Vertiv CYBEX™ SCMV2160DPH, SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE Firmware Version 44404-E7E7 Peripheral Sharing Devices

Security Target

Doc No: 2149-001-D102C2
Version: 1.15
4 January 2022

Vertiv
1050 Dearborn Dr,
Columbus, OH 43085

Prepared by:

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

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

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

1.1 DOCUMENT ORGANIZATION

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

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

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

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

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

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

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

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

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

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

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

1.2 SECURITY TARGET REFERENCE

ST Title:	Vertiv CYBEX™ SCMV2160DPH, SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE Firmware Version 44404-E7E7 Peripheral Sharing Devices Security Target
ST Version:	1.15
ST Date:	4 January 2022

1.3 TOE REFERENCE

TOE Identification:	Vertiv CYBEX™ SCMV2160DPH, SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE Firmware Version 44404-E7E7 Peripheral Sharing Devices
TOE Developer:	Vertiv
TOE Type:	Peripheral Sharing Device (Other Devices and Systems)

1.4 TOE OVERVIEW

The Vertiv 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 Vertiv Peripheral Sharing Devices:

- Video Security
    - Computer video input interfaces are isolated through the use of separate electronic components, power and ground domains
    - The display is isolated by dedicated, read-only, Extended Display Identification Data (EDID) emulation for each computer
    - Access to the monitor's EDID is blocked
    - Access to the Monitor Control Command Set (MCCS commands) is blocked
    - Both DisplayPort and High-Definition Multimedia Interface (HDMI) video peripherals are supported on the SCMV2160DPH, SC840DPE and SC940DPE models. HDMI peripherals are supported on the SC840HE and SC940HE models, and DVI peripherals are supported on the SC840DVIE and SC940DVIE models

    - Video input is accepted as DisplayPort or HDMI on the SCMV2160DPH, SC840DPE and SC940DPE models. HDMI video input is supported on the SC840HE and SC940HE models, and DVI video input is supported on the SC840DVIE and SC940DVIE models
- 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
- Hardware Anti-Tampering
    - Special holographic tampering evident labels on the product's enclosure provide a clear visual indication if the product has been opened or compromised

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

Figure 1 is a simplified block diagram showing the TOE keyboard and mouse data path for two ports. A Host Emulator (HE) communicates with the user keyboard via the USB protocol. The Host Emulator converts user 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 key stroke is converted by the selected DE into a bi-directional stream to communicate with the computer.

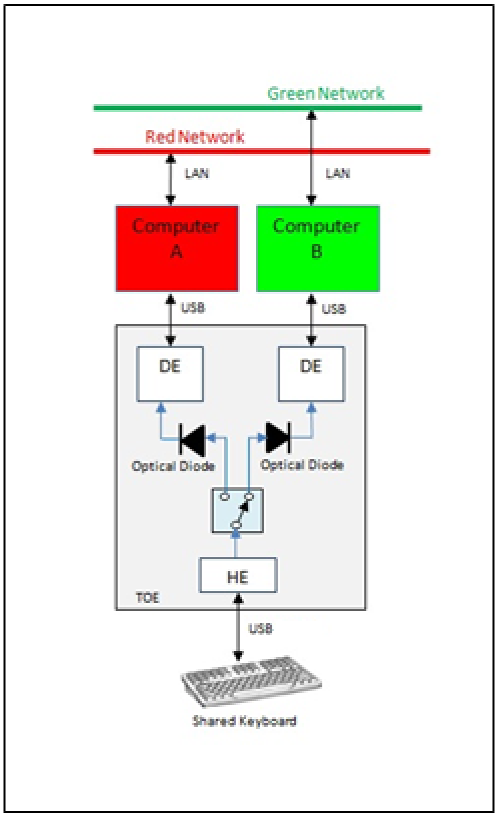


Figure 1 – Simplified Switching Diagram

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

1.4.1 TOE Environment

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

Component	Description
Connected Computers	1-16 General purpose computers
Keyboard	General purpose USB keyboard
Mouse	General purpose USB mouse
User display	Standard computer display (HDMI 2.0, DVI-D, or DisplayPort 1.1, 1.2 or 1.3)
Vertiv KVM Cables	USB Type-A to USB Type-B (keyboard and mouse) Video cable (DisplayPort, DVI-D, and HDMI)

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Evaluated Configuration

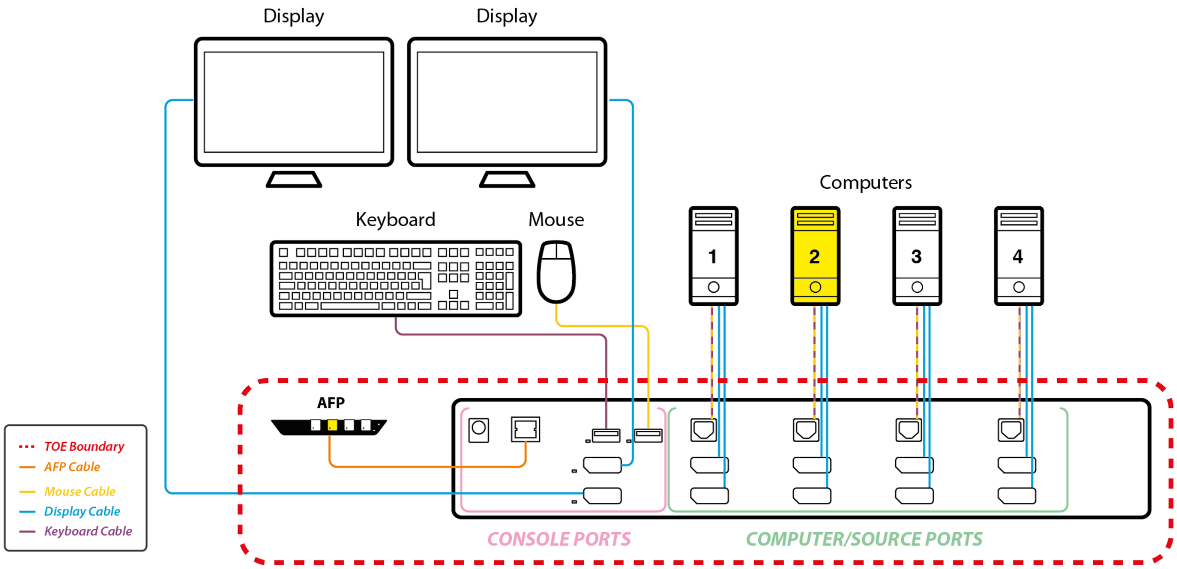


Figure 2 – KVM Switch Evaluated Configuration

Figure 2 shows a basic evaluated configuration for KVM Switches (SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE). In the evaluated configuration, the TOE is connected to four computers. The video input is DisplayPort, HDMI or DVI-D, and one or two displays are connected. The devices are used with an AFP004 remote control.

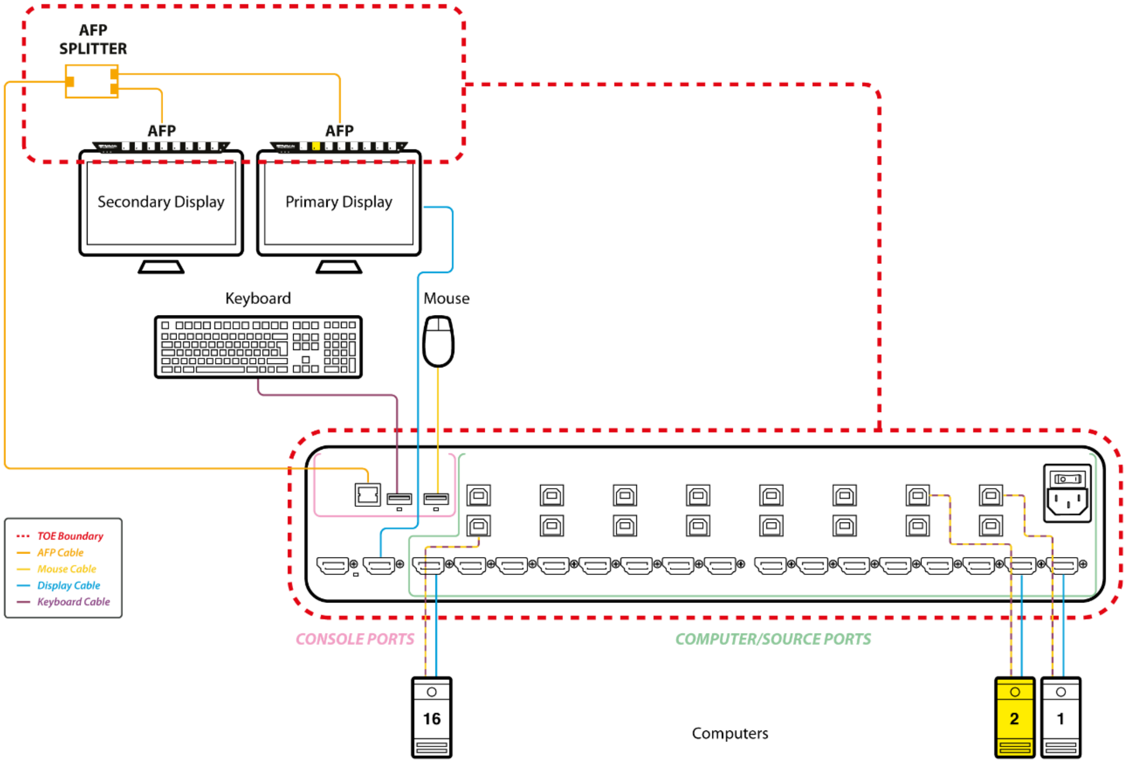


Figure 3 – KVM Multiviewer Evaluated Configuration

Figure 3 shows a basic evaluated configuration for the Multiviewer Switch (SCMV2160DPH). In the evaluated configuration, the TOE is connected to up to sixteen computers. The video input is DisplayPort or HDMI and two displays are connected. The device is used with two AFP008 remote control units, and an AFPSPLITTER. Use of the remote control splitter is described in Section 9.3.

1.5.2 Physical Scope

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

Family	Family Description	Part Number	Model	Tamper Evident labels	Video in	Video out	Number of supported displays	Keyboard, Mouse
Multiviewer	Secure KVM Multiviewer	CGA18699	SCMV2160DPH	Yes	DP/HDMI	DP/HDMI	2	Yes
Economy KVM	Secure KVMs	CGA19544	SC840DVIE	Yes	DVI	DVI	1	Yes
		CGA19545	SC940DVIE	Yes	DVI	DVI	2	Yes
		CGA19546	SC840HE	Yes	HDMI	HDMI	1	Yes
		CGA19547	SC940HE	Yes	HDMI	HDMI	2	Yes
		CGA19548	SC840DPE	Yes	DP/HDMI	DP/HDMI	1	Yes
		CGA19549	SC940DPE	Yes	DP/HDMI	DP/HDMI	2	Yes

Table 2 – TOE Peripheral Sharing Devices and Features

Description	Part Number	Model
Dual Active Front Panel (AFP) splitter kit for Secure Desktop Matrix	CGA17497	AFPSPLITTER
CYBEX™ Active Front Panel 8 Button Remote Control	CGA14335	AFP0008
CYBEX™ Active Front Panel 4 Button Remote Control	CGA14332	AFP0004

Table 3 – TOE Active Front Panel Devices

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:

- CYBEX™ SC SERIES SECURE SWITCHES SCMV200DPH MULTIVIEWER, 590-2307-501 Rev. B
- CYBEX™ SC SERIES SECURE SWITCHES SC800E/SC900E Quick Installation Guide, 590-2283-501 Rev. B

Guidance may be downloaded from the Vertiv website (www.vertiv.com) in .pdf format.

The following guidance is available upon request by emailing support.avocent@vertiv.com:

- Vertiv CYBEX™ SCMV2160DPH, SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE Firmware Version 44404-E7E7 Peripheral Sharing Devices Common Criteria Guidance Supplement, Version 1.2

1.5.3 Logical Scope

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

Functional Classes	Description
User Data Protection	The TOE provides secure switching capabilities for video, keyboard and mouse, display. The TOE ensures that only authorized peripheral devices may be used.
Protection of the TSF[1]	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. The TOE provides reliable timestamps in support of the audit function.
TOE Access	The TOE provides a continuous indication of which computer is currently selected.

Table 4 – Logical Scope of the TOE

[1] TOE Security Functionality

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

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

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

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST claims exact conformance with the National Information Assurance Partnership (NIAP) PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and Video/Display Devices [CFG_PSD-KM-VI_V1.0], which references the Protection Profile for Peripheral Sharing Device Version 4.0 [PP_PSD_V4.0], the modules listed in Section 2.4. The Technical Decisions in Table 5 apply to the PP and the modules and have been accounted for in the ST and in the evaluation.

Technical Decision	PP or Module
TD0506	[MOD_VI_V1.0]
TD0507	[MOD_KM_V1.0]
TD0514	[MOD_VI_V1.0]
TD0518	[PP_PSD_V4.0]
TD0539	[MOD_VI_V1.0]
TD0583	[PP_PSD_V4.0]

Technical Decision	PP or Module
TD0584	[MOD_VI_V1.0]
TD0586	[MOD_VI_V1.0]
TD0593	[MOD_KM_V1.0], [MOD_VI_V1.0]

Table 5 – Applicable Technical Decisions

2.3 PACKAGE CLAIM

This Security Target does not claim conformance with any package.

2.4 MODULE CLAIM

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

- PP-Module for Keyboard/Mouse Devices, Version 1.0
- PP-Module for Video/Display Devices, Version 1.0

2.5 CONFORMANCE RATIONALE

The TOE Keyboard, Video, Mouse (KVM), and Multiviewer devices are inherently consistent with the Compliant Targets of Evaluation described in the [PP_PSD_V4.0] and in the PP modules listed in Section 2.4, and with the PP-Configuration for Peripheral Sharing Device, 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 2.4.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 6 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[2] 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.

[2] 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 6 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

There are no Organizational Security Policies applicable to this TOE.

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 7.

Assumptions	Description
A.NO_TEMPEST	Computers and peripheral devices connected to the PSD are not TEMPEST approved. 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 7 – Assumptions

4 SECURITY OBJECTIVES

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

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

4.1 SECURITY OBJECTIVES FOR THE TOE

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

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td><b>O.COMPUTER_INTERFACE_ISOLATION</b></td><td>The PSD shall prevent unauthorized data flow to ensure that the PSD and its connected peripheral devices cannot be exploited in an attempt to leak data. The TOE-Computer interface shall be isolated from all other PSD-Computer interfaces while TOE is powered.
Addressed by:
<table>
<tr><td>MOD_VI</td><td>FDP_APC_EXT.1/VI, FDP_PDC_EXT.1</td></tr>
<tr><td>MOD_KM</td><td>FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1, FDP_SWI_EXT.3</td></tr>
</table></td></tr>
<tr><td><b>O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED</b></td><td>The PSD shall not allow data to transit a PSD-Computer interface while the PSD is unpowered.
Addressed by:
<table>
<tr><td>MOD_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><b>O.USER_DATA_ISOLATION</b></td><td>The PSD shall route user data, such as keyboard entries, only to the computer selected by the user. The PSD shall provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
Addressed by:
<table>
<tr><td>MOD_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><b>O.NO_USER _DATA_RETENTION</b></td><td>The PSD shall not retain user data in non-volatile memory after power up or, if supported, factory reset.
Addressed by:<table><tr><td>PP_PSD</td><td>FDP_RIP_EXT.1</td></tr><tr><td>MOD_KM</td><td>FDP_RIP.1/KM</td></tr></table></td></tr>
<tr><td><b>O.NO_OTHER _EXTERNAL _INTERFACES</b></td><td>The PSD shall not have any external interfaces other than those implemented by the TSF.
Addressed by:<table><tr><td>PP_PSD</td><td>FDP_PDC_EXT.1</td></tr></table></td></tr>
<tr><td><b>O.LEAK _PREVENTION _SWITCHING</b></td><td>The PSD shall ensure that there are no switching mechanisms that allow signal data leakage between connected computers.
Addressed by:<table><tr><td>PP_PSD</td><td>FDP_SWI_EXT.1, FDP_SWI_EXT.2(1), FDP_SWI_EXT.2(2)</td></tr></table></td></tr>
<tr><td><b>O.AUTHORIZED _USAGE</b></td><td>The TOE shall explicitly prohibit or ignore unauthorized switching mechanisms, either because it supports only one connected computer or because it allows only authorized mechanisms to switch between connected computers. Authorized switching mechanisms shall require express user action restricted to console buttons, console switches, console touch screen, wired remote control, and peripheral devices using a guard. Unauthorized switching mechanisms include keyboard shortcuts, also known as “hotkeys,” automatic port scanning, control through a connected computer, and control through keyboard shortcuts. Where applicable, the results of the switching activity shall be indicated by the TSF so that it is clear to the user that the switching mechanism was engaged as intended.
A conformant TOE may also provide a management function to configure some aspects of the TSF. If the TOE provides this functionality, it shall ensure that whatever management functions it provides can only be performed by authorized administrators and that an audit trail of management activities is generated.
Addressed by:</td></tr>
</table>

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

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

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td><b>O.SELF_TEST _FAIL_INDICATION</b></td><td>The PSD shall provide clear and visible user indications in the case of a self-test failure.
Addressed by:<table><tr><td>PP_PSD</td><td>FPT_TST_EXT.1</td></tr></table></td></tr>
<tr><td><b>O.PROTECTED _EDID</b></td><td>The TOE shall read the connected display Extended Display Identification Data (EDID) once during the TOE power up or reboot sequence and prevent any EDID channel write transactions that connected computers initiate.
Addressed by:<table><tr><td>MOD_VI</td><td>FDP_PDC_EXT.2/VI, FDP_SPR_EXT.1/DP, FDP_SPR_EXT.1/DVI-D, FDP_SPR_EXT.1/HDMI</td></tr></table></td></tr>
<tr><td><b>O.UNIDIRECTIONAL _VIDEO</b></td><td>The TOE shall enforce unidirectional video data flow from the connected computer video interface to the display interface only.
Addressed by:<table><tr><td>MOD_VI</td><td>FDP_UDF_EXT.1/VI</td></tr></table></td></tr>
<tr><td><b>O.EMULATED_INPUT</b></td><td>The TOE shall emulate the keyboard and/or mouse functions from the TOE to the connected computer.
Addressed by:<table><tr><td>MOD_KM</td><td>FDP_PDC_EXT.2/KM, FDP_PDC_EXT.3/KM</td></tr></table></td></tr>
<tr><td><b>O.UNIDIRECTIONAL _INPUT</b></td><td>The TOE shall enforce unidirectional keyboard and/or mouse device’s data flow from the peripheral device to only the selected computer.
Addressed by:<table><tr><td>MOD_KM</td><td>FDP_UDF_EXT.1/KM</td></tr></table></td></tr>
</table>

Table 8 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

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

Table 9 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

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

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

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

Threat or Assumption	Security Objective(s)	Rationale
T.UNAUTHORIZED _DEVICES	O.REJECT _UNAUTHORIZED _ENDPOINTS	The TOE's ability to reject unauthorized endpoints mitigates the threat of unauthorized devices being used to communicate with connected computers.
	O.REJECT _UNAUTHORIZED _PERIPHERAL	The TOE's ability to reject unauthorized peripherals mitigates the threat of unauthorized devices being used to communicate with connected computers.
	O.EMULATED_INPUT	The TOE's emulation of keyboard/mouse data input ensures that a connected computer will only receive this specific type of data through a connected peripheral.
	O.UNIDIRECTIONAL _VIDEO	The TOE's limitation of supported video protocol interfaces prevents the connection of unauthorized devices.
T.LOGICAL _TAMPER	O.NO_TOE_ACCESS	The TOE's prevention of logical access to its firmware, software, and memory mitigates the threat of logical tampering.
	O.EMULATED_INPUT	The TOE's emulation of keyboard/mouse data input prevents logical tampering of the TSF ensuring that only known inputs to it are supported.
T.PHYSICAL _TAMPER	O.ANTI_TAMPERING	The TOE mitigates the threat of physical tampering through use of an enclosure that provides tamper detection functionality.
	O.TAMPER_EVIDENT _LABEL	The TOE mitigates the threat of physical tampering through use of tamper evident labels that reveal physical tampering attempts.
T.REPLACEMENT	O.TAMPER_EVIDENT _LABEL	The TOE's use of a tamper evident label that provides authenticity of the device mitigates the threat that it is substituted for a replacement device during the acquisition process.

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

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

Table 10 – Security Objectives Rationale

5 EXTENDED COMPONENTS DEFINITION

The extended components definition is presented in Appendix C of the Protection Profile for Peripheral Sharing Device [PP_PSD_V4.0] and in the modules for keyboard/mouse devices [MOD_KM_V1.0], and display devices [MOD_VI_1.0]. It is repeated here to ensure the completeness of this ST.

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

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

Table 11 – Functional Families of Extended Components

5.1 CLASS FDP: USER DATA PROTECTION

5.1.1 FDP_APC_EXT Active PSD Connections

Family Behavior

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

Component Leveling

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

Management: FDP_APC_EXT.1

No specific management functions are identified.

Audit: FDP_APC_EXT.1

There are no auditable events foreseen.

FDP_APC_EXT.1 Active PSD Connections

Hierarchical to: No other components.

Dependencies: No dependencies

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

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

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

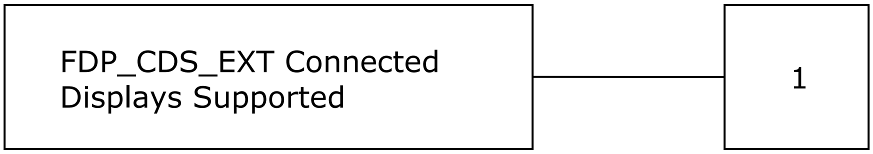
FDP_APC_EXT.1.4 The TSF shall ensure that no data transits the TOE when the TOE is in a failure state.

5.1.2 FDP_CDS_EXT Connected Displays Supported

Family Behavior

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

Component Leveling



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

Management: FDP_CDS_EXT.1

There are no specific management functions identified.

Audit: FDP_CDS_EXT.1

There are no auditable events foreseen.

FDP_CDS_EXT.1 Connected Displays Supported

Hierarchical to: No other components

Dependencies: No other components

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

5.1.3 FDP_FIL_EXT Device Filtering

Family Behavior

Components in this family define the requirements for device filtering.

Component Leveling

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

Management: FDP_FIL_EXT.1

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

- Ability to configure whitelist/blacklist members

Audit: FDP_FIL_EXT.1

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

- Configuration of whitelist/blacklist members

FDP_FIL_EXT.1 Device Filtering

Hierarchical to: No other components

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

FDP_FIL_EXT.1.1 The TSF shall have [*selection: configurable, fixed*] device filtering for [*assignment: list of supported peripheral interface types*] interfaces.

FDP_FIL_EXT.1.2 The TSF shall consider all [*assignment: blacklist name*] blacklisted devices as unauthorized devices for [*assignment: list of supported peripheral interface types*] interfaces in peripheral device connections.

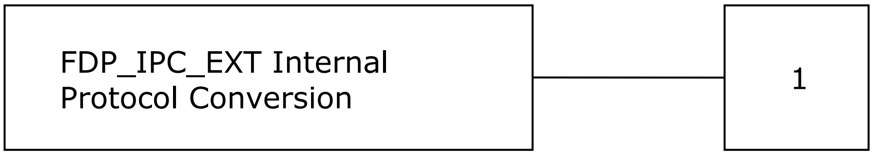
FDP_FIL_EXT.1.3 The TSF shall consider all [*assignment: whitelist name*] whitelisted devices as authorized devices for peripheral device connections only if they are not on the [*assignment: blacklist name*] blacklist or otherwise unauthorized.

5.1.4 FDP_IPC_EXT Internal Protocol Conversion

Family Behavior

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

Component Leveling



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

Management: FDP_IPC_EXT.1

There are no specific management functions identified.

Audit: FDP_IPC_EXT.1

There are no auditable events foreseen.

FDP_IPC_EXT.1 Internal Protocol Conversion

Hierarchical to: No other components

Dependencies: FDP_PDC_EXT.2 Authorized Connection Protocols

FDP_IPC_EXT.1.1 The TSF shall convert the [*assignment: original protocol*] protocol at the [*assignment: TOE external interface(s)*] into the [*assignment: converted protocol*] protocol within the TOE.

FDP_IPC_EXT.1.2 The TSF shall output the [*assignment: converted protocol*] protocol from inside the TOE to [*assignment: TOE external interface(s)*] as [*selection: [assignment: original protocol] protocol*], *[assignment: converted protocol] protocol*].

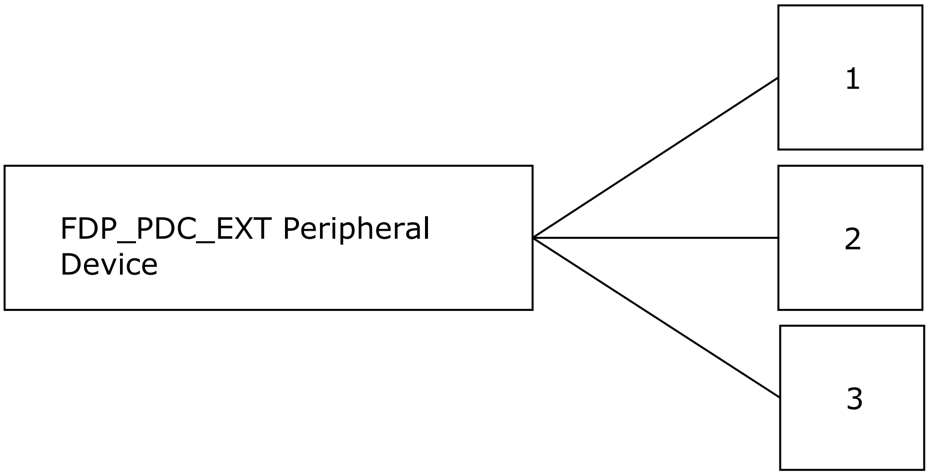
5.1.5 FDP_PDC_EXT Peripheral Device Connection

Family Behavior

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

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

Component Leveling



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

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

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

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

No specific management functions are identified.

Audit: FDP_PDC_EXT.1

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

- Acceptance or rejection of a peripheral

Audit: FDP_PDC_EXT.2, FDP_PDC_EXT.3

There are no specific auditable events foreseen.

FDP_PDC_EXT.1 Peripheral Device Connection

Hierarchical to:	No other components.
Dependencies:	No dependencies
FDP_PDC_EXT.1.1	The TSF shall reject connections with unauthorized devices upon TOE power up and upon connection of a peripheral device to a powered-on TOE.
FDP_PDC_EXT.1.2	The TSF shall reject connections with devices presenting unauthorized interface protocols upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

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

FDP_PDC_EXT.1.4 The TOE shall not have wireless interfaces.

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

FDP_PDC_EXT.2 Authorized Devices

Hierarchical to: No other components.

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

FDP_PDC_EXT.2.1 The TSF shall allow connections with authorized devices as defined in [*assignment: devices specified in the PP or PP-Module in which this SFR is defined*] and [*assignment: devices specified in another PP or PP-Module that shares a PP Configuration with the PP or PP-Module in which this SFR is defined*] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.2.2 The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*assignment: devices specified in the PP or PP Module in which this SFR is defined*] and [*assignment: devices specified in another PP or PP-Module that shares a PP-Configuration with the PP or PP-Module in which this SFR is defined*] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.3 Authorized Connection Protocols

Hierarchical to: No other components.

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

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

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

5.1.6 FDP_RDR_EXT Re-Enumeration Device Rejection

Family Behavior

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

Component Leveling

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

Management: FDP_RDR_EXT.1

No specific management functions are identified.

Audit: FDP_RDR_EXT.1

There are no specific auditable events foreseen.

FDP_RDR_EXT.1 Re-Enumeration Device Rejection

Hierarchical to: No other components.

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

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

5.1.7 FDP_RIP_EXT Residual Information Protection

Family Behavior

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

Component Leveling

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

Management: FDP_RIP_EXT.1

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

- Ability to trigger the TSF's purge function

Audit: FDP_RIP_EXT.1

There are no auditable events foreseen.

FDP_RIP_EXT.1 Residual Information Protection

Hierarchical to: No other components.

Dependencies: No dependencies

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

5.1.8 FDP_SPR_EXT Sub-Protocol Rules

Family Behavior

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

Component Leveling

FDP_SPR_EXT Sub-Protocol Rules
1

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

Management: FDP_SPR_EXT.1

No specific management functions are identified.

Audit: FDP_SPR_EXT.1

There are no auditable events foreseen.

FDP_SPR_EXT.1 Sub-Protocol Rules

Hierarchical to: No other components.

Dependencies: FDP_PDC_EXT.3 Authorized Connection Protocols

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

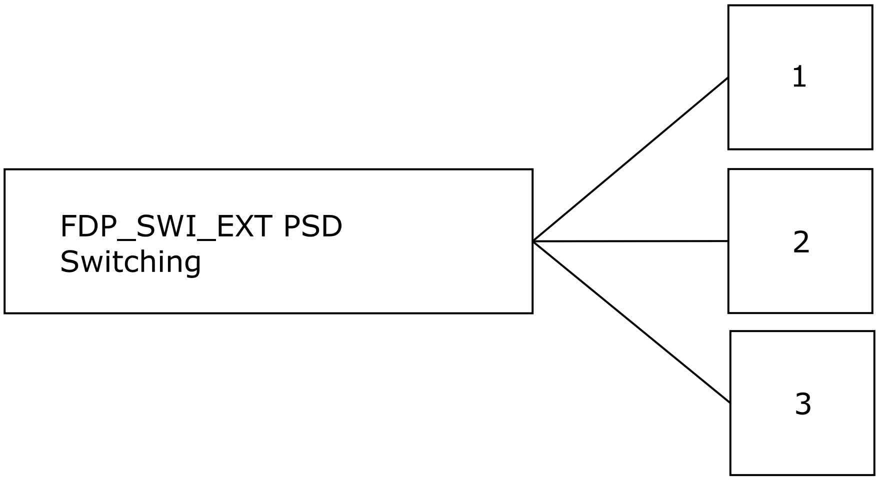
- block the following video/display sub-protocols:
  - [*assignment: list of blocked sub-protocols*]
- allow the following video/display sub-protocols:
  - [*assignment: list of allowed sub-protocols*].

5.1.9 FDP_SWI_EXT PSD Switching

Family Behavior

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

Component Leveling



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

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

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

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

No specific management functions are identified.

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

There are no auditable events foreseen.

FDP_SWI_EXT.1 PSD Switching

Hierarchical to: No other components.

Dependencies: No dependencies

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

FDP_SWI_EXT.2 PSD Switching Methods

Hierarchical to: No other components.

Dependencies: FDP_SWI_EXT.1 PSD Switching

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

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

FDP_SWI_EXT.3 Tied Switching

Hierarchical to: No other components.

Dependencies: FDP_SWI_EXT.1 PSD Switching

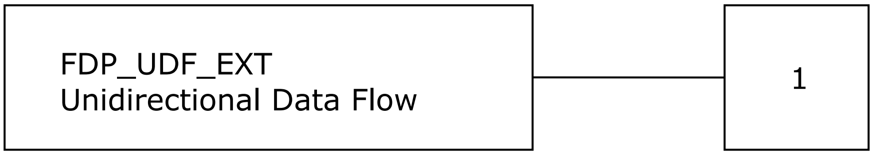
FDP_SWI_EXT.3.1 The TSF shall ensure that [*assignment: two or more tied peripheral devices*] are always switched together to the same connected computer.

5.1.10 FDP_UDF_EXT Unidirectional Data Flow

Family Behavior

Components in this family define unidirectional transmission of user data.

Component Leveling



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

Management: FDP_UDF_EXT.1

No specific management functions are identified.

Audit: FDP_UDF_EXT.1

There are no auditable events foreseen.

FDP_UDF_EXT.1 Unidirectional Data Flow

Hierarchical to: No other components.

Dependencies: FDP_APC_EXT.1 Active PSD Connections

FDP_UDF_EXT.1.1 The TSF shall ensure [*assignment: type of data*] data transits the TOE unidirectionally from the [*assignment: origin point of data*] interface to the [*assignment: destination point of data*] interface.

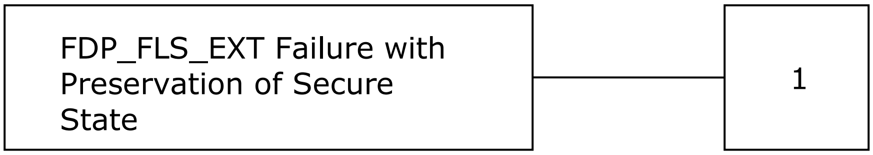
5.2 CLASS FPT: PROTECTION OF THE TSF

5.2.1 FPT_FLS_EXT Failure with Preservation of Secure State

Family Behavior

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

Component Leveling



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

Management: FPT_FLS_EXT.1

No specific management functions are identified.

Audit: FPT_FLS_EXT.1

There are no auditable events foreseen.

FPT_FLS_EXT.1 Failure with Preservation of Secure State

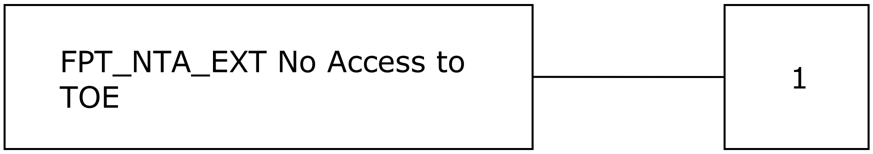
Hierarchical to:	No other components.
Dependencies:	FPT_TST.1 TSF Testing FPT_PHP.3 Resistance to Physical Attack
FPT_FLS_EXT.1.1	The TSF shall preserve a secure state when the following types of failures occur: failure of the power-on self-test and [*selection: failure of the anti-tamper function, no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

5.2.2 FPT_NTA_EXT No Access to TOE

Family Behavior

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

Component Leveling



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

Management: FPT_NTA_EXT.1

No specific management functions are identified.

Audit: FPT_NTA_EXT.1

There are no auditable events foreseen.

FPT_NTA_EXT.1 No Access to TOE

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

5.2.3 FPT_TST_EXT TSF Testing

Family Behavior

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

Component Leveling

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

Management: FPT_TST_EXT.1

No specific management functions are identified.

Audit: FPT_TST_EXT.1

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

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

FPT_TST_EXT.1 TSF Testing

Hierarchical to:	No other components.
Dependencies:	FPT_TST.1 TSF Testing
FPT_TST_EXT.1.1	The TSF shall respond to a self-test failure by providing users with a [*selection: visual, auditory*] indication of failure and by shutdown of normal TSF functions.

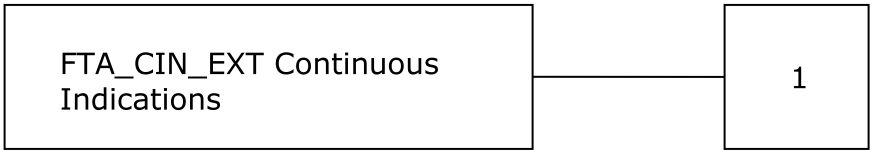
5.3 CLASS FTA: TOE ACCESS

5.3.1 FTA_CIN_EXT Continuous Indications

Family Behavior

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

Component Leveling



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

Management: FTA_CIN_EXT.1

No specific management functions are identified.

Audit: FTA_CIN_EXT.1

There are no auditable events foreseen.

FTA_CIN_EXT.1 Continuous Indications

Hierarchical to: No other components.

Dependencies: FDP_APC_EXT.1 Active PSD Connections

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

FTA_CIN_EXT.1.2 The TSF shall implement the visible indication using the following mechanism: **easily visible graphical and/or textual markings of each source video on the display,** [*selection: a button, a panel with lights, a screen with dimming function, a screen with no dimming function, [assignment: description of visible indication]*].

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

6 SECURITY FUNCTIONAL REQUIREMENTS

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

6.1 CONVENTIONS AND APPLICABILITY

6.1.1 Conventions

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

- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Selection: Indicated by surrounding brackets and italics, e.g., [*selected item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Iteration operations for iterations within the Protection Profile and associated modules are identified with a slash ('/') and an identifier (e.g. "/KM").
- Where an SFR does not apply equally to all devices, an additional tag has been added to indicate the products to which the SFR applies. This tag provides the applicable model names in brackets (e.g. FDP_SPR_EXT/DVI-D Sub-Protocol Rules (DVI-D Protocol) (SC840DPE, SC940DPE)). Additionally, a number is appended to the SFR identifier where multiple iterations of the SFR are required.

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

6.1.2 Section Applicability

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

TOE Model	Sections Describing Security Functionality
SCMV2160DPH	Section 6.2 and Section 6.3
SC840DVIE	Section 6.2 and Section 6.4
SC940DVIE	Section 6.2 and Section 6.5
SC840HE	Section 6.2 and Section 6.6

TOE Model	Sections Describing Security Functionality
SC940HE	Section 6.2 and Section 6.7
SC840DPE	Section 6.2 and Section 6.8
SC940DPE	Section 6.2 and Section 6.9

Table 12 – Devices and Applicable Sections

6.2 SECURITY FUNCTIONAL REQUIREMENTS FOR ALL DEVICES

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

Class	Identifier	Name	Source
User Data Protection (FDP)	FDP_APC_EXT.1/KM	Active PSD Connections	[MOD_KM_V1.0]
	FDP_APC_EXT.1/VI	Active PSD Connections	[MOD_VI_V1.0]
	FDP_FIL_EXT.1/KM	Device Filtering (Keyboard/Mouse)	[MOD_KM_V1.0]
	FDP_PDC_EXT.1	Peripheral Device Connection	[PP_PSD_V4.0] [MOD_VI_V1.0][3] [MOD_KM_V1.0][4]
	FDP_PDC_EXT.2/KM	Authorized Devices (Keyboard/Mouse)	[MOD_KM_V1.0]
	FDP_PDC_EXT.2/VI	Peripheral Device Connection (Video Output)	[MOD_VI_V1.0]
	FDP_PDC_EXT.3/KM	Authorized Connection Protocols (Keyboard/Mouse)	[MOD_KM_V1.0]

[3] 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.

[4] 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
	FDP_PDC_EXT.3/VI	Authorized Connection Protocols (Video Output)	[MOD_VI_V1.0]
	FDP_RDR_EXT.1	Re-Enumeration Device Rejection	[MOD_KM_V1.0]
	FDP_RIP_EXT.1	Residual Information Protection	[PP_PSD_V4.0]
	FDP_RIP.1/KM	Residual Information Protection (Keyboard Data)	[MOD_KM_V1.0]
	FDP_SWI_EXT.1	PSD Switching	[PP_PSD_V4.0]
	FDP_SWI_EXT.3	Tied Switching	[MOD_KM_V1.0]
	FDP_UDF_EXT.1/KM	Unidirectional Data Flow (Keyboard/Mouse)	[MOD_KM_V1.0]
	FDP_UDF_EXT.1/VI	Unidirectional Data Flow (Video Output)	[MOD_VI_V1.0]
Protection of the TSF (FPT)	FPT_FLS_EXT.1	Failure with Preservation of Secure State	[PP_PSD_V4.0]
	FPT_NTA_EXT.1	No Access to TOE	[PP_PSD_V4.0]
	FPT_PHP.1	Passive Detection of Physical Attack	[PP_PSD_V4.0]
	FPT_TST.1	TSF testing	[PP_PSD_V4.0]
	FPT_TST_EXT.1	TSF Testing	[PP_PSD_V4.0]
TOE Access (FTA)	FTA_CIN_EXT.1	Continuous Indications	[PP_PSD_V4.0] [MOD_VI_V1.0][5]

Table 13 – Summary of Security Functional Requirements

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

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 ~~or from~~ the interfaces selected by the user.

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

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

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

6.2.1.2 FDP_APC_EXT.1/VI Active PSD Connections

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

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

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

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

6.2.1.3 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.

6.2.1.4 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.

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

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

- ***authorized devices as defined in the PP-Module for 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.

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

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

- ***authorized devices 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.

6.2.1.7 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*].

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

FDP_PDC_EXT.3.1/VI The TSF shall have interfaces for the [*DVI-D, HDMI, DisplayPort*] protocols.

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

6.2.1.9 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.

6.2.1.10 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.

6.2.1.11 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**.

6.2.1.12 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*].

6.2.1.13 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.

6.2.1.14 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.

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

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, auditory*] 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 ADDITIONAL SECURITY REQUIREMENTS FOR SCMV2160DPH

Section 6.3 details the additional security functional requirements that are satisfied by the SCMV2160DPH TOE device.

Class	Identifier	Name	Source
User Data Protection (FDP)	FDP_CDS_EXT.1(2)	Connected Displays Supported (SCMV2160DPH, SC940DVIE, SC940HE, SC940DPE)	[MOD_VI_V1.0]
	FDP_IPC_EXT.1	Internal Protocol Conversion (SCMV2160DPH, SC840DPE, SC940DPE)	[MOD_VI_V1.0]
	FDP_SPR_EXT.1/DP	Sub-Protocol Rules (DisplayPort Protocol) (SCMV2160DPH, SC840DPE, SC940DPE)	[MOD_VI_V1.0]
	FDP_SPR_EXT.1/HDMI	Sub-Protocol Rules (HDMI Protocol) (SCMV2160DPH, SC840HE, SC940HE, SC840DPE, SC940DPE)	[MOD_VI_V1.0]

Class	Identifier	Name	Source
	FDP_SWI_EXT.2(2)	PSD Switching Methods (SCMV2160DPH)	[PP_PSD_V4.0] [MOD_KM_V1.0][6]

Table 14 – Summary of Additional Security Functional Requirements for SC2160DPH

6.3.1 User Data Protection (FDP)

6.3.1.1 FDP_CDS_EXT.1(2) Connected Displays Supported (SCMV2160DPH, SC940DVIE, SC940HE, SC940DPE)

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

6.3.1.2 FDP_IPC_EXT.1 Internal Protocol Conversion (SCMV2160DPH, SC840DPE, SC940DPE)

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

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

6.3.1.3 FDP_SPR_EXT.1/DP Sub-Protocol Rules (DisplayPort Protocol) (SCMV2160DPH, SC840DPE, SC940DPE)

FDP_SPR_EXT.1.1/DP The TSF shall apply the following rules for the [*DisplayPort*] protocol:

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

6.3.1.4 FDP_SPR_EXT.1/HDMI Sub-Protocol Rules (HDMI Protocol) (SCMV2160DPH, SC840HE, SC940HE, SC840DPE, SC940DPE)

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

[6] 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(1).

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

6.3.1.5 FDP_SWI_EXT.2(2) PSD Switching Methods (SCMV2160DPH)

FDP_SWI_EXT.2.1(2) 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(2) The TSF shall ensure that switching can be initiated only through express user action using [*console buttons, wired remote control, peripheral devices using a guard*].

6.4 ADDITIONAL SECURITY REQUIREMENTS FOR SC840DVIE

Section 6.4 details the additional security functional requirements that are satisfied by the SC840DVIE TOE device.

Class	Identifier	Name	Source
User Data Protection (FDP)	FDP_CDS_EXT.1(1)	Connected Displays Supported (SC840DVIE, SC840HE, SC840DPE)	[MOD_VI_V1.0]
	FDP_SPR_EXT.1/DVI-D	Sub-Protocol Rules (DVI-D Protocol) (SC840DVIE, SC940DVIE)	[MOD_VI_V1.0]

Class	Identifier	Name	Source
	FDP_SWI_EXT.2(1)	PSD Switching Methods (SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE)	[PP_PSD_V4.0] [MOD_KM_V1.0][7]

Table 15 – Summary of Additional Security Functional Requirements for SC840DVIE

6.4.1 User Data Protection (FDP)

6.4.1.1 FDP_CDS_EXT.1(1) Connected Displays Supported (SC840DVIE, SC840HE, SC840DPE)

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

6.4.1.2 FDP_SPR_EXT.1/DVI-D Sub-Protocol Rules (DVI-D Protocol) (SC840DVIE, SC940DVIE)

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*].

6.4.1.3 FDP_SWI_EXT.2(1) PSD Switching Methods (SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE)

FDP_SWI_EXT.2.1(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(1) The TSF shall ensure that switching can be initiated only through express user action using [*console buttons, wired remote control*].

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

6.5 ADDITIONAL SECURITY REQUIREMENTS FOR SC940DVIE

Section 6.5 details the security functional requirements that are satisfied by the SC940DVIE TOE device.

Class	Identifier	Name	Source
User Data Protection (FDP)	FDP_CDS_EXT.1(2)	Connected Displays Supported (SCMV2160DPH, SC940DVIE, SC940HE, SC940DPE)	[MOD_VI_V1.0]
	FDP_SPR_EXT.1/DVI-D	Sub-Protocol Rules (DVI-D Protocol) (SC840DVIE, SC940DVIE)	[MOD_VI_V1.0]
	FDP_SWI_EXT.2(1)	PSD Switching Methods (SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE)	[PP_PSD_V4.0] [MOD_KM_V1.0][8]

Table 16 – Summary of Additional Security Functional Requirements for SC940DVIE

6.5.1 User Data Protection (FDP)

6.5.1.1 FDP_CDS_EXT.1(2) Connected Displays Supported (SCMV2160DPH, SC940DVIE, SC940HE, SC940DPE)

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

6.5.1.2 FDP_SPR_EXT.1/DVI-D Sub-Protocol Rules (DVI-D Protocol) (SC840DVIE, SC940DVIE)

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,*

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

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

6.5.1.3 FDP_SWI_EXT.2(1) PSD Switching Methods (SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE)

FDP_SWI_EXT.2.1(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(1) The TSF shall ensure that switching can be initiated only through express user action using [*console buttons, wired remote control*].

6.6 ADDITIONAL SECURITY REQUIREMENTS FOR SC840HE

Section 6.6 details the additional security functional requirements that are satisfied by the SC840HE TOE device.

Class	Identifier	Name	Source
User Data Protection (FDP)	FDP_CDS_EXT.1(1)	Connected Displays Supported (SC840DVIE, SC840HE, SC840DPE)	[MOD_VI_V1.0]
	FDP_SPR_EXT.1/HDMI	Sub-Protocol Rules (HDMI Protocol) (SCMV2160DPH, SC840HE, SC940HE, SC840DPE, SC940DPE)	[MOD_VI_V1.0]
	FDP_SWI_EXT.2(1)	PSD Switching Methods (SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE)	[PP_PSD_V4.0] [MOD_KM_V1.0][9]

Table 17 – Summary of Additional Security Functional Requirements for SC840HE

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

6.6.1 User Data Protection (FDP)

6.6.1.1 FDP_CDS_EXT.1(1) Connected Displays Supported (SC840DVIE, SC840HE, SC840DPE)

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

6.6.1.2 FDP_SPR_EXT.1/HDMI Sub-Protocol Rules (HDMI Protocol) (SCMV2160DPH, SC840HE, SC940HE, SC840DPE, SC940DPE)

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

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

6.6.1.3 FDP_SWI_EXT.2(1) PSD Switching Methods (SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE)

FDP_SWI_EXT.2.1(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(1) The TSF shall ensure that switching can be initiated only through express user action using [*console buttons, wired remote control*].

6.7 ADDITIONAL SECURITY REQUIREMENTS FOR SC940HE

Section 6.7 details the additional security functional requirements that are satisfied by the SC940HE TOE device.

Class	Identifier	Name	Source
User Data Protection (FDP)	FDP_CDS_EXT.1(2)	Connected Displays Supported (SCMV2160DPH, SC940DVIE, SC940HE, SC940DPE)	[MOD_VI_V1.0]
	FDP_SPR_EXT.1/HDMI	Sub-Protocol Rules (HDMI Protocol) (SCMV2160DPH, SC840HE, SC940HE, SC840DPE, SC940DPE)	[MOD_VI_V1.0]
	FDP_SWI_EXT.2(1)	PSD Switching Methods (SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE)	[PP_PSD_V4.0] [MOD_KM_V1.0] [10]

Table 18 – Summary of Additional Security Functional Requirements for SC940HE

6.7.1 User Data Protection (FDP)

6.7.1.1 FDP_CDS_EXT.1(2) Connected Displays Supported (SCMV2160DPH, SC940DVIE, SC940HE, SC940DPE)

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

6.7.1.2 FDP_SPR_EXT.1/HDMI Sub-Protocol Rules (HDMI Protocol) (SCMV2160DPH, SC840HE, SC940HE, SC840DPE, SC940DPE)

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

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

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

6.7.1.3 FDP_SWI_EXT.2(1) PSD Switching Methods (SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE)

FDP_SWI_EXT.2.1(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(1) The TSF shall ensure that switching can be initiated only through express user action using [*console buttons, wired remote control*].

6.8 ADDITIONAL SECURITY REQUIREMENTS FOR SC840DPE

Section 6.8 details the additional security functional requirements that are satisfied by the SC840DPE TOE device.

Class	Identifier	Name	Source
User Data Protection (FDP)	FDP_CDS_EXT.1(1)	Connected Displays Supported (SC840DVIE, SC840HE, SC840DPE)	[MOD_VI_V1.0]
	FDP_IPC_EXT.1	Internal Protocol Conversion (SCMV2160DPH, SC840DPE, SC940DPE)	[MOD_VI_V1.0]
	FDP_SPR_EXT.1/DP	Sub-Protocol Rules (DisplayPort Protocol) (SCMV2160DPH, SC840DPE, SC940DPE)	[MOD_VI_V1.0]
	FDP_SPR_EXT.1/HDMI	Sub-Protocol Rules (HDMI Protocol) (SCMV2160DPH, SC840HE, SC940HE, SC840DPE, SC940DPE)	[MOD_VI_V1.0]

Class	Identifier	Name	Source
	FDP_SWI_EXT.2(1)	PSD Switching Methods (SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE)	[PP_PSD_V4.0] [MOD_KM_V1.0][11]

Table 19 – Summary of Additional Security Functional Requirements for SC840DPE

6.8.1 User Data Protection (FDP)

6.8.1.1 FDP_CDS_EXT.1(1) Connected Displays Supported (SC840DVIE, SC840HE, SC840DPE)

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

6.8.1.2 FDP_IPC_EXT.1 Internal Protocol Conversion (SCMV2160DPH, SC840DPE, SC940DPE)

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

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

6.8.1.3 FDP_SPR_EXT.1/DP Sub-Protocol Rules (DisplayPort Protocol) (SCMV2160DPH, SC840DPE, SC940DPE)

FDP_SPR_EXT.1.1/DP The TSF shall apply the following rules for the [*DisplayPort*] protocol:

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

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

6.8.1.4 FDP_SPR_EXT.1/HDMI Sub-Protocol Rules (HDMI Protocol) (SCMV2160DPH, SC840HE, SC940HE, SC840DPE, SC940DPE)

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

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

6.8.1.5 FDP_SWI_EXT.2(1) PSD Switching Methods (SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE)

FDP_SWI_EXT.2.1(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(1) The TSF shall ensure that switching can be initiated only through express user action using [*console buttons, wired remote control*].

6.9 ADDITIONAL SECURITY REQUIREMENTS FOR SC940DPE

Section 6.9 details the additional security functional requirements that are satisfied by the SC940DPE TOE device.

Class	Identifier	Name	Source
User Data Protection (FDP)	FDP_CDS_EXT.1(2)	Connected Displays Supported (SCMV2160DPH, SC940DVIE, SC940HE, SC940DPE)	[MOD_VI_V1.0]
	FDP_IPC_EXT.1	Internal Protocol Conversion (SCMV2160DPH, SC840DPE, SC940DPE)	[MOD_VI_V1.0]

Class	Identifier	Name	Source
	FDP_SPR_EXT.1/DP	Sub-Protocol Rules (DisplayPort Protocol) (SCMV2160DPH, SC840DPE, SC940DPE)	[MOD_VI_V1.0]
	FDP_SPR_EXT.1/HDMI	Sub-Protocol Rules (HDMI Protocol) (SCMV2160DPH, SC840HE, SC940HE, SC840DPE, SC940DPE)	[MOD_VI_V1.0]
	FDP_SWI_EXT.2(1)	PSD Switching Methods (SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE)	[PP_PSD_V4.0] [MOD_KM_V1.0][12]

Table 20 – Summary of Additional Security Functional Requirements for SC940DPE

6.9.1 User Data Protection (FDP)

6.9.1.1 FDP_CDS_EXT.1(2) Connected Displays Supported (SCMV2160DPH, SC940DVIE, SC940HE, SC940DPE)

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

6.9.1.2 FDP_IPC_EXT.1 Internal Protocol Conversion (SCMV2160DPH, SC840DPE, SC940DPE)

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

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

6.9.1.3 FDP_SPR_EXT.1/DP Sub-Protocol Rules (DisplayPort Protocol) (SCMV2160DPH, SC840DPE, SC940DPE)

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,*

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

  - *HDCP,*
  - *MCCS*]
- allow the following video/display sub-protocols:
  - [*EDID from display to computer,*
  - *HPD from display to computer,*
  - *Link Training*].

6.9.1.4 FDP_SPR_EXT.1/HDMI Sub-Protocol Rules (HDMI Protocol) (SCMV2160DPH, SC840HE, SC940HE, SC840DPE, SC940DPE)

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

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

6.9.1.5 FDP_SWI_EXT.2(1) PSD Switching Methods (SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE)

FDP_SWI_EXT.2.1(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(1) The TSF shall ensure that switching can be initiated only through express user action using [*console buttons, wired remote control*].

7 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 21.

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

Table 21 – Security Assurance Requirements

8 SECURITY REQUIREMENTS RATIONALE

8.1 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

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

8.2 DEPENDENCY RATIONALE

Table 22 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)	None	N/A
FDP_CDS_EXT.1(2)	None	N/A
FDP_FIL_EXT.1/KM	FDP_PDC_EXT.1	Included
FDP_IPC_EXT.1	FDP_PDC_EXT.2	Included
FDP_PDC_EXT.1	None	N/A
FDP_PDC_EXT.2/KM	FDP_PDC_EXT.1	Included
FDP_PDC_EXT.2/VI	FDP_PDC_EXT.2	Included
FDP_PDC_EXT.3/KM	FDP_PDC_EXT.1	Included
FDP_PDC_EXT.3/VI	FDP_PDC_EXT.2	Included
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/DVI-D	FDP_PDC_EXT.3	Included
FDP_SPR_EXT.1/HDMI	FDP_PDC_EXT.3	Included
FDP_SWI_EXT.1	None	N/A
FDP_SWI_EXT.2	FDP_SWI_EXT.1	Included
FDP_SWI_EXT.3	FDP_SWI_EXT.1	Included

SFR	Dependencies	Rationale Statement
FDP_UDF_EXT.1/KM	FDP_APC_EXT.1	Included
FDP_UDF_EXT.1/VI	FDP_APC_EXT.1	Included
FPT_FLS_EXT.1	FPT_TST.1 FPT_PHP.3	Included Included 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 22 – Functional Requirement Dependencies

8.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE

The TOE assurance requirements for this ST consist of the requirements indicated in the [PP_PSD_V4.0].

9 TOE SUMMARY SPECIFICATION

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

Unless otherwise stated, the description applies to all devices.

9.1 USER DATA PROTECTION

9.1.1 System Controller

Each device includes a System Controller which is responsible for device management, user interaction, system control security functions, and device monitoring. It receives user input from the switches on the front panel, 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 by pressing a button on the wired remote control. The front panel button of the selected computer is illuminated. Switching can only be initiated through express user action.

The Multiviewer device (SCMV2160DPH) may be switched with peripheral devices using a guard[13]. This is done by moving the mouse to the edge of the screen while pressing the left CTRL key.

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

9.1.1.1 Active PSD Connections

The TOE ensures that data flows only between the peripherals and the connected computer selected by the user. 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.

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

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

9.1.1.2 Connected Computer Interfaces

The connected computers are attached to the TOE as follows:

- The TOE connects to the keyboard and mouse port using a USB A to USB B cable. The USB A end attaches to the computer, and the USB B end attaches to the TOE.
- The TOE is connected to the computer video port using a video cable supporting DisplayPort, HDMI, or DVI-D interface.

The TOE will not recognize the following unauthorized devices:

- USB Mass Storage Device
- Any unauthorized device connected to the TOE through a USB hub

The TOE does not support the PS/2 protocol, and does not include an interface that would allow connection of a PS/2 device.

TOE Security Functional Requirements addressed: FDP_PDC_EXT.1.

9.1.1.3 Residual Information Protection

The Letter of Volatility is included as Annex A.

TOE Security Functional Requirements addressed: FDP_RIP_EXT.1.

9.1.2 Keyboard and Mouse Switching Functionality

9.1.2.1 Keyboard and Mouse Enumeration

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

The Static Random Access Memory (SRAM) in the host and device emulator circuitry stores USB Host stack parameters and up to the last 4 key codes. User data may be briefly retained; however, there are no data buffers. Data is erased during power off of the KVM, and when the user switches channels. When the TOE switches from one computer to another, the system controller sends a blank report to the Device Emulator to clear it of any key stroke information. The System Controller ensures 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. It is important to note that USB peripheral data is never saved in the Device Emulator buffer. It is passed to the computer immediately.

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

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

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

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

9.1.2.2 Keyboard and Mouse Switching Functionality

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

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

Since the keyboard and mouse function are emulated by the TOE, the connected computer is not able to send data to the keyboard that would allow it to indicate that Caps Lock, Num Lock or Scroll Lock are set. These are indicated on the TOE front panel, on the right hand side, as shown in Figure 7 in Section 9.3.

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

9.1.2.3 Keyboard and Mouse Compatible Device Types

The TOE employs fixed device filtering and accepts only USB HID devices at the keyboard and mouse peripheral ports. Only USB Type A connections are permitted. The TOE does not support a wireless connection to a mouse, keyboard or USB hub.

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

9.1.2.4 Re-Enumeration Device Rejection

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

TOE Security Functional Requirements addressed: FDP_RDR_EXT.1.

9.1.3 Video Switching Functionality

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

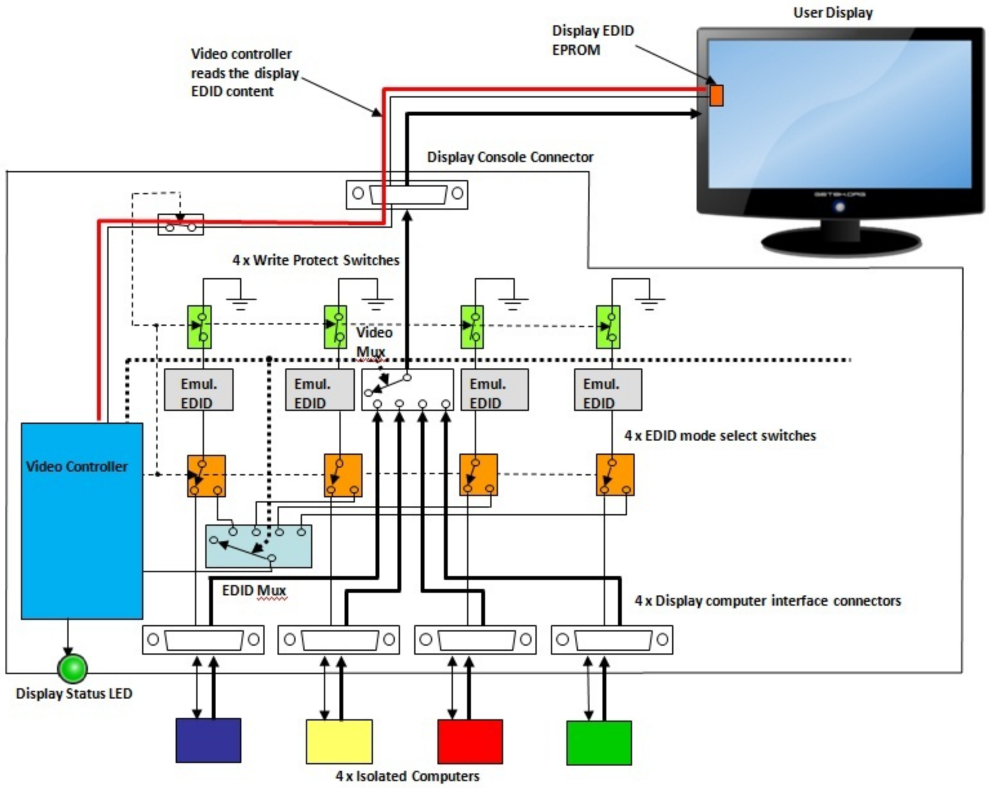


Figure 4 – Display EDID Read Function

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.

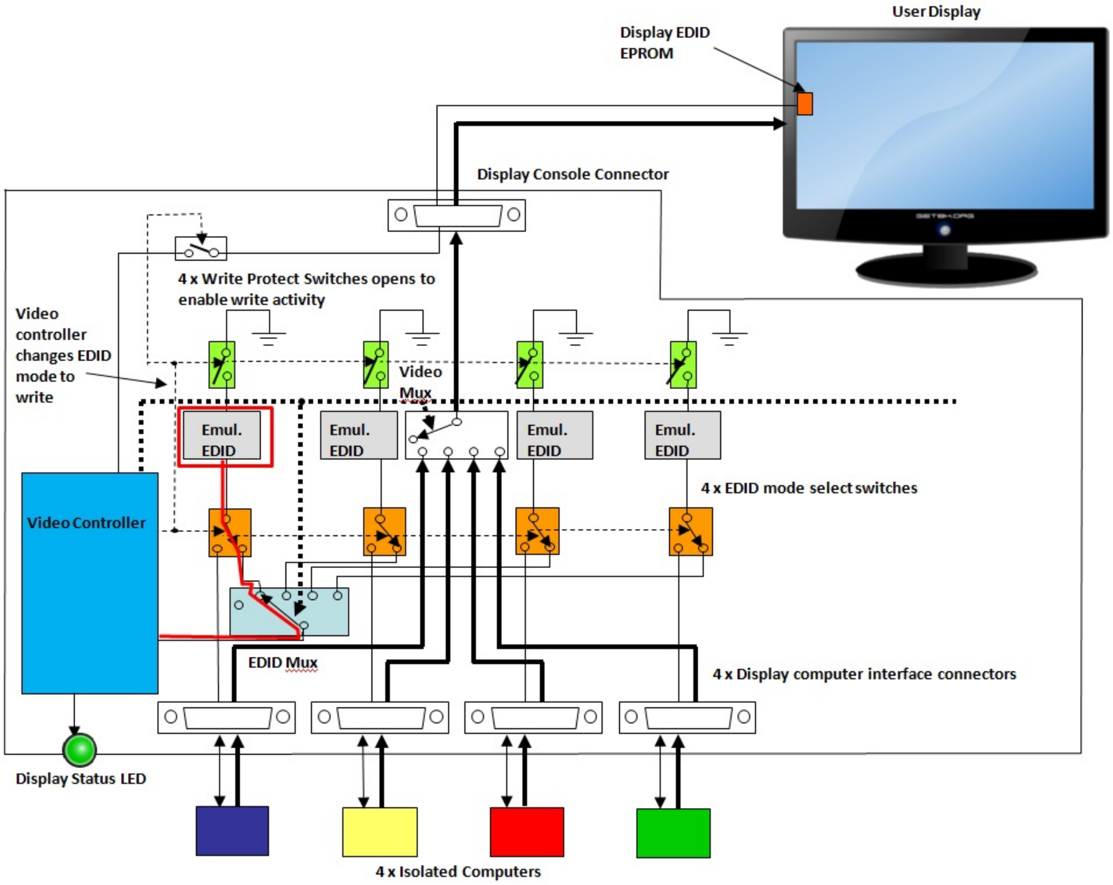

User Display
Display EDID EPROM
Display Console Connector
4 x Write Protect Switches opens to enable write activity
Video controller changes EDID mode to write
Video Mux
Emul. EDID
Emul. EDID
Emul. EDID
Emul. EDID
4 x EDID mode select switches
Video Controller
EDID Mux
4 x Display computer interface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

Figure 5 – Display EDID Write Function

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

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

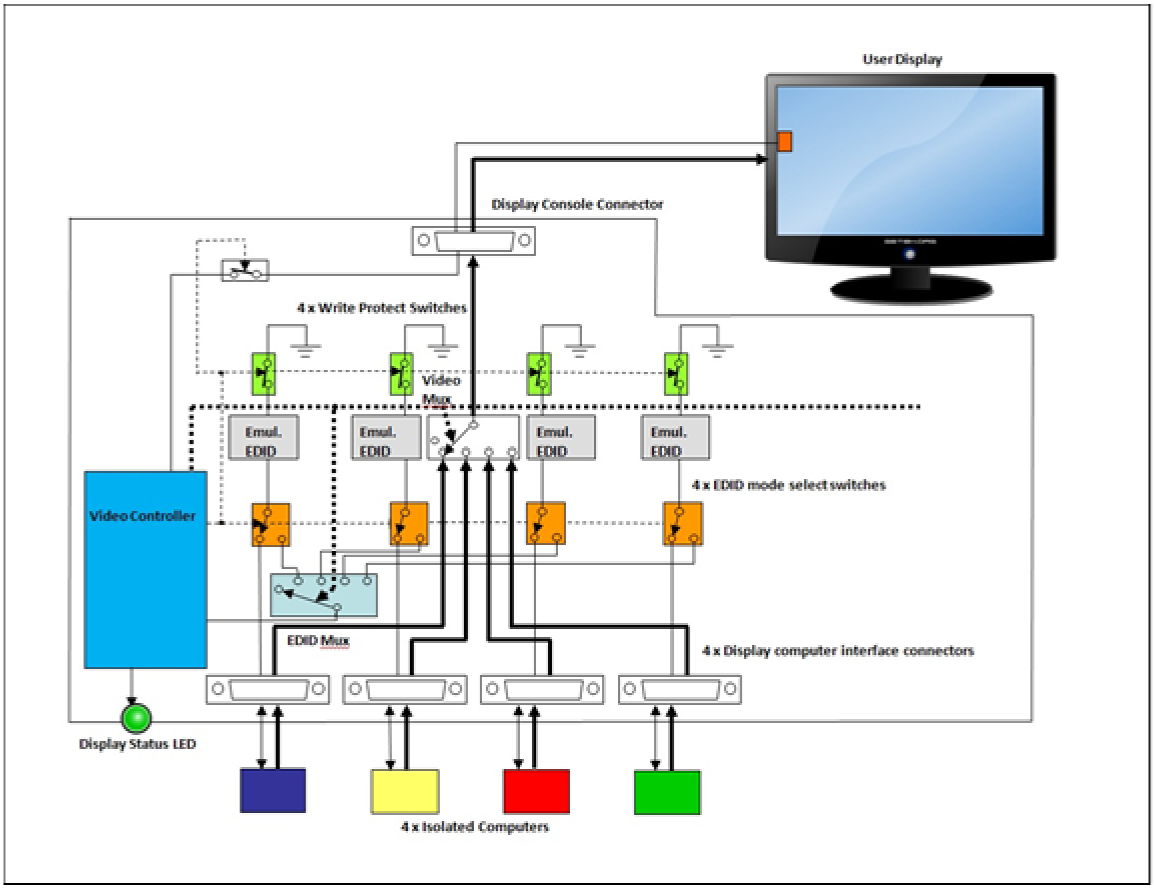


Figure 6 – Display Normal Mode

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

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

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

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

The TOE will reject any display device that does not present valid EDID content. A Light Emitting Diode (LED) on the rear panel of the TOE will indicate a rejected display device.

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

- For DisplayPort connections, the TOE video function filters the AUX channel by converting it to I2C EDID only. DisplayPort video is converted into an HDMI video stream, and the I2C EDID lines connected to the emulated EDID EEPROM functions as shown in the figures above. This allows EDID to be passed from the display to the computer (as described above), and allows Hot-Plug Detection (HPD) and Link Training information to pass through the TOE. AUX channel threats are mitigated through the conversion from DisplayPort to HDMI protocols. Traffic types including USB, Ethernet, MCCS, and EDID write from the computer to the display are blocked by the TOE. High-bandwidth Digital Content Protection (HDCP) and Consumer Electronics Control (CEC) functions are not connected.
    - The DisplayPort protocol is supported on the SCMV2160DPH, SC840DPE and SC940DPE devices.
- For DVI-D connections, EDID information is allowed to pass from the display to the computer, as described above. HPD information is also allowed to pass. Other protocols, including Audio Return Channel (ARC), EDID from the computer to the display, HDMI Ethernet and Audio Return Channel (HEAC), HDMI Ethernet Channel (HEC) and MCCS are blocked. HDCP and Consumer Electronics Control (CEC) functions are not connected.
    - The DVI-D protocol is supported on the SC840DVIE and SC940DVIE devices.
- For HDMI connections, EDID information is allowed to pass from the display to the computer, as described above. HPD information is also allowed to pass. Other protocols, including Audio Return Channel (ARC), EDID from the computer to the display, HDMI Ethernet and Audio Return Channel (HEAC), and HDMI Ethernet Channel (HEC) are blocked. HDCP and Consumer Electronics Control (CEC) functions are not connected.
    - The HDMI protocol is supported on the SCMV2160DPH, SC840HE, SC940HE, SC840DPE and SC940DPE devices.

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

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

TOE Security Functional Requirements addressed: FDP_IPC_EXT.1, FDP_SPR_EXT.1/DP, FDP_SPR_EXT.1/DVI-D, FDP_SPR_EXT.1/HDMI, FDP_SPR_EXT.1/USB.

9.1.3.1 Video Compatible Device Types

The TOE accepts any DisplayPort, DVI-D or HDMI display device at the video peripheral ports, as appropriate for the device. DisplayPort protocol peripherals are supported on the SCMV2160DPH, SC840DPE and SC940DPE devices. DVI-D protocol peripherals are supported on the SC840DVIE and SC940DVIE devices. HDMI protocol peripherals are supported on the SCMV2160DPH, SC840HE, SC940HE, SC840DPE and SC940DPE devices. The TOE does not support a wireless connection to a video display.

The SC840DVIE, SC840HE, SC840DPE devices support a single video display peripheral, and the SCMV2160DPH, SC940DVIE, SC940HE, SC940DPE devices support two video display peripherals.

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

9.2 PROTECTION OF THE TSF

9.2.1 No Access to TOE

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

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

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

TOE Security Functional Requirements addressed: FPT_NTA_EXT.1.

9.2.2 Passive Anti-tampering Functionality

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

Additionally, each device is fitted with one or more holographic Tampering Evident Labels placed at critical locations on the TOE enclosure. If the label is removed, the word 'VOID' appears on both the label and the product surface.

TOE Security Functional Requirements addressed: FPT_PHP.1.

9.2.3 TSF Testing

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

- Verification of the front panel push-buttons.
- Verification of the integrity of the microcontroller firmware.
- Verification of computer port isolation. This is tested by sending test packets to various interfaces and attempting to detect this traffic at all other interfaces.

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

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

9.3 TOE ACCESS

9.3.1 Continuous Indications

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

Figure 6 shows the selection buttons.

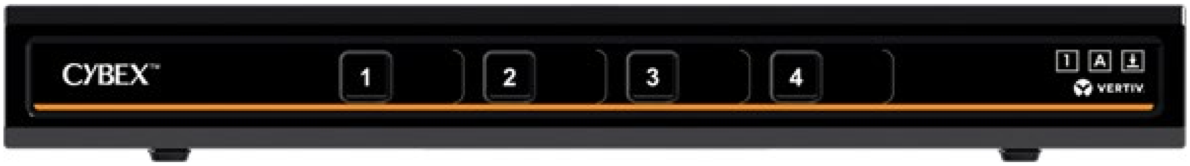


Figure 7 – Channel Selection

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

TOE Security Functional Requirements addressed: FTA_CIN_EXT.1.

9.3.2 Wired Remote Control

The SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE and SC940DPE KVM devices are used with the AFP004 Active Front Panel (AFP) remote control. The AFP sits on the display and is physically connected to the TOE device using an RS232 cable. The buttons on the AFP illuminate to indicate the selected channel.

The SCMV2160DPH is used with two AFP0008 remote control units and an AFPSPLITTER splitter, as shown in Figure 8. One AFP0008 is used to select channels 1-8 on the primary display, and the other is used to select channels 9-

16 on the secondary display. This allows the user to view two channels simultaneously.

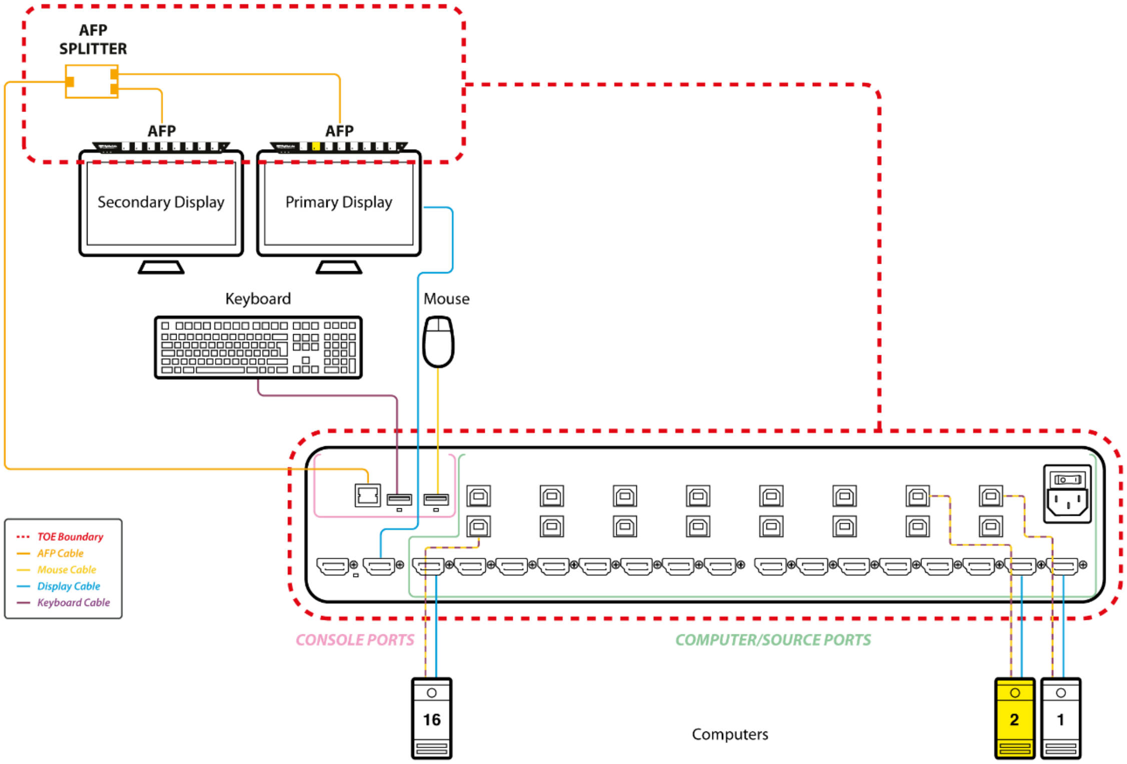


Figure 8 – AFP Splitter Implementation with SCMV2160DPH

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

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

10TERMINOLOGY AND ACRONYMS

10.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
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 23 – Terminology

10.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
ARC	Audio Return Channel
CC	Common Criteria
CEC	Consumer Electronics Control
DE	Device Emulator
DVI	Digital Visual Interface
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

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

Table 24 – Acronyms

11 REFERENCES

Identifier	**Title**
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017
[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_1.0]	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, 19 July 2019

Table 25 – References

ANNEX A – LETTER OF VOLATILITY

The table below provides volatility information and memory types for the Vertiv Peripheral Sharing Devices with Keyboard, Video and Mouse. User data is not retained in any TOE device when the power is turned off.

Product Models	No. in each product	Function, Manufacturer and Part Number	Storage Type	Size	Power Source (if not the TOE)	Volatility	Contains User Data
SC840DVIE SC940DVIE SC840HE SC940HE SC840DPE SC940DPE	1	System Controller, Host emulators: ST Microelectronics STM32F446ZCT	Embedded SRAM[1]	128KB		Volatile	May contain user data
			Embedded Flash[2]	256KB		Non-Volatile	No user data
			Embedded EEPROM[3]	4KB		Non-Volatile	No user data
			OTP Memory	512bytes		Non-Volatile	No user data
	0 in KM, 1 in KVM SH, 2 in KVM DH	Video Controller: ST Microelectronics STM32F070C6T6	Embedded SRAM[1]	16KB		Volatile	No user data
			Embedded Flash[2]	128KB		Non-Volatile	No user data
			Embedded EEPROM[3]	4KB		Non-Volatile	No user data
	4	Device emulators: ST Microelectronics STM32F070C6T6	Embedded SRAM[1]	6KB	Connected computer	Volatile	May contain user data
			Embedded Flash[2]	32KB		Non-Volatile	No user data
			Embedded EEPROM[3]	4KB		Non-Volatile	No user data
	0 in KM, 4 in 4P SH or 8 in 4P DH	EDID Emulator: ST Microelectronics M24C02-WMN6TP	EEPROM[4]	2 KB		Non-Volatile	No user data

Product Models	No. in each product	Function, Manufacturer and Part Number	Storage Type	Size	Power Source (if not the TOE)	Volatility	Contains User Data
SCMV2160DPH	1	System Controller, Host emulators: ST Microelectronics STM32F446ZCT	Embedded SRAM[1]	128KB		Volatile	May contain user data
			Embedded Flash[2]	256KB		Non-Volatile	No user data
			Embedded EEPROM[3]	4KB		Non-Volatile	No user data
			OTP Memory	512bytes		Non-Volatile	No user data
	1	Video Controller; ST Microelectronics STM32F070C6T6	Embedded SRAM[1]	16KB		Volatile	No user data
			Embedded Flash[2]	128KB		Non-Volatile	No user data
			Embedded EEPROM[3]	4KB		Non-Volatile	No user data
	4	Video Combiner FPGA	Embedded RAM	2,188Kb		Volatile	User data – video frame
	4	Video Combiner EEPROM	SPI Flash	512Mb		Non-Volatile	No user data
	4	Video Combiner RAM	DDR memory	4Gb		Volatile	User data – video frame
	16	Device emulators; ST Microelectronics STM32F070C6T6	Embedded SRAM[1]	6KB	Connected computer	Volatile	May contain user data
			Embedded Flash[2]	32KB		Non-Volatile	No user data
			Embedded EEPROM[3]	4KB		Non-Volatile	No user data
	16	EDID Emulator; ST Microelectronics M24C02-WMN6TP	EEPROM[4]	2 KB		Non-Volatile	No user data

Table 26 – Letter of Volatility

Notes:

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

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

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

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

ANNEX B – SFR DEVICE MATRIX

Table 27 indicates the SFRs supported by each device.

	FDP_APC_EXT.1/KM	FDP_APC_EXT.1/VI	FDP_CDS_EXT.1(1)	FDP_CDS_EXT.1(2)	FDP_FIL_EXT.1/KM	FDP_IPC_EXT.1	FDP_PDC_EXT.1	FDP_PDC_EXT.2/KM	FDP_PDC_EXT.2/VI	FDP_PDC_EXT.3/KM	FDP_PDC_EXT.3/VI	FDP_RDR_EXT.1	FDP_RIP_EXT.1	FDP_RIP.1/KM	FDP_SPR_EXT.1/DP	FDP_SPR_EXT.1/DVI-D	FDP_SPR_EXT.1/HDMI	FDP_SWI_EXT.1	FDP_SWI_EXT.2(1)	FDP_SWI_EXT.2(2)	FDP_SWI_EXT.3	FDP_UDF_EXT.1/KM	FDP_UDF_EXT.1/VI	FPT_FLS_EXT.1	FPT_NTA_EXT.1	FPT_PHP.1	FPT_TST.1	FPT_TST_EXT.1	FTA_CIN_EXT.1
SCMV2160DPH	X	X		X	X	X	X	X	X	X	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X	X	X
SC840DVIE	X	X	X		X		X	X	X	X	X	X	X	X		X		X	X		X	X	X	X	X	X	X	X	X
SC940DVIE	X	X		X	X		X	X	X	X	X	X	X	X		X		X	X		X	X	X	X	X	X	X	X	X
SC840HE	X	X	X		X		X	X	X	X	X	X	X	X			X	X	X		X	X	X	X	X	X	X	X	X
SC940HE	X	X		X	X		X	X	X	X	X	X	X	X			X	X	X		X	X	X	X	X	X	X	X	X
SC840DPE	X	X	X		X	X	X	X	X	X	X	X	X	X	X		X	X	X		X	X	X	X	X	X	X	X	X
SC940DPE	X	X		X	X	X	X	X	X	X	X	X	X	X	X		X	X	X		X	X	X	X	X	X	X	X	X
AFP0004*																		X	X		X					X			X
AFP0008*																		X	X		X					X			X
AFPSPLITTER *																		X	X		X					X			X

Table 27 – Security Functional Requirements and Devices

*The Active Front Panel remote control devices contribute to the enforcement of the specified SFRs. These devices are only used with another TOE device.