IHSE K487-1PHCA-N, K487-1PHSA-N, K487-1PHCRA-N, K487-1PHSRA-N, K497-1PHCA-N, K497-1PHSA-N, K497-1PHCRA-N, K497-1PHSRA-N Firmware Version 44404-E7E7 Isolator Devices

Security Target

Doc No: 2149-001-D102E1
Version: 1.5
3 November 2022

IHSE GmbH
Benzstraße 1
88094 Oberteuringen
Germany

Prepared by:

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

DOCUMENT HISTORY

Rev.	Issue Date	Description	Author	Reviewer
0.1draft	16 January 2020	Initial draft for developer review	Teresa MacArthur	Dawn Adams
0.2	18 February 2020	Initial draft for evaluation	Teresa MacArthur	
0.3	23 April 2020	ST Split	Teresa MacArthur	
0.4	21 June 2020	Consistency with other STs.	Teresa MacArthur	
0.5	1 July 2020	Developer comments	Teresa MacArthur	
0.6	10 July 2020	Addressed evaluator comments	Teresa MacArthur	
0.7	21 July 2020	Added TD	Teresa MacArthur	
0.8	5 January 2021	Addressed NIAP and CSE comments on other STs to date	Teresa MacArthur	
0.9	19 May 2021	Added TDs	Teresa MacArthur	
1.0	8 June 2021	Added TD	Teresa MacArthur	
1.1	18 January 2022	Addressed Evaluator ORs	Ben Buttera	
1.2	4 August 2022	Added TD	Ben Buttera	
1.3	3 October 2022	Corrected failure state indicator	Rafeh Mohammed	
1.4	25 October 2022	AGD version update	Ben Buttera	
1.5	3 November 2022	AGD version update	Ben Buttera	

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 Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

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

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

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

1.2 SECURITY TARGET REFERENCE

ST Title:	K487-1PHCA-N, K487-1PHSA-N, K487-1PHCRA-N, K487-1PHSRA-N, K497-1PHCA-N, K497-1PHSA-N, K497-1PHCRA-N, K497-1PHSRA-N Firmware Version 44404-E7E7 Isolator Devices Security Target
ST Version:	1.5
ST Date:	3 November 2022

1.3 TOE REFERENCE

TOE Identification:	K487-1PHCA-N, K487-1PHSA-N, K487-1PHCRA-N, K487-1PHSRA-N, K497-1PHCA-N, K497-1PHSA-N, K497-1PHCRA-N, K497-1PHSRA-N Firmware Version 44404-E7E7 Isolator Devices
TOE Developer:	IHSE GmbH
TOE Type:	Peripheral Sharing Device (Other Devices and Systems)

1.4 TOE OVERVIEW

The IHSE Isolator devices ensure unidirectional flow of data between peripheral devices and a secure connected computer.

The following security features are provided by the IHSE Isolator devices:

- Video Security
    - The display is isolated through a dedicated, read-only, Extended Display Identification Data (EDID) emulation function
    - Access to the monitor's EDID is blocked
    - Access to the Monitor Control Command Set (MCCS commands) is blocked
    - DisplayPort (DP) and High-Definition Multimedia Interface (HDMI) video peripheral devices are supported
- Keyboard and Mouse Security
    - The keyboard and mouse are isolated by dedicated, Universal Serial Bus (USB) device emulation
    - 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
- Audio Security
    - One-way computer to speaker sound flow is enforced through unidirectional optical data diodes
- 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

IHSE Isolator devices use isolated microcontrollers to emulate connected peripherals in order to prevent an unauthorized data flow through bit-by-bit signaling.

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

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

Component	Description
Connected Computer	General purpose computer
Keyboard	General purpose USB keyboard
Mouse	General purpose USB mouse
Audio output device	Analog audio output device (speakers or headphones)
User display	Standard computer display (HDMI 2.0, or DisplayPort 1.1, 1.2 or 1.3)
IHSE Cables	USB Type-A to USB Type-B (keyboard and mouse) Video cable (DisplayPort or HDMI) 3.5mm stereo cable (Audio cable)

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Evaluated Configuration

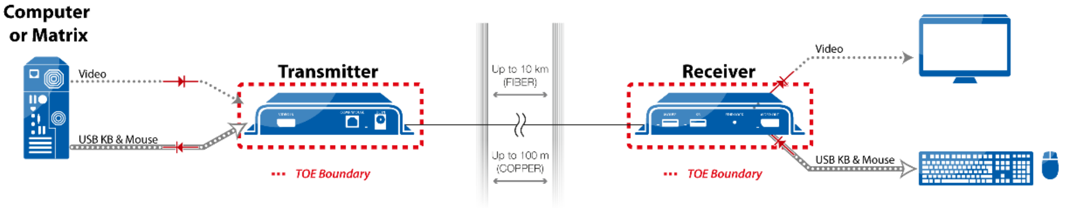


Figure 1 – Isolator Evaluated Configuration

In the evaluated configuration, the isolator device is connected to the computer and to the video, keyboard and mouse and audio peripherals to ensure unidirectional communications. The audio connection is not shown in the diagram.

1.5.2 Physical Scope

The TOE consists of the devices shown in Table 2.

Family	Description	Part Number	Model	Tamper Evident labels	Analog Audio	Video in	Video out	Number of supported displays	KM
Isolator devices supporting DisplayPort and HDMI video, Keyboard and Mouse and Audio	Copper HD KVMA Isolated Secure Extender	CGA20108	K487-1PHCA-N	Yes	Yes	DP/HDMI	DP/HDMI	1	Yes
	Fiber HD KVMA Isolated Secure Extender	CGA20109	K487-1PHSA-N	Yes	Yes	DP/HDMI	DP/HDMI	1	Yes
	Copper HD KVMA Isolated Redundant Secure Extender	CGA20408	K487-1PHCRA-N	Yes	Yes	DP/HDMI	DP/HDMI	1	Yes
	Fiber HD KVMA Isolated Redundant Secure Extender	CGA20409	K487-1PHSRA-N	Yes	Yes	DP/HDMI	DP/HDMI	1	Yes
	Copper UHD KVMA Isolated Secure Extender	CGA20110	K497-1PHCA-N	Yes	Yes	DP/HDMI	DP/HDMI	1	Yes
	Fiber UHD KVMA Isolated Secure Extender	CGA20111	K497-1PHSA-N	Yes	Yes	DP/HDMI	DP/HDMI	1	Yes
	Copper UHD KVMA Isolated Redundant Secure Extender	CGA20410	K497-1PHCRA-N	Yes	Yes	DP/HDMI	DP/HDMI	1	Yes
	Fiber UHD KVMA Isolated Redundant Secure Extender	CGA20411	K497-1PHSRA-N	Yes	Yes	DP/HDMI	DP/HDMI	1	Yes

Table 2 – TOE Peripheral Sharing Devices and Features

1.5.2.1 TOE Delivery

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

1.5.2.2 TOE Guidance

The TOE includes the following guidance documentation:

- QUICK SETUP Draco vario Secure Extender K487-1PHCA-N, K487-1PHCRA-N, K487-1PHSA-N, K487-1PHSRA-N Document no.: q487_0001 Rev.: 0001
  - https://www.ihse.de/wp-content/uploads/files/quick-setups/q487_0001.pdf
- QUICK SETUP Draco vario Secure Extender K497-1PHCA-N, K497-1PHCRA-N, K497-1PHSA-N, K497-1PHSRA-N Document no.: q497_0001 Rev.: 0001
  - https://www.ihse.de/wp-content/uploads/files/quick-setups/q497_0001.pdf

Guidance may be downloaded from the IHSE website (www.ihse.com) in .pdf format.

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

- IHSE K487-1PHCA-N, K487-1PHSA-N, K487-1PHCRA-N, K487-1PHSRA-N, K497-1PHCA-N, K497-1PHSA-N, K497-1PHCRA-N, K497-1PHSRA-N Firmware Version 44404-E7E7 Isolator Devices Common Criteria Guidance Supplement Version 1.5

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 3 summarizes the logical scope of the TOE.

Functional Classes	Description
User Data Protection	The TOE enforces unidirectional data flow for keyboard and mouse, display, and audio output. 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.

Table 3 – 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 PP-CONFIGURATION CONFORMANCE CLAIM

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

This PP-Configuration includes the following components:

- Base-PP: Protection Profile for Peripheral Sharing Device, Version 4.0 [PP_PSD_V4.0]
- PP-Module: PP-Module for Keyboard/Mouse Devices, Version 1.0 [MOD_KM_V1.0]
- PP-Module: PP-Module for Video/Display Devices, Version 1.0 [MOD_VI_V1.0]
- PP-Module: PP-Module for Analog Audio Output Devices, Version 1.0 [MOD_AO_V1.0]

2.3 TECHNICAL DECISIONS

The Technical Decisions in Table 4 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]
TD0557	[MOD_AO_V1.0]
TD0583	[PP_PSD_V4.0]
TD0584	[MOD_VI_V1.0]
TD0585	[MOD_AO_V1.0]
TD0586	[MOD_VI_V1.0]
TD0593	[MOD_AO_V1.0], [MOD_KM_V1.0], [MOD_VI_V1.0]
TD0620	[MOD_VI_V1.0]

Table 4 – Applicable Technical Decisions

2.4 PACKAGE CLAIM

This Security Target does not claim conformance with any package.

2.5 CONFORMANCE RATIONALE

The TOE Isolator devices are inherently consistent with the Compliant Targets of Evaluation described in the [PP_PSD_V4.0] (Use Case 2) and in the PP modules listed in Section 2.2, and with the PP-Configuration for Peripheral Sharing Device[2], Analog Audio Output Devices, Keyboard/Mouse Devices, and Video/Display Devices [CFG_PSD-AO-KM-VI_V1.0].

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

[2] Peripheral Sharing Device

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 5 lists the threats described in Section 3.1 of the [PP_PSD_V4.0] and [MOD_AO_V1.0]. Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.DATA_LEAK	A connection via the PSD[3] 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.

[3] Peripheral Sharing Device

Threat	Description
T.FAILED	Detectable failure of a PSD may cause an unauthorized information flow or weakening of PSD security functions.
T.MICROPHONE_USE	A malicious agent could use an unauthorized peripheral device such as a microphone, connected to the TOE audio out peripheral device interface to eavesdrop or transfer data across an air-gap through audio signaling.
T.AUDIO_REVERSED	A malicious agent could repurpose an authorized audio output peripheral device by converting it to a low-gain microphone to eavesdrop on the surrounding audio or transfer data across an air-gap through audio signaling.

Table 5 – 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 6.

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.

Assumptions	Description
A.USER_ALLOWED_ACCESS	All PSD users are allowed to interact with all connected computers. It is not the role of the PSD to prevent or otherwise control user access to connected computers. Computers or their connected network shall have the required means to authenticate the user and to control access to their various resources.
A.NO_SPECIAL_ANALOG _CAPABILITIES	The computers connected to the TOE are not equipped with special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, digital signal processing function, or analog video capture function.
A.NO_MICROPHONES	Users are trained not to connect a microphone to the TOE audio output interface.

Table 6 – 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_AO</td><td>FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1</td></tr>
<tr><td>MOD_VI</td><td>FDP_APC_EXT.1/VI, FDP_PDC_EXT.1</td></tr>
<tr><td>MOD_KM</td><td>FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1</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_AO</td><td>FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1</td></tr>
<tr><td>MOD_VI</td><td>FDP_APC_EXT.1/VI, FDP_PDC_EXT.1</td></tr>
<tr><td>MOD_KM</td><td>FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1</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.</td></tr>
</table>

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td></td><td>Addressed by:
<table>
<tr><td>MOD_AO</td><td>FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1</td></tr>
<tr><td>MOD_VI</td><td>FDP_APC_EXT.1/VI, FDP_PDC_EXT.1</td></tr>
<tr><td>MOD_KM</td><td>FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1</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>
</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</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</td></tr>
</table>

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td></td><td>activities is generated.
Addressed by:<table><tr><td>PP_PSD</td><td>FDP_SWI_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_AO</td><td>FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1</td></tr><tr><td>MOD_VI</td><td>FDP_APC_EXT.1/VI, FDP_PDC_EXT.1</td></tr><tr><td>MOD_KM</td><td>FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1</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_AO</td><td>FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1</td></tr><tr><td>MOD_VI</td><td>FDP_PDC_EXT.2/VI, FDP_PDC_EXT.3/VI, FDP_IPC_EXT.1, FDP_SPR_EXT.1/DP, FDP_SPR_EXT.1/HDMI</td></tr><tr><td>MOD_KM</td><td>FDP_APC_EXT.1/KM, FDP_FIL_EXT.1/KM, FDP_PDC_EXT.1, FDP_RDR_EXT.1, FDP_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_PDC_EXT.1, FDP_RDR_EXT.1</td></tr></table></td></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.</td></tr>
</table>

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td></td><td>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>
<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>
</table>

<table>
<tr><th>Security Objective</th><th>Description</th></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/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.UNIDIRECTIONAL _AUDIO_OUT</b></td><td>The PSD shall enforce the unidirectional flow of audio data from the analog audio computer interface to the analog audio peripheral interface.
Addressed by:<table><tr><td>MOD_AO</td><td>FDP_APC_EXT.1/AO, FDP_AFL_EXT.1, FDP_UDF_EXT.1/AO</td></tr></table></td></tr>
<tr><td><b>O.COMPUTER_TO _AUDIO_ISOLATION</b></td><td>The PSD shall isolate the analog audio output function from all other TOE functions.
Addressed by:<table><tr><td>MOD_AO</td><td>FDP_APC_EXT.1/AO, FDP_UDF_EXT.1/AO</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 7 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

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

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

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

Threat or Assumption	Security Objective(s)	Rationale
T.DATA_LEAK	O.COMPUTER _INTERFACE _ISOLATION	Isolation of computer interfaces prevents data from leaking between them without authorization.

Threat or Assumption	Security Objective(s)	Rationale
	O.COMPUTER _INTERFACE _ISOLATION _TOE_UNPOWERED	Maintaining interface isolation while the TOE is in an unpowered state ensures that data cannot leak between computer interfaces.
	O.USER_DATA _ISOLATION	The TOE's routing of data only to the selected computer ensures that it will not leak to any others.
	O.NO_OTHER _EXTERNAL _INTERFACES	The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked.
	O.PERIPHERAL_PORTS _ISOLATION	Isolation of peripheral ports prevents data from leaking between them without authorization.
	O.UNIDIRECTIONAL _INPUT	The TOE's enforcement of unidirectional input for keyboard/mouse data prevents leakage of computer data through a connected peripheral interface.
	O.PROTECTED_EDID	The TOE's protection of the EDID interface prevents its use as a vector for unauthorized data leakage via this channel.
	O.UNIDIRECTIONAL _VIDEO	The TOE's enforcement of unidirectional output for video data protects against data leakage via connected computers by ensuring that no video data can be input to a connected computer through this interface.
T.SIGNAL_LEAK	O.COMPUTER _INTERFACE _ISOLATION	Isolation of computer interfaces prevents data leakage through bit-wise signaling because there is no mechanism by which the signal data can be communicated.
	O.NO_OTHER _EXTERNAL _INTERFACES	The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked through bitwise signaling.

Threat or Assumption	Security Objective(s)	Rationale
	O.LEAK_PREVENTION_SWITCHING	The TOE’s use of switching methods that are not susceptible to signal leakage helps mitigate the signal leak threat.
	O.UNIDIRECTIONAL_INPUT	The TOE’s enforcement of unidirectional input for keyboard/mouse data prevents leakage of computer data through bit-by-bit signaling to a connected peripheral interface.
	O.PROTECTED_EDID	The TOE’s protection of the EDID interface prevents its use as a vector for bit-by-bit signal leakage via this channel.
	O.UNIDIRECTIONAL_VIDEO	The TOE’s enforcement of unidirectional output for video data protects against signaling leakage via connected computers by ensuring that no video data can be input to a connected computer through this interface.
	O.UNIDIRECTIONAL_AUDIO_OUT	O.UNIDIRECTIONAL_AUDIO_OUT mitigates this threat by preventing the exploitation of the analog audio output to receive signaled data from a connected computer. Analog audio output in standard computers may be exploited to become audio input in some audio codecs. Audio devices such as headphones may also be used as low-gain dynamic microphones. If the TOE design assures that analog audio reverse signal attenuation is below the noise floor level then the audio signal may not be recovered from the resultant audio stream. This prevents potential misuse of headphones connected to the TOE for audio eavesdropping.

Threat or Assumption	Security Objective(s)	Rationale
	O.COMPUTER_TO _AUDIO_ISOLATION	O.COMPUTER_TO_AUDIO_ISOLATION mitigates this threat by ensuring that analog audio output converted to input by a malicious driver cannot pick up signals from other computer interfaces. A TOE design that ensures that audio signals are not leaked to any other TOE interface can effectively prevent a potential signaling leakage across the TOE through analog audio.
T.RESIDUAL _LEAK	O.NO_USER_DATA _RETENTION	The TOE's lack of data retention ensures that a residual data leak is not possible.
	O.PROTECTED_EDID	The TOE's protection of the EDID interface prevents the leakage of residual data by ensuring that no such data can be written to EDID memory.
T.UNINTENDED _USE	O.AUTHORIZED _USAGE	The TOE's support for only switching mechanisms that require explicit user action to engage ensures that a user has sufficient information to avoid interacting with an unintended computer.
T.UNAUTHORIZED _DEVICES	O.REJECT _UNAUTHORIZED _ENDPOINTS	The TOE's ability to reject unauthorized endpoints mitigates the threat of unauthorized devices being used to communicate with connected computers.
	O.REJECT _UNAUTHORIZED _PERIPHERAL	The TOE's ability to reject unauthorized peripherals mitigates the threat of unauthorized devices being used to communicate with connected computers.
	O.EMULATED_INPUT	The TOE's emulation of keyboard/mouse data input ensures that a connected computer will only receive this specific type of data through a connected peripheral.
	O.UNIDIRECTIONAL _VIDEO	The TOE's limitation of supported video protocol interfaces prevents the connection of unauthorized devices.

Threat or Assumption	Security Objective(s)	Rationale
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.
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.

Threat or Assumption	Security Objective(s)	Rationale
T.MICROPHONE_USE	O.UNIDIRECTIONAL_AUDIO_OUT	O.UNIDIRECTIONAL_AUDIO_OUT mitigates this threat by attenuating the strength of any inbound transmission of audio data through the TOE from a connected peripheral. If the TOE design ensures that analog audio reverse signal attenuation is below the noise floor level then any audio signal should not have sufficient strength to be usable.
T.AUDIO_REVERSED	O.UNIDIRECTIONAL_AUDIO_OUT	O.UNIDIRECTIONAL_AUDIO_OUT mitigates this threat by ensuring that the TOE’s audio peripheral interface(s) are exclusively used to output audio.
A.NO_TEMPEST	OE.NO_TEMPEST	If the TOE’s operational environment does not include TEMPEST approved equipment, then the assumption is satisfied.
A.NO_PHYSICAL	OE.PHYSICAL	If the TOE’s operational environment provides physical security, then the assumption is satisfied.
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.
A.NO _MICROPHONES	OE.NO _MICROPHONES	The assumption is upheld by the objective since the users in the environment are trained not to connect a microphone to the TOE audio output interface,

Table 9 – Security Objectives Rationale

5 EXTENDED COMPONENTS DEFINITION

The extended components definition is presented in Appendix C of the Protection Profile for Peripheral Sharing Device [PP_PSD_V4.0] and in the modules for analog audio output devices [MOD_AO_V1.0], keyboard/mouse devices [MOD_KM_V1.0], and display devices [MOD_VI_1.0]. It is repeated here to ensure the completeness of this ST.

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

Functional Class	Functional Families
User Data Protection (FDP)	FDP_AFL_EXT Audio Filtration
	FDP_APC_EXT Active PSD Connections
	FDP_FIL_EXT Device Filtering
	FDP_IPC_EXT Internal Protocol Conversion
	FDP_PDC_EXT Peripheral Device Connection
	FDP_PUD_EXT Powering Unauthorized Devices
	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

Table 10 – Functional Families of Extended Components

5.1 CLASS FDP: USER DATA PROTECTION

5.1.1 FDP_AFL_EXT Audio Filtration

Family Behavior

Components in this family define the requirements for device filtering.

Component Leveling

FDP_AFL_EXT Audio Filtration
1

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

Management: FDP_AFL_EXT.1

No specific management functions are identified.

Audit: FDP_AFL_EXT.1

No specific audit functions are defined.

FDP_AFL_EXT.1 Device Filtering

Hierarchical to: No other components.

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

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

Frequency (kHz)	Minimum Attenuation (dB)	Maximum Voltage After Attenuation
14	23.9	127.65 mV
15	26.4	95.73 mV
16	30.8	57.68 mV
17	35.0	35.57 mV
18	38.8	22.96 mV
19	43.0	14.15 mV
20	46.0	10.02 mV
30	71.4	0.53 mV
40	71.4	0.53 mV
50	71.4	0.53 mV
60	71.4	0.53 mV

5.1.2 FDP_APC_EXT Active PSD Connections

Family Behavior

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

Component Leveling

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

Management: FDP_APC_EXT.1

No specific management functions are identified.

Audit: FDP_APC_EXT.1

There are no auditable events foreseen.

FDP_APC_EXT.1 Active PSD Connections

Hierarchical to: No other components.

Dependencies: No dependencies

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

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

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

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

5.1.3 FDP_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.

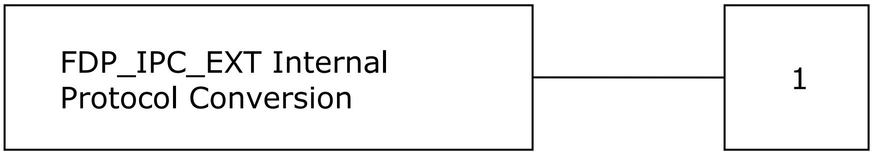
FDP_FIL_EXT.1.3 The TSF shall consider all [*assignment: whitelist name*] whitelisted devices as authorized devices for peripheral device connections only if they are not on the [*assignment: blacklist name*] blacklist or otherwise unauthorized.

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*].

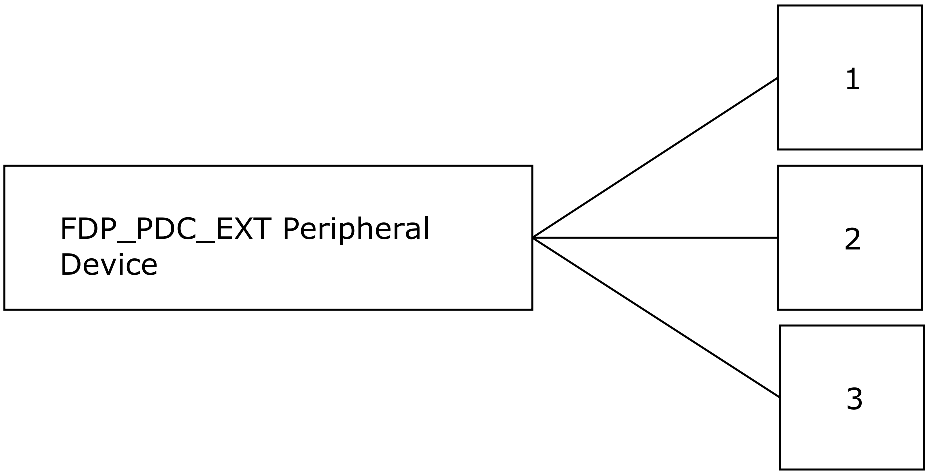
5.1.5 FDP_PDC_EXT Peripheral Device Connection

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_PUD_EXT Powering Unauthorized Devices

Family Behavior

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

Component Leveling

FDP_PUD_EXT Powering Unauthorized Devices
1

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

Management: FDP_PUD_EXT.1

No specific management functions are identified.

Audit: FDP_PUD_EXT.1

There are no specific auditable events foreseen.

FDP_PUD_EXT.1 Powering Unauthorized Devices

Hierarchical to: No other components.

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

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

5.1.7 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.

5.1.8 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.

5.1.9 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:

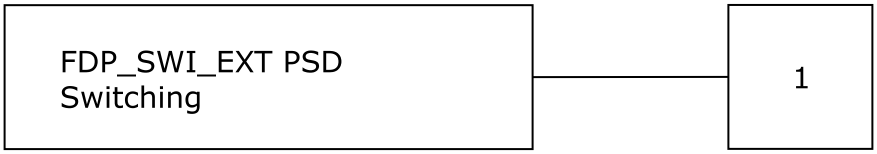
- block the following video/display sub-protocols:
  - [*assignment: list of blocked sub-protocols*]
- allow the following video/display sub-protocols:
  - [*assignment: list of allowed sub-protocols*].

5.1.10 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.

Management: FDP_SWI_EXT.1

No specific management functions are identified.

Audit: FDP_SWI_EXT.1

There are no auditable events foreseen.

FDP_SWI_EXT.1 PSD Switching

Hierarchical to: No other components.

Dependencies: No dependencies

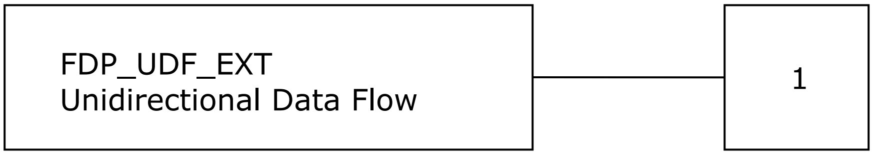
FDP_SWI_EXT.1.1 The TSF shall ensure that [*selection: the TOE supports only one connected computer, switching can be initiated only through express user action*].

5.1.11 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.

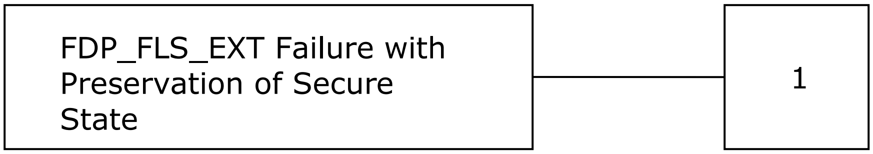
5.2 CLASS FPT: PROTECTION OF THE TSF

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

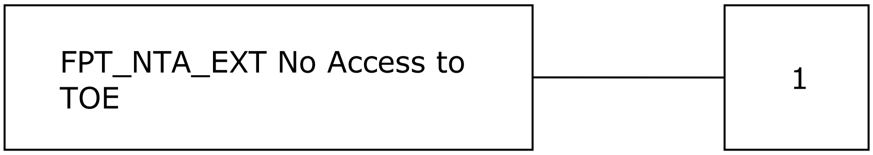
FPT_FLS_EXT.1.1 The TSF shall preserve a secure state when the following types of failures occur: failure of the power-on self-test and [*selection: failure of the anti-tamper function, no other failures*].

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.

6 SECURITY REQUIREMENTS

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

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. 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 are identified with a slash (‘/’) and an identifier (e.g. “/KM”).

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

6.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components.

Class	Identifier	Name	Source
User Data Protection (FDP)	FDP_AFL_EXT.1	Audio Filtration	[MOD_AO_V1.0]
	FDP_APC_EXT.1/AO	Active PSD Connections	[MOD_AO_V1.0]
	FDP_APC_EXT.1/KM	Active PSD Connections	[MOD_KM_V1.0]
	FDP_APC_EXT.1/VI	Active PSD Connections	[MOD_VI_V1.0]
	FDP_FIL_EXT.1/KM	Device Filtering (Keyboard/Mouse)	[MOD_KM_V1.0]
	FDP_IPC_EXT.1	Internal Protocol Conversion	[MOD_VI_V1.0]

Class	Identifier	Name	Source
	FDP_PDC_EXT.1	Peripheral Device Connection	[PP_PSD_V4.0] [MOD_AO_V1.0][4] [MOD_VI_V1.0][5] [MOD_KM_V1.0][6]
	FDP_PDC_EXT.2/AO	Peripheral Device Connection (Audio Output)	[MOD_AO_V1.0]
	FDP_PDC_EXT.2/KM	Authorized Devices (Keyboard/Mouse)	[MOD_KM_V1.0]
	FDP_PDC_EXT.2/VI	Authorized Devices (Video Output)	[MOD_VI_V1.0]
	FDP_PDC_EXT.3/KM	Authorized Connection Protocols (Keyboard/Mouse)	[MOD_KM_V1.0]
	FDP_PDC_EXT.3/VI	Authorized Connection Protocols (Video Output)	[MOD_VI_V1.0]
	FDP_PUD_EXT.1	Powering Unauthorized Devices	[MOD_AO_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_SPR_EXT.1/DP	Sub-Protocol Rules (DisplayPort Protocol)	[MOD_VI_V1.0]

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

[5] 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.

[6] 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_SPR_EXT.1/HDMI	Sub-Protocol Rules (HDMI Protocol)	[MOD_VI_V1.0]
	FDP_SWI_EXT.1	PSD Switching	[PP_PSD_V4.0]
	FDP_UDF_EXT.1/AO	Unidirectional Data Flow (Audio Output)	[MOD_AO_V1.0]
	FDP_UDF_EXT.1/KM	Unidirectional Data Flow (Keyboard/Mouse)	[MOD_KM_V1.0]
	FDP_UDF_EXT.1/VI	Unidirectional Data Flow (Video Output)	[MOD_VI_V1.0]
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]

Table 11 – Summary of Security Functional Requirements

6.2.1 User Data Protection (FDP)

6.2.1.1 FDP_AFL_EXT.1 Audio Filtration

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

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

Frequency (kHz)	Minimum Attenuation (dB)	Maximum Voltage After Attenuation
18	38.8	22.96 mV
19	43.0	14.15 mV
20	46.0	10.02 mV
30	71.4	0.53 mV
40	71.4	0.53 mV
50	71.4	0.53 mV
60	71.4	0.53 mV

Table 12 – Audio Filtration Specifications

6.2.1.2 FDP_APC_EXT.1/AO Active PSD Connections

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

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

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

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

6.2.1.3 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.

6.2.1.4 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.

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

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

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

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

6.2.1.6 FDP_IPC_EXT.1 Internal Protocol Conversion

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].

6.2.1.7 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.2.1.11 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*].

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

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

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

6.2.1.13 FDP_PUD_EXT.1 Powering Unauthorized Devices

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

6.2.1.14 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.

6.2.1.15 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.

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

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

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

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

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

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

6.2.1.18 FDP_SWI_EXT.1 PSD Switching

FDP_SWI_EXT.1.1 The TSF shall ensure that [*the TOE supports only one connected computer*].

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

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

6.2.1.20 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 interfaces to the [*TOE [keyboard, mouse]*] interface.

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

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

6.2.2 Protection of the TSF (FPT)

6.2.2.1 FPT_FLS_EXT.1 Failure with Preservation of Secure State

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

6.2.2.2 FPT_NTA_EXT.1 No Access to TOE

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

6.2.2.3 FPT_PHP.1 Passive Detection of Physical Attack

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

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

6.2.2.4 FPT_TST.1 TSF Testing

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

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

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

6.2.2.5 FPT_TST_EXT.1 TSF Testing

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

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 13.

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[7] 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 13 – Security Assurance Requirements

[7] Configuration Management

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

Table 7 provides a mapping between the SFRs and Security Objectives.

6.4.2 Dependency Rationale

Table 14 identifies the Security Functional Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependencies	Rationale Statement
FDP_AFL_EXT.1	FDP_PDC_EXT.1	Included
FDP_APC_EXT.1/AO	None	N/A
FDP_APC_EXT.1/KM	None	N/A
FDP_APC_EXT.1/VI	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/AO	FDP_PDC_EXT.1	Included
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_PUD_EXT.1	FDP_PDC_EXT.1	Included
FDP_RDR_EXT.1	FDP_PDC_EXT.1	Included
FDP_RIP_EXT.1	None	N/A
FDP_SPR_EXT.1/DP	FDP_PDC_EXT.3	Included
FDP_SPR_EXT.1/HDMI	FDP_PDC_EXT.3	Included
FDP_SWI_EXT.1	None	N/A
FDP_UDF_EXT.1/AO	FDP_APC_EXT.1	Included
FDP_UDF_EXT.1/KM	FDP_APC_EXT.1	Included
FDP_UDF_EXT.1/VI	FDP_APC_EXT.1	Included

SFR	Dependencies	Rationale Statement
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

Table 14 – Functional Requirement Dependencies

6.4.3 Security Assurance Requirements Rationale

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

7 TOE SUMMARY SPECIFICATION

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

7.1 USER DATA PROTECTION

7.1.1 PSD Switching

The TOE supports only one connected computer.

TOE Security Functional Requirements addressed: FDP_SWI_EXT.1.

7.1.1.1 Active PSD Connections

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

7.1.1.2 Connected Computer Interfaces

The connected computers are attached to the TOE as follows:

- The TOE connects to the keyboard and mouse port using a USB A to USB B cable. The USB A end attaches to the computer, and the USB B end attaches to the TOE
- The TOE is connected to the computer video port using a video cable supporting DisplayPort or HDMI
- The TOE audio-in is connected to the computer audio-out using a 1/8" stereo plug cable

TOE Security Functional Requirements addressed: FDP_PDC_EXT.1.

7.1.1.3 Residual Information Protection

The Letter of Volatility is included as Annex A.

TOE Security Functional Requirements addressed: FDP_RIP_EXT.1.

7.1.2 Keyboard and Mouse Functionality

7.1.2.1 Keyboard and Mouse Enumeration

The TOE determines whether 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 Isolator device.

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.

7.1.2.2 Keyboard and Mouse Data Stream

Figure 1 is a simplified block diagram showing the TOE keyboard and mouse data path. A Host Emulator (HE) communicates with the user keyboard via the USB protocol. The Host Emulator converts user key strokes into unidirectional serial data. An isolated Device Emulator (DE) is connected to the data switch on one side and to the computer on the other side. Each key stroke is converted by the selected DE into a bi-directional stream to communicate with the computer. Figure 3 shows an extended isolator.

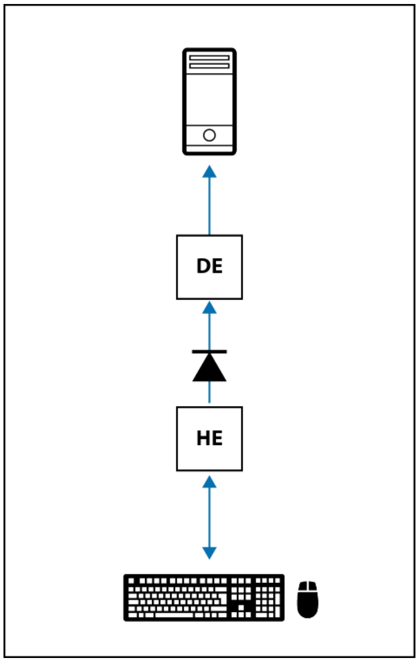


Figure 2 – Simplified Isolator Diagram

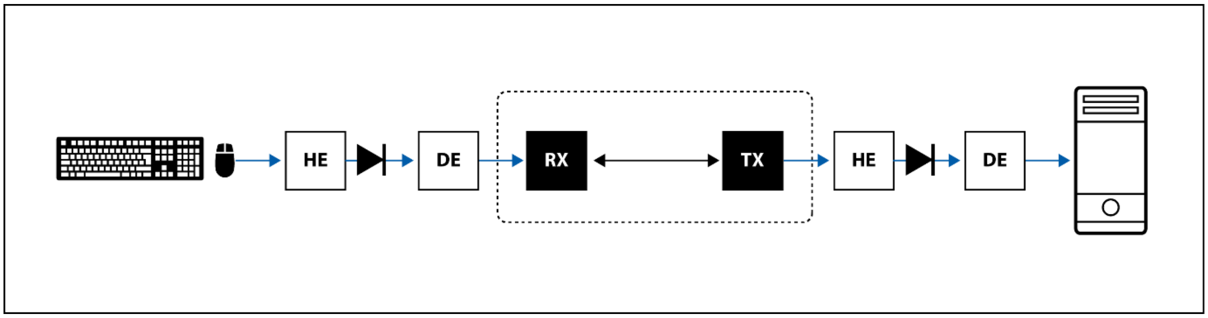


Figure 3 – Extended Isolator Diagram

The combined mouse and keyboard data stream is passed through an optical data diode to the host device emulator. The optical data diode is an opto-coupler designed to physically prevent reverse data flow.

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.

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

7.1.2.3 Keyboard and Mouse Compatible Device Types

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

The device filtering for the keyboard and mouse is fixed. All blacklisted devices are unauthorized for the keyboard and mouse connections. Whitelisted keyboard and mouse devices are authorized.

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

7.1.2.4 Re-Enumeration Device Rejection

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

TOE Security Functional Requirements addressed: FDP_RDR_EXT.1.

7.1.3 Video 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.

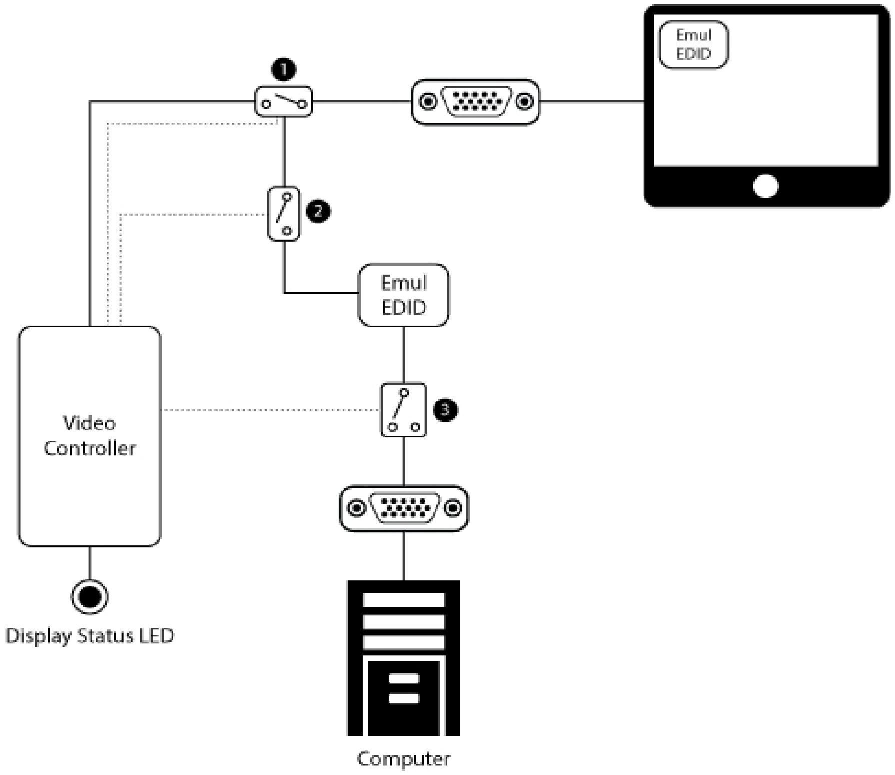


Figure 4 – Display EDID Read Function

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. For this, Switch 1 is closed, and Switch 2 and Switch 3 are open. If data is not valid, TOE operation will cease and wait for the display peripheral to be changed.

In the next step, Switch 1 and Switch 3 are open, and Switch 2 is closed. The video controller writes the EDID content into the emulated EDID Electrically Erasable Programmable Read-Only Memory (EEPROM) chip.

The video controller uses the I2C lines to write to the emulated EDID EEPROM chip. Once the write operation is complete, the video controller switches to normal operating mode. In this mode, Switch 1 and Switch 2 are closed, and Switch 3 is open.

In the normal operation mode, the Emulated EDID EEPROM chip is switched to the computer to enable reading of the EDID information. The write protect switch (Switch 2) is switched to protected mode (i.e. it is closed) to prevent any attempt to write to the EEPROM or to transmit MCCS commands.

In normal mode, the power to the emulated EDID EEPROM is received from the computer through the video cable.

During TOE normal operation, any attempt by the connected computer to affect the EDID channel is blocked by the architecture.

The EDID function is emulated by an independent emulation EEPROM chip. This chip reads 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, and HDMI 2.0:

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

Channel (HEAC), and HDMI Ethernet Channel (HEC) are blocked. HDCP and Consumer Electronics Control (CEC) functions are not connected

The TOE video function blocks MCCS write transactions through the emulated EDID EEPROM. The emulated EEPROM supports only EDID read transactions.

Following a failed self-test, or when the TOE is powered off, all video input signals are isolated from the video output interface by the active video re-driver. The Emulated EDID EEPROM may still operate since it is powered by the computer.

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

7.1.3.1 Video Compatible Device Types

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

TOE Security Functional Requirements addressed: FDP_PDC_EXT.1, FDP_PDC_EXT.2/VI, FDP_PDC_EXT.3/VI.

7.1.4 Audio Functionality

The TOE audio data flow path is unidirectional and includes filtering by design.

Unidirectional flow data diodes prevent audio data flow from an audio device to a selected computer. The audio interface is electrically isolated from other interfaces, and from other TOE circuitry. An analog to digital and digital to analog conversion is performed to filter out high frequencies. These features ensure that the audio filtration specification requirements are met.

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

When the TOE is powered off, an audio isolation relay is open, thereby isolating the audio input from the computer interface from all other circuitry and interfaces. Following a failed self-test, the TOE will de-energize this audio isolation relay to isolate the audio input. The audio subsystem does not store, convert or delay audio data flows.

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

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

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

7.1.4.1 Audio Compatible Device Types

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

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

7.2 PROTECTION OF THE TSF

7.2.1 No Access to TOE

The connected computer does not have access to TOE firmware or memory, with the exception of EDID data, which is accessible from the TOE to the connected computer.

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

TOE Security Functional Requirements addressed: FPT_NTA_EXT.1.

7.2.2 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.

7.2.3 TSF Testing

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

- Verification of the integrity of the microcontroller firmware

If the self-test fails, the LED on the back panel blinks green to indicate the failure. The TOE 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.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
AO	AO refers to the requirements for Audio Output Devices.
AUX	AUX refers to the auxiliary channel, particularly as it applies to the DisplayPort protocol.
KM	KM refers to the requirements for Keyboard/Mouse Devices.
VI	VI refers to the requirements for Video Output Devices.

Table 15 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
ARC	Audio Return Channel
CC	Common Criteria
CEC	Consumer Electronics Control
CM	Configuration Management
dB	decibel
DC	Direct Current
DE	Device Emulator
DP	DisplayPort
EDID	Extended Display Identification Data
EEPROM	Electrically Erasable Programmable Read-Only Memory
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
kHz	kilohertz
LED	Light Emitting Diode
MCCS	Monitor Control Command Set
mV	millivolt
NIAP	National Information Assurance Partnership
OTP	One Time Programming
PP	Protection Profile
PSD	Peripheral Sharing Device
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 16 – Acronyms

9 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_AO_V1.0]	PP-Module for Analog Audio Output Devices, Version 1.0, 2019-07-19
[MOD_KM_V1.0]	PP-Module for Keyboard/Mouse Devices, Version 1.0, 2019-07-19
[MOD_VI_1.0]	PP-Module for Video/Display Devices, Version 1.0, 2019-07-19
[CFG_PSD-AO-KM-VI_V1.0]	PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, and Video/Display Devices, 19 July 2019

Table 17 – References

ANNEX A – LETTER OF VOLATILITY

The table below provides volatility information and memory types for the IHSE Isolator Devices. User data is not retained in any TOE device when the power is turned off.

Product Model	Number in each product	Function, Manufacturer and Part Number	Storage Type	Size	Power Source (if not the TOE)	Volatility	Contains User Data
K487-1PHCA-N K487-1PHSA-N K487-1PHCRA-N K487-1PHSRA-N K497-1PHCA-N K497-1PHSA-N K497-1PHCRA-N K497-1PHSRA-N	2	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
	2	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
	2	EDID emulators: ST Microelectronics M24C02-WMN6TP	EEPROM[4]	2KB		Non-Volatile	No user data

Notes:

[1] SRAM stores USB Host stack parameters and up to the last 4 key-codes. Data is erased during power off of the Isolator device. 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 computer 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 (display Plug & Play) and contains no user data.