Assurance Activity Report for
Vertiv CYBEX™ SCUSBHIDFILTER Firmware Version 40404-0E7 and Vertiv CYBEX™ SCKM140PP4 KM Switch Firmware Version 40404-0E7 Peripheral Sharing Devices

Vertiv CYBEX™ SCUSBHIDFILTER Firmware Version 40404-0E7 Security Target Version: 1.15, January 5, 2022
and
Vertiv CYBEX™ SCKM140PP4 KM Switch Firmware Version 40404-0E7 Security Target, Version: 1.18 January 13, 2022

Protection Profile for Peripheral Sharing Device, Version: 4.0
PP-Module for Keyboard/Mouse Devices, Version 1.0

AAR Version 1.2, January 28, 2022

Evaluated by:

2400 Research Blvd, Suite 395
Rockville, MD 20850

Prepared for:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Vertiv
1050 Dearborn Dr.
Columbus, OH 43085

The Author of the Security Target:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

The TOE Evaluation was Sponsored by:
Vertiv
1050 Dearborn Dr.
Columbus, OH 43085

Evaluation Personnel:
Kenneth Lasoski
Joshua Gola
Acumen Security
2400 Research Blvd, Suite 395
Rockville, MD 20850

Common Criteria Version
Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version
CEM Version 3.1 Revision 5

Contents

`

1 Overview 7
2 Assurance Activities Identification 8
3 Equivalency Analysis 9
3.1 Microcontroller and Firmware Analysis 9
3.2 Peripheral Port Equivalency 9
4 Test Environment 10
4.1 Test Bed # 1 10
4.1.1 Test Equipment 12
4.1.1.1 Computers 12
4.1.1.2 Software 13
4.1.2 Test Time & Location 13
***4.1.3* Configuration Information 13**
4.1.3.1 **Product: SCUSBHIDFILTER (Isolator)** 13
4.1.3.2 **Product: SKM140PP4 (Switch)** 13
4.1.3.3 **Remote Control: SCAFP0004** 13
5 Detailed Test Cases (TSS, Isolation Document, and Guidance Activities) 14
5.1 TSS, Isolation Document, and Guidance Activities (User Data Protection) 14
5.1.1 FDP_APC_EXT.1 14
5.1.1.1 FDP_APC_EXT.1 Isolation Document 1 14
5.1.1.1 FDP_APC_EXT.1 TSS 1 14
5.1.1.2 FDP_APC_EXT.1 Guidance 1 15
5.1.2 FDP_APC_EXT.1/KM 15
5.1.2.1 FDP_APC_EXT.1/KM Isolation Document 1 15
5.1.2.2 FDP_APC_EXT.1/KM TSS 1 15
5.1.2.3 FDP_APC_EXT.1/KM Guidance 1 16
5.1.3 FDP_FIL_EXT.1/KM 16
5.1.3.1 FDP_FIL_EXT.1/KM Isolation Document 1 16
5.1.3.2 FDP_FIL_EXT.1/KM TSS 1 16
5.1.3.3 FDP_FIL_EXT.1/KM Guidance 1 16
5.1.4 FDP_PDC_EXT.1 17
5.1.4.1 FDP_PDC_EXT.1 Isolation Document 1 17
5.1.4.2 FDP_PDC_EXT.1 TSS 1 17
5.1.4.3 FDP_PDC_EXT.1 TSS 2 17
5.1.4.4 FDP_PDC_EXT.1 TSS 3 17
5.1.4.5 FDP_PDC_EXT.1 TSS 4 18
5.1.4.6 FDP_PDC_EXT.1 Guidance 1 18
5.1.4.7 FDP_PDC_EXT.1 Guidance 2 18
5.1.4.8 FDP_PDC_EXT.1 Guidance 3 19
5.1.4.9 FDP_PDC_EXT.1 Guidance 4 19
5.1.4.10 FDP_PDC_EXT.1/KM Guidance 5 19
5.1.5 FDP_PDC_EXT.2/KM 19
5.1.5.1 FDP_PDC_EXT.2/KM Isolation Document 1 19

5.1.5.2 FDP_PDC_EXT.2/KM TSS 1 20
5.1.5.3 FDP_PDC_EXT.2/KM Guidance 1 20
5.1.6 FDP_PDC_EXT.3/KM 20
5.1.6.1 FDP_PDC_EXT.3/KM Isolation Document 1 20
5.1.6.2 FDP_PDC_EXT.3/KM TSS 1 20
5.1.6.3 FDP_PDC_EXT.3/KM TSS 2 20
5.1.6.4 FDP_PDC_EXT.3/KM Guidance 1 21
5.1.7 FDP_RDR_EXT.1 21
5.1.7.1 FDP_RDR_EXT.1 Isolation Document 1 21
5.1.7.2 FDP_RDR_EXT.1 TSS 1 21
5.1.7.3 FDP_RDR_EXT.1 Guidance 1 21
5.1.8 FDP_RIP_EXT.1 22
5.1.8.1 FDP_RIP_EXT.1 Isolation Document 1 22
5.1.8.2 FDP_RIP_EXT.1 TSS 1 22
5.1.8.3 FDP_RIP_EXT.1 TSS 2 22
5.1.8.4 FDP_RIP_EXT.1 Guidance 1 23
5.1.9 FDP_RIP.1/KM 23
5.1.9.1 FDP_RIP.1/KM Isolation Document 1 23
5.1.9.2 FDP_RIP.1/KM TSS 1 23
5.1.9.3 FDP_RIP.1/KM TSS 2 23
5.1.9.4 FDP_RIP.1/KM Guidance 1 24
5.1.10 FDP_SWI_EXT.1 24
5.1.10.1 FDP_SWI_EXT.1 Isolation Document 1 24
5.1.10.2 FDP_SWI_EXT.1 TSS 1 24
5.1.10.3 FDP_SWI_EXT.1 TSS 2 24
5.1.10.4 FDP_SWI_EXT.1 Guidance 1 25
5.1.11 FDP_SWI_EXT.2 25
5.1.11.1 FDP_SWI_EXT.2 Isolation Document 1 25
5.1.11.2 FDP_SWI_EXT.2 TSS 1 25
5.1.11.3 FDP_SWI_EXT.2 Guidance 1 25
5.1.12 FDP_SWI_EXT.3 26
5.1.12.1 FDP_SWI_EXT.3 Isolation Document 1 26
5.1.12.2 FDP_SWI_EXT.3 TSS 1 26
5.1.12.3 FDP_SWI_EXT.3 Guidance 1 26
5.1.13 FDP_UDF_EXT.1/KM 27
5.1.13.1 FDP_UDF_EXT.1/KM Isolation Document 1 27
5.1.13.2 FDP_UDF_EXT.1/KM TSS 1 27
5.1.13.3 FDP_UDF_EXT.1/KM TSS 2 27
5.1.13.4 FDP_UDF_EXT.1/KM Guidance 1 28
5.2 TSS, Isolation Document, and Guidance Activities (Protection of the TSF) 28
5.2.1 FPT_FLS_EXT.1 28
5.2.2 FPT_NTA_EXT.1 28
5.2.2.1 FPT_NTA_EXT.1 Isolation Document 1 28
5.2.2.2 FPT_NTA_EXT.1 TSS 1 28
5.2.2.3 FPT_NTA_EXT.1 Guidance 1 28
5.2.3 FPT_PHP.1 29
5.2.3.1 FPT_PHP.1 Isolation Document 1 29
5.2.3.2 FPT_PHP.1 TSS 1 29

5.2.3.3 FPT_PHP.1 Guidance 1 29
5.2.4 FPT_PHP.3 29
5.2.4.1 FPT_PHP.3 Isolation Document 1 30
5.2.4.2 FPT_PHP.3 TSS 1 30
5.2.4.3 FPT_PHP.3 Guidance 1 30
5.2.4.4 FPT_PHP.3 Guidance 2 30
5.2.5 FPT_TST.1 31
5.2.5.1 FPT_TST.1 Isolation Document 1 31
5.2.5.2 FPT_TST.1 TSS 1 31
5.2.5.3 FPT_TST.1 TSS 2 31
5.2.5.4 FPT_TST.1 TSS 3 32
5.2.5.5 FPT_TST.1 TSS 4 32
5.2.5.6 FPT_TST.1 Guidance 1 33
5.2.6 FPT_TST_EXT.1 33
5.2.6.1 FPT_TST_EXT.1 Isolation Document 1 33
5.2.6.2 FPT_TST.EXT.1 TSS 1 33
5.2.6.3 FPT_TST_EXT.1 Guidance 1 33
5.2.6.4 FPT_TST_EXT.1 Guidance 2 34
5.3 TSS, Isolation Document, and Guidance Activities (TOE Access) 34
5.3.1 FTA_CIN_EXT.1 34
5.3.1.1 FTA_CIN_EXT.1 Isolation Document 1 34
5.3.1.2 FTA_CIN_EXT.1 TSS 1 35
5.3.1.3 FTA_CIN_EXT.1 TSS 2 35
5.3.1.4 FTA_CIN_EXT.1 Guidance 1 35
5.3.1.5 FTA_CIN_EXT.1 Guidance 2 35
6 Test Activities – Isolator 37
6.1 Test Matrix 37
***6.1.1* FDP_PDC_EXT.1 - Test 1** 37
***6.1.2* FDP_PDC_EXT.1 – Test 2** 37
***6.1.3* FDP_PDC_EXT.1 – Test 3** 38
***6.1.4* FPT_PHP.1 – Test 1** 39
***6.1.5* FPT_PHP.1 – Test 2** 40
***6.1.6* FPT_TST.1 – Test 1** 40
***6.1.7* FPT_TST_EXT.1 - Test 1** 41
***6.1.8* FDP_PDC_EXT.1 - Test 1** 42
***6.1.9* FDP_PDC_EXT.1 – Test 2** 43
***6.1.10* FDP_APC_EXT.1 - Test 1** 45
***6.1.11* FDP_APC_EXT.1 - Test 2** 46
***6.1.12* FDP_APC_EXT.1 - Test 3** 48
***6.1.13* FDP_APC_EXT.1 - Test 4** 50
***6.1.14* FDP_APC_EXT.1 - Test 5** 51
***6.1.15* FDP_FIL_EXT.1 - Test 1** 52
***6.1.16* FDP_RDR_EXT.1 – Test 1** 54
7 Test Activities – Switch 56
7.1 Test Matrix 56
***7.1.1* PDP_PDC_EXT.1 – Test 1** 56

7.1.2 **PDP_PDC_EXT.1 – Test 2** 56
7.1.3 **PDP_PDC_EXT.1 – Test 3** 57
7.1.4 **FPT_PHP.1 – Test 1** 58
7.1.5 **FPT_PHP.1 – Test 2** 59
7.1.6 **FPT_PHP.3 – Test 1** 59
7.1.7 **FPT_TST.1 – Test 1** 61
7.1.8 **FPT_TST_EXT.1 – Test 1** 62
7.1.9 **FTA_CIN_EXT.1 – Test 1** 63
7.1.10 **FDP_APC_EXT.1 – Test 1** 65
7.1.11 **FDP_APC_EXT.1 – Test 2** 66
7.1.12 **FDP_APC_EXT.1 – Test 3** 68
7.1.13 **FDP_APC_EXT.1 – Test 4** 70
7.1.14 **FDP_APC_EXT.1 – Test 5** 72
7.1.15 **FDP_PDC_EXT.1 – Test 1** 73
7.1.16 **FDP_PDC_EXT.1 – Test 2** 75
7.1.17 **FDP_FIL_EXT.1 – Test 1** 76
7.1.18 **FDP_FIL_EXT.1 – Test 2** 78
7.1.19 **FDP_RDR_EXT.1 – Test 1** 78
8 Security Assurance Requirements **81**
8.1 ADV_FSP.1 Basic Functional Specification **81**
8.1.1 ADV_FSP.1 81
8.1.1.1 ADV_FSP.1 Activity 1 81
8.2 AGD_OPE.1 Operational User Guidance **81**
8.2.1 AGD_OPE.1 81
8.2.1.1 AGD_OPE.1 Activity 1 81
8.3 AGD_PRE.1 Preparative Procedures **82**
8.3.1 AGD_PRE.1 82
8.3.1.1 AGD_PRE.1 Activity 1 82
8.4 ALC Assurance Activities **82**
8.4.1 ALC_CMC.1 82
8.4.1.1 ALC_CMC.1 Activity 1 82
8.4.2 ALC_CMS.1 82
8.4.2.1 ALC_CMS.1 Activity 1 82
8.5 ATE_IND.1 Independent Testing – Conformance **82**
8.5.1 ATE_IND.1 82
8.5.1.1 ATE_IND.1 Activity 1 82
8.6 AVA_VAN.1 Vulnerability Survey **83**
8.6.1 AVA_VAN.1 83
8.6.1.1 AVA_VAN.1 Activity 1 83
9 Conclusion **85**
10 Evaluation Evidence **86**
11 References **87**

1 Overview

The Vertiv Secure Universal Serial Bus (USB) Human Interface Device (HID) Filter is connected between a computer and a USB keyboard/mouse. It ensures unidirectional flow of data between keyboard and mouse peripheral devices and a secure connected computer.

The following security features are provided by the Vertiv Secure USB HID Filter:

- Keyboard and Mouse Security
  - The keyboard and mouse are isolated by dedicated, 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.
- 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.

The SCKM140PP4 Keyboard, Mouse (KM) switch allows users to share keyboard and mouse peripherals amongst four connected computers.

The following security features are provided by the Vertiv Secure KM Switch:

- Keyboard and Mouse Security
  - The keyboard and mouse are isolated by dedicated, USB device emulation for each computer
  - One-way, peripheral-to-computer data flow is enforced through unidirectional optical data diodes
  - Communication from computer-to-keyboard/mouse is blocked
  - Non-HID (Human Interface Device) data transactions are blocked
- Hardware Anti-Tampering
  - Special holographic tampering evident labels on the product's enclosure provide a clear visual indication if the product has been opened or compromised
  - Any attempt to open the product enclosure will activate an anti-tampering system, making the product inoperable and indicating tampering via blinking Light Emitting Diodes (LEDs)

2 Assurance Activities Identification

The Assurance Activities contained within this document include all those defined within the Protection Profile for Peripheral Sharing Device, Version: 4.0 and the following PP module:

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

SFRs have been selected in accordance with PP-Configuration for Peripheral Sharing Device Keyboard/Mouse Devices, 19 July 2019 and on the selections within the PP and module.

3 Equivalency Analysis

The following equivalency analysis provides a per category analysis of key areas of differentiation for each hardware function to determine the minimum subset to be used in testing. The areas examined will use the areas and analysis description provided in the supporting documentation for the [PP].

3.1 Microcontroller and Firmware Analysis

All Vertiv PSD switches use 32-bit microcontrollers from STMicroelectronics detailed in the Letter of Volatility (Annex A) of the Vertiv CYBEX™ SCKM140PP4 Firmware Version 40404-0E7 Security Target.

All of the security functionality is provided on the system controller board. The basic system controller board supports the exact same functionality independent on the number of output ports.

3.2 Peripheral Port Equivalency

As stated in TD0593, equivalency arguments between ports are allowed. All of the peripheral ports provide the exact same functionality and computer interface protocol (USB). All testing (unless otherwise explicitly stated in the Test Report) was carried out by testing two connected computer ports at a time, then moving the test computers over to two other ports and repeated this process until all permutations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC.

4 Test Environment

4.1 Test Bed # 1

The figures below depict a diagram of the TOE evaluated configuration used for testing:

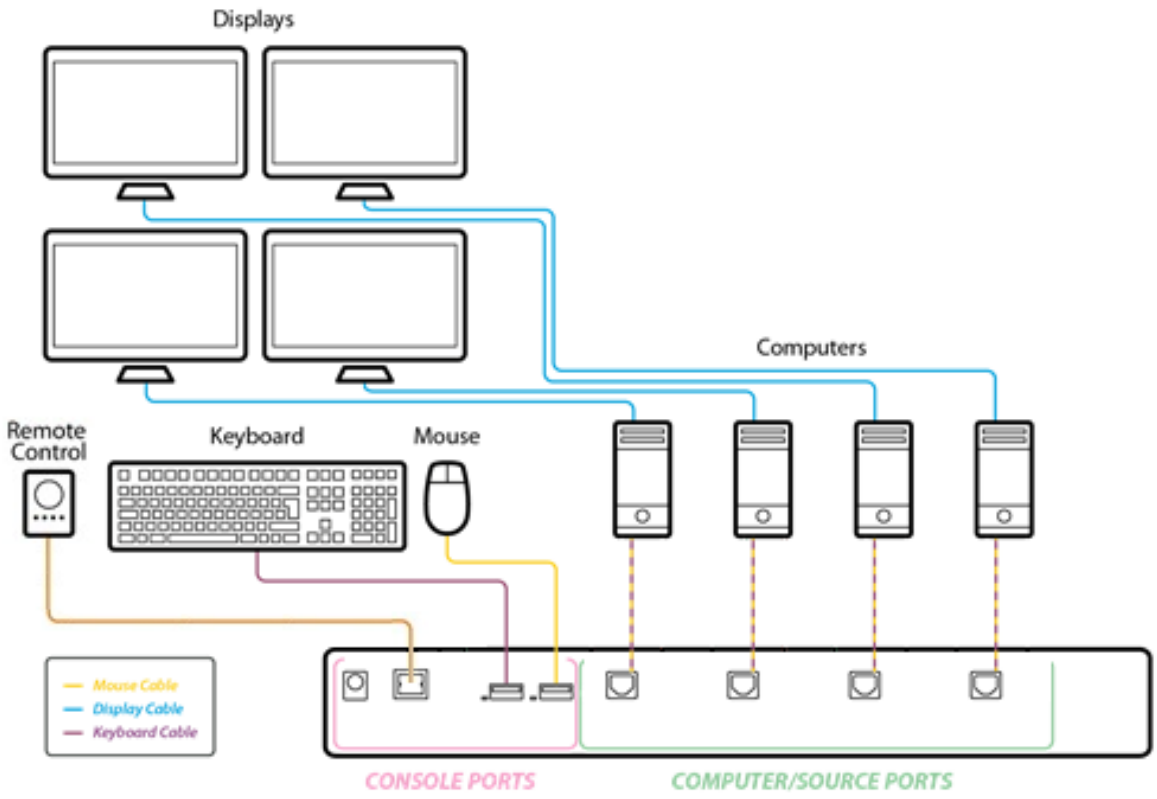
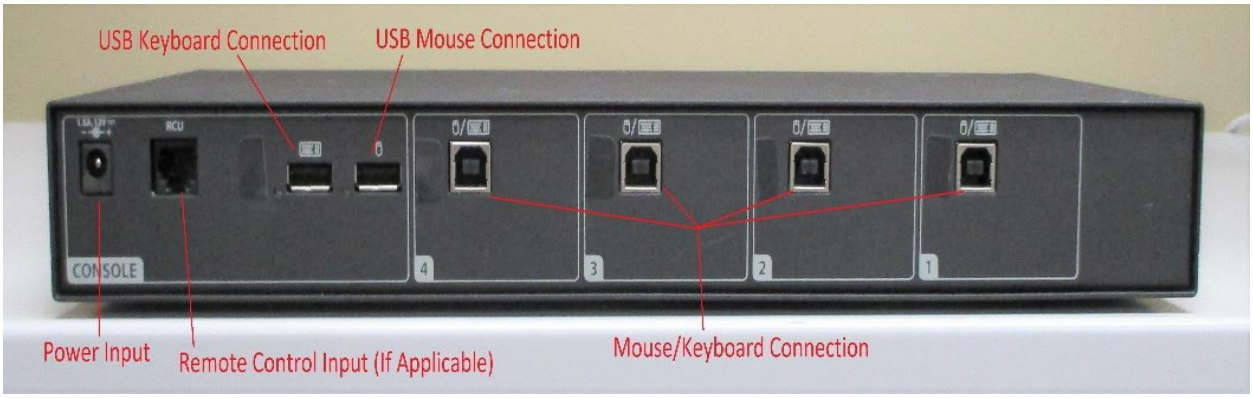


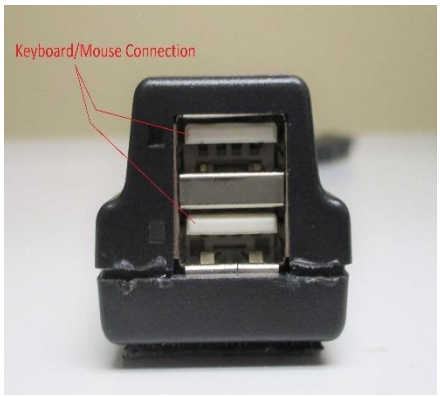
Figure 1 KM Switch TOE Diagram

Figure 2 USB Filter TOE Diagram

Below is a visual representation of the Switch TOE:



Below is a visual representation of the Isolator TOE:



4.1.1 Test Equipment

The following test environment is in use throughout the testing process.

4.1.1.1 Computers

The evaluator used two test computers (Computer #1 and #2) as well as a Lab PC. The device being tested was connected to one or both computers, as well as the lab PC to conduct testing.

Name	OS	Hardware	Version	Function
Computer #1	Windows 10	HP ProDesk 600 G4	10.0.19041	Test Workstation – This computer will be connected to the KM and provide keyboard, mouse, video, audio, and user authentication data when needed.
Computer #2	Windows 10	HP ProDesk 600 G4	10.0.19041	Test Workstation – This computer will be connected to the KM and provide keyboard, mouse, video, audio, and user authentication data when needed.
LAB PC	Windows 10	Dell Vostro Desktop	10.0.19041	Lab Workstation – This computer will be external to the TOE and be used in measuring the KMs data output.

4.1.1.2 Software

Name	Version
Teledyne LeCroy USB Protocol Suite™	7.60
USBlyzer (USB Analyzer Software)	2.1
Microsoft Device Manager	10.0.19041
Microsoft Notepad	10.0.19041

4.1.2 Test Time & Location

All testing was carried out on-site in Ottawa, Ontario by Acumen Security personnel. Initial receipt and inspection of the TOE occurred in March 2020. The general timeline for testing spanned from March 2020 to October 2021, with periods of inactivity in-between. Much of the testing for the TOE was achieved during the October and November 2020 timeframes as well as October of 2021. For the entire duration of the testing, the TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. Only individuals authorized by Acumen Security were allowed access to the rooms where the devices were kept stored. At the start of each day, the test bed was verified to ensure that it was not compromised. This was achieved by inspecting the tamper seals, enclosures, and cabling for signs of tampering. All evaluation documentation was always kept with the evaluator. In addition, all the necessary precautions and safety protocols were followed.

4.1.3 **Configuration Information**

The following devices were tested:

4.1.3.1 **Product: SCUSBHIDFILTER (Isolator)**

- Name: CYBEX™ Secure USB HID Filter
- Number of Ports: 2 Ports
- Connection Type: USB

4.1.3.2 **Product: SKM140PP4 (Switch)**

- Number of Ports: 4 Ports
- Connection Type: USB

4.1.3.3 **Remote Control: SCAFP0004**

- Number of Buttons: 4 Buttons
- Connection Type: RS232 Cable

5 Detailed Test Cases (TSS, Isolation Document, and Guidance Activities)

The following is a list of the documents consulted:

- [ASE_I] Vertiv CYBEX™ SCUSBHIDFILTER Firmware Version 40404-0E7 Security Target, v1.15, January 5, 2022
- [ASE_S] Switch, Vertiv CYBEX™ SCKM140PP4 KM Switch Firmware Version 40404-0E7 Security Target, v 1.18, January 13, 2022
- [Isol_I] Vertiv CYBEX™ SCUSBHIDFILTER Firmware Version 40404-0E7 Isolation Document, v1.5, December 10, 2020
- [Isol_S] Vertiv CYBEX™ SCKM140PP4 KM Switch Firmware Version 40404-0E7 Isolation Document, v1.6, April 8, 2021
- [CC_Supp_I] Isolator, Vertiv CYBEX™ SCUSBHIDFILTER Firmware Version 40404-0E7 Common Criteria Guidance Supplement, v1.8, January 17, 2022
- [CC_Supp_S] Switch, Vertiv CYBEX™ SCKM140PP4 KM Switch Firmware Version 40404-0E7 Common Criteria Guidance Supplement, v1.8, November 23, 2021
- [2282] CYBEX™ SC Series Secure Switches SC800/900DPH, SC800/900DVI, and SCKM100PP4 Quick Installation Guide, 590-2282-501B
- [2297] CYBEX™ SECURE USB FILTERS, 590-2297-501A
- [Testplan_I] Test Report for Vertiv CYBEX™ SCUSBHIDFILTER Firmware Version 40404-0E7 Peripheral Sharing Device, Version 1.1, January 28, 2022
  [Testplan_S] Test Report for Vertiv CYBEX™ SCKM140PP4 KM Switch Firmware Version 40404-0E7 Peripheral Sharing Device, Version 1.2, January 28, 2022

5.1 TSS, Isolation Document, and Guidance Activities (User Data Protection)

5.1.1 FDP_APC_EXT.1

5.1.1.1 FDP_APC_EXT.1 Isolation Document 1

Objective	The evaluator shall review the Isolation Documentation and Assessment as described in Appendix D of this PP and ensure that it adequately describes the isolation concepts and implementation in the TOE and why it can be relied upon to provide proper isolation between connected computers whether the TOE is powered on or powered off.
Evaluator Findings	Both [Isol_I] and [Isol_S] were reviewed. The isolation concepts are well-defined in both documents. Both documents have the same construction. Section 2.3 in both documents, states “Isolation is maintained when the power is off.” Section 2.4 ‘Power Isolation’ in [Isol_I] “Keyboard and mouse device emulators are independently powered by the connected computer hosts. The use of unidirectional data diodes in the peripheral path prevents power signaling through these external power planes.” Section 2.4 of [Isol_S] describes how the ‘Power Supply Module’ operates in the TOE. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.1.1 FDP_APC_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the conditions under which the TOE enters a failure state.
Evaluator Findings	[ASE_S] sections 7.2 and 7.3 describe the conditions upon which the TOE enters a failure state. [ASE_I] section 7.2 describes the conditions upon which the TOE enters a failure state.

	Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.1.2 FDP_APC_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance describes how a user knows when the TOE enters a failure state.
Evaluator Findings	[CC_Supp_I] section 4.2 and [CC_Supp_S] section 4.2 both describe how a user knows the TOE is in an error state. [CC_Supp_I] states "As the product powers up, it performs a self-test procedure. Following failure of a self-test, the device will enter an error state. The error state is indicated by flashing of the Light Emitting Diode. At this point, the device will be inoperable. It will not accept input from any peripheral device. "and [CC_Supp_S] states, "As the product powers up, it performs a self-test procedure. Following failure of a self-test, the device will enter an error state. The error state is indicated by sequential flashing of the Light Emitting Diodes and by a clicking noise. At this point, the device will be inoperable. It will not accept input from any peripheral device." Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.2 FDP_APC_EXT.1/KM

5.1.2.1 FDP_APC_EXT.1/KM Isolation Document 1

Objective	The evaluator shall examine the Isolation Document and verify it describes how the TOE ensures that no data or electrical signals flow between connected computers in both cases (powered on, powered off).
Evaluator Findings	The evaluator examined the Isolation Documents [Isol_I] and [Isol_S] to determine the verdict of this evaluation activity. Both Isolation Documents have the same construction. Section 2.1 has a data flows description. The 'Main Components in the Data Path' section 2.3 provides an explanation of all data flow isolation. This explains how isolation is maintained with or without power applied. The document states "There is no means for the power source to affect the isolation. Isolation is maintained when the power is off." in section 2.3. The 'Isolation Means Justification' section 3 describes the isolation enforcement policy for various aspects of the TOE. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.2.2 FDP_APC_EXT.1/KM TSS 1

Objective	There are no TSS EAs for this component beyond what the PSD PP requires.
Evaluator Findings	Not Applicable

Verdict	Not Applicable/Pass

5.1.2.3 FDP_APC_EXT.1/KM Guidance 1

Objective	There are no guidance EAs for this component beyond what the PSD PP requires.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.3 FDP_FIL_EXT.1/KM

5.1.3.1 FDP_FIL_EXT.1/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this SFR.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.3.2 FDP_FIL_EXT.1/KM TSS 1

Objective	The evaluator shall examine the TSS and verify that it describes whether the PSD has configurable or fixed device filtering. [Conditional - If “configurable” is selected in FDP_FIL_EXT.1.1/KM, then:] the evaluator shall examine the TSS and verify that it describes the process of configuring the TOE for whitelisting and blacklisting KM peripheral devices, including information on how this function is restricted to administrators. The evaluator shall verify that the TSS does not allow TOE device filtering configurations that permit unauthorized devices on KM interfaces.
Evaluator Findings	The evaluator confirmed that the selection is fixed. The evaluator examined Section 7.1.2.3 titled ‘Keyboard and Mouse Compatible Device Types’ in both [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. 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. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.3.3 FDP_FIL_EXT.1/KM Guidance 1

Objective	[Conditional - If “configurable” is selected in FDP_FIL_EXT.1.1/KM, then:] the evaluator shall examine the guidance documentation and verify that it describes the process of configuring the TOE for whitelisting and blacklisting KM peripheral devices and the administrative privileges required to do this.

Evaluator Findings	The evaluator examined both [ASE_I] and [ASE_S] to determine that 'Configurable' has not been selected. Therefore, this evaluation activity is not applicable.
Verdict	Not Applicable/Pass

5.1.4 FDP_PDC_EXT.1

5.1.4.1 FDP_PDC_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.1.4.2 FDP_PDC_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the compatible devices for each peripheral port type supported by the TOE. The description must include sufficient detail to justify any PP-Modules that extend this PP and are claimed by the TOE (e.g., if the ST claims the Audio Input PP-Module, then the TSS shall reference one or more audio input devices as supported peripherals).
Evaluator Findings	The evaluator examined the section titled 'User Data Protection' in section 7.1 in both [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. The compatible device type for each peripheral port type is described in the section 7.1.2.3 titled 'Keyboard and Mouse Compatible Device Types' in both STs. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.4.3 FDP_PDC_EXT.1 TSS 2

Objective	The evaluator shall verify that the TSS describes the interfaces between the PSD and computers and the PSD and peripherals and ensure that the TOE does not contain wireless connections for these interfaces.
Evaluator Findings	The evaluator confirmed that the [ASE_I] and [ASE_S] indicates that there are no wireless peripherals allowed in this configuration. The 'Keyboard and Mouse Compatible Device Types' section 7.1.2.3 indicates that the TOE does not support a wireless connection to a mouse, keyboard or USB hub. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.4.4 FDP_PDC_EXT.1 TSS 3

Objective	The evaluator shall verify that the list of peripheral devices and interfaces supported by the TOE does not include any prohibited peripheral devices or interface protocols specified in Appendix E.

Evaluator Findings	The evaluator examined the section titled 'User Data Protection' in both [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes the allowed peripheral devices and protocols in 'Keyboard and Mouse Compatible Device Types'. The TOE does not allow non-compliant devices. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.4.5 FDP_PDC_EXT.1 TSS 4

Objective	The evaluator shall verify that the TSS describes all external physical interfaces implemented by the TOE, and that there are no external interfaces that are not claimed by the TSF.
Evaluator Findings	The evaluator examined the section 7.1 titled 'User Data Protection' in both [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes computer connections, remote control ports (Switch only), and keyboard/mouse peripheral interfaces. The TOE is compliant to the PSD PP Appendix E and does not include any unclaimed external interfaces. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.4.6 FDP_PDC_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance provides clear direction for the connection of computers and peripheral devices to the TOE.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined the user guidance documentation, [2297] and [2282]. The product guidance documents provide clear instructions describing how to connect peripheral devices to the TOE. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.4.7 FDP_PDC_EXT.1 Guidance 2

Objective	The evaluator shall verify that the operational user guidance provides clear direction for the usage and connection of TOE interfaces, including general information for computer, power, and peripheral devices.
Evaluator Findings	The evaluator examined the guidance, [2297] and [2282], to determine the verdict of this evaluation activity. The evaluator examined the user guidance documentation. The product guidance documents provide clear instructions on how to connect peripheral devices, power and computers. [2297] section 1 and 2 and [2282] sections 1-4 demonstrate this. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.4.8 FDP_PDC_EXT.1 Guidance 3

Objective	The evaluator shall determine if interfaces that receive or transmit data to or from the TOE present a risk that these interfaces could be misused to import or export user data.
Evaluator Findings	The evaluator examined the guidance, [2282] sections 1-4 and [2297] sections 1 and 2, to determine the verdict of this evaluation activity. The product guidance documents provide connectivity details. The [CC-Supp] section 1 provides additional instructions on usage, including environmental requirements required to alleviate the risk of data loss. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.4.9 FDP_PDC_EXT.1 Guidance 4

Objective	The evaluator shall verify that the operational user guidance describes the visual or auditory indications provided to a user when the TOE rejects the connection of a device.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The [2297] section 1 and [2282] section 4 discuss the acceptance/rejection of a device. When no device is detected, the LED is off. When the TOE rejects a device, an LED on the port blinks green. When the TOE accepts a device, the LED is solid green. There are no audible indications. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.4.10 FDP_PDC_EXT.1/KM Guidance 5

Objective	The evaluator shall verify that the operational user guidance describes devices authorized for use with the TOE in accordance with the authorized peripheral device connections.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The [2297] sections 1 and 2 and [2282] sections 1-4 describe the authorized devices for use with the TOE. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.5 FDP_PDC_EXT.2/KM

5.1.5.1 FDP_PDC_EXT.2/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this SFR.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.5.2 FDP_PDC_EXT.2/KM TSS 1

Objective	TSS evaluation activities for this SFR are performed under FDP_PDC_EXT.1.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.5.3 FDP_PDC_EXT.2/KM Guidance 1

Objective	Guidance evaluation activities for this SFR are performed under FDP_PDC_EXT.1.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.6 FDP_PDC_EXT.3/KM

5.1.6.1 FDP_PDC_EXT.3/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this SFR.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.6.2 FDP_PDC_EXT.3/KM TSS 1

Objective	The evaluator shall examine the TSS and verify it describes which types of peripheral devices that the PSD supports.
Evaluator Findings	The evaluator examined the section 7.1 titled 'User Data Protection' in both Security Targets to determine the verdict of this evaluation activity. The evaluator confirmed that the TSS describes which peripherals are used in the 'Keyboard and Mouse Compatible Device Types' section 7.1.2.3. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.6.3 FDP_PDC_EXT.3/KM TSS 2

Objective	The evaluator shall examine the TSS to verify that keyboard or mouse device functions are emulated from the TOE to the connected computer.
Evaluator Findings	The evaluator examined the section titled 'Keyboard and Mouse Functionality' in both [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. The evaluator confirmed that both [ASE_I] and [ASE_S] and section 7.1.2.2 indicates that the keyboard and mouse function are emulated by the TOE. Based on these findings, this evaluation activity is considered satisfied.

Verdict	Pass

5.1.6.4 FDP_PDC_EXT.3/KM Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.7 FDP_RDR_EXT.1

5.1.7.1 FDP_RDR_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.7.2 FDP_RDR_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes how the TSF identifies and rejects a device that attempts to enumerate again as a different device.
Evaluator Findings	The evaluator examined the section 7.1.2 titled 'Keyboard and Mouse Functionality' in both [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. The evaluator confirmed that this section discusses Keyboard and Mouse Enumeration and indicates that 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. This section also states that 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. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.7.3 FDP_RDR_EXT.1 Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.8 FDP_RIP_EXT.1

5.1.8.1 FDP_RIP_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.8.2 FDP_RIP_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS includes a Letter of Volatility that provides the following information: • Which TOE components have non-volatile memory, the non-volatile memory technology, manufacturer/part number, and memory sizes; • Any data and data types that the TOE may store on each one of these components; • Whether or not each one of these parts is used to store user data and how this data may remain in the TOE after power down; and • Whether the specific component may be independently powered by something other than the TOE (e.g., by a connected computer). Note that user configuration and TOE settings are not considered user data for purposes of this requirement. Note that user configuration and TOE settings are not considered user data for purposes requirement.
Evaluator Findings	The Letter of Volatility is provided as Annex A in both [ASE_I] and [ASE_S] STs. The evaluator confirmed that this section lists each component, its function, manufacture and part number, the type of data stored and whether the storage is volatile, or non-volatile. It also indicates the power source. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.8.3 FDP_RIP_EXT.1 TSS 2

Objective	The evaluator shall verify that the Letter of Volatility provides assurance that user data is not stored in TOE non-volatile memory or storage.
Evaluator Findings	The evaluator examined the ST Annex A titled 'Letter of Volatility' in both [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. The Letter of Volatility is provided as Annex A in the Security Target. The evaluator confirmed that this section indicates that user data is not stored in non-volatile memory or storage. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.8.4 FDP_RIP_EXT.1 Guidance 1

Objective	There are no guidance Evaluation Activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.9 FDP_RIP.1/KM

5.1.9.1 FDP_RIP.1/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.9.2 FDP_RIP.1/KM TSS 1

Objective	The evaluator shall verify that the TSS indicates whether or not the TOE has user data buffers.
Evaluator Findings	The evaluator examined the section 7.1.2 titled 'Keyboard and Mouse Functionality' in the [ASE_I] and [ASE_S] switch to determine the verdict of this evaluation activity. The evaluator confirmed that Section 7.1.2.1 indicates that the Serial Random Access Memory (SRAM) in the host and device emulator circuitry stores USB Host stack parameters and up to the last 4 key codes. User data may be briefly retained; however, there are no data buffers. Data is erased during power off of the KM, and when the user switches channels. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.9.3 FDP_RIP.1/KM TSS 2

Objective	The evaluator shall verify that the TSS describes how all keyboard data stored in volatile memory is deleted upon switching computers.
Evaluator Findings	The evaluator examined the section 7.1.2 titled 'Keyboard and Mouse Functionality' in the [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. The evaluator confirmed that Section 7.1.2.1 indicates that data is erased during power off of the KM, and when the user switches channels. When the TOE switches from one computer to another, the system controller ensures that the keyboard and mouse stacks are deleted, and that any data received from the keyboard in the first 100 milliseconds following switching is deleted. This is done to ensure that any data buffered in the keyboard microcontroller is not passed to the newly selected computer. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.9.4 FDP_RIP.1/KM Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.10 FDP_SWI_EXT.1

5.1.10.1 FDP_SWI_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.10.2 FDP_SWI_EXT.1 TSS 1

Objective	If the ST includes the selection the “TOE supports only one connected computer”, the evaluator shall verify that the TSS indicates that the TOE supports only one connected computer.
Evaluator Findings	The evaluator examined FDP_SWI_EXT.1 in the ‘Security Functional Requirements’ section 6.2 of both [ASE_I] and [ASE_S]. In [ASE_I] ‘The TOE supports only one connected computer’ is selected. Section 7.1.1 [ASE_I] states: “The SCUSBHIDFILTER supports only one connected computer.” In [ASE_S] this selection is not included. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.10.3 FDP_SWI_EXT.1 TSS 2

Objective	If the ST includes the selection “switching can be initiated only through express user action”, the evaluator shall verify that the TSS describes the TOE supported switching mechanisms and that those mechanisms can be initiated only through express user action.
Evaluator Findings	The evaluator examined the section titled ‘System Controller’ (7.1.1) in the [ASE_I] and [ASE_S] isolator to determine the verdict of this evaluation activity. Section 7.1.1 [ASE_I] states: “The SCUSBHIDFILTER supports only one connected computer.” Switching does not apply to the filter.

	7.1.1. of the [ASE-S] states that switching is done through the front panel buttons or a remote control. Express user action is required to perform switching. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.10.4 FDP_SWI_EXT.1 Guidance 1

Objective	If the ST includes the selection “switching can be initiated only through express user action”, the evaluator shall verify that the operational user guidance describes the TOE supported switching mechanisms.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The switching mechanisms are described in the [2282] section 5. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.11 FDP_SWI_EXT.2

5.1.11.1 FDP_SWI_EXT.2 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.11.2 FDP_SWI_EXT.2 TSS 1

Objective	The evaluator shall verify that the TSS describes the TOE supported switching mechanisms. The evaluator shall verify that the TSS does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms. The evaluator shall verify that the described switching mechanisms can be initiated only through express user action according to the selections.
Evaluator Findings	The evaluator examined the section 7.1.1 titled ‘System Controller’ in the [ASE_I] and [ASE_S] switch to determine the verdict of this evaluation activity. The evaluator confirmed that the Switch supports switching using the front panel buttons and remote control. Switching can only be initiated through express user action. The TSS does not include automatic port scanning, control through a connected computer and control through keyboard shortcuts. The Isolator only supports one connected computer. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.11.3 FDP_SWI_EXT.2 Guidance 1

Objective	The evaluator shall verify that the operational user guidance describes the TOE supported switching mechanisms. The evaluator shall verify that the operational user guidance does not

	include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The switching mechanisms are described in [2282] section 5. The guide includes instructions on how the user performs switching. It does not include automatic port scanning, control through a computer or control through keyboard shortcuts. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.12 FDP_SWI_EXT.3

5.1.12.1 FDP_SWI_EXT.3 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.12.2 FDP_SWI_EXT.3 TSS 1

Objective	The evaluator shall verify that the TSS does not indicate that keyboard and mouse devices may be switched independently to different connected computers.
Evaluator Findings	The evaluator examined the section 7.1.2 titled 'Keyboard and Mouse Functionality' in the [ASE_I] and [ASE_S] switch to determine the verdict of this evaluation activity. The evaluator confirmed that this section in [ASE_I] discusses keyboard and mouse switching. The 'TOE Access' Section 7.1.2.1, indicates that the TOE user switches between computers by pressing the corresponding front panel button on the device. The mouse and keyboard are switched together – never independently. The Isolator only supports one connected computer as stated in the TSS of [ASE_I]. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.12.3 FDP_SWI_EXT.3 Guidance 1

Objective	The evaluator shall verify that the guidance does not describe how to switch the keyboard and mouse devices independently to different connected computers.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. Section 5 of [2282] states that the user must press the appropriate button on the front panel to do the switching, or using the remote control. All switching is performed manually. There is no way to switch the keyboard and mouse independently. The guidance documents do not state that the keyboard and mouse can be switched independently. The Isolator only supports one connected computer.

	Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.13 FDP_UDF_EXT.1/KM

5.1.13.1 FDP_UDF_EXT.1/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.13.2 FDP_UDF_EXT.1/KM TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes if and how keyboard Caps Lock, Num Lock, and Scroll Lock indications are displayed by the TOE and to verify that keyboard internal LEDs are not changed by a connected computer.
Evaluator Findings	The evaluator examined the section 7.1.2 titled 'Keyboard and Mouse Functionality' in both [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. The evaluator confirmed that this section explains how the flows to the keyboard/mouse are unidirectional. It states that 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 TSS also indicates [ASE_S] that the use of Caps lock, Num lock and Scroll lock are indicated on the TOE front panel. The TSS in [ASE_S] and [ASE_I] also state: "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." The evaluator confirmed that the Isolator does not contain any Caps Lock, Num Lock, or Scroll Lock indications. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.13.3 FDP_UDF_EXT.1/KM TSS 2

Objective	The evaluator shall examine the TSS to verify that keyboard and mouse functions are unidirectional from the TOE keyboard/mouse peripheral interface to the TOE keyboard/mouse computer interface.
Evaluator Findings	The evaluator examined the section 7.1.2 titled 'Keyboard and Mouse Functionality' in both [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. The evaluator confirmed that this section explains how the flows to the keyboard/mouse are unidirectional. It states that 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.

	Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.13.4 FDP_UDF_EXT.1/KM Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.2 TSS, Isolation Document, and Guidance Activities (Protection of the TSF)

5.2.1 FPT_FLS_EXT.1

Not Applicable. This SFR is evaluated in conjunction with FPT_TST.1.

5.2.2 FPT_NTA_EXT.1

5.2.2.1 FPT_NTA_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.2.2.2 FPT_NTA_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that the TSS documents that connected computers and peripherals do not have access to TOE software, firmware, and TOE memory, except as described above.
Evaluator Findings	The evaluator examined Section 7.2.1 'No Access to TOE' in both [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that firmware is executed on SRAM with the appropriate protections to prevent external access and tampering of code or stacks. Firmware cannot be read or rewritten using JTAG tools. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.2.3 FPT_NTA_EXT.1 Guidance 1

Objective	The evaluator shall check the operational user guidance to ensure any configurations required to comply with this SFR are defined.

Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Secure Operation' section 4 of the CC Guidance Supplement provides a description of the firmware and its accessibility. No additional configuration is required to comply with this SFR. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.3 FPT_PHP.1

5.2.3.1 FPT_PHP.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.2.3.2 FPT_PHP.1 TSS 1

Objective	The evaluator shall verify that the TSS indicates that the TOE provides unambiguous detection of physical tampering of the TOE enclosure and TOE remote controller (if applicable). The evaluator shall verify that the TSS provides information that describes how the TOE indicates that it has been tampered with.
Evaluator Findings	The evaluator examined the section titled 'Passive Detection of Physical Tampering' in [ASE_S] and [ASE_I] to determine the verdict of this evaluation activity. The evaluator confirmed that the tamper evident seals are described in this section. If a seal is removed, the word VOID appears to indicate the TOE has been tampered with. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.3.3 FPT_PHP.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance describes the mechanism by which the TOE provides unambiguous detection of physical tampering and provides the user with instructions for verifying that the TOE has not been tampered with.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The [CC_Supp_S] and [CC_Supp_I] in sections 4.4 and 4.3, respectively, provides a description of the tamper labels applied to the TOE, and directs users to contact Technical Support if the enclosure appears to have been tampered with. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.4 FPT_PHP.3

Note: FPT_PHP.3 only applies to the Switch and not the Isolator device.

5.2.4.1 FPT_PHP.3 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.2.4.2 FPT_PHP.3 TSS 1

Objective	The evaluator shall verify that the TSS describes the TOE's reaction to opening the device enclosure or damaging/exhausting the anti-tampering battery associated with the enclosure.
Evaluator Findings	The evaluator examined the section titled 'Resistance to Physical Attack' in [ASE_S] section 7.2.2.2 to determine the verdict of this evaluation activity. The evaluator confirmed that this section discusses the TOE's response to a tamper event. If the enclosure is opened, the anti-tamper circuitry causes a fuse on the system controller to melt and renders the TOE inoperable. Additionally, if the self-test detects that the battery is depleted or failing, the anti-tampering function will be triggered. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.4.3 FPT_PHP.3 Guidance 1

Objective	The evaluator shall examine the operational user guidance and verify that the guidance provides users with information on how to recognize a device where the anti-tampering functionality has been activated.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. [2282] includes a warning that there is active tamper detection in the device. Users are instructed to contact Technical Support when the tamper event occurs. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.4.4 FPT_PHP.3 Guidance 2

Objective	The evaluator shall verify that the operational user guidance warns the user of the actions that will cause the anti-tampering functionality to disable the device.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The [2282] includes a warning that there is active tamper detection in the device or remote. Users are instructed that if the enclosure appears to have been tampered with, or if all the port LEDs flash sequentially, they are to contact Technical Support. The [CC-Supp_S] section 4.4 also states that "Opening the device will cause it to become permanently disabled. Depletion of the anti-tampering circuitry battery will also cause the device to become permanently disabled."

	It also states “Opening the device will cause it to become permanently disabled . Depletion of the anti-tampering circuitry battery will also cause the remote control device to become permanently disabled.” Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.5 FPT_TST.1

5.2.5.1 FPT_TST.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.2.5.2 FPT_TST.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the self- tests that are performed on start up or on reset (if “upon reset button activation” is selected). The evaluator shall verify that the self-tests cover at least the following: a) a test of the user interface – in particular, tests of the user control mechanism (e.g., checking that the front panel push-buttons are not jammed); and b) if “active anti-tamper functionality” is selected, a test of any antitampering mechanism (e.g., checking that the backup battery is functional).
Evaluator Findings	The evaluator examined the section titled ‘TSF Testing’ section 7.2.3 in [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. The evaluator confirmed that this section discusses the self-test and what it encompasses: Switch • Verification of the front panel push-buttons • Verification of the active anti-tampering functionality including the continued functionality of the backup battery • Verification of the integrity of the microcontroller firmware • Verification of computer port isolation. This is tested by sending test packets to various interfaces and attempting to detect this traffic at all other interfaces Isolator • Verification of the integrity of the microcontroller firmware Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.5.3 FPT_TST.1 TSS 2

Objective	The evaluator shall verify that the TSS describes how the TOE ensures a shutdown upon a self-test failure or a failed anti-tampering function, if present. If there are instances when a

	shutdown does not occur (e.g., a failure is deemed non-security relevant), those cases are identified and a rationale is provided explaining why the TOE's ability to enforce its security policies is not affected.
Evaluator Findings	The evaluator examined the section 7.2.3 titled 'TSF Testing' in both [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that if the self-test fails, the front panel LEDs blink. The Switch also makes a clicking sound. The TOE disables the PSD switching functionality and enters a disabled state. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.5.4 FPT_TST.1 TSS 3

Objective	The evaluator shall check the TSS to verify that it describes the TOE behavior in case of self-test failure. The evaluator shall verify that the described TOE behavior includes shutting down the PSD functionality once the failure is detected.
Evaluator Findings	The evaluator examined the section 7.2.3 titled 'TSF Testing' in both [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that if the self-test fails, the front panel LEDs blink. The Switch also makes a clicking sound. The TOE disables the PSD switching functionality and enters a disabled state. In Section 7.2.3 'TSF Testing' for [ASE_S] it states "If the self-test fails, the Light Emitting Diodes (LEDs) on the device blink and the device makes a clicking sound to indicate the failure. The TOE disables the data flow functionality, and remains in a disabled state until the self-test is rerun and passes. The user can cause the self-test to be rerun by unplugging the device and plugging it back in." In Section 7.2.3 'TSF Testing' for [ASE_I] it states "If the self-test fails, the Light Emitting Diode (LED) on the device blinks to indicate the failure. The TOE disables the data flow functionality, and remains in a disabled state until the self-test is rerun and passes. The user can cause the self-test to be rerun by unplugging the device and plugging it back in. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.5.5 FPT_TST.1 TSS 4

Objective	The evaluator shall examine the TSS to verify that it describes how users verify the integrity of the selections in FPT_TST.1.2 and FPT_TST.1.3. This method can include restarting the TOE, a dedicated self-test, or some other method.
Evaluator Findings	The evaluator examined the section titled 'TSF Testing' section 7.2.3 in both [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. [ASE_S] and [ASE_I] state that the TOE performs a self-test at initial start-up. The user can cause the self-test to be rerun by unplugging the device and plugging it back in Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.5.6 FPT_TST.1 Guidance 1

Objective	The evaluators shall verify that the operational user guidance describes how users verify the integrity of the selections in FPT_TST.1.2 and FPT_TST.1.3. This method can include restarting the TOE, a dedicated self-test, or some other method.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Self Tests' section 4.1 of both [CC_Supp_I] and [CC_Supp_S] provide instructions on how to initiate a self-test. The guidance states that a self-test is performed at power-up. In the case of a failure, users are directed to contact Vertiv Technical Support. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.6 FPT_TST_EXT.1

5.2.6.1 FPT_TST_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.2.6.2 FPT_TST.EXT.1 TSS 1

Objective	The evaluator shall check the TSS to verify that it describes the TOE behavior in case of self-test failure. The evaluator shall verify that the described TOE behavior includes shutting down the PSD functionality once the failure is detected.
Evaluator Findings	The evaluator examined the section titled 'TSF Testing' section 7.2.3 in both [ASE_I] and [ASE_S] to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that if the self-test fails, the front panel LEDs blink and the Switch TOE makes a clicking sound. The TOE disables the PSD switching functionality and enters a disabled state. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.6.3 FPT_TST_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance: a) describes how the results of self-tests are indicated to the user; b) provides the user with a clear indication of how to recognize a failed self-test; and c) details the appropriate actions to be completed in the event of a failed self-test.

Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Self Tests' and 'Error State' sections of the [CC_Supp_I] and [CC_Supp_S] describe how a successful or failed self-test is indicated, and explains what the operator has to do if there is a failure. Following a successful self-test, the device operates normally. Following failure of a self-test, the device will enter an error state. The error state is indicated by sequential flashing of the Light Emitting Diodes. The switch additionally makes a clicking noise. At this point, the device will be inoperable. It will not accept input from any peripheral device or pass output to any peripheral device. In the event of a failed self-test, users are directed to contact Vertiv Technical Support. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.6.4 FPT_TST_EXT.1 Guidance 2

Objective	The evaluator shall verify that the operational user guidance provides adequate information on TOE self-test failures, their causes, and their indications.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Self Tests' section 4 of both [CC_Supp_I] and [CC_Supp_S] describe a self-test failure that may be caused by an unexpected input at power up, or by a failure in the device integrity. Self-test failures are indicated by sequentially blinking LEDs for the switch and the flashing LED of the isolator. The Switch also emits a clicking sound for any self-test failure. To exit self-test mode, the device can be power cycles. Section 4.2 describes the error mode: As the product powers up, it performs a self-test procedure. Following failure of a self-test, the device will enter an error state. The error state is indicated by flashing of the Light Emitting Diode (and by clicking noise on the Switch). At this point, the device will be inoperable. It will not accept input from any peripheral device. The user can cause the self-test to be rerun by unplugging the device and plugging it back in. Based on these findings, the evaluation activity is considered satisfied.
Verdict	Pass

5.3 TSS, Isolation Document, and Guidance Activities (TOE Access)

5.3.1 FTA_CIN_EXT.1

5.3.1.1 FTA_CIN_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.3.1.2 FTA_CIN_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describes how the TOE behaves on power up and on reset, if applicable, regarding which computer interfaces are active, if any.
Evaluator Findings	The evaluator examined the section 7.3 titled 'TOE Access' in [ASE_S] to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that on power up or power up following reset, all peripherals are connected to channel #1, and the corresponding push button LED will be illuminated. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.3.1.3 FTA_CIN_EXT.1 TSS 2

Objective	The evaluator shall verify that the TSS documents the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.
Evaluator Findings	The evaluator examined the section 7.3 titled 'TOE Access' and [ASE_S] to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes the switching functionality. The description and figure show how the selected channel is indicated and that no conflicting information is displayed. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.3.1.4 FTA_CIN_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance notes which computer connection is active on TOE power up or on recovery from reset, if applicable. If a reset option is available, use of this feature must be described in the operational user guidance.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined both [CC_Supp_I] and [CC_Supp_S]. The 'Selected Channel at Startup', Section 4.2 states that Channel 1 is selected by default when the device is started or reset. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.3.1.5 FTA_CIN_EXT.1 Guidance 2

Objective	The evaluator shall verify that the operational user guidance documents the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined the product Quick Installation Guides [2282] and [2297]. [2297] is for the Isolator and describes in section 1 how the TOE indicates if it is accepted or rejected by the TOE.

	[2282] is for the Switch. The guide describes the behavior of the TOE indicators in section 4 and 2 respectively. The document provides a diagram and a description of the channel indicators and a description of the indicator behavior when the switching mechanism is in use. This behavior ensures that no conflicting information is displayed by the indicators. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

6 Test Activities – Isolator

6.1 Test Matrix

PP Module	Security Functional Requirements	Result
Peripheral Sharing Devices Module will test security implementation and resistance to physical tampering of the TOE.	FDP_PDC_EXT.1 (Test Cases 1, 2, 3) FPT_PHP.1 (Test Cases 1, 2) FPT_TST.1 (Test Case 1) FPT_TST_EXT.1 (Test Case 1)	PASS
Keyboard and Mouse Devices Module will test security functionality of keyboard/mouse types to be connected to the TOE.	FDP_APC_EXT.1 (Test Cases 2, 3, 5) FDP_PDC_EXT.1 (Test Cases 1, 2) FDP_FIL_EXT.1 (Test Case 1) FDP_RDR_EXT.1 (Test Case 1)	PASS

6.1.1 FDP_PDC_EXT.1 - Test 1

Item	*Data/Description*
Test ID	*FDP_PDC_EXT.1 – Test 1*
Objective	The evaluator shall check the TOE and its supplied cables and accessories to ensure that there are no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.
Test Equipment Used	N/A
Test Objective Step	1. Check the supplied cables and accessories to ensure there are no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.
Expected Output	1. Supplied cables and accessories contain no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.
Pass/Fail Explanation	The evaluator confirmed that all supplied cables and accessories contain no external wired interfaces. This excludes computer interfaces, peripheral device interfaces, and power interfaces.
Unit Tested	SCUSBHIDFILTER
Result	PASS

6.1.2 FDP_PDC_EXT.1 – Test 2

Item	*Data/Description*
Test ID	*FDP_PDC_EXT.1 – Test 2*
Objective	The evaluator shall check the TOE for radio frequency certification information to ensure that the TOE does not support wireless interfaces.
Test Equipment Used	N/A
Test Objective Step	1. Check the TOE for radio frequency certification information to ensure that the TOE does not support wireless interfaces.
Expected Output	1. The TOE does not support wireless interfaces.

Pass/Fail Explanation	The evaluator has checked the TOE for radio frequency certification information and verified the TOE does not support wireless interfaces.
Unit Tested	SCUSBHIDFILTER
Result	PASS

6.1.3 FDP_PDC_EXT.1 – Test 3

Item	***Data/Description***
Test ID	*FDP_PDC_EXT.1 – Test 3*
Objective	The evaluator shall verify that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections (Appendix E). For this test, verify device rejection through TOE user indication in accordance with the operational user guidance, an immediate cessation of traffic following device detection or enumeration, or incompatibility of the device interface with the peripheral interface, and through no such device appearing in the real-time hardware information console.
Test Equipment Used	Device Manager, BYEASY USB Hub, PS/2 to USB Adapter, Perixx PS/2 Optical Mouse, HSL BADUSB, Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Objective Steps	1. Ensure the TOE is powered off. Open a real-time hardware information console on the connected computer. 2. Attempt to connect a USB mass storage device to the TOE peripheral interface. 3. Power on the TOE. Verify the device is rejected. 4. Ensure the USB mass storage device is disconnected, and then attempt to connect it to the TOE peripheral interface again. 5. Verify the device is rejected. 6. Power off the TOE. Connect an unauthorized USB device to a USB hub, and attempt to connect the USB hub to the TOE peripheral interface. 7. Power on the TOE. Verify the device is rejected. 8. Ensure the USB hub is disconnected, and then attempt to connect it to the TOE peripheral interface again. 9. Verify the device is rejected. 10. Power off the TOE. Attempt to connect any Personal System/2 (PS/2) device directly to the TOE peripheral interface. 11. Power on the TOE. Verify the device is rejected. 12. Ensure the PS/2 device is disconnected, and then attempt to connect it directly to the TOE peripheral interface again. 13. Verify the device is rejected.
Expected Output	1. TOE is powered off. A real-time hardware information console application is running on the connected computer. 2. Connected a USB mass storage to the TOE peripheral interface. 3. TOE is powered on; the device is rejected. 4. Disconnect the USB mass storage device, connect it to the TOE peripheral interface. 5. The device is rejected. 6. TOE is powered off. Connect unauthorized USB device to USB hub, connected it to the TOE peripheral interface again. 7. TOE is powered on; the device is rejected.

	8. Disconnected the USB hub, connected it to the TOE peripheral interface. 9. The device is rejected. 10. TOE is powered on. Attempted to connect a PS/2 device directly to the TOE peripheral interface. 11. TOE is powered on; the device is rejected (The PS/2 device cannot be connected as the TOE contains no PS/2 ports). 12. PS/2 device is already disconnected; attempted to connect it to the TOE peripheral interface. 13. The device is rejected (The PS/2 device cannot be connected as the TOE contains no PS/2 ports).
Test Execution	1. TOE was powered off. A real-time hardware information console application was running on the connected computer. 2. Connected a USB mass storage to the TOE peripheral interface. 3. TOE was powered on; the device was rejected. 4. Disconnected the USB mass storage device, connected it to the TOE peripheral interface. 5. The device was rejected. 6. TOE was powered off. Connected an unauthorized USB device to USB hub, connected it to the TOE peripheral interface again. 7. TOE was powered on; the device was rejected. 8. Disconnected the USB hub, connected it to the TOE peripheral interface. 9. The device was rejected. 10. TOE was powered on. Attempted to connect a PS/2 device directly to the TOE peripheral interface. 11. TOE was powered on; the device was rejected (The PS/2 device cannot be connected as the TOE contains no PS/2 ports). 12. PS/2 device was already disconnected; attempted to connect it to the TOE peripheral interface. 13. The device was rejected (The PS/2 device cannot be connected as the TOE contains no PS/2 ports).
Pass/Fail Explanation	The evaluator confirmed that the TOE ports properly rejects unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections in (Appendix E). The output of the hardware console indicated a device rejection while unauthorized devices were connected and again across power cycling the TOE.
Unit Tested	SCUSBHIDFILTER
Result	PASS

6.1.4 FPT_PHP.1 – Test 1

Item	***Data/Description***
Test ID	*FPT_PHP.1 – Test 1*
Objective	The evaluator shall verify, for each tamper evident seal or label affixed to the TOE encloser and TOE remote controller (if applicable), that any attempts to open the enclosure or remove the seal results in the seal being damaged in a manner that is consistent with the operational user guidance.
Test Equipment Used	N/A
Test Objective Step	1. Remove the tamper evident seals from the TOE.

Expected Output	1. Removal of tamper evident seals results in seals being damaged irreversibly.
Test Execution	1. Removal of tamper evident seals resulted in seals being damaged irreversibly.
Pass/Fail Explanation	The evaluator confirmed that any attempt to open the enclosure or remove the seal results in the seal being damaged in a manner that is consistent with the operational user guidance.
Unit Tested	SCUSBHIDFILTER
Result	PASS

6.1.5 FPT_PHP.1 – Test 2

Item	***Data/Description***
Test ID	*FPT_PHP.1 – Test 2*
Objective	The evaluator shall verify that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.
Test Equipment Used	N/A
Test Objective Step	1. Attempt to remove the tamper evident seals from the TOE without damaging the tampering indicators.
Expected Output	1. The tampering indicators will be damaged and clearly display that the TOE has been tampered with.
Test Execution	1. The TOE tampering mechanism displays “VOID” on the TOE indicating that the unit was tampered with.
Pass/Fail Explanation	The evaluator confirmed that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.
Unit Tested	SCUSBHIDFILTER
Result	PASS

6.1.6 FPT_TST.1 – Test 1

Item	***Data/Description***
Test ID	*FPT_TST.1 – Test 1*
Objective	The evaluator shall trigger the conditions specified in the TSS that are used to initiate TSF self-testing and verify that successful completion of the self-tests can be determined by following the corresponding steps in operational guidance.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Objective Steps	1. The TOE will be powered off, ensure the TOE is removed from a power source (computer) before proceeding. 2. The evaluator will connect a power source (computer) to the TOE and observe the TOE performs a start-up self-test diagnostic for the following criteria: o Verification of the integrity of the microcontroller firmware. 3. Upon completion of the self-testing diagnostic the TOE will power on into operational mode.
Expected Output	1. The TOE will be powered off before proceeding.

	2. The evaluator will connect a power source (computer) to the TOE and observe the TOE performs a start-up self-test diagnostic for the following criteria: o Verification of the integrity of the microcontroller firmware. 3. Upon completion of the self-testing diagnostic the TOE will power on into operational mode.
Test Execution	1. The TOE was powered off before proceeding. 2. The evaluator connected the TOE to a power source (computer) and observed the TOE perform a start-up self-test diagnostic for the following criteria: o Verification of the integrity of the microcontroller firmware – The evaluator confirmed that the firmware is loaded onto the TOE during manufacturing as read-only firmware. Therefore, when the TOE performed its self-test diagnostic it is understood that a successful operational mode startup determines that no changes to the firmware have occurred. Upon completion of the self-testing diagnostic the TOE powered into operational mode. The evaluator confirmed that the verification step was successfully complete and self-testing diagnostics were performed.
Pass/Fail Explanation	The evaluator confirmed that successful completion of the self-tests can be determined by following the corresponding steps in operational guidance. The TOE successfully powered up into an operational state after completion of the self-test diagnostic.
Unit Tested	SCUSBHIDFILTER
Result	PASS

6.1.7 FPT_TST_EXT.1 - Test 1

Item	***Data/Description***
Test ID	*FPT_TST_EXT.1 – Test 1*
Objective	The evaluator shall cause a TOE self-test failure and verify that the TOE responds by disabling normal functions and provides proper indications to the user.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor, Identiv SCR3310 USB UA Device.
Test Objective Steps	1. The TOE will be powered off, ensure the TOE is removed from a power source (computer) before proceeding. 2. The evaluator will connect a power source (computer) to the TOE. The evaluator will plug in an illegal device (Identiv SCR3310) into one of the TOE's USB ports. This will cause the unit to enter a Self-test failure mode where the TOE will be powered on, but unusable. The front panel lights will continue to flash but the TOE remains inoperable. 3. The evaluator shall ensure no keyboard or mouse is being output from the TOE while it is in self-test failure state.
Expected Output	1. TOE will be powered off. 2. The TOE will power on in self-test failure mode, providing visual indication by the front panel lights flashing. 3. No keyboard or mouse will be usable or visible while TOE is in self-test failure state.

Test Execution	1. TOE was powered off. 2. The TOE powered on in self-test failure mode, providing visual indication by the front panel lights flashing. 3. No keyboard or mouse was usable or visible while TOE was in self-test failure state.
Pass/Fail Explanation	The evaluator invoked the self-test failure mode and observed that the TOE responds by disabling normal functions and provides proper indications to the user.
Unit Tested	SCUSBHIDFILTER
Result	PASS

6.1.8 FDP_PDC_EXT.1 - Test 1

Item	***Data/Description***
Test ID	*FDP_PDC_EXT.1 – Test 1*
Objective	The evaluator shall verify that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections. For this test, verify device rejection through TOE user indication in accordance with the operational user guidance, an immediate cessation of traffic following device detection or enumeration, no traffic captured on the USB sniffer or analyzer software other than NAK transactions or system messages, or incompatibility of the device interface with the peripheral interface. Also verify device rejection through examination of the USB sniffer or analyzer software for no traffic captured other than NAK transactions or system messages and through examination of the real-time hardware console for no display of new USB devices (recognized or not recognized). Repeat this test for each keyboard/mouse TOE peripheral interface. Perform steps 1-7 for each of the following unauthorized devices: • USB audio headset • USB camera • USB printer • USB user authentication device connected to a TOE keyboard/mouse peripheral interface • USB wireless LAN dongle
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, USBlyzer, Teledyne Lecroy USB Sniffer, MPOW Headset with USB Connector, Logitech USB Camera, HP Deskjet USB Printer, Identiv USB UA Device, Wireless LAN Dongle, BYEASY USB Hub, Dell Keyboard with Smart Card Reader, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor, Device Manager.
Test Objective Steps	1. Ensure the TOE is powered off and connected to a computer. Run USB analyzer software on the connected computer and connect a USB sniffer to

	the TOE keyboard/mouse peripheral interface. Open the real-time hardware information console. 2. Attempt to connect the unauthorized device to the USB sniffer: • USB Audio headset • USB Camera • USB Printer • USB user authentication device connected to a TOE K/M peripheral interface • USB wireless LAN dongle 3. Power on the TOE. Verify the device is rejected. 4. Ensure the unauthorized device is disconnected from the USB sniffer, then attempt to connect it to the USB sniffer again. 5. Verify the device is rejected. 6. Repeat steps 1 through 5 with a USB hub connected between the USB device and USB sniffer and observe that the results are identical. 7. Repeat steps 1-6 with a composite device with non-HID device classes and verify that the non-HID functions are rejected, or the entire device is rejected.
Expected Output	1. TOE is powered off. USB analyzer software is running, and USB sniffer connected. 2. User will connect each unauthorized device to the USB sniffer. 3. TOE is powered on. Device will be rejected. 4. Device disconnect then reconnected. 5. Device will be rejected. 6. Devices will remain rejected through USB hub. 7. Device will be rejected.
Test Execution	1. TOE was powered off. USB analyzer software was running, and USB sniffer was connected. 2. User connected each unauthorized device to the USB sniffer. 3. TOE was powered on. Device was rejected. 4. The device was disconnect then reconnected. 5. Device was rejected. 6. Devices remained rejected through USB hub. 7. Device was rejected.
Pass/Fail Explanation	The evaluator observed the output of the USB analyzer software and confirmed that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections. The devices listed in step 2 were all properly rejected including when attached to a USB hub.
Unit Tested	SCUSBHIDFILTER
Result	PASS

6.1.9 FDP_PDC_EXT.1 – Test 2

Item	***Data/Description***
Test ID	*FDP_PDC_EXT.1 – Test 2*

Objective	The evaluator shall verify that the TOE KM ports do not reject authorized devices and devices with authorized protocols as per the authorized peripheral device connections. Repeat this test for each of the following four device types: • Barcode reader; • Keyboard or Keypad; • Mouse, Touchscreen, Trackpad, or Trackball; and • PS/2 to USB adapter (with a connected PS/2 keyboard or mouse).
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Notepad, Netum USB Barcode Reader, PS/2 to USB Adapter, Perixx Optical PS/2 Mouse, Dell P2319H Monitor.
Test Objective Steps	1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Run an instance of a text editor on a connected computer. 2. Ensure the TOE is powered off. 3. Connect the authorized device to the TOE peripheral interface: • Barcode reader; • Keyboard or Keypad; • Mouse, Touchscreen, Trackpad, or Trackball; and • PS/2 to USB adapter (with a connected PS/2 keyboard or mouse). 4. Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present. 5. Ensure the connected computer is selected and send inputs using the authorized devices. Verify that the input is received into the text editor or on the screen of the connected computer. 6. Disconnect the authorized device, and then reconnect it to the TOE KM peripheral device interface. 7. Verify the TOE user indication described in the operational user guidance is not present. 8. Send inputs using the authorized devices. Verify that the input is received into the text editor or on the screen of the connected computer.
Expected Output	1. TOE is configured, text editor application is running on connected computer. 2. TOE powered off. 3. User will connect each authorized device throughout test. 4. TOE is powered on. User indication will not be present. 5. Input from authorized device is present via text editor. 6. Authorized device connected to TOE KM port. 7. User indication will not be present. 8. Input from authorized device is present via text editor.

	1. TOE was configured, text editor application was running on connected computer. 2. TOE was powered off. 3. User connected each authorized device throughout test. 4. TOE was powered on. User indication was not present. 5. Input from authorized device is present via text editor. 6. Authorized device was connected to TOE KM port. 7. User indication was not present. 8. Input from the authorized device was present via text editor.
Pass/Fail Explanation	The evaluator observed the output of the USB analyzer to confirm that the TOE KM ports do not reject authorized devices and devices with authorized protocols as per the authorized peripheral device connections. The evaluator has confirmed that authorized devices were accepted by the TOE and the input was successfully received via the text editor.
Unit Tested	SCUSBHIDFILTER
Result	PASS

6.1.10 FDP_APC_EXT.1 - Test 1

Item	***Data/Description***
Test ID	*FDP_APC_EXT.1 – Test 1*
Objective	*[Conditional: Perform this test if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP]* While performing this test, ensure that switching is always initiated through express user action. This test verifies the functionality of the TOE's KM switching methods.
Note	• This test is not applicable to this configuration as "the TOE supports only one connected computer" is selected in FDP_SWI_EXT.1.1 and the TOE does not support this feature.
Testbed	N/A
Test Equipment Used	N/A
Test Objective Steps	1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect an authorized peripheral device for each peripheral device type selected in FDP_PDC_EXT.3.1/KM. Run an instance of a text editor on each connected computer. 2. Connect a display to each computer in order to see all computers at the same time, turn on the TOE, and enter text or move the cursor to verify which connected computer is selected. 3. For each switching method selected in FDP_SWI_EXT.2.2, switch selected computers in accordance with the operational user guidance, and verify that it succeeds. 4. For each peripheral device type selected in FDP_PDC_EXT.3.1/KM, attempt to switch the device to more than one computer at once and verify that the TOE ignores all such commands or otherwise prevents the operation from executing. 5. *[Conditional: If "keyboard" is selected in FDP_PDC_EXT.3.1/KM, then]* attempt to control the computer selection using the following standard keyboard shortcuts, where '#' represents a computer channel number, and

	verify that the selected computer is not switched: • Control - Control - # - Enter • Shift - Shift - # • Num Lock - Minus - # • Scroll Lock - Scroll Lock - # • Scroll Lock - Scroll Lock - Function # • Scroll Lock - Scroll Lock - arrow (up or down) • Scroll Lock - Scroll Lock - # - enter • Control - Shift - Alt - # - Enter • Alt - Control - Shift - # 6. *[Conditional: If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then]* attempt to switch to other connected computers using the pointing device and verify that it does not succeed. 7. *[Conditional: If "peripheral devices using a guard" is selected in FDP_SWI_EXT.2.2, then]* attempt to switch to other connected computers using the peripheral device and guard by only performing some of the steps outlined in the operational user guidance, and verify that it does not succeed.
Expected Output	N/A
Pass/Fail Explanation	*"Switching can be initiated only through express user action"* has not been selected in in FDP_SWI_EXT.1.1. Therefore, this evaluation activity is not applicable.
Unit Tested	N/A
Result	Non-Applicable/Pass

6.1.11 FDP_APC_EXT.1 - Test 2

Item	***Data/Description***
Test ID	*FDP_APC_EXT.1 – Test 2*
Objective	This test verifies the functionality for correct data flows of a mouse and keyboard during different power states of the selected computer.
Notes	• Steps 3 through 10 are not applicable to this TOE as "the TOE supports only one connected computer" is selected in FDP_SWI_EXT.1.1.
Test Equipment Used	Teledyne Lecroy USB sniffer, USBlyzer, Notepad, Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor, Identiv USB UA Device.
Test Objective Steps	1. Continue with the test setup from Test 1 and for each connected computer, connect a USB sniffer between it and the TOE or open the USB analyzer software. Perform steps 2-12 with each connected computer as the selected computer. 2. Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer. *[Conditional: Perform steps 3-10 if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.]*

	3. [If “mouse” is selected in FDP_PDC_EXT.3.1/KM, then] switch the TOE to each connected computer and use the mouse to position the mouse cursor at the center of each display. Switch the TOE back to the originally selected computer. 4. [If “keyboard is selected in FDP_PDC_EXT.3.1/KM, then] use the keyboard to enter text into the text editor. [If “mouse” is selected in FDP_PDC_EXT.3.1/KM, then] use the mouse to move the cursor to the bottom right corner of the display. 5. Switch to each connected computer and verify that the actions taken in Step 4 did not occur on any of the non-selected computers. 6. Switch to the originally selected computer. Continue exercising the functions of the peripheral device(s) and examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent. 7. Disconnect and reconnect the TOE interface cables connected to the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent. 8. Reboot the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent. 9. Enter sleep or suspend mode in the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers to verify that no traffic is sent. 10. Exit sleep or suspend mode on the selected computer. Examine the USB protocol analyzers on each of the non-selected computers to verify that no traffic is sent. Ensure that any text in the Text Editor application is deleted. 11. Perform step 12 when the TOE is off and then in a failure state. 12. Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that no results are observed on the selected computer and that no traffic is captured using the USB analyzer.
Expected Output	1. USB analyzer will be connected between PC and TOE, USB analyzer software will be running on computer. 2. USB traffic is seen on the selected computer. 3. This step is not applicable to this TOE as “the TOE supports only one connected computer” is selected in FDP_SWI_EXT.1.1. 4. This step is not applicable to this TOE as “the TOE supports only one connected computer” is selected in FDP_SWI_EXT.1.1. 5. This step is not applicable to this TOE as “the TOE supports only one connected computer” is selected in FDP_SWI_EXT.1.1. 6. This step is not applicable to this TOE as “the TOE supports only one connected computer” is selected in FDP_SWI_EXT.1.1. 7. This step is not applicable to this TOE as “the TOE supports only one connected computer” is selected in FDP_SWI_EXT.1.1. 8. This step is not applicable to this TOE as “the TOE supports only one connected computer” is selected in FDP_SWI_EXT.1.1. 9. This step is not applicable to this TOE as “the TOE supports only one connected computer” is selected in FDP_SWI_EXT.1.1. 10. This step is not applicable to this TOE as “the TOE supports only one connected computer” is selected in FDP_SWI_EXT.1.1. 11. TOE will be powered off, then in a failure state. 12. No USB traffic is seen on the non-selected and selected computers.

Test Execution	1. USB analyzer was connected between PC and TOE, USB analyzer software was running on the computer. 2. USB traffic was seen on the selected computer. 3. This step is not applicable to this TOE as "the TOE supports only one connected computer" is selected in FDP_SWI_EXT.1.1. 4. This step is not applicable to this TOE as "the TOE supports only one connected computer" is selected in FDP_SWI_EXT.1.1. 5. This step is not applicable to this TOE as "the TOE supports only one connected computer" is selected in FDP_SWI_EXT.1.1. 6. This step is not applicable to this TOE as "the TOE supports only one connected computer" is selected in FDP_SWI_EXT.1.1. 7. This step is not applicable to this TOE as "the TOE supports only one connected computer" is selected in FDP_SWI_EXT.1.1. 8. This step is not applicable to this TOE as "the TOE supports only one connected computer" is selected in FDP_SWI_EXT.1.1. 9. This step is not applicable to this TOE as "the TOE supports only one connected computer" is selected in FDP_SWI_EXT.1.1. 10. This step is not applicable to this TOE as "the TOE supports only one connected computer" is selected in FDP_SWI_EXT.1.1. 11. TOE was powered off, then in a failure state. 12. No USB traffic was seen on the non-selected and selected computers.
Pass/Fail Explanation	Correct data flows of a mouse and keyboard during different power states of the selected computer has been tested. The evaluator has confirmed that data flow is transmitted to the correct computers at the accurate times. The expected USB traffic was observed on the selected computer and no traffic was observed when in a powered off state and during a failure state.
Unit Tested	SCUSBHIDFILTER
Result	PASS

6.1.12 FDP_APC_EXT.1 - Test 3

Item	***Data/Description***
Test ID	*FDP_APC_EXT.1 – Test 3*
Objective	This test verifies that the TOE properly enforces unidirectional flow and isolation.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Device Manager, Razor Mamba Gaming Mouse, Teledyne Lecroy USB Sniffer, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Test Objective Steps	1. Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. *[Perform steps 2 – 12 with each connected computer as the selected computer]* 2. Ensure the TOE is powered on and connect a display directly to the selected computer. Open a real-time hardware information console on the selected computer. *[If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then perform steps 3 - 4]* 3. Connect a gaming mouse with programmable LEDs directly to the selected computer and attempt to configure the LEDs using the mouse application running on the selected computer. Verify that the mouse programmable LEDs change state.

	4. Disconnect the gaming mouse from the selected computer and connect it to the TOE mouse peripheral device port through the USB sniffer. Attempt to configure the LEDs using the mouse application running on the selected computer. Verify that the mouse programmable LEDs do not change state and that no traffic is sent and captured by the USB sniffer while the evaluator is not moving the mouse. *[If "keyboard" is selected in FDP_PDC_EXT.3.1/KM, then perform step 5]* 5. Connect a keyboard to the peripheral device interface through the USB sniffer. Use a keyboard emulation software application running on the selected computer to turn the keyboard Num Lock, Caps Lock, and Scroll Lock LEDs on and off. Verify that the LEDs on the keyboard do not change state and that no traffic is sent and captured by the USB sniffer. 6. Power down the TOE and disconnect the peripheral interface USB cable from the TOE to the selected computer and the peripheral devices from the TOE. 7. Power up the TOE and ensure the selected computer has not changed (this should have no effect on the selected computer because it was disconnected in the previous step). Reconnect the peripheral devices disconnected in step 6 to the TOE. 8. [If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] check that immediately following the connection, the mouse LEDs are illuminated (indicating that the peripheral devices are powered on, although the selected computer is not connected). [If "keyboard" is selected in FDP_PDC_EXT.3.1/KM, then] check that immediately following the connection, the Num Lock, Caps Lock, and Scroll Lock keyboard LEDs are blinking momentarily and then stay off (indicating that the keyboard is powered on, although the selected computer is not connected). 9. Turn the TOE off and disconnect the peripheral devices connected in step 6. 10. Reconnect the first computer interface USB cable to the TOE. 11. Turn on the TOE and check the computer real-time hardware information console for the presence of the peripheral devices connected in step 6 and disconnected in step 9. The presence of the TOE peripheral devices in the information console when the peripheral devices are not connected to the TOE indicates that the TOE emulates the KM devices. 12. *[Conditional]* If the TOE keyboard and mouse do not appear in the listed devices, repeat the following steps for both mouse and keyboard to simulate USB traffic: • Connect a USB generator to the TOE peripheral device interface port. • Configure the USB generator to enumerate as a generic HID mouse/keyboard device and then to generate a random stream of mouse/keyboard report packets. • Connect a USB sniffer device between the TOE computer interface and the USB port on the first computer to capture the USB traffic between the TOE and the first computer. • Turn on the TOE and verify that no packets cross the TOE following the device enumeration.
Expected Output	1. TOE is configured correctly. 2. TOE is powered on; selected computer has display connected. Hardware information console is open on computer. 3. Mouse programmable LED does change state. 4. Mouse programmable LED does not change state, no USB traffic is generated. 5. Keyboard LEDs do not change state and no USB traffic is generated. 6. TOE is powered off, peripheral cable unplugged. 7. TOE is powered on, peripheral cable reconnected.

	8. Mouse: LEDs should be illuminated. Keyboard: LEDs blink momentarily then stay off. 9. TOE powered off; peripherals disconnected. 10. USB cable reconnected. 11. Hardware management console will indicate emulated peripheral devices. 12. No packets should be captured following the device enumeration.
Test Execution	1. TOE was configured correctly. 2. TOE was powered on; selected computer had display connected. Hardware information console was open on computer. 3. Mouse programmable LED did change state. 4. Mouse programmable LED did not change state, no USB traffic was generated. 5. Keyboard LEDs did not change state and no USB traffic was generated. 6. TOE was powered off; peripheral cable was unplugged. 7. TOE was powered on; peripheral cable was reconnected. 8. Mouse: LEDs are illuminated. Keyboard: LEDs blinked momentarily then stayed off. 9. TOE was powered off; peripherals were disconnected. 10. USB cable was reconnected. 11. Hardware management console indicated emulated peripheral devices. 12. This step is non-applicable / pass as the TOE successfully emulated the keyboard and mouse.
Pass/Fail Explanation	Unidirectional flow and isolation of USB traffic has been tested. The evaluator has confirmed that USB traffic is enforced properly and in a single direction. This was tested on all four connected computers. Mouse LEDs are illuminated when expected, and change state only when not attached to a USB analyzer. Keyboard LEDs blink momentarily when connected and do not change state when attached to an analyzer. The devices were properly emulated by the TOE and no packets were captured following enumeration.
Unit Tested	SCUSBHIDFILTER
Result	PASS

6.1.13 FDP_APC_EXT.1 - Test 4

Item	***Data/Description***
Test ID	*FDP_APC_EXT.1 – Test 4*
Objective	*[Conditional: Perform this test if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP]* This test verifies correct data flow while the TOE is powered on or powered off.
Notes	• This test is not applicable to this configuration as "the TOE supports only one connected computer" is selected in FDP_SWI_EXT.1.1 and the TOE does not support this feature. • TD0507 has been incorporated into FDP_APC_EXT.1 – Test 4.
Test Equipment Used	N/A
Test Objective Steps	1. Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. Connect a display directly to each connected computer. Perform steps 2-10 for each connected computer.

	2. Connect a USB sniffer between a non-selected TOE KM computer interface and its computer. Run USB protocol analyzer software on all remaining computers. 3. Turn on the TOE and observe the TOE enumeration data flow in the protocol analyzer connected to the selected computer and is not in any other USB protocol analyzers or the USB sniffer. 4. Ensure the TOE is switched to the first computer. 5. Reboot the first computer. Verify that no USB traffic is captured on all non-selected computer USB protocol analyzers. 6. Generate intensive USB HID traffic by moving the mouse at high speed and/or holding down the keyboard space key at the same time. Verify that no new USB traffic is captured on all non-selected computer USB protocol analyzers. 7. Perform steps 8 and 9 for each TOE keyboard/mouse peripheral interface. 8. Connect a USB dummy load into the TOE KM peripheral device interface. Verify that no new USB traffic is captured on all non-selected computer USB protocol analyzers. Remove the plug after the step is completed. 9. Connect a switchable 5-volt power supply with any compatible USB plug into the TOE KM peripheral device interface. Modulate the 5-volt supply (i.e., cycle on and off) manually at various speeds from approximately one cycle per five seconds to one cycle per second. Verify that no new USB traffic is captured on all non-selected computer USB analyzers. 10. Turn off the TOE. Verify that no new traffic is captured.
Expected Output	N/A
Pass/Fail Explanation	*"Switching can be initiated only through express user action"* has not been selected in in FDP_SWI_EXT.1.1. Therefore, this evaluation activity is not applicable.
Unit Tested	N/A
Result	Non-Applicable/Pass

6.1.14 FDP_APC_EXT.1 - Test 5

Item	***Data/Description***
Test ID	*FDP_APC_EXT.1 – Test 5*
Objective	This test verifies that the TOE does not send data to different computers connected to the same interface at different times. Repeat this test for each TOE KM computer port.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Notepad, USBlyzer, Dell P2319H Monitor.
Test Objective Steps	1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect an authorized peripheral device for each peripheral device type selected in FDP_PDC_EXT.3.1/KM. Connect two computers to a different display and run an instance of a text editor and USB analyzer software on each computer. 2. Connect the first computer to the TOE and ensure it is selected and that no other computers are connected. 3. Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer.

	4. Disconnect the first computer. Generate intensive USB HID traffic by moving the mouse at high speed and/or holding down the keyboard space key at the same time. 5. Cease generation of the USB HID traffic, connect the second computer to the same port and ensure it is selected. 6. Verify that no results from the previous use of the peripheral device are observed on the selected computer and that no traffic is sent and captured using the USB analyzer. 7. Reboot the TOE and repeat step 6. 8. Turn off the TOE and repeat step 6. 9. Restart the TOE and repeat step 6. 10. Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer.
Expected Output	1. Authorized peripheral devices connected, display connected to each computer, text editor and USB analyzer running on each computer. 2. Only the first computer is connected and selected. 3. USB traffic captured on selected computer. 4. Computer disconnected; USB traffic generated. 5. Second computer connected to first computers port. 6. No USB traffic should leak over from first computer. 7. TOE rebooted. No USB data captured. 8. TOE powered off. No USB data captured. 9. TOE rebooted. No USB data captured. 10. Expected USB traffic generated on selected computer.
Test Execution	1. Authorized peripheral devices were connected, display was connected to each computer, text editor and USB analyzer was running on each computer. 2. Only the first computer was connected and selected. 3. USB traffic was captured on selected computer. 4. Computer was disconnected; USB traffic was generated. 5. Second computer was connected to first computers port. 6. No USB traffic leaked over from the first computer. 7. TOE was rebooted. No USB data was captured. 8. TOE was powered off. No USB data was captured. 9. TOE was restarted. No USB data was captured. 10. Expected USB traffic was generated on selected computer.
Pass/Fail Explanation	Data flow through the same interface has been observed and tested. The evaluator confirms that the TOE does not send data to different computers connected to the same interface at different times.
Unit Tested	SCUSBHIDFILTER
Result	PASS

6.1.15 FDP_FIL_EXT.1 - Test 1

Item	***Data/Description***
Test ID	*FDP_FIL_EXT.1 – Test 1*
Objective	Perform the test steps in FDP_PDC_EXT.1 with all devices on the PSD KM blacklist and verify that they are rejected as expected.

Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, USBlyzer, Teledyne Lecroy USB Sniffer, Device Manager, MPOW Headset with USB Connector, Logitech USB Camera, HP Deskjet USB Printer, Identiv USB UA Device, Wireless LAN Dongle, BYEASY USB Hub, Dell Keyboard with Smart Card Reader, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Test Objective Steps	1. Ensure the TOE is powered off and connected to a computer. Run USB analyzer software on the connected computer and connect a USB sniffer to the TOE keyboard/mouse peripheral interface. Open the real-time hardware information console. 2. Attempt to connect the unauthorized device to the USB sniffer: • USB audio headset • USB camera • USB printer • USB user authentication device connected to a TOE keyboard/mouse peripheral interface • USB wireless LAN dongle 3. Power on the TOE. Verify the device is rejected. 4. Ensure the unauthorized device is disconnected from the USB sniffer, then attempt to connect it to the USB sniffer again. 5. Verify the device is rejected. 6. Repeat steps 1 through 5 with a USB hub connected between the USB device and USB sniffer and observe that the results are identical. 7. Repeat steps 1-6 with a composite device with non-HID device classes and verify that the non-HID functions are rejected, or the entire device is rejected.
Expected Output	1. TOE is powered off. USB analyzer software is running, and USB sniffer connected. 2. User will connect each device to the USB sniffer. 3. TOE is powered on. Device will be rejected. 4. Device disconnect then reconnected. 5. Device will be rejected. 6. Devices will remain rejected through USB hub. 7. Device will be rejected.
Test Execution	1. TOE was powered off. USB analyzer software was running, and USB sniffer was connected. 2. User connected each device to the USB sniffer. 3. TOE was powered on. Device was rejected. 4. Device disconnect then reconnected. 5. Device was rejected. 6. Devices remain rejected through USB hub. 7. Device was rejected.
Pass/Fail Explanation	All devices on the PSD KM blacklist were tested and are rejected as expected. The evaluator confirms that the blacklist in place rejects all devices found in step 2. The evaluator confirmed through observation of the USB analyzer software that all blacklisted devices are rejected initially after power-on, after reconnecting, and whilst connected to a USB hub.
Unit Tested	SCUSBHIDFILTER
Result	PASS

6.1.16 FDP_RDR_EXT.1 – Test 1

Item	*Data/Description*
Test ID	*FDP_RDR_EXT.1 – Test 1*
Objective	The evaluator shall use a BadUSB, programmable keyboard, and/or USB Rubber Ducky as a malicious USB device to perform the following tests.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, Device Manager, HSL BADUSB, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Test Objective Steps	1. Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. Ensure the TOE is powered off and connect a USB sniffer between the TOE and a computer. Open a real-time hardware information console. 2. Configure the malicious USB device as a HID-class device and to re-enumerate as a mass storage device. 3. Connect the malicious USB device to the TOE KM peripheral interface. 4. Power on the TOE and active the re-enumeration after 1 minute. 5. Verify device rejection per TOE guidance, the cessation traffic passed in the USB sniffer, and the absence of the device and any new device in the information console. 6. Remove the malicious USB device and reconfigure as a HID-class device and to re-enumerate as a mass storage device. 7. Connect the malicious USB device to the TOE KM peripheral interface and active the re-enumeration after 1 minute. 8. Verify device rejection per TOE guidance, the cessation of traffic passed in the USB sniffer, and the absence of the device and any new devices in the information console.
Expected Output	1. TOE is powered off. USB sniffer is configured correctly, and hardware information console is open. 2. USB device will be configured correctly. 3. USB Device connected to peripheral interface. 4. TOE is powered on. 5. Device will not appear in hardware information console. 6. USB device will be configured correctly. 7. USB Device connected to peripheral interface. 8. Device will not appear in hardware information console.
Test Execution	1. The evaluator ensured the TOE was powered off. A USB sniffer was connected between the TOE and a computer. A hardware information console was open on the selected computer. 2. The malicious USB device was configured as a HID-class device and then to re-enumerate as a mass storage device. The USB device was pre-programmed to replicate the two functions if the toggle switch on the device was set to the “middle” position. 3. The evaluator connected the USB Device to the TOE KM peripheral interface. 4. The TOE was powered on and re-enumeration was active after 1 minute.

	5. The evaluator verified device rejected by the cessation of traffic passed to the USB sniffer and the absence of the device in hardware information console. 6. The evaluator removed the malicious USB device. The device was reconfigured as a HID-class device and then to re-enumerate as a mass storage device. 7. The evaluator connected the USB Device to the TOE KM peripheral interface and re-enumeration was activated after 1 minute. 8. The evaluator verified device rejected by the cessation of traffic passed to the USB sniffer and the absence of the device in hardware information console.
Pass/Fail Explanation	The evaluator configured the USB device accordingly and verified that the device was rejected appropriately. The TOE rejects the device and no new devices appear in the hardware console after re-enumeration.
Unit Tested	SCUSBHIDFILTER
Result	PASS

7 Test Activities – Switch

7.1 Test Matrix

PP Module	Security Functional Requirements	Result
Peripheral Sharing Devices Module will test security implementation and resistance to physical tampering of the TOE.	FDP_PDC_EXT.1 (Test Cases 1, 2, 3) FPT_PHP.1 (Test Cases 1, 2) FPT_TST.1 (Test Case 1) FPT_TST_EXT.1 (Test Case 1) FPT_PHP.3 (Test Case 1) FTA_CIN_EXT.1 (Test Case 1)	PASS
Keyboard and Mouse Devices Module will test security functionality of keyboard/mouse types to be connected to the TOE.	FDP_APC_EXT.1 (Test Cases 1, 2, 3, 4, 5) FDP_PDC_EXT.1 (Test Cases 1, 2) FDP_FIL_EXT.1 (Test Case 1) FDP_RDR_EXT.1 (Test Case 1)	PASS

7.1.1 PDP_PDC_EXT.1 – Test 1

Item	*Data/Description*	
Test ID	*FDP_PDC_EXT.1 – Test 1*	
Objective	The evaluator shall check the TOE and its supplied cables and accessories to ensure that there are no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.	
Test Equipment Used	N/A	
Test Objective Step	1. Check the supplied cables and accessories to ensure there are no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.	
Expected Output	1. Supplied cables and accessories contain no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.	
Test Execution	1. Supplied cables and accessories contained no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.	
Pass/Fail Explanation	The evaluator confirmed that all supplied cables and accessories contain no external wired interfaces. This excludes computer interfaces, peripheral device interfaces, and power interfaces.	
Units Tested	SCKM140PP4	SCAFP0004
Result	PASS	PASS

7.1.2 PDP_PDC_EXT.1 – Test 2

Item	*Data/Description*
Test ID	*FDP_PDC_EXT.1 – Test 2*
Objective	The evaluator shall check the TOE for radio frequency certification information to ensure that the TOE does not support wireless interfaces.
Test Equipment Used	N/A
Test Objective Step	1. Check the TOE for radio frequency certification information to ensure that the TOE does not support wireless interfaces.
Expected Output	1. The TOE does not support wireless interfaces.

Test Execution	1. The TOE does not contain any radio frequency certification information.	
Pass/Fail Explanation	The evaluator has checked the TOE for radio frequency certification information and verifies the TOE does not support wireless interfaces.	
Units Tested	SCKM140PP4	SCAFP0004
Result	PASS	PASS

7.1.3 PDP_PDC_EXT.1 – Test 3

Item	***Data/Description***
Test ID	*FDP_PDC_EXT.1 – Test 3*
Objective	The evaluator shall verify that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections (Appendix E). For this test, verify device rejection through TOE user indication in accordance with the operational user guidance, an immediate cessation of traffic following device detection or enumeration, or incompatibility of the device interface with the peripheral interface, and through no such device appearing in the real-time hardware information console.
Notes	• The TOE does not contain any PS/2 input, therefore any attempt to directly connect a PS/2 interface to the TOE will result in the device being rejected.
Test Equipment Used	Device Manager, BYEASY USB Hub, PS/2 to USB Adapter, Perixx PS/2 Optical Mouse, HSL BADUSB, Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Objective Steps	1. Ensure the TOE is powered off. Open a real-time hardware information console on the connected computer. 2. Attempt to connect a USB mass storage device to the TOE peripheral interface. 3. Power on the TOE. Verify the device is rejected. 4. Ensure the USB mass storage device is disconnected, and then attempt to connect it to the TOE peripheral interface again. 5. Verify the device is rejected. 6. Power off the TOE. Connect an unauthorized USB device to a USB hub, and attempt to connect the USB hub to the TOE peripheral interface. 7. Power on the TOE. Verify the device is rejected. 8. Ensure the USB hub is disconnected, and then attempt to connect it to the TOE peripheral interface again. 9. Verify the device is rejected. 10. Power off the TOE. Attempt to connect any Personal System/2 (PS/2) device directly to the TOE peripheral interface. 11. Power on the TOE. Verify the device is rejected. 12. Ensure the PS/2 device is disconnected, and then attempt to connect it directly to the TOE peripheral interface again. 13. Verify the device is rejected.
Expected Output	1. TOE is powered off. A real-time hardware information console application is running on the connected computer. 2. Connected a USB mass storage to the TOE peripheral interface. 3. TOE is powered on; the device is rejected. 4. Disconnect the USB mass storage device, connect it to the TOE peripheral interface.

	5. The device is rejected. 6. TOE is powered off. Connect unauthorized USB device to USB hub, connected it to the TOE peripheral interface again. 7. TOE is powered on; the device is rejected. 8. Disconnected the USB hub, connected it to the TOE peripheral interface. 9. The device is rejected. 10. TOE is powered on. Attempted to connect a PS/2 device directly to the TOE peripheral interface. 11. TOE is powered on; the device is rejected (The PS/2 device cannot be connected as the TOE contains no PS/2 ports). 12. PS/2 device is already disconnected; attempted to connect it to the TOE peripheral interface. 13. The device is rejected (The PS/2 device cannot be connected as the TOE contains no PS/2 ports).
Test Execution	1. TOE was powered off. A real-time hardware information console application was running on the connected computer. 2. Connected a USB mass storage to the TOE peripheral interface. 3. TOE was powered on; the device was rejected. 4. Disconnected the USB mass storage device, connected it to the TOE peripheral interface. 5. The device was rejected. 6. TOE was powered off. Connected an unauthorized USB device to USB hub, connected it to the TOE peripheral interface again. 7. TOE was powered on; the device was rejected. 8. Disconnected the USB hub, connected it to the TOE peripheral interface. 9. The device was rejected. 10. TOE was powered on. Attempted to connect a PS/2 device directly to the TOE peripheral interface. 11. TOE was powered on; the device was rejected (The PS/2 device cannot be connected as the TOE contains no PS/2 ports). 12. PS/2 device was already disconnected; attempted to connect it to the TOE peripheral interface. 13. The device was rejected (The PS/2 device cannot be connected as the TOE contains no PS/2 ports).
Pass/Fail Explanation	The evaluator confirmed that the TOE ports properly rejects unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections in (Appendix E). The output of the hardware console indicated a device rejection while unauthorized devices were connected and again across power cycling the TOE.
Remote Controller Used	SCAFP0004
Unit Tested	SCKM140PP4
Result	PASS

7.1.4 FPT_PHP.1 – Test 1

Item	***Data/Description***
Test ID	*FPT_PHP.1 – Test 1*

Objective	The evaluator shall verify, for each tamper evident seal or label affixed to the TOE encloser and TOE remote controller (if applicable), that any attempts to open the enclosure or remove the seal results in the seal being damaged in a manner that is consistent with the operational user guidance.	
Test Equipment Used	N/A	
Test Objective Step	1. Removed the tamper evident seals from the TOE.	
Expected Output	1. Removal of tamper evident seals results in seals being damaged irreversibly.	
Test Execution	1. Removal of tamper evident seals resulted in seals being damaged irreversibly.	
Pass/Fail Explanation	The evaluator confirms that any attempt to open the enclosure or remove the seal results in the seal being damaged in a manner that is consistent with the operational user guidance.	
Units Tested	SKM140PP4	SCAFP0004
Result	PASS	PASS

7.1.5 FPT_PHP.1 – Test 2

Item	***Data/Description***	
Test ID	*FPT_PHP.1 – Test 2*	
Objective	The evaluator shall verify that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.	
Test Equipment Used	N/A	
Test Objective Step	1. Attempt to remove the tamper evident seals from the TOE without damaging the tampering indicators.	
Expected Output	1. The tampering indicators will be damaged and clearly display that the TOE has been tampered with.	
Test Execution	1. The TOE tampering mechanism displays “VOID” on the TOE indicating that the unit was tampered with.	
Pass/Fail Explanation	The evaluator confirms that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.	
Units Tested	SKM140PP4	SCAFP0004
Result	PASS	PASS

7.1.6 FPT_PHP.3 – Test 1

Item	***Data/Description***
Test ID	*FPT_PHP.3 – Test 1*
Objective	In the following testing the evaluator shall attempt to gain physical access to the TOE internal circuitry (enough access to allow the insertion of tools to tamper with the internal circuitry). The TOE anti- tampering function is expected to trigger, causing an irreversible change to the TOE functionality. The evaluator then shall verify that the anti-tampering triggering provides the expected user indications and also disables the TOE. TOE disabling means that the user would not be able to use the TOE for any purpose – all peripheral devices and computers are isolated

Notes	• TD0583 has been incorporated into FPT_PHP.3 – Test 1.
Test Equipment Used	N/A
Test Objective Steps	1. [Conditional: this step is applicable for TOEs having a remote controller] The evaluator shall attempt to open the PSD remote controller enclosure enough to gain access to its internal circuitry and observe that the TOE is both permanently disabled and provides the proper indications that is has been tampered with in accordance with the operational user guidance. 2. The evaluator shall attempt to open the PSD enclosure enough to gain access to its internal circuitry and observe that the TOE is both permanently disabled and provides the proper indication that it has been tampered with in accordance with the operational user guidance. 3. The evaluator shall attempt to access the TOE settings to reset the tampering state and verify that it is not possible to recover from the tampered state. 4. The evaluator shall acquire a copy of the TOE that has been previously tampered with. 5. The evaluator shall power on the TOE and verify that the tampering indicator is displayed.
Expected Output	1. Remote controller displays proper indications that unit has been tampered with. 2. Removed tamper proof seals from PSD, the seals show “VOID” to indicate the unit has been tampered with. Once PSD has been opened the anti-tampering mechanism releases and renders the unit permanently disabled. 3. Attempted to reset the tampering state, could not recover the PSD from tampered state. 4. Evaluator has acquired a copy of the TOE that has been previously tampered with. 5. Tampering indicator on TOE is displayed, unit is rendered permanently disabled.
	1. The evaluator removed the tamper proof seals from the remote control. The seals showed “VOID” to indicate the unit has been tampered with. Once the remote control had been opened the anti-tampering mechanism released and rendered the unit permanently disabled. The remote control displayed the proper visual indications using its LEDs to prove the unit had been tampered with. 2. The evaluator removed the tamper proof seals from PSD. The seals showed “VOID” to indicate the unit had been tampered with. Once the PSD had been opened the anti-tampering mechanism released and rendered the unit permanently disabled. The PSD displayed the proper visual indications using its LEDs to prove the unit had been tampered with. 3. The evaluator attempted to reset the tampering state by re-arming/resetting the anti-tampering trigger. The evaluator could not recover the PSD from its tampered state. 4. The evaluator had acquired a copy of the TOE that has been previously tampered with. 5. The evaluator confirms the tampering indicator on TOE is displayed, and the unit is rendered permanently disabled.
Pass/Fail Explanation	The evaluator confirmed that the anti-tampering triggering provides the expected user indications and disables the TOE. The TOE remained in a disabled state and

	could not be recovered. In addition, the TOE provided the appropriate tamper indications after attempting to access the internals of the device.	
Units Tested	SKM140PP4	SCAFP0004
Result	PASS	PASS

7.1.7 FPT_TST.1 – Test 1

Item	***Data/Description***
Test ID	*FPT_TST.1 – Test 1*
Objective	The evaluator shall trigger the conditions specified in the TSS that are used to initiate TSF self-testing and verify that successful completion of the self-tests can be determined by following the corresponding steps in operational guidance.
Notes	• The evaluator followed the TSF Testing section as outline in the security target. The security target specifically states that the TOE will perform all self-tests as outlines in the test objective steps section below. If any of the self-tests fail the LEDs on the front panel blink and the unit will make a clicking sound and the test would be considered a fail.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Objective Steps	1. The TOE must be powered off, ensure the power cable is removed from the TOE before proceeding. 2. The evaluator will connect the power cable to the TOE and observe the TOE performs a start-up self-test diagnostic for the following criteria: o Verification of the front panel push buttons o Verification of the active anti-tampering functionality including the continued functionality of the backup battery o Verification of the integrity of the microcontroller firmware o Verification of computer port isolation 3. Upon completion of the self-testing diagnostic the TOE will power on into operational mode and channel 1 will be selected by default.
Expected Output	1. The TOE will be powered off, the power cable is removed from the TOE before proceeding. 2. The evaluator will connect the power cable to the TOE and observe the TOE performs a start-up self-test diagnostic for the following criteria: o Verification of the front panel push buttons o Verification of the active anti-tampering functionality including the continued functionality of the backup battery o Verification of the integrity of the microcontroller firmware o Verification of computer port isolation 3. Upon completion of the self-testing diagnostic the TOE will power on into operational mode and channel 1 will be selected by default.
Test Execution	1. The TOE was powered off and the evaluator removed the power cable from the TOE before proceeding. 2. The evaluator connected the power cable to the TOE and observed the TOE perform a start-up self-test diagnostic for the following criteria: o Verification of the front panel push buttons – The evaluator confirmed the front panel push buttons retained their secure state and no tampering or damage was present on the push buttons. o Verification of the anti-tampering functionality including the continued functionality of the backup battery – The evaluator

	confirmed that during self-testing the backup batteries status is evaluated to ensure depletion or failure of the battery is not detected. Therefore, when the TOE performed its self-test diagnostic it is understood that a successful operational mode startup determines that no changes to the batteries state have been detected. ○ Verification of the integrity of the microcontroller firmware – The evaluator confirmed that the firmware is loaded onto the TOE during manufacturing as read-only firmware. Therefore, when the TOE performed its self-test diagnostic it is understood that a successful operational mode startup determines that no changes to the firmware have occurred. ○ Verification of computer port isolation – The evaluator confirmed during self-testing packets are sent to various interfaces and attempts are made to detect traffic on other interfaces. If any traffic is detected the test fails and the TOE enters a disabled state. Therefore, any successful power on into operational mode is deemed a pass for this portion of self-testing. 3. Upon completion of the self-testing diagnostics the TOE powered into operational mode and channel #1 was selected by default. The evaluator confirmed that all three verifications steps were successfully complete and self-testing diagnostics were performed.
Pass/Fail Explanation	The evaluator confirmed that successful completion of the self-tests can be determined by following the corresponding steps in operational guidance. The TOE successfully powered up into an operational state after completion of the self-test diagnostic.
Remote Controller Used	SCAFP0004
Unit Tested	SCKM140PP4
Result	PASS

7.1.8 FPT_TST_EXT.1 – Test 1

Item	***Data/Description***
Test ID	*FPT_TST_EXT.1 – Test 1*
Objective	The evaluator shall cause a TOE self-test failure and verify that the TOE responds by disabling normal functions and provides proper indications to the user.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Objective Steps	1. The TOE must be powered off, ensure the power cable is removed from the TOE before proceeding. 2. Firmly press any of the front panel buttons on the TOE while simultaneously plugging in the power cable. This will cause the unit to enter a Self-test failure mode where the TOE will be powered on, but unusable. The front panel lights will continue to cycle between the computers connected but the TOE remains inoperable. 3. The evaluator shall ensure no keyboard or mouse is being output from the TOE while it is in self-test failure state.

Expected Output	1. TOE will be powered off, cable unplugged from back of TOE. 2. The TOE will power on in self-test failure mode, providing visual indication by cycling through the LED computer channels on the front panel display and the TOE will make a clicking noise. 3. No keyboard or mouse will be usable or visible while TOE is in self-test failure state.
Test Execution	1. TOE was powered off; cable was unplugged from back of TOE. 2. The TOE powered on in self-test failure mode, providing visual indication by cycling through the LED computer channels on the front panel display and a clicking noise was produced by the TOE. 3. No keyboard or mouse was usable or visible while TOE was in self-test failure state.
Pass/Fail Explanation	The evaluator invoked the self-test failure mode and observed that the TOE responds by disabling normal functions and provides proper indications to the user.
Remote Controller Used	SCAFP0004
Unit Tested	SCKM140PP4
Result	PASS

7.1.9 FTA_CIN_EXT.1 – Test 1

Item	***Data/Description***
Test ID	*FTA_CIN_EXT.1 – Test 1*
Objective	The evaluator shall verify which computer connection is active on TOE power up or on recovery from reset. The evaluator shall also verify the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Objective Steps	1. The evaluator shall configure the TOE and its operational environment in accordance with the operational user guidance. 2. The evaluator shall select a connected computer and power down the TOE, then power up the TOE and verify that the expected selected computer is indicated in accordance with the TSS and that the connection is active. 3. The evaluator shall repeat this process for every possible selected TOE configuration. 4. [Conditional] If "*upon reset button activation*" is selected in FPT_TST.1.1, then the evaluator shall repeat this process for each TOE configuration using the reset function rather than power-down and power-up. 5. The evaluator shall verify that the TOE selected computer indications are always on (i.e., continuous) and fully visible to the TOE user. 6. [Conditional] If the TOE allows peripherals to have active interfaces with different computers at the same time, the evaluator shall verify that each permutation has its own selection indications.

	7. [Conditional] If "*a screen with dimming function*" is selected, the evaluator shall verify that indications are visible at minimum brightness settings in standard room illumination conditions. 8. [Conditional] If "*multiple indicators which never display conflicting information*" is selected, the evaluator shall verify that either all indicators reflect the same status at all times, or the indicator for the most recently used switching mechanism displays the correct switching status and that all other indicators display the correct status or no status
Expected Output	1. The TOE and its operational environment have been configured in accordance with the operational user guidance. 2. A computer will be selected, then the TOE will be powered down. The TOE will then be powered up and the evaluator will verify that the expected selected computer is indicated in accordance with the TSS and that the connection is active. 3. This process will be repeated for every possible selected TOE configuration. 4. This process will be repeated for every possible TOE configuration using the reset function rather than power-down and power-up. 5. The selected computer indications on the TOE are always on and fully visible to the TOE user. 6. The TOE shall allow peripheral to have active indications with different computers at the same time. 7. "A *screen with dimming function*" was not selected, therefore testing for this step is non-applicable. 8. The indicators always reflect the same status, or the indicator for the most recently used switching mechanism displays the correct switching status and that all other indicators display the correct status or no status.
Test Execution	1. The TOE and its operational environment have been configured in accordance with the operational user guidance. 2. A computer was selected, then the TOE was powered down. The TOE was then powered up and the evaluator verified that the expected selected computer was indicated in accordance with the TSS and that the connection was active. 3. This process was repeated for every possible selected TOE configuration. 4. "U*pon reset button activation*" was not selected in FPT_TST.1.1, therefore this step was not tested. 5. The selected computer indications on the TOE were always on and fully visible to the TOE user. 6. The TOE allowed peripherals to have active indications with different computers at the same time. 7. "A *screen with dimming function*" was not selected, therefore testing for this step is non-applicable. 8. The indicators always reflect the same status, or the indicator for the most recently used switching mechanism displays the correct switching status and that all other indicators display the correct status or no status.
Pass/Fail Explanation	The evaluator confirms the TOE properly indicates which computer connection is active on TOE power up, and are always on and fully visible. The evaluator also verified the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.
Remote Controller Used	SCAFP0004

Unit Tested	SCKM140PP4
Result	PASS

7.1.10 FDP_APC_EXT.1 – Test 1

Item	***Data/Description***
Test ID	*FDP_APC_EXT.1 – Test 1*
Objective	*[Conditional: Perform this test if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP]* While performing this test, ensure that switching is always initiated through express user action. This test verifies the functionality of the TOE's KM switching methods.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Notepad, Dell P2319H Monitor.
Test Objective Steps	1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect an authorized peripheral device for each peripheral device type selected in FDP_PDC_EXT.3.1/KM. Run an instance of a text editor on each connected computer. 2. Connect a display to each computer in order to see all computers at the same time, turn on the TOE, and enter text or move the cursor to verify which connected computer is selected. 3. For each switching method selected in FDP_SWI_EXT.2.2, switch selected computers in accordance with the operational user guidance, and verify that it succeeds. 4. For each peripheral device type selected in FDP_PDC_EXT.3.1/KM, attempt to switch the device to more than one computer at once and verify that the TOE ignores all such commands or otherwise prevents the operation from executing. 5. *[Conditional: If "keyboard" is selected in FDP_PDC_EXT.3.1/KM, then]* attempt to control the computer selection using the following standard keyboard shortcuts, where '#' represents a computer channel number, and verify that the selected computer is not switched: • Control - Control - # - Enter • Shift - Shift - # • Num Lock - Minus - # • Scroll Lock - Scroll Lock - # • Scroll Lock - Scroll Lock - Function # • Scroll Lock - Scroll Lock - arrow (up or down) • Scroll Lock - Scroll Lock - # - enter • Control - Shift - Alt - # - Enter • Alt - Control - Shift - # 6. *[Conditional: If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then]* attempt to switch to other connected computers using the pointing device and verify that it does not succeed. 7. *[Conditional: If "peripheral devices using a guard" is selected in FDP_SWI_EXT.2.2, then]* attempt to switch to other connected computers using the peripheral device and guard by only performing some of the steps

	outlined in the operational user guidance, and verify that it does not succeed.
Expected Output	1. TOE is configured and a text editor is running on each connected computer. 2. User will be able to see each computer at the same time. TOE will be powered on and user will be able to verify selected computer with cursor. 3. User will be able to switch between selected computers. 4. The TOE will prevent the user from switching to more than one computer at once. 5. The TOE will not respond to such standard keyboard shortcuts. 6. User will not be able to switch between computers using the pointing device. 7. "Peripheral devices using a guard" is not selected in FDP_SWI_EXT.2.2, therefore this step is non-applicable.
Test Execution	1. TOE was configured and a text editor was running on each connected computer. 2. User was able to see each computer at the same time. TOE was powered on and user was able to verify selected computer with cursor. 3. User was able to switch between selected computers. 4. The TOE did prevent the user from switching to more than one computer at once. 5. The TOE did not respond to such standard keyboard shortcuts. 6. User was not able to switch between computers using the pointing device. 7. "Peripheral devices using a guard" was not selected in FDP_SWI_EXT.2.2, therefore this step is non-applicable.
Pass/Fail Explanation	The functionality of the TOE's KM switching methods has been tested successfully. The evaluator has confirmed that the TOE prevents the user from switching between more than one computer at once. This was tested on all four connected computers.
Remote Controller Used	SCAFP0004
Unit Tested	SCKM140PP4
Result	PASS

7.1.11 FDP_APC_EXT.1 – Test 2

Item	***Data/Description***
Test ID	*FDP_APC_EXT.1 – Test 2*
Objective	This test verifies the functionality for correct data flows of a mouse and keyboard during different power states of the selected computer.
Test Equipment Used	Teledyne Lecroy USB sniffer, USBlyzer, Notepad, Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Test Objective Steps	1. Continue with the test setup from Test 1 and for each connected computer, connect a USB sniffer between it and the TOE or open the USB analyzer software. Perform steps 2-12 with each connected computer as the selected computer. 2. Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer.

	[Conditional: Perform steps 3-10 if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.] 3. [If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] switch the TOE to each connected computer and use the mouse to position the mouse cursor at the center of each display. Switch the TOE back to the originally selected computer. 4. [If "keyboard is selected in FDP_PDC_EXT.3.1/KM, then] use the keyboard to enter text into the text editor. [If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] use the mouse to move the cursor to the bottom right corner of the display. 5. Switch to each connected computer and verify that the actions taken in Step 4 did not occur on any of the non-selected computers. 6. Switch to the originally selected computer. Continue exercising the functions of the peripheral device(s) and examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent. 7. Disconnect and reconnect the TOE interface cables connected to the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent. 8. Reboot the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent. 9. Enter sleep or suspend mode in the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers to verify that no traffic is sent. 10. Exit sleep or suspend mode on the selected computer. Examine the USB protocol analyzers on each of the non-selected computers to verify that no traffic is sent. Ensure that any text in the Text Editor application is deleted. 11. Perform step 12 when the TOE is off and then in a failure state. 12. Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that no results are observed on the selected computer and that no traffic is captured using the USB analyzer.
Expected Output	1. USB analyzer will be connected between PC and TOE, USB analyzer software will be running on computer. 2. USB traffic is seen on the selected computer. 3. The mouse curser will be placed in the center of the display. 4. The mouse curser will be placed in the bottom right corner of the display. 5. The mouse curser will not have moved from its original place when switching between computers. 6. No USB traffic is seen on the non-selected computers. 7. No USB traffic is seen on the non-selected computers. 8. No USB traffic is seen on the non-selected computers. 9. No USB traffic is seen on the non-selected computers. 10. No USB traffic is seen on the non-selected computers. Text in editor is deleted. 11. TOE will be powered off, then in a failure state. 12. No USB traffic is seen on the non-selected and selected computers.
Test Execution	1. USB analyzer was connected between PC and TOE, USB analyzer software was running on the computer. 2. USB traffic was seen on the selected computer. 3. The mouse curser was placed in the center of the display. 4. The mouse curser was placed in the bottom right corner of the display.

	5. The mouse curser did not move from its original place when switching between computers. 6. No USB traffic was seen on the non-selected computers. 7. No USB traffic was seen on the non-selected computers. 8. No USB traffic was seen on the non-selected computers. 9. No USB traffic was seen on the non-selected computers. 10. No USB traffic was seen on the non-selected computers. Text in editor was deleted. 11. TOE was powered off, then in a failure state. 12. No USB traffic was seen on the non-selected and selected computers.
Pass/Fail Explanation	Correct data flows of a mouse and keyboard during different power states of the selected computer has been tested. The evaluator has confirmed that data flow is transmitted to the correct computers at the accurate times. The expected USB traffic was observed on the selected computer and no traffic was observed when in a powered off state and during a failure state. The expected KM input was shown on the currently selected computer and not shown on non-selected computers. No output was observed on non-selected computers while rebooting, suspending or putting the selected computer to sleep.
Remote Controller Used	SCAFP0004
Unit Tested	SCKM140PP4
Result	PASS

7.1.12 FDP_APC_EXT.1 – Test 3

Item	***Data/Description***
Test ID	*FDP_APC_EXT.1 – Test 3*
Objective	This test verifies that the TOE properly enforces unidirectional flow and isolation.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Device Manager, Razor Mamba Gaming Mouse, Teledyne Lecroy USB Sniffer, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Test Objective Steps	1. Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. *[Perform steps 2 – 12 with each connected computer as the selected computer]* 2. Ensure the TOE is powered on and connect a display directly to the selected computer. Open a real-time hardware information console on the selected computer. *[If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then perform steps 3 - 4]* 3. Connect a gaming mouse with programmable LEDs directly to the selected computer and attempt to configure the LEDs using the mouse application running on the selected computer. Verify that the mouse programmable LEDs change state. 4. Disconnect the gaming mouse from the selected computer and connect it to the TOE mouse peripheral device port through the USB sniffer. Attempt to configure the LEDs using the mouse application running on the selected computer. Verify that the mouse programmable LEDs do not change state and that no traffic is sent and captured by the USB sniffer while the evaluator is not moving the mouse.

	[If "keyboard" is selected in FDP_PDC_EXT.3.1/KM, then perform step 5] 5. Connect a keyboard to the peripheral device interface through the USB sniffer. Use a keyboard emulation software application running on the selected computer to turn the keyboard Num Lock, Caps Lock, and Scroll Lock LEDs on and off. Verify that the LEDs on the keyboard do not change state and that no traffic is sent and captured by the USB sniffer. 6. Power down the TOE and disconnect the peripheral interface USB cable from the TOE to the selected computer and the peripheral devices from the TOE. 7. Power up the TOE and ensure the selected computer has not changed (this should have no effect on the selected computer because it was disconnected in the previous step). Reconnect the peripheral devices disconnected in step 6 to the TOE. 8. [If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] check that immediately following the connection, the mouse LEDs are illuminated (indicating that the peripheral devices are powered on, although the selected computer is not connected). [If "keyboard" is selected in FDP_PDC_EXT.3.1/KM, then] check that immediately following the connection, the Num Lock, Caps Lock, and Scroll Lock keyboard LEDs are blinking momentarily and then stay off (indicating that the keyboard is powered on, although the selected computer is not connected). 9. Turn the TOE off and disconnect the peripheral devices connected in step 6. 10. Reconnect the first computer interface USB cable to the TOE. 11. Turn on the TOE and check the computer real-time hardware information console for the presence of the peripheral devices connected in step 6 and disconnected in step 9. The presence of the TOE peripheral devices in the information console when the peripheral devices are not connected to the TOE indicates that the TOE emulates the KM devices. 12. *[Conditional]* If the TOE keyboard and mouse do not appear in the listed devices, repeat the following steps for both mouse and keyboard to simulate USB traffic: • Connect a USB generator to the TOE peripheral device interface port. • Configure the USB generator to enumerate as a generic HID mouse/keyboard device and then to generate a random stream of mouse/keyboard report packets. • Connect a USB sniffer device between the TOE computer interface and the USB port on the first computer to capture the USB traffic between the TOE and the first computer. • Turn on the TOE and verify that no packets cross the TOE following the device enumeration.
Expected Output	1. TOE is configured correctly. 2. TOE is powered on; selected computer has display connected. Hardware information console is open on computer. 3. Mouse programmable LED does change state. 4. Mouse programmable LED does not change state, no USB traffic is generated. 5. Keyboard LEDs do not change state and no USB traffic is generated. 6. TOE is powered off, peripheral cable unplugged. 7. TOE is powered on, peripheral cable reconnected. 8. Mouse: LEDs should be illuminated. Keyboard: LEDs blink momentarily then stay off.

	9. TOE powered off; peripherals disconnected. 10. USB cable reconnected. 11. Hardware management console will indicate emulated peripheral devices. 12. No packets should be captured following the device enumeration.
Test Execution	1. TOE was configured correctly. 2. TOE was powered on; selected computer had display connected. Hardware information console was open on computer. 3. Mouse programmable LED did change state. 4. Mouse programmable LED did not change state, no USB traffic was generated. 5. Keyboard LEDs did not change state and no USB traffic was generated. 6. TOE was powered off; peripheral cable was unplugged. 7. TOE was powered on; peripheral cable was reconnected. 8. Mouse: LEDs are illuminated. Keyboard: LEDs blinked momentarily then stayed off. 9. TOE was powered off; peripherals were disconnected. 10. USB cable was reconnected. 11. Hardware management console indicated emulated peripheral devices. 12. 12. No packets were captured following the device enumeration.
Pass/Fail Explanation	Unidirectional flow and isolation of USB traffic has been tested. The evaluator has confirmed that USB traffic is enforced properly and in a single direction. This was tested on all four connected computers. Mouse LEDs are illuminated when expected, and change state only when not attached to a USB analyzer. Keyboard LEDs blink momentarily when connected and do not change state when attached to an analyzer. The devices were properly emulated by the TOE and no packets were captured following enumeration.
Remote Controller Used	SCAFP0004
Unit Tested	SCKM140PP4
Result	PASS

7.1.13 FDP_APC_EXT.1 – Test 4

Item	***Data/Description***
Test ID	*FDP_APC_EXT.1 – Test 4*
Objective	*[Conditional: Perform this test if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP]* This test verifies correct data flow while the TOE is powered on or powered off.
Notes	• TD0507 has been incorporated into FDP_APC_EXT.1 – Test 4.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, USBlyzer, HSL USB Dummy Load, Dr. Meter DC Power Supply, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor, Spliced USB Type-A Cable.

Test Objective Steps	1. Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. Connect a display directly to each connected computer. Perform steps 2-10 for each connected computer. 2. Connect a USB sniffer between a non-selected TOE KM computer interface and its computer. Run USB protocol analyzer software on all remaining computers. 3. Turn on the TOE and observe the TOE enumeration data flow in the protocol analyzer connected to the selected computer and is not in any other USB protocol analyzers or the USB sniffer. 4. Ensure the TOE is switched to the first computer. 5. Reboot the first computer. Verify that no USB traffic is captured on all non-selected computer USB protocol analyzers. 6. Generate intensive USB HID traffic by moving the mouse at high speed and/or holding down the keyboard space key at the same time. Verify that no new USB traffic is captured on all non-selected computer USB protocol analyzers. 7. Perform steps 8 and 9 for each TOE keyboard/mouse peripheral interface. 8. Connect a USB dummy load into the TOE KM peripheral device interface. Verify that no new USB traffic is captured on all non-selected computer USB protocol analyzers. Remove the plug after the step is completed. 9. Connect a switchable 5-volt power supply with any compatible USB plug into the TOE KM peripheral device interface. Modulate the 5-volt supply (i.e., cycle on and off) manually at various speeds from approximately one cycle per five seconds to one cycle per second. Verify that no new USB traffic is captured on all non-selected computer USB analyzers. 10. Turn off the TOE. Verify that no new traffic is captured.
Expected Output	1. TOE is configured, display will be connected to each computer. 2. USB analyzer software running, USB sniffer properly implemented. 3. USB traffic only being captured on selected computer. 4. First computer selected via TOE. 5. No USB traffic captured on all non-selected computers. 6. No USB traffic captured on all non-selected computers. 7. Perform steps 8 and 9 for each KM interface. 8. No USB traffic captured on all non-selected computers. 9. No USB traffic captured on all non-selected computers. 10. No USB traffic captured on all non-selected computers.
Test Execution	1. TOE was configured, display was connected to each computer. 2. USB analyzer software was running, USB sniffer was properly implemented. 3. USB traffic was only being captured on selected computer. 4. First computer was selected via TOE. 5. No USB traffic was captured on all non-selected computers. 6. No USB traffic was captured on all non-selected computers. 7. Performed steps 8 and 9 for each KM interface. 8. No USB traffic was captured on all non-selected computers. 9. No USB traffic was captured on all non-selected computers. 10. No USB traffic was captured on all non-selected computers.

Pass/Fail Explanation	Correct data flow while the TOE is powered on or powered off has been tested. The evaluator confirms that USB traffic is only captured on selected authorized computers. This was tested on all four connected computers.
Remote Controller Used	SCAFP0004
Unit Tested	SCKM140PP4
Result	PASS

7.1.14 FDP_APC_EXT.1 – Test 5

Item	***Data/Description***
Test ID	*FDP_APC_EXT.1 – Test 5*
Objective	This test verifies that the TOE does not send data to different computers connected to the same interface at different times. Repeat this test for each TOE KM computer port.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Notepad, USBlyzer, Dell P2319H Monitor.
Test Objective Steps	1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect an authorized peripheral device for each peripheral device type selected in FDP_PDC_EXT.3.1/KM. Connect two computers to a different display and run an instance of a text editor and USB analyzer software on each computer. 2. Connect the first computer to the TOE and ensure it is selected and that no other computers are connected. 3. Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer. 4. Disconnect the first computer. Generate intensive USB HID traffic by moving the mouse at high speed and/or holding down the keyboard space key at the same time. 5. Cease generation of the USB HID traffic, connect the second computer to the same port and ensure it is selected. 6. Verify that no results from the previous use of the peripheral device are observed on the selected computer and that no traffic is sent and captured using the USB analyzer. 7. Reboot the TOE and repeat step 6. 8. Turn off the TOE and repeat step 6. 9. Restart the TOE and repeat step 6. 10. Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer.
Expected Output	1. Authorized peripheral devices connected, display connected to each computer, text editor and USB analyzer running on each computer. 2. Only the first computer is connected and selected. 3. USB traffic captured on selected computer. 4. Computer disconnected; USB traffic generated. 5. Second computer connected to first computers port. 6. No USB traffic should leak over from first computer.

	7. TOE rebooted. No USB data captured. 8. TOE powered off. No USB data captured. 9. TOE rebooted. No USB data captured. 10. Expected USB traffic generated on selected computer.
Test Execution	1. Authorized peripheral devices were connected, display was connected to each computer, text editor and USB analyzer was running on each computer. 2. Only the first computer was connected and selected. 3. USB traffic was captured on selected computer. 4. Computer was disconnected; USB traffic was generated. 5. Second computer was connected to first computers port. 6. No USB traffic leaked over from the first computer. 7. TOE was rebooted. No USB data was captured. 8. TOE was powered off. No USB data was captured. 9. TOE was rebooted. No USB data was captured. 10. Expected USB traffic was generated on selected computer.
Pass/Fail Explanation	Data flow through the same interface has been observed and tested. The evaluator confirmed that the TOE does not send data to different computers connected to the same interface at different times. No residual USB traffic from other computers connected to the same port was observed during power cycles. USB traffic was seen only on the connected and selected computer.
Remote Controller Used	SCAFP0004
Unit Tested	SCKM140PP4
Result	PASS

7.1.15 FDP_PDC_EXT.1 – Test 1

Item	***Data/Description***
Test ID	*FDP_PDC_EXT.1 – Test 1*

Objective	The evaluator shall verify that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections. For this test, verify device rejection through TOE user indication in accordance with the operational user guidance, an immediate cessation of traffic following device detection or enumeration, no traffic captured on the USB sniffer or analyzer software other than NAK transactions or system messages, or incompatibility of the device interface with the peripheral interface. Also verify device rejection through examination of the USB sniffer or analyzer software for no traffic captured other than NAK transactions or system messages and through examination of the real-time hardware console for no display of new USB devices (recognized or not recognized). Repeat this test for each keyboard/mouse TOE peripheral interface. Perform steps 1-7 for each of the following unauthorized devices: • USB audio headset • USB camera • USB printer • USB user authentication device connected to a TOE keyboard/mouse peripheral interface • USB wireless LAN dongle
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, USBlyzer, Teledyne Lecroy USB Sniffer, MPOW Headset with USB Connector, Logitech USB Camera, HP Deskjet USB Printer, Identiv USB UA Device, Wireless LAN Dongle, BYEASY USB Hub, Dell Keyboard with Smart Card Reader, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor, Device Manager.
Test Objective Steps	1. Ensure the TOE is powered off and connected to a computer. Run USB analyzer software on the connected computer and connect a USB sniffer to the TOE keyboard/mouse peripheral interface. Open the real-time hardware information console. 2. Attempt to connect the unauthorized device to the USB sniffer: • USB Audio headset • USB Camera • USB Printer • USB user authentication device connected to a TOE K/M peripheral interface • USB wireless LAN dongle 3. Power on the TOE. Verify the device is rejected. 4. Ensure the unauthorized device is disconnected from the USB sniffer, then attempt to connect it to the USB sniffer again. 5. Verify the device is rejected. 6. Repeat steps 1 through 5 with a USB hub connected between the USB device and USB sniffer and observe that the results are identical. 7. Repeat steps 1-6 with a composite device with non-HID device classes and verify that the non-HID functions are rejected, or the entire device is rejected.

Expected Output	1. TOE is powered off. USB analyzer software is running, and USB sniffer connected. 2. User will connect each unauthorized device to the USB sniffer. 3. TOE is powered on. Device will be rejected. 4. Device disconnect then reconnected. 5. Device will be rejected. 6. Devices will remain rejected through USB hub. 7. Device will be rejected.
Test Execution	1. TOE is configured, text editor application is running on connected computer. 2. TOE powered off. 3. User will connect each authorized device throughout test. 4. TOE is powered on. User indication will not be present. 5. Input from authorized device is present via text editor. 6. Authorized device connected to TOE KM port. 7. User indication will not be present.
Pass/Fail Explanation	The evaluator observed the output of the USB analyzer software and confirmed that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections. The devices listed in step 2 were all properly rejected including when attached to a USB hub.
Unit Tested	SCKM140PP4
Result	PASS

7.1.16 FDP_PDC_EXT.1 – Test 2

Item	***Data/Description***
Test ID	*FDP_PDC_EXT.1 – Test 2*
Objective	The evaluator shall verify that the TOE KM ports do not reject authorized devices and devices with authorized protocols as per the authorized peripheral device connections. Repeat this test for each of the following four device types: • Barcode reader; • Keyboard or Keypad; • Mouse, Touchscreen, Trackpad, or Trackball; and • PS/2 to USB adapter (with a connected PS/2 keyboard or mouse).
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Notepad, Netum USB Barcode Reader, PS/2 to USB Adapter, Perixx Optical PS/2 Mouse, Dell P2319H Monitor.
Test Objective Steps	1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Run an instance of a text editor on a connected computer. 2. Ensure the TOE is powered off. 3. Connect the authorized device to the TOE peripheral interface: • Barcode reader; • Keyboard or Keypad; • Mouse, Touchscreen, Trackpad, or Trackball; and

	• PS/2 to USB adapter (with a connected PS/2 keyboard or mouse). 4. Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present. 5. Ensure the connected computer is selected and send inputs using the authorized devices. Verify that the input is received into the text editor or on the screen of the connected computer. 6. Disconnect the authorized device, and then reconnect it to the TOE KM peripheral device interface. 7. Verify the TOE user indication described in the operational user guidance is not present. 8. Send inputs using the authorized devices. Verify that the input is received into the text editor or on the screen of the connected computer.
Expected Output	1. TOE was configured, text editor application was running on connected computer. 2. TOE was powered off. 3. User connected each authorized device throughout test. 4. TOE was powered on. User indication was not present. 5. Input from authorized device is present via text editor. 6. Authorized device was connected to TOE KM port. 7. User indication was not present. 8. Input from the authorized device was present via text editor.
Test Output	1. TOE was configured, text editor application was running on connected computer. 2. TOE was powered off. 3. User connected each authorized device throughout test. 4. TOE was powered on. User indication was not present. 5. Input from authorized device is present via text editor. 6. Authorized device was connected to TOE KM port. 7. User indication was not present. 8. Input from the authorized device was present via text editor.
Pass/Fail Explanation	The evaluator observed the output of the USB analyzer to confirm that the TOE KM ports do not reject authorized devices and devices with authorized protocols as per the authorized peripheral device connections. The evaluator has confirmed that authorized devices were accepted by the TOE and the input was successfully received via the text editor.
Unit Tested	SCKM140PP4
Result	PASS

7.1.17 FDP_FIL_EXT.1 – Test 1

Item	***Data/Description***
Test ID	*FDP_FIL_EXT.1 – Test 1*
Objective	Perform the test steps in FDP_PDC_EXT.1 with all devices on the PSD KM blacklist and verify that they are rejected as expected.

Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, USBlyzer, Teledyne Lecroy USB Sniffer, Device Manager, MPOW Headset with USB Connector, Logitech USB Camera, HP Deskjet USB Printer, Identiv USB UA Device, Wireless LAN Dongle, BYEASY USB Hub, Dell Keyboard with Smart Card Reader, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Test Objective Steps	1. Ensure the TOE is powered off and connected to a computer. Run USB analyzer software on the connected computer and connect a USB sniffer to the TOE keyboard/mouse peripheral interface. Open the real-time hardware information console. 2. Attempt to connect the unauthorized device to the USB sniffer: • USB audio headset • USB camera • USB printer • USB user authentication device connected to a TOE keyboard/mouse peripheral interface • USB wireless LAN dongle 3. Power on the TOE. Verify the device is rejected. 4. Ensure the unauthorized device is disconnected from the USB sniffer, then attempt to connect it to the USB sniffer again. 5. Verify the device is rejected. 6. Repeat steps 1 through 5 with a USB hub connected between the USB device and USB sniffer and observe that the results are identical. 7. Repeat steps 1-6 with a composite device with non-HID device classes and verify that the non-HID functions are rejected, or the entire device is rejected.
Expected Output	1. TOE is powered off. USB analyzer software is running, and USB sniffer connected. 2. User will connect each device to the USB sniffer. 3. TOE is powered on. Device will be rejected. 4. Device disconnect then reconnected. 5. Device will be rejected. 6. Devices will remain rejected through USB hub. 7. Device will be rejected.
Test Execution	1. TOE was powered off. USB analyzer software was running, and USB sniffer was connected. 2. User connected each device to the USB sniffer. 3. TOE was powered on. Device was rejected. 4. Device disconnect then reconnected. 5. Device was rejected. 6. Devices remain rejected through USB hub. 7. Device was rejected.
Pass/Fail Explanation	All devices on the PSD KM blacklist were tested and are rejected as expected. The evaluator confirms that the blacklist in place rejects all devices found in step 2. The evaluator confirmed through observation of the USB analyzer software that all blacklisted devices are rejected initially after power-on, after reconnecting, and whilst connected to a USB hub.
Unit Tested	SCKM140PP4
Result	PASS

7.1.18 FDP_FIL_EXT.1 – Test 2

Item	*Data/Description*
Test ID	*FDP_FIL_EXT.1 – Test 2*
Objective	*[Conditional: Perform this only if "configurable" is selected in FDP_FIL_EXT.1.1/KM]* In the following steps the evaluator shall verify that whitelisted and blacklisted devices are treated correctly.
Notes	• This test is not applicable to this configuration as "fixed" is selected in FDP_FIL_EXT.1.1/KM and the TOE does not support these features.
Test Equipment Used	N/A
Test Objective Steps	1. Ensure the TOE and the Operational Environment are configured in accordance with the operation guidance. 2. Connect to the TOE KM peripheral device interface a composite device which contains a HID class and a non-HID class. 3. Configure the TOE KM CDF to whitelist the composite device. 4. Verify that the HID-Class part is accepted and that the non-HID class part is rejected through real time device console and USB sniffer capture, or that the entire device is rejected. 5. Configure the TOE KM CDF to blacklist the device. 6. Verify that both the HID-class part and the non-HID-class part is rejected through real-time device console and USB sniffer capture.
Expected Output	N/A
Pass/Fail Explanation	"Configurable" has not been selected in FDP_FIL_EXT.1.1/KM. Therefore, this evaluation activity is not applicable.
Unit Tested	N/A
Result	Non-Applicable/Pass

7.1.19 FDP_RDR_EXT.1 – Test 1

Item	*Data/Description*
Test ID	*FDP_RDR_EXT.1 – Test 1*
Objective	The evaluator shall use a BadUSB, programmable keyboard, and/or USB Rubber Ducky as a malicious USB device to perform the following tests.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, Device Manager, HSL BADUSB, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Test Objective Steps	1. Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. Ensure the TOE is powered off and connect a USB sniffer between the TOE and a computer. Open a real-time hardware information console. 2. Configure the malicious USB device as a HID-class device and to re-enumerate as a mass storage device. 3. Connect the malicious USB device to the TOE KM peripheral interface. 4. Power on the TOE and active the re-enumeration after 1 minute.

	5. Verify device rejection per TOE guidance, the cessation traffic passed in the USB sniffer, and the absence of the device and any new device in the information console. 6. Remove the malicious USB device and reconfigure as a HID-class device and to re-enumerate as a mass storage device. 7. Connect the malicious USB device to the TOE KM peripheral interface and active the re-enumeration after 1 minute. 8. Verify device rejection per TOE guidance, the cessation of traffic passed in the USB sniffer, and the absence of the device and any new devices in the information console.
Expected Output	1. TOE is powered off. USB sniffer is configured correctly, and hardware information console is open. 2. USB device will be configured correctly. 3. USB Device connected to peripheral interface. 4. TOE is powered on. 5. Device will not appear in hardware information console. 6. USB device will be configured correctly. 7. USB Device connected to peripheral interface. 8. Device will not appear in hardware information console.
Test Execution	1. The evaluator ensured the TOE was powered off. A USB sniffer was connected between the TOE and a computer. A hardware information console was open on the selected computer. 2. The malicious USB device was configured as a HID-class device and then to re-enumerate as a mass storage device. The USB device was pre-programmed to replicate the two functions if the toggle switch on the device was set to the "middle" position. 3. The evaluator connected the USB Device to the TOE KM peripheral interface. 4. The TOE was powered on and re-enumeration was active after 1 minute. 5. The evaluator verified device rejected by the cessation of traffic passed to the USB sniffer and the absence of the device in hardware information console. 6. The evaluator removed the malicious USB device. The device was reconfigured as a HID-class device and then to re-enumerate as a mass storage device. 7. The evaluator connected the USB Device to the TOE KM peripheral interface and re-enumeration was activated after 1 minute. 8. The evaluator verified device rejected by the cessation of traffic passed to the USB sniffer and the absence of the device in hardware information console.
Pass/Fail Explanation	The evaluator configured the USB device accordingly and verified that the device was rejected appropriately. The TOE rejects the device and no new devices appear in the hardware console after re-enumeration.
Unit Tested	SCKM140PP4
Result	PASS

8 Security Assurance Requirements

8.1 ADV_FSP.1 Basic Functional Specification

8.1.1 ADV_FSP.1

8.1.1.1 ADV_FSP.1 Activity 1

Objective	There are no specific Evaluation Activities associated with these SARs. The Evaluation Activities listed in this PP are associated with the applicable SFRs; since these are directly associated with the SFRs, the tracing element ADV_FSP.1.2D is implicitly already done, and no additional documentation is necessary. The functional specification documentation is provided to support the evaluation activities described in Section 5.2 and other activities described for AGD, and ATE SARs. The requirements on the content of the functional specification information are implicitly assessed by virtue of the other Evaluation Activities being performed. If the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided.
Evaluator Findings	Sufficient interface information was available in the TSS of the [ASE_I] and [ASE_S] and Vertiv Common Criteria Guidance Supplement documents [CC_Supp_I] and [CC_Supp_S] to perform the evaluation activities.
Verdict	Pass

8.2 AGD_OPE.1 Operational User Guidance

8.2.1 AGD_OPE.1

8.2.1.1 AGD_OPE.1 Activity 1

Objective	The operational user guidance does not have to be contained in a single document. Guidance to users and Administrators can be spread among documents or web pages. The developer should review the Evaluation Activities contained in Section 5.2 of this PP to ascertain the specifics of the guidance for which the evaluator will be checking. This will provide the necessary information for the preparation of acceptable guidance.
Evaluator Findings	The evaluator examined the guidance documents to perform this evaluation. The Guidance documents consisted of: • [CC_Supp_I] Isolator, Vertiv CYBEX™ SCUSBHIDFILTER Firmware Version 40404-0E7 Common Criteria Guidance Supplement, v1.8, January 17, 2022 • [CC_Supp_S] Switch, Vertiv CYBEX™ SCKM140PP4 KM Switch Firmware Version 40404-0E7 Common Criteria Guidance Supplement, v1.8, November 23, 2021 • [2297] CYBEX™ SECURE USB FILTERS, 590-2297-501 Rev. A • [2282] CYBEX™ SC Series Secure Switches SC800/900DPH, SC800/900DVI, and SCKM100PP4 Quick Installation Guide, 590-2282-501B The Guidance activities in Section 5.2 of the PP were used to perform the evaluation in addition to those activities prescribed by the CEM. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

8.3 AGD_PRE.1 Preparative Procedures

8.3.1 AGD_PRE.1

8.3.1.1 AGD_PRE.1 Activity 1

Objective	As with the operational user guidance, the developer should look to the Evaluation Activities contained in Section 5.2 of this PP to determine the required content with respect to preparative procedures.
Evaluator Findings	The evaluator examined the guidance documents for both the Isolator and the Switch to perform this evaluation. The required Guidance assurance activities are recorded within this report. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

8.4 ALC Assurance Activities

8.4.1 ALC_CMC.1

8.4.1.1 ALC_CMC.1 Activity 1

Objective	The “evaluation evidence required by the SARs” in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance, the evaluator implicitly confirms the information required by this component.
Evaluator Findings	Both [ASE_I] and [ASE_S] were used to determine the identification of the TOE. This was also corroborated by the identification in the TOE user guidance documents for both the Switch and Isolator. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

8.4.2 ALC_CMS.1

8.4.2.1 ALC_CMS.1 Activity 1

Objective	Given the scope of the TOE and its associated evaluation evidence requirements, this component’s Evaluation Activities are covered by the Evaluation Activities listed for ALC_CMC.1.
Evaluator Findings	Covered by ALC_CMC.1.
Verdict	Pass

8.5 ATE_IND.1 Independent Testing – Conformance

8.5.1 ATE_IND.1

8.5.1.1 ATE_IND.1 Activity 1

Objective	The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the CEM and the body of

	this PP's Evaluation Activities. While it is not necessary to have one test case per test listed in an Evaluation Activity, the evaluator must document in the test plan that each applicable testing requirement in the PP is covered. The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary. The test plan describes the composition of each platform to be tested and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test equipment or tools. For each piece of equipment or tool, an argument (not just an assertion) should be provided that the equipment or tool will not adversely affect the performance of the functionality by the TOE and its platform. The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.
Evaluator Findings	The evaluator created a test plan and executed all the tests in the test plan. The results of all the testing are included in the test plan. Based on this document, this evaluation activity is considered satisfied.
Verdict	Pass

8.6 AVA_VAN.1 Vulnerability Survey

8.6.1 AVA_VAN.1

8.6.1.1 AVA_VAN.1 Activity 1

Objective	As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in peripheral sharing devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.

Evaluator Findings	The evaluators documented their analysis and testing of potential vulnerabilities with respect to this requirement. Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included several combinations of the following words: *Vertiv, Vertiv KM, Vertiv Firmware, Firmware Version 40404-0E7, Vertiv Peripheral Sharing Device, SCKM140PP4, SCUSHIDFILTER, Cybex, AFP0004, NAK transaction, USB HID traffic and STMicroelectronics 32-Bit* to ensure sufficient coverage under AVA. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below. • National Vulnerability Database: https://nvd.nist.gov/vuln/search • Vertiv Support: https://www.vertiv.com/en-ca/support/ • Generic Internet Search: https://google.com The search was performed on January 12, 2022. The evaluation team found no vulnerabilities were applicable to the TOE version or hardware. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

9 Conclusion

The testing shows that all test cases required for conformance have passed testing.

10 Evaluation Evidence

- [ASE_I] Vertiv CYBEX™ SCUSBHIDFILTER Firmware Version 40404-0E7 Security Target, v1.15, January 5, 2022
- [ASE_S] Switch, Vertiv CYBEX™ SCKM140PP4 KM Switch Firmware Version 40404-0E7 Security Target, v 1.18, January 13, 2022
- [Isol_I] Vertiv CYBEX™ SCUSBHIDFILTER Firmware Version 40404-0E7 Isolation Document, v1.5, December 10, 2020
- [Isol_S] Vertiv CYBEX™ SCKM140PP4 KM Switch Firmware Version 40404-0E7 Isolation Document, v1.6, April 8, 2021
- [CC_Supp_I] Isolator, Vertiv CYBEX™ SCUSBHIDFILTER Firmware Version 40404-0E7 Common Criteria Guidance Supplement, v1.8, January 19, 2022
- [CC_Supp_S] Switch, Vertiv CYBEX™ SCKM140PP4 KM Switch Firmware Version 40404-0E7 Common Criteria Guidance Supplement, v1.8, January 19, 2021
- [2282] CYBEX™ SC Series Secure Switches SC800/900DPH, SC800/900DVI, and SCKM100PP4 Quick Installation Guide, 590-2282-501B
- [2297] CYBEX™ SECURE USB FILTERS, 590-2297-501A
- [Testplan_I] Test Report for Vertiv CYBEX™ SCUSBHIDFILTER Firmware Version 40404-0E7 Peripheral Sharing Device, Version 1.1, January 18, 2022
  [Testplan_S] Test Report for Vertiv CYBEX™ SCKM140PP4 KM Switch Firmware Version 40404-0E7 Peripheral Sharing Device, Version 1.1, January 18, 2022

11 References

- [PP_PSD_V4.0] Protection Profile for Peripheral Sharing Device, July 19, 2019
- [MOD_KM_V1.0] PP-Module for Keyboard/Mouse Devices, July 19, 2019
- [CFG_PSD-KM _v1.0] PP-Configuration for Peripheral Sharing Device, Keyboard and Mouse Devices, July 19, 2019

End of Document