_EXT.1/KM DEVICE FILTERING (KEYBOARD/MOUSE) (MOD_KM_V1.0)

**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.

#### 5.2.2.6 FDP_PDC_EXT.1 PERIPHERAL DEVICE CONNECTION (PP_PSD_V4.0)

**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.

#### 5.2.2.7 FDP_PDC_EXT.1/KM PERIPHERAL DEVICE CONNECTION (MOD_KM_V1.0)

**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.

#### 5.2.2.8 FDP_PDC_EXT.2/KM AUTHORIZED DEVICES (KEYBOARD/MOUSE) (MOD_KM_V1.0)

**FDP_PDC_EXT.2.1/KM**

The TSF shall allow connections with authorized devices **and functions** as defined in [*Appendix E*] and **[**

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

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

**FDP_PDC_EXT.2.2/KM**

The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*Appendix E*] and **[**

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

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

#### 5.2.2.9 FDP_PDC_EXT.2/VI PERIPHERAL DEVICE CONNECTION (VIDEO OUTPUT) (MOD_VI_V1.0)

**FDP_PDC_EXT.2.1/VI**

The TSF shall allow connections with authorized devices as defined in [*Appendix E*] 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*] 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.

#### 5.2.2.10 FDP_PDC_EXT.3/KM AUTHORIZED CONNECTION PROTOCOLS (KEYBOARD/MOUSE) (MOD_KM_V1.0)

**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*].

#### 5.2.2.11 FDP_PDC_EXT.3/VI AUTHORIZED CONNECTION PROTOCOLS (VIDEO OUTPUT) (MOD_VI_V1.0)

**FDP_PDC_EXT.3.1/VI**

The TSF shall have interfaces for the [DVI-D] protocols.

**FDP_PDC_EXT.3.2/VI [TD0942]**
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]].

#### 5.2.2.12 FDP_RDR_EXT.1 RE-ENUMERATION DEVICE REJECTION (MOD_KM_V1.0)

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

#### 5.2.2.13 FDP_RIP_EXT.1 RESIDUAL INFORMATION PROTECTION (PP_PSD_V4.0)

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

#### 5.2.2.14 FDP_RIP.1/KM RESIDUAL INFORMATION PROTECTION (MOD_KM_V1.0)

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

#### 5.2.2.15 FDP_RIP_EXT.2 PURGE OF RESIDUAL INFORMATION (PP_PSD_V4.0)

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

#### 5.2.2.16 FDP_SPR_EXT.1/DVI-D SUB-PROTOCOL RULES (DVI-D PROTOCOL) (MOD_VI_V1.0)

**FDP_SPR_EXT.1.1/DVI-D**
The TSF shall apply the following rules for the [*DVI-D*] protocol:

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

#### 5.2.2.17 FDP_SWI_EXT.1 PSD SWITCHING (PP_PSD_V4.0)

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

#### 5.2.2.18 FDP_SWI_EXT.2 PSD SWITCHING METHODS (PP_PSD_V4.0)

**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].

#### 5.2.2.19 FDP_SWI_EXT.3 TIED SWITCHING (MOD_KM_V1.0)

**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.

#### 5.2.2.20 FDP_UDF_EXT.1/KM UNIDIRECTIONAL DATA FLOW (KEYBOARD/MOUSE) (MOD_KM_V1.0)

**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.

#### 5.2.2.21 FDP_UDF_EXT.1/VI UNIDIRECTIONAL DATA FLOW (VIDEO OUTPUT) (MOD_VI_V1.0)

**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.

### 5.2.3 IDENTIFICATION AND AUTHENTICATION (FIA)

#### 5.2.3.1 FIA_UAU.2 USER AUTHENTICATION BEFORE ANY ACTION (PP_PSD_V4.0)

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

#### 5.2.3.2 FIA_UID.2 USER IDENTIFICATION BEFORE ANY ACTION (PP_PSD_V4.0)

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

### 5.2.4 SECURITY MANAGEMENT (FMT)

#### 5.2.4.1 FMT_MOF.1 MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOR (PP_PSD_V4.0)

**FMT_MOF.1.1**
The TSF shall restrict the ability to [*modify the behavior of*] the functions [*Restore to factory default*] to [*the authorized administrators*].

#### 5.2.4.2 FMT_SMF.1 SPECIFICATION OF MANAGEMENT FUNCTIONS (PP_PSD_V4.0)

**FMT_SMF.1.1**
The TOE shall be capable of performing the following management functions: [*Restore to factory default, create administrator account, change password*].

#### 5.2.4.3 FMT_SMR.1 SECURITY ROLES (PP_PSD_V4.0)

**FMT_SMR.1.1**
The TSF shall maintain the roles [*administrators*].

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

### 5.2.5 PROTECTION OF THE TSF (FPT)

#### 5.2.5.1 FPT_FLS_EXT.1 FAILURE WITH PRESERVATION OF SECURE STATE (PP_PSD_V4.0)

**FPT_FLS_EXT.1.1**
The TSF shall preserve a secure state when the following types of failures occur: failure of the power-on self-test and [failure of the anti-tamper function].

#### 5.2.5.2 FPT_NTA_EXT.1 NO ACCESS TO TOE (PP_PSD_V4.0)

**FPT_NTA_EXT.1.1**
TOE firmware, software, and memory shall not be accessible via the TOE's external ports, with the following exceptions: [the **Extended Display Identification Data** (EDID) memory of Video TOEs may be accessible from connected computers; the configuration data, settings, and logging data that may be accessible by authorized administrators].

#### 5.2.5.3 FPT_PHP.1 PASSIVE DETECTION OF PHYSICAL ATTACK (PP_PSD_V4.0)

**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.

#### 5.2.5.4 FPT_PHP.3 RESISTANCE TO PHYSICAL ATTACK (PP_PSD_V4.0)

**FPT_PHP.3.1 [TD0583]**
The TSF shall resist [a physical attack for the purpose of gaining access to the internal components, to damage the anti-tamper battery, to drain or exhaust the anti-tamper battery] to the [TOE enclosure and any remote controllers] by the attacked component becoming permanently disabled.

#### 5.2.5.5 FPT_STM.1 RELIABLE TIME STAMPS (PP_PSD_V4.0)

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

#### 5.2.5.6 FPT_TST.1 TSF TESTING (PP_PSD_V4.0)

**FPT_TST.1.1**
The TSF shall run a suite of self-tests [*during initial start-up and at the conditions* **[no other conditions]**] to demonstrate the correct operation of [*user control functions and* **[active anti-tamper functionality]**].

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

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

#### 5.2.5.7 FPT_TST_EXT.1 TSF TESTING (PP_PSD_V4.0)

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

### 5.2.6 TOE ACCESS (FTA)

#### 5.2.6.1 FTA_CIN_EXT.1 CONTINUOUS INDICATIONS (PP_PSD_V4.0)

**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].

## 5.3 TOE SFR DEPENDENCIES RATIONALE FOR SFRS

The PP and any relevant Modules contain(s) all the requirements claimed in this ST. As such, the dependencies are not applicable since the PP has been approved.

## 5.4 SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST are taken directly from the PP and any relevant Modules, which is/are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in Table 14.

**Table 14 – Security Assurance Requirements**

| Assurance Class | Assurance Components | Component Description |
|---|---|---|
| Security Target | 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 |
| Development | ADV_FSP.1 | Basic Functional Specification |
| Guidance Documents | AGD_OPE.1 | Operational User Guidance |
| | AGD_PRE.1 | Preparative Procedures |
| Life Cycle Support | ALC_CMC.1 | Labelling of the TOE |
| | ALC_CMS.1 | TOE CM Coverage |
| Tests | ATE_IND.1 | Independent Testing – Conformance |
| Vulnerability Assessment | AVA_VAN.1 | Vulnerability Survey |

## 5.5 ASSURANCE MEASURES

The TOE satisfied the identified assurance requirements. This section identifies the Assurance Measures applied by High Sec Labs Ltd. to satisfy the assurance requirements. The following table lists the details.

**Table 15 – TOE Security Assurance Measures**

| SAR Component | How the SAR will be met |
|---|---|
| ASE_TSS.1.1C Refinement | The TOE summary specification describes how the TOE meets each SFR. It also provides evidence that the security functions are suitable to meet the TOE security requirements. |
| ADV_FSP.1 | Evaluation Activities listed in the PP are associated with the applicable SFRs; since these are directly associated with the SFRs, the tracing element ADV_FSP.1.2D is implicitly already done, and no additional documentation is necessary. The functional specification documentation is provided to support the evaluation and other activities described for AGD, and ATE SARs. The requirements on the content of the functional specification information are implicitly assessed by virtue of the other Evaluation Activities being performed. |
| AGD_OPE.1 | The Administrative Guide provides descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance. |

| SAR Component | How the SAR will be met |
|---|---|
| AGD_PRE.1 | The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration. |
| ALC_CMC.1 | The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated. |
| ALC_CMS.1 | The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated. |
| ATE_IND.1 | High Sec Labs will provide the TOE for testing. |
| AVA_VAN.1 | High Sec Labs will provide the TOE for testing.<br>High Sec Labs will provide a document identifying the list of software and hardware components. |

# 6. TOE SUMMARY SPECIFICATION

## 6.1 TOE SUMMARY SPECIFICATION SFR DESCRIPTION

This section includes the security functional requirements for this ST.

### 6.1.1 SECURITY AUDIT (FAU)

#### 6.1.1.1 FAU_GEN.1 AUDIT DATA GENERATION (PP_PSD_V4.0)

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

- OTP log
  - The OTP log maintains the critical events in parallel with the Critical RAM log. This log stores up to 64 events and does not overwrite. It stops recording when the log is full.
- Critical (Random Access Memory (RAM)) Logs
  - Self-test failure – a record of the latest self-test failure is recorded with error code information
  - Peripheral device rejection
  - Restore to factory default event
  - Changes to the primary administrator password
- Non-critical (Random Access Memory (RAM)) Logs
  - Peripheral device acceptance
  - Non-security related configuration changes
  - Administrator login
  - Administrator logout
  - Creation and removal of administrator accounts
  - Administrator password changes (other than for the primary administrator)

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

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

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

The TOE does not offer any configuration for "Start-up and shutdown of the audit functions". The logs are generated by default.

### 6.1.2 USER DATA PROTECTION (FDP)

#### 6.1.2.1 FDP_APC_EXT.1 ACTIVE PSD CONNECTIONS (PP_PSD_V4.0), FDP_APC_EXT.1/KM ACTIVE PSD CONNECTIONS (MOD_KM_V1.0) AND FDP_APC_EXT.1/VI ACTIVE PSD CONNECTIONS (MOD_VI_V1.0)

The TOE ensures that data flows only between the peripherals and the connected computer selected by the user. No data transits the TOE when the TOE is powered off, or when the TOE is in a failure state. A failure state occurs when the TOE fails a self-test when powering on. Any attempt to separate the pieces of the enclosure to access the internal circuitry will trigger the anti-tampering function or if the self-test detects that the battery is depleted or failing, the anti-tampering function will be triggered which would trigger the failure mode.

#### 6.1.2.2 FDP_CDS_EXT.1 CONNECTED DISPLAYS SUPPORTED (MOD_VI_V1.0)

A single video display is supported at a time.

#### 6.1.2.3 FDP_FIL_EXT.1/KM DEVICE FILTERING (KEYBOARD/MOUSE) (MOD_KM_V1.0) AND FDP_PDC_EXT.2/KM AUTHORIZED DEVICES (KEYBOARD/MOUSE) (MOD_KM_V1.0)

The TOE employs fixed device filtering and accepts only USB HID devices at the keyboard and mouse peripheral ports. Only USB connections over custom 32 pin ruggedized cables are permitted. The TOE does not support a wireless connection to a mouse, keyboard or USB hub. TOE distinguishes HID from non-HID USB traffic by means of a host emulator which is a microcontroller that enumerates the keyboard and verifies that it is a permitted device type. The TOE enumerates the device, verifies the permitted type, uses fixed filtering, and rejects unauthorized interface protocols.

#### 6.1.2.4 FDP_PDC_EXT.1 PERIPHERAL DEVICE CONNECTION (PP_PSD_V4.0), FDP_PDC_EXT.1 PERIPHERAL DEVICE CONNECTION (MOD_KM_V1.0), FDP_PDC_EXT.2/VI PERIPHERAL DEVICE CONNECTION (VIDEO OUTPUT) (MOD_VI_V1.0) AND FDP_PDC_EXT.3/VI AUTHORIZED CONNECTION PROTOCOLS (VIDEO OUTPUT) (MOD_VI_V1.0)

The TOE accepts any DVI-D display device at the video peripheral port. The TOE does not support a wireless connection to a video display.

The connected computers are attached to the TOE as follows:

- The TOE connects to the keyboard and mouse port using a ruggedized 32 pin cable that supports USB.
- The TOE is connected to the computer video port using a ruggedized 32 pin cable that supports DVI-D video.

The list of peripheral devices and interfaces supported by the TOE does not include any prohibited devices or protocols specified in Appendix E, and all external physical interfaces implemented by the TOE are claimed by the TSF, with no unclaimed external interfaces present.

Also, TOE can read the connected display EDID information during power-on or reboot automatically.

#### 6.1.2.5 FDP_PDC_EXT.3/KM AUTHORIZED CONNECTION PROTOCOLS (KEYBOARD/MOUSE) (MOD_KM_V1.0), FDP_RIP.1/KM RESIDUAL INFORMATION PROTECTION (MOD_KM_V1.0),FDP_UDF_EXT.1/KM UNIDIRECTIONAL DATA FLOW (KEYBOARD/MOUSE) (MOD_KM_V1.0) AND FDP_RDR_EXT.1 RE-ENUMERATION DEVICE REJECTION (MOD_KM_V1.0)

If a connected device attempts to re-enumerate as a different USB device type, it will be rejected by the TOE. The TOE determines whether or not a peripheral device that has been plugged into the keyboard and mouse peripheral ports is allowed to operate with the TOE.

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

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

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

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

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

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.

#### 6.1.2.6 FDP_RDR_EXT.1 RE-ENUMERATION DEVICE REJECTION (MOD_KM_V1.0)

If a connected device attempts to re-enumerate as a different USB device type, it will be rejected by the TOE.

#### 6.1.2.7 FDP_RIP_EXT.1 RESIDUAL INFORMATION PROTECTION (PP_PSD_V4.0) AND FDP_RIP_EXT.2 PURGE OF RESIDUAL INFORMATION (PP_PSD_V4.0)

The Letter of Volatility is included as Annex A.

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

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

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

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

#### 6.1.2.8 FDP_SPR_EXT.1/DVI-D SUB-PROTOCOL RULES (DVI-D PROTOCOL) (MOD_VI_V1.0) AND FDP_UDF_EXT.1/VI UNIDIRECTIONAL DATA FLOW (VIDEO OUTPUT) (MOD_VI_V1.0)

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

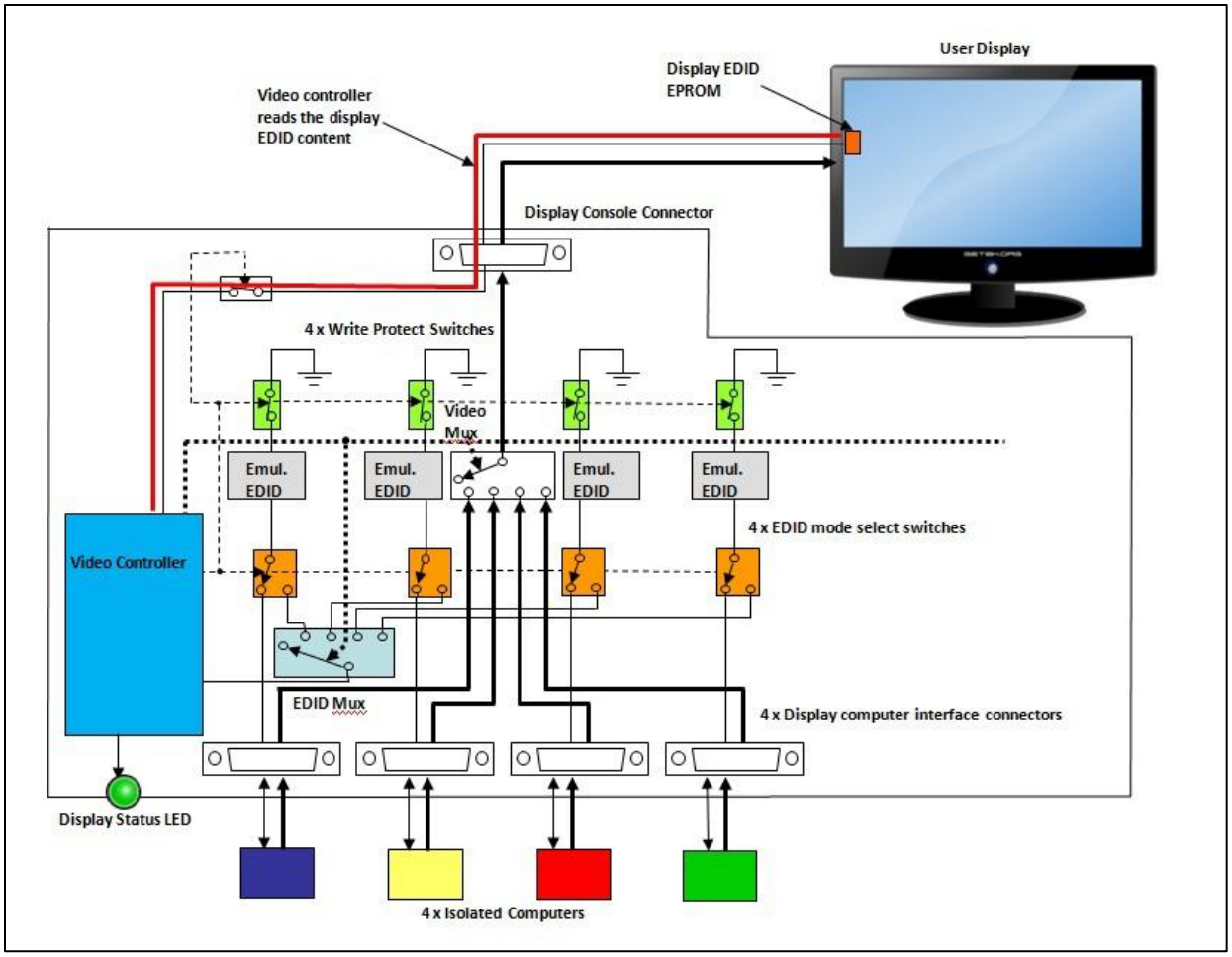



**Figure 4 – Display EDID Read Function**

An EDID read event only occurs as the TOE is being powered up. The video controller reads the EDID content from the display device to verify that it is valid and usable. If data is not valid, TOE operation will cease and wait for the display peripheral to be changed.

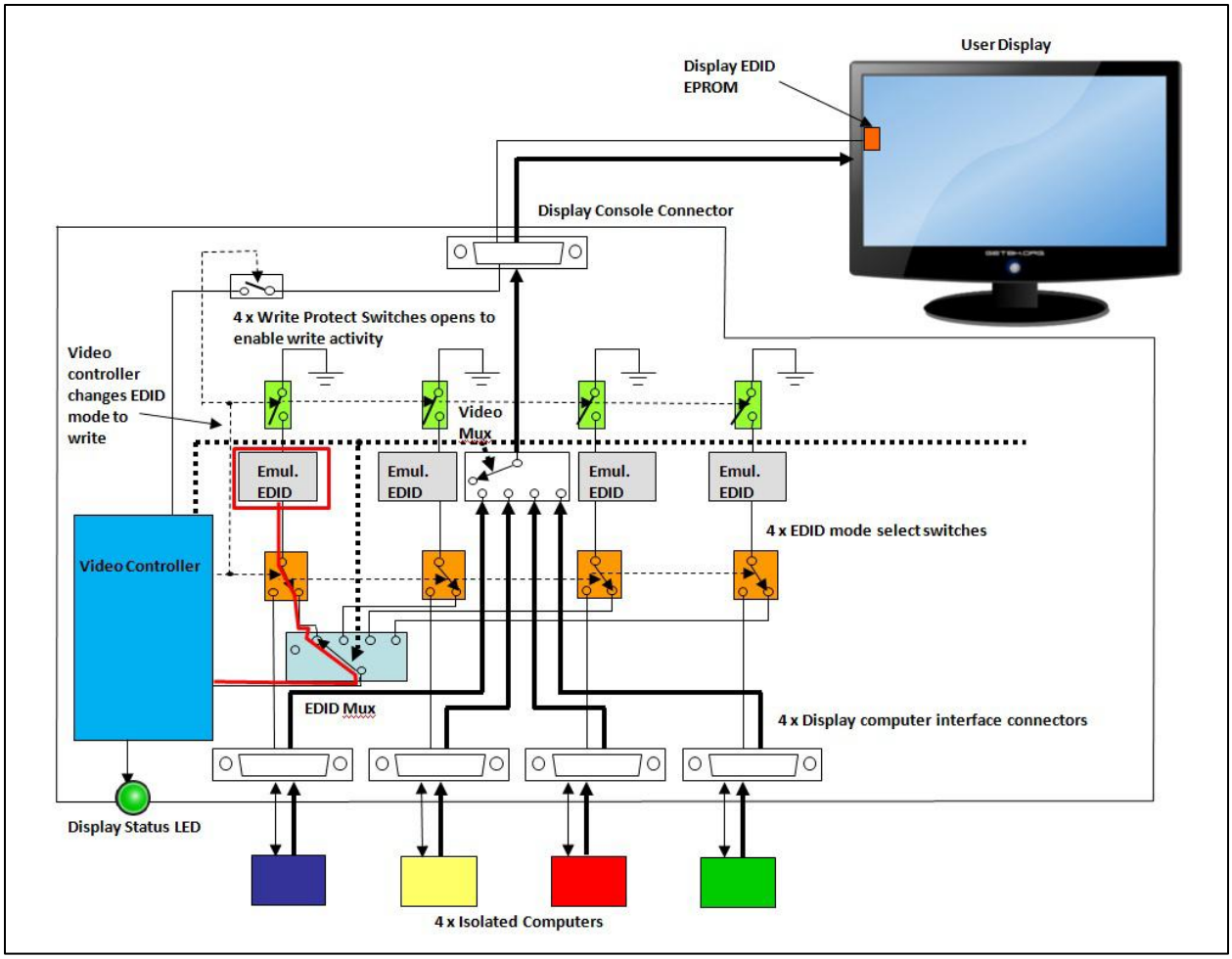



**Figure 5 – Display EDID Write Function**

Red line in the Figure 5 illustrates the video controller (shown in blue) as it writes the EDID content into the first channel emulated EDID Electrically Erasable Programmable Read-Only Memory (EEPROM) chip (shown in gray). The thick lines in this figure indicate native video lines, and the thin lines indicate Inter-Integrated Circuit (I2C) lines. The EDID multiplexer couples the I2C lines to the first EDID mode switch (shown in orange). The first EDID mode switch switches the video controller I2C lines to the first emulated EDID EEPROM chip (shown in gray). The chip write protect switch opens to enable writing. The video controller uses the I2C lines to write to the first emulated EDID EEPROM chip. Once the write operation is complete and verified, the video controller switches the EDID multiplexer to the next channel and the operation repeats until all chips are programmed. Once the write operation is complete, the video controller switches to normal operating mode, as shown in Figure 7 below.

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

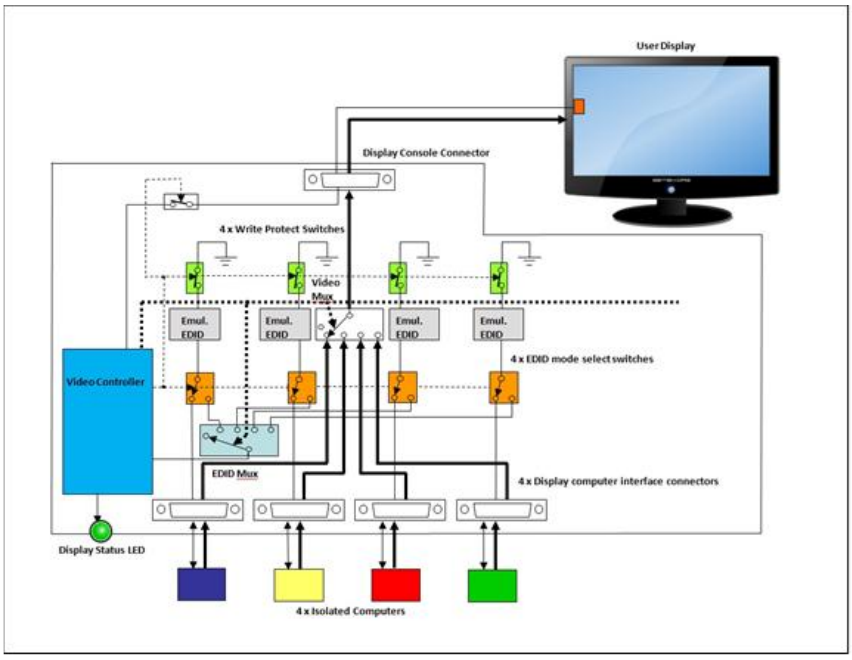



**Figure 6 – Display Normal Mode**

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

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

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

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

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

The TOE supports DVI-D video. EDID information is allowed to pass from the display to the computer, as described above. Hot-Plug Detection (HPD) information is also allowed to pass. Other protocols, including Audio Return Channel (ARC), EDID from the computer to the display, HDMI Ethernet and Audio Return Channel (HEAC), HDMI Ethernet Channel (HEC) and MCCS are blocked. High-bandwidth Digital Content Protection (HDCP) and Consumer Electronics Control (CEC) functions are not connected.

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

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

#### 6.1.2.9 FDP_SWI_EXT.1 PSD SWITCHING (PP_PSD_V4.0) AND FDP_SWI_EXT.2 PSD SWITCHING METHODS (PP_PSD_V4.0)

The TOE 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 buttons on the front panel or from the wired remote control, and drives the TOE channel select lines that control switching circuits within the TOE.

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

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

The user determines the host computer to be connected to the peripherals by pressing a button on the TOE front panel or on the wired remote control device. The front panel button of the selected computer is illuminated. Switching can only be initiated through express user action.

#### 6.1.2.10 FDP_SWI_EXT.3 TIED SWITCHING (MOD_KM_V1.0)

Figure 7 is a simplified block diagram showing the TOE keyboard and mouse data path for two ports. A Host Emulator (HE) communicates with the user keyboard via the USB protocol. The Host Emulator converts user key strokes into unidirectional serial data.

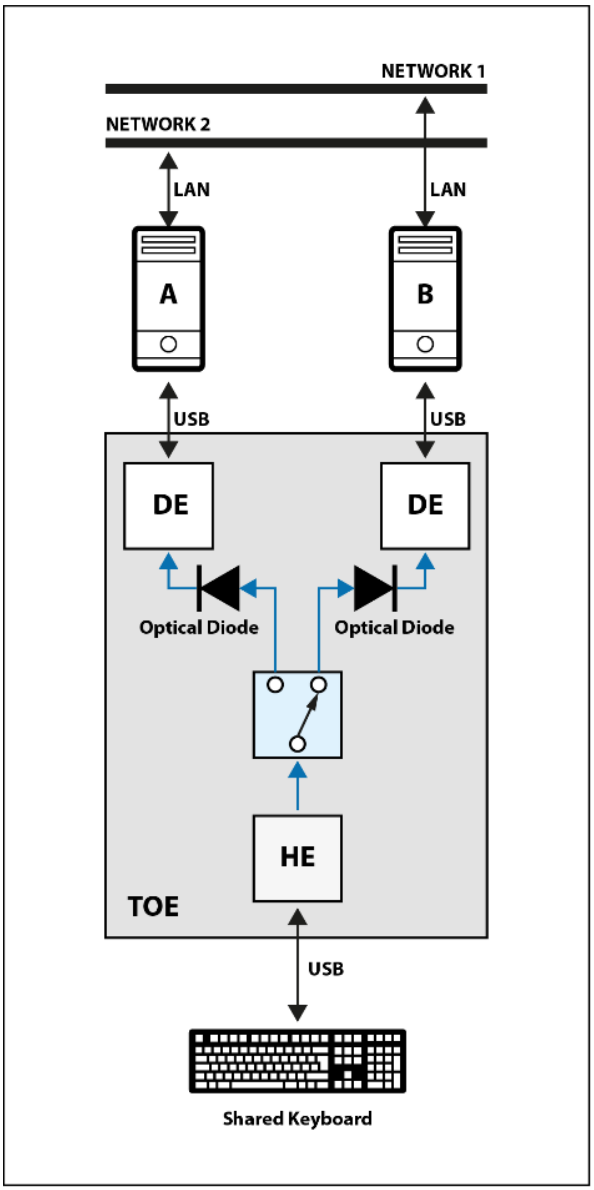



**Figure 7 – Simplified Switching Diagram**

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

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

Since the keyboard and mouse function are emulated by the TOE, the connected computer is not able to send data to the keyboard that would allow it to indicate that Caps Lock, Num Lock or Scroll Lock are set.

### 6.1.3 IDENTIFICATION AND AUTHENTICATION (FIA) AND SECURITY MANAGEMENT (FMT)

#### 6.1.3.1 FIA_UAU.2 USER AUTHENTICATION BEFORE ANY ACTION (PP_PSD_V4.0), FIA_UID.2 USER IDENTIFICATION BEFORE ANY ACTION (PP_PSD_V4.0), FMT_MOF.1 MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOR (PP_PSD_V4.0), FMT_SMF.1 SPECIFICATION OF MANAGEMENT FUNCTIONS (PP_PSD_V4.0) AND FMT_SMR.1 SECURITY ROLES (PP_PSD_V4.0)

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

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

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

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

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

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

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

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

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

### 6.1.4 PROTECTION OF THE TSF (FPT)

#### 6.1.4.1 FPT_FLS_EXT.1 FAILURE WITH PRESERVATION OF SECURE STATE (PP_PSD_V4.0), FPT_TST.1 TSF TESTING (PP_PSD_V4.0) AND FPT_TST_EXT.1 TSF TESTING (PP_PSD_V4.0)

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

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

If the self-test fails, the LEDs on the front panel blinks and/or the device makes a clicking sound to indicate the failure. The TOE disables the PSD switching functionality and remains in a disabled state until the self-test is rerun by device restart and the self-test passes.

There are no cases when a shutdown does not result in a self-test failure.

The users can verify the integrity of the TSF and TSF Data. The user can create a self-test failure by power-up the KVM while holding channel #1 button.

The device performs a self-test procedure for the backup battery upon each power-up. If the self-test detects that the battery is depleted or failing, a warning is indicated by abnormal LED behavior, ultimately leading to the anti-tampering function being triggered if the self-test fails. The battery is not a field replaceable item, and replacement should not be attempted by a user. If errors occur when using the product and the battery is suspected, contact HSL Technical Support.

#### 6.1.4.2 FPT_PHP.3 RESISTANCE TO PHYSICAL ATTACK (PP_PSD_V4.0)

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

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

When the anti-tampering mechanism on the KVM switch is triggered, an event is recorded in the TOE internal non-volatile memory with the time and date. This record may be read from the audit logs.

When the anti-tampering mechanism on the remote control is triggered, the device becomes permanently disabled. The channels in the remote constantly switch and the HID and display indications keeps on blinking which is the indication to the user of remote being tempered.

#### 6.1.4.3 FPT_NTA_EXT.1 NO ACCESS TO TOE (PP_PSD_V4.0)

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

- EDID data is accessible to connected computers from the TOE.
- Authorized administrators use a connected computer to access configuration data and settings.
- Authorized administrators use a connected computer to access TOE audit records.

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

#### 6.1.4.4 FPT_PHP.1 PASSIVE DETECTION OF PHYSICAL ATTACK (PP_PSD_V4.0)

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

Additionally, the device is fitted with holographic Tampering Evident Labels placed at critical locations on the TOE enclosure. If the label is removed, the word 'VOID' appears on both the label and the product surface. The remote control also has a holographic Tampering Evident Label placed at a critical location.

#### 6.1.4.5 FPT_STM.1 RELIABLE TIME STAMPS (PP_PSD_V4.0)

Each device includes a real-time clock powered by a battery. The purpose of the clock is to provide an accurate timestamp for audited events. The time is set during production using the Central Time Zone. Administrators are not permitted to modify the time. Time is not provided to external devices, so there is no requirement to coordinate time zones or change to daylight savings time. The battery is designed to power the unit for a minimum of ten years. If the battery fails, the device enters the tampered mode. The user must then replace the device.

### 6.1.5 TOE ACCESS (FTA)

#### 6.1.5.1 FTA_CIN_EXT.1 CONTINUOUS INDICATIONS (PP_PSD_V4.0)

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

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

# 7. ANNEX A – LETTER OF VOLATILITY

The table below provides volatility information and memory types for the High Sec Labs SK41D-4TR Peripheral Sharing Device. User data is not retained when the power is turned off.

**Table 16 – Letter of Volatility**

| Product Model | Number in each product | Function, Manufacturer and Part Number | Storage Type | Size | Power Source (if not the TOE) | Volatility | Contains User Data | Effect of RFD |
|---|---|---|---|---|---|---|---|---|
| SK41D-4TR | 1 | System Controller, Host emulators: ST Microelectronics STM32F446ZCT | Embedded SRAM[1] | 128 KB | Connected computer | Volatile | May contain user data | Data is purged |
| | | | Embedded Flash[2] | 256 KB | | Non-Volatile | No user data | Firmware is retained |
| | | | Embedded EEPROM | 4 KB | | Non-Volatile | No user data | Data is purged on RFD |
| | | | OTP Memory | 512 bytes | | Non-Volatile | No user data | Log data is retained |
| | 5 | Video Controller: ST Microelectronics STM32F070C6T6 | Embedded SRAM | 16 KB | Connected computer | Volatile | No user data | Data is purged |
| | | | Embedded Flash | 128 KB | | Non-Volatile | No user data | Firmware is retained |
| | | | Embedded EEPROM | 4 KB | | Non-Volatile | No user data | Data is purged on RFD |
| | 4 | Device emulators: ST Microelectronics STM32F070C6T6 | Embedded SRAM | 6 KB | Connected computer | Volatile | May contain user data | Data is purged |
| | | | Embedded Flash | 32 KB | | Non-Volatile | No user data | Firmware is |

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

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

| Product Model | Number in each product | Function, Manufacturer and Part Number | Storage Type | Size | Power Source (if not the TOE) | Volatility | Contains User Data | Effect of RFD |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | retained |
| | | | Embedded EEPROM | 4 KB | | Non-Volatile | No user data | Data is purged on RFD |

# 8. ACRONYM TABLE

Acronyms should be included as an Appendix in each document.

**Table 17 – Acronyms**

| Acronym | Definition |
|---|---|
| **CC** | Common Criteria |
| **DVI-D** | Digital Visual Interface-Digital only |
| **EDID** | Extended Display Identification Port |
| **EEPROM** | Electrically Erasable Programmable Read-Only Memory |
| **GUI** | Graphical User Interface |
| **HID** | Human Interface Device |
| **IP** | Internet Protocol |
| **KM** | Keyboard, Mouse |
| **KVM** | Keyboard, Video and Mouse |
| **LED** | Light Emitting Diodes |
| **MCCS** | Monitor Control Command Set |
| **NIAP** | Nation Information Assurance Partnership |
| **OTP** | One Time Programming |
| **PC** | Personal Computer |
| **PP** | Protection Profile |
| **PSD** | Peripheral Sharing Device |
| **PS/2** | Personal System/2 |
| **RCU** | Remote Control Unit |
| **RFD** | Restore to Factory Default |
| **SFR** | Security Functional Requirement |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSS** | TOE Summary Specification |
| **USB** | Universal Serial Bus |
| **VDC** | Volts Direct Current |